What's New

Clarity LIMS v6.0 and later includes project automations, which allow you to automate actions that are performed on samples after they have been accessioned. These actions are performed through an automation script triggered from the Projects & Samples screen. For example, you can write a script to validate container names, populate sample fields, assign samples to workflows, or email a company after a project is submitted. Each automation script must use the standard Clarity LIMS automation mechanism that includes the Clarity LIMS API. For more information on project automations, refer to *Automations Configuration Screen* on page 134 and *Add and Configure Automations* on page 135.

Clarity LIMS v6.2.1 is a patch release that fixes issues related to the following functions:

- Search-indexer performance
- Basic search failure when searching with a large number of custom fields in the system
- Necessary handling of controls for a configured step

Clarity LIMS v6.2 includes an operating system (OS) migration to Oracle Linux v8.8 and v8.9. The upgrade also includes new account management options, including:

- Adding an account.
- Editing an account (including the account custom fields).
- Viewing an account.
- Deleting an account.

There is also a red alert dot that displays when the Configuration settings in LabLink are not configured correctly.

Clarity LIMS v6 also includes technology updates and performance improvements. For details, refer to the following release notes:

- *Clarity LIMS v6.2.1 Release Notes* on page 335
- *Clarity LIMS v6.2 Release Notes* on page 337
- *Clarity LIMS v6.1 Release Notes* on page 339
- *Clarity LIMS v6.0.1 Release Notes*
- *Clarity LIMS v6.0 Release Notes* on page 340

Getting Started

The Dashboards, Projects & Samples, and Lab View screens facilitate the day-to-day tasks of the lab manager and lab scientist.

Overview dashboard—Provides summary information about lab activity. Use this dashboard to view workflow status, sample status, and alerts.

Projects dashboard—Provides a dynamic view of current lab activity. Use this dashboard to help manage projects and the flow of samples through the lab.

Projects & Samples—Allows for project and sample management. Use this screen to create and manage projects, add samples, and assign samples to workflows.

Lab View—Lists the protocols and steps used in the lab, and the number of samples queued for each step. Use this screen to see recent activities, in progress steps, and steps that are ready to be worked on.

For a brief description of dashboard and screen elements, turn on pop-up help hints—select Help (?) next to the search bar, and then hover the cursor over the area of interest.

Technical Overview

This section provides an overview of the components of Clarity LIMS. For technical requirements, refer to *Technical Requirements* on page 5.

Environment Overview

Clarity LIMS is built on a platform that is easy to customize and supports off-the-shelf hardware, common database systems, and industry-standard data formats.

We offer both on-premise and Illumina cloud hosted deployment models. Both offerings use the same underlying software and security model as explained in the *Clarity LIMS Security and Privacy* technical note, available for download from the Illumina website.

For on-premise deployments, we provide flexibility in selecting tools that suit your needs and existing IT infrastructure. The Clarity LIMS environment includes:

- Application server
- Database
- File server
- Web client

Depending on the details of your contract with Illumina, the environment can also include:

- Automation Workers

For cloud deployments, the hardware is scaled upward by Illumina as required.

System Architecture

For on-premise deployments, you can separate application and file server functions from the database functions by installing them on discrete hardware platforms. Alternatively, you can combine them on a single server hardware platform. Base your decision on the size of your installation and how much data your laboratory processes.

Whichever solution you choose, Illumina requires that the Clarity LIMS server environment reside on dedicated hardware, free from other Illumina or third-party server products. The server environment must also be on a 1 Gbs or faster network. The network should not contain links with a capacity lower than 100 Mbps on any network-connected devices, such as routers, firewalls, and switches.

The Clarity LIMS installation installs Apache Tomcat 9.0, Apache Webserver v2 (used as a proxy), ElasticSearch and RabbitMQ to support search, and Open JDK 8.0. These software versions are the only versions that Clarity LIMS supports. The software packages are supplied by Illumina.

For Illumina cloud hosted deployments, Illumina fully manages the system deployment and maintenance.

Application Server

Clarity LIMS uses a web application served by the Apache Tomcat server to manage the creation, collection, and retrieval of data and results. This core server is built on a Java architecture and allows for rapid deployment and custom configuration for other on-premise and Illumina cloud hosted deployments.

For both on-premise and Illumina cloud hosted deployments, the application requires the following standard secure ports for web and file communications:

- Web communications: Port 80, 443
- File communications: Port 22

Depending on included instrument integrations, additional open ports may be required.

For Illumina cloud hosted deployments, a site-to-site VPN connection, using IPSEC, might be required for instrument integrations. The most current list of required open ports is included in the preinstallation documentation that is provided during an implementation project.

Database and File Server

Clarity LIMS supports PostgreSQL database to record data generated by the client, and references to file locations on the Clarity LIMS file server.

If the system needs to export a file, it issues a call to the database to find the file location on the file server. We recommend that you store files on a server or file system separate from the Clarity LIMS application server, such as a Network Attached Storage (NAS) appliance.

When handling data, Clarity LIMS saves files in their original format. The advantages of saving files in their original format are as follows:

- The size of files is restricted only by the size of your file system.
- You benefit from the built-in error-correction and integrity-checking features included in the file system.

The amount of storage space required by Clarity LIMS depends on the following:

- The number of samples your laboratory processes each day.
- The instruments you use.

- The number of files you save to the Clarity LIMS system.

Illumina can work with you to recommend an appropriate amount of storage space.

> We do not recommend that you place the Clarity LIMS file server on a remote mount to a Windows server. We recommend you discuss other network storage devices, such as high availability NAS, with your hardware and supported operating system vendors.

Web Client

User-centric, goal-based design has become the new standard in software interfaces. Clarity LIMS has a clean, helpful, easy-to-use interface. It is a lightweight web application that provides:

- A simple, fast, and efficient way for lab scientists to identify work they need to complete.
- The tools necessary to complete and record that work quickly and efficiently.

Automation Workers

The Clarity LIMS Automation Worker allows specifically designed scripts to automate and extend the functionality of Clarity LIMS. You can integrate a wide variety of laboratory instruments and software.

The Automation Worker runs as a Windows Service or as a Linux daemon. You can install the Automation Worker on any computer with a supported OS on your Clarity LIMS network. When you install multiple copies on different machines on your network, Clarity LIMS automatically distributes work across the machines to improve system performance.

> Only one Automation Worker node can be installed on a Windows server.

Mixpanel

Mixpanel™ is a system that provides Illumina with information about how users interact with the Clarity LIMS web client. We do this by tracking which features are being used, and how often. Gathering this information allows us to determine which interactions are most common, and how our users proceed through protocol steps and tasks. We can then use this information to improve system performance and ultimately enhance the user experience.

All data are collected anonymously. We collect data on Clarity LIMS usage only. We do not collect specific sample names, projects, or values entered. We do track total usage (number of samples selected, how many protocol steps executed, and so on). Data are collected across all customers for analysis in one group. We do not directly track which site is doing which work. If you require more information about Mixpanel, contact the Illumina Support team.

Security

All client traffic is encrypted over secure HTTP (HTTPS). To ensure the security of the transactions between Clarity LIMS and clients, on-premise deployments require a purchased certificate. The certificate should be from a well-known vendor such as DigiCert, Entrust, or QuoVadis. For information on the policies, processes, and controls enacted for security and privacy of data in Illumina cloud hosted deployments, see the *Clarity LIMS Security and Privacy Technical Note*, available for download from the Illuminawebsite.

Technical Requirements

The following information is a summary of the technical requirements for an on-premise or cloud based deployment of Clarity LIMS v6 and later. To install and use Clarity LIMS, the client and server systems must meet these requirements. Clarity LIMS is designed to run on standard commodity hardware. The requirements provide general guidelines for your hardware configuration. You can obtain specific configuration quotes from the hardware vendor of your choice.

Before installing Clarity LIMS, you must also organize, install, and/or configure some essential components. For details on these components and installation and configuration instructions, refer to the *Pre-Installation Requirements* on page 232.

Allow enough time for the procurement of your hardware and software. Make sure that all components are installed and configured before proceeding with the installation of Clarity LIMS.

Production Server Requirements

For on-premise deployments, Clarity LIMS has two levels of recommended hardware. For larger labs in full production, we strongly suggest the high-throughput requirements.

The production server must be configured in US locale.

Recommended

- Server class 64-bit CPU with at least eight cores at 2.9 GHz
- 20 MB cache per core
- 32 GB RAM
  - 6 GB allocated to Tomcat
  - 6 GB allocated to the database
  - 2 GB allocated to ElasticSearch
- 100 GB hard disk drive space for the operating system, application, and log storage
- 1 Gbps Ethernet network or faster

High-throughput

- Server class 64-bit CPU with at least 16 cores at 2.9 GHz
- 20 MB cache per core
- 64 GB RAM
  - 8 GB allocated to Tomcat
  - 8 GB allocated to the database
  - 2 GB allocated to ElasticSearch
- 100 GB hard disk drive space for the operating system, application, and log storage

- 1 Gbps Ethernet network or faster

Memory requirements must be discussed at the beginning of the project, before ordering hardware.

The amount of hard disk drive space required is contingent on the frequency and amount of data generated in your lab. We recommend that you take inventory of all instruments that will be used with Clarity LIMS and calculate the amount of data generated for each of them.

To make sure that your data are protected, we recommend that your Clarity LIMS server contain redundant storage and that you perform regular backups.

For robust network performance, make sure that there are no bottlenecks lower than 100 Mbps on any connected network devices (routers, firewalls, switches). This is especially important when handling the large amounts of data produced by certain instruments.

The physical hardware specifications described are also valid for Virtual Machine (VM) environments. If you have questions about your VM architecture, contact Illumina Support.

For Illumina cloud hosted deployments, Illumina sizes the system accordingly for system load. We reserve the right to archive auditing information to maintain system performance as the data set grows.

If your subscription is not renewed for your Illumina cloud hosted deployment, at your request, we will supply you with an export of all user data. In practice, we will provide a database dump and details on the database schema for you to pull out any data you need going forward.

Server Operating System Requirements

For on-premise deployments, Clarity LIMS has been qualified to run with the following server operating systems versions:

- RedHat Enterprise Linux v8.8 and v8.9 (64-bit)
- Oracle Linux v8.8 and v8.9 (64-bit)

SELinux is not supported and must be set to either permissive or disabled mode.

For Illumina cloud hosted deployments, Illumina uses the latest qualified Oracle Linux version.

Database Requirements

For on-premise deployments, Clarity LIMS has been qualified to run with PostgreSQL 15.6.

For Illumina cloud hosted deployments, Illumina uses the latest qualified PostgreSQL version.

Web Client Requirements

The following client requirements apply to both on-premise and Illumina cloud hosted deployments.

Hardware

- 64-bit processor (dual-core 3.0 GHz)

- 8 GB RAM

Operating Systems

- Windows 10

> Microsoft Surface Pro support is for all operations only when a mouse is used. Touch screen support is for read-only lab work. Running samples through steps is not supported.

- Linux (restricted to the server-supported versions listed previously)
- Macintosh OS X (12 Monterey or later)
- iOS 15 on iPad running Safari browser

> iPad support is for read-only lab work. Running samples through steps is not supported.

Web Browsers

- Google Chrome (latest update)
- Mozilla Firefox (latest update)
- Apple Safari on iPad only (latest update)

Other Requirements

- 1280 x 800 or higher
- Cookies and JavaScript must be enabled

For both on-premise and Illumina cloud hosted deployments, a 20 Mbs network connection speed from client to server is required. If remote access via VPN is needed for LDAP or instrument integrations, we recommend 100 Mbs network connection speed between your site and the hosted instance.

Automation Worker Requirements

The following requirements apply to automation workers installed on premise, for both on premise deployments and Illumina cloud hosted deployments, to support instrument integrations.

Hardware

- 64-bit processor
- 1 Gb RAM
- Hard disk drive space equivalent to twice the size of the largest file you are planning to transfer

Operating Systems

- Windows 10
- RedHat Enterprise Linux v8.8 and v8.9
- Oracle Linux v8.8 and v8.9

Applications

- Linux – Illumina installs Java Open JDK 8.0 update 362 (1.8.0_362)
- Windows – Clients must install Java Open JDK 8.0 update 362 (1.8.0_292)

Lab Work and Dashboards Overview

Lab View is the main screen in Clarity LIMS. It shows the protocols and steps used in the lab and the number of samples queued for each step. Use this screen to do the following:

- See recent lab activities.
- See in-progress steps and steps that are ready to be worked on.
- Start or continue working on samples.
- View and follow up on *Alert Notifications* on page 12.

The Projects dashboard helps with managing projects and the day-to-day flow of samples through the lab. This dashboard provides a dynamic, project-centric view of current lab activity. It allows for the management of projects and the day-to-day flow of samples through the lab.

The Overview Dashboard displays summary information about the current activity in the lab. It provides lab managers with at-a-glance information about workflow, sample status, and alerts across projects. The dashboard is dynamic and updates automatically as changes occur in the lab.

For a brief description of the screen elements, turn on pop-up help hints—select Help (?) next to the search bar, and then hover the cursor over the area of interest.

Overview Dashboard

The Overview Dashboard displays summary information about the current activity in the lab. It provides lab managers with at-a-glance information about workflow, sample status, and alerts across projects. The dashboard is dynamic and updates automatically as changes occur in the lab.

By default, the system administrator and facility administrator roles have access to the Overview Dashboard. However, access is a configurable role-based permission. For details, see *Configure Role-Based Permissions* on page 158.

For a brief description of the dashboard elements, turn on pop-up help hints—select Help (?) next to the search bar), and hover the cursor over the area of interest.

Overall Status Bar

The Overall Status bar provides a snapshot of lab activity.

- Projects—The number of open and pending projects currently in Clarity LIMS. This number does not include closed projects.
- Samples—The number of samples in open and pending projects.

- Workflows—The number of workflows in which the samples are currently being worked through in the lab.
- Alerts—The number of unresolved alerts in the system. To trigger alerts, select Request manager review as the next step for a sample (in the Assign Next Steps screen).

Workflows

This section shows information for the lab workflows that currently have samples uploaded to them. Workflows are listed in alphabetical order.

For each workflow, the following information is shown:

- Projects—The total number of projects containing samples that are currently in the workflow. This number includes samples that are in progress in the workflow and samples that have completed the workflow.
- In progress samples—The number of samples that are currently in progress in the workflow.
- Completed samples—The number of samples that have completed the workflow.
- Protocols—The names of the protocols that are included in the workflow.
- Samples—The number of samples in each protocol of that workflow.

Protocol Capacity

If configuring the sample capacity of a protocol (see *Configure Protocols* on page 98), Clarity LIMS uses color coding to indicate the percentage of the protocol capacity that is being used.

The percentage of capacity is calculated according to the total number of samples that are currently assigned to all occurrences of the protocol (ie, across all workflows).

- Blue indicates that the number of samples currently in the protocol is less than or equal to the configured capacity.
- Yellow indicates that the number of samples currently in the protocol is between 100% - 200% of the configured capacity.
- Orange indicates that the number of samples currently in the protocol is greater than 200% of the configured capacity.

While the protocol for a particular workflow may have few, or even zero, samples assigned to it, its capacity might still display in yellow or orange. This display would occur if the number of samples in other occurrences of the protocol exceeds its configured capacity.

Hover over a protocol to view more information about its configured capacity and the total number of samples assigned to it.

Projects Dashboard

The Projects provides a dynamic, project-centric view of current lab activity. It allows for the management of projects and the day-to-day flow of samples through the lab.

Overall Status Bar

The Overall Status bar provides a snapshot of current lab activity.

- Projects—The number of open and pending projects currently in Clarity LIMS. This number does not include closed projects.
- Samples—The number of samples in open and pending projects.
- Workflows—The number of workflows in which the samples are currently being worked through in the lab.
- Alerts—The number of unresolved alerts in the system. To trigger alerts, select Request manager review as the next step for a sample (in the Assign Next Steps screen).

Project, Sample, Workflow Snapshot

Additional information provides a snapshot summary of projects and samples, including the workflows to which samples are assigned.

No Workflow Assigned

- The number of projects containing samples that do not have a workflow assigned to them.
- The number of samples that do not have a workflow assigned to them.

In Progress

- The number of projects containing samples that are in progress and being worked on in the lab.
- The number of samples that are in progress and being worked on in the lab.

Workflow Complete

- The number of projects in which all samples have completed all workflows assigned to them.
- The number of samples that have completed all workflows assigned to them.

Projects Table

By default, all open projects display in the Projects table and are sorted by creation date (most recent first).

- Select any project in the table to view its details on the right.
- Projects that have unresolved alerts display an icon in the upper-right corner.

The Projects table allows filtering to display projects that meet certain criteria.

The drop-down list provides several filters. Consider filtering for the following use cases:

- Completed projects—Prepare data and invoices to be sent to clients.
- Projects containing samples that do not have a workflow assigned to them—Find the projects containing these samples, assign workflows to the samples, and start working on them in the lab.
- Projects assigned to a particular workflow or to a particular project—View and manage their progress in the lab. In this case, type the workflow/project name into the filter box and press the Enter key.

View Project Summary Information

Select a project to display summary information about the workflows and samples related to that project. The summary includes the following information:

- The number of samples in the project that have not been assigned a workflow.
- The workflows to which samples in the project are assigned. If needed, scroll to see all the workflows.
- The number of samples involved in each workflow.
- Any unresolved alerts in the project. Select the alert to view and resolve it.
- The project completion percentage.

View Project Workflow Details

Below the Projects table and summary, the workflows for the selected project are listed.

- Directly under each workflow name, the number of in-progress and completed samples currently in the workflow.
- Select In-progress samples to view all in-progress samples across all protocols in the Samples table.
- Select the Completed samples count to view those completed samples in the Samples table.

To view workflow details:

1. To the right of the workflow name, select the arrow.
   The expanded workflow details area shows the following information:
   - All protocols included in the workflow, and the number of samples in each of those protocols.
   - The percentage of project samples currently assigned to each protocol (represented by blue shading). Hover over the shading to see this percentage. The percentage is derived from the number of samples in the protocol divided by the total number of samples in the workflow.
2. Select a protocol to see the steps it includes and the samples assigned to those steps.

View Step and Sample Details

Select a protocol to see the following information display in the Samples table:

- The steps included in the protocol, and the submitted and derived samples that are in each of those steps.
- The sample name and the first three sample custom fields.

In the Samples table, the following features are available:

- Search for samples—Select a submitted or derived sample name to search for that sample (see also *Searching for Samples*).
- View Alerts—Select an alert to go to the step in which the manager review was requested.

Run Automations on Derived Samples

Run automations on derived samples directly from the Samples table.

1. Select one or more derived samples (Ctrl + click to select multiple).
2. In the upper-right corner of the Samples table, expand the drop-down list and select an automation.
3. If the automation requires input, a prompt to enter a value displays. Enter a value and select Continue.

   If the parameter name is truncated, hover over it to view the full name.

4. As the automation runs, the status is shown in the samples list.
   For details on configuring an automation, see *Add and Configure Automations* on page 135.

Alert Notifications

As lab scientists work with samples in the lab, they may request a manager to review a sample at a certain step in the workflow. When a request for review occurs, an alert notification displays in Lab View, in the Recent Activities area.

1. In Lab View, in the Recent Activities area, select an alert to go directly to the step containing the sample to be reviewed.
2. Review the sample, add a comment, and select Finish Review.

You can also view and resolve alerts from *Projects Dashboard* on page 9.

Work with Projects

Clarity LIMS uses projects as the basis for all work performed in the system. All samples must be added to an existing project.

A project stores the following information:

- The client and account associated with the project.
- The priority of the project (Low, Standard, High).
- The samples submitted to the project.
- Project status (Pending, Open, Closed).
- The date the project was opened and closed.
- Files associated with the project.
- Any configured custom fields.

Create Projects

Before adding samples to Clarity LIMS, create a project to store them.

By default, you can create projects. However, this role-based permission is configurable. For details, see *Configure Role-Based Permissions* on page 158.

1. On the Projects and Samples tab, select New Project.
2. On the Properties tab, in the Project Details section, complete the following tasks:
   - Type a descriptive name for the project.
   - If creating a new account, type the name directly into the field. Otherwise, select an existing account from the drop-down list.
   - If creating a new client, type the name directly into the field. Otherwise, select an existing client from the drop-down list.
   - By default, the project opened date is set to the current date. To change this date, select the Opened field and select a date from the calendar.
   - If necessary, edit the project priority. The default is Standard.
3. On the Custom Fields tab, complete the additional details for this project. Mandatory fields are indicated with yellow shading.
4. [Optional] To upload a file to the project:
   - Select the Files tab, then select Upload File.
   - Select Choose File, browse for and select the file, and select Upload.
5. Select Save.
   The new project displays in the Projects list. Samples can now be added.

View and Modify Projects

View, Modify and Delete a Project

To view, modify, or delete a project, complete the following steps:

1. Navigate to the Projects and Samples tab.
2. In the Projects list, select the project.
   The Project Details screen displays the details for the selected project.
3. To modify project details, select the field and edit as required (see *Create Projects* on page 12).
4. Select Save.
5. To delete the project, select Delete.

Before deleting a project, consider the following details:

- Deleting a project also deletes any samples it contains.
- By default, projects can be deleted provided no work has been recorded (or is in progress) on the samples. However, this role-based permission is configurable.

- If the samples contained in a project have recorded or in-progress protocol steps, the project cannot be deleted without special user permissions.

  For information on role-based permissions, see *Configure Role-Based Permissions* on page 158.

View and Modify Project Status

To view and update the project status, complete the following steps:

1. Navigate to the Projects and Samples tab.
2. In the Projects list, select a project.
   On the Properties tab in the Project Details area, the Status slider indicates the status of the project.
3. To move the slider and change the project status, select the desired status.

View and Modify Custom Fields

To view and modify custom fields, complete the following steps:

1. Navigate to the Projects and Samples tab.
2. In the Projects list, select a project.
3. In the Project Details area, navigate to the Custom Fields tab.
4. Select a field to modify and edit as required (see *Create Projects* on page 12).
5. Select Save.

Download / Upload Files

To download, view, and upload project files, complete the following steps:

1. Navigate to the Projects and Samples tab.
2. In the Projects list, select a project.
3. In the Project Details area, navigate to the Files tab.
   Files currently associated with the project are displayed.
4. To download and view a project file, select the file.
5. To upload a file:
   a. Select Upload File.
   b. Select Choose File.
   c. Browse for the file, select it, and select Upload.

Add Samples to Projects

Clarity LIMS uses projects as the basis for all work performed in the system. There are two ways to add samples to projects:

- Upload a sample list (Excel spreadsheet) to a project. See *Upload and Modify Samples* on page 16

- Add samples individually to one or more projects. See *Sample Accessioning* on page 20.

Create Sample Lists

To process many samples, add them to Clarity LIMS by importing a Microsoft Excel spreadsheet file (*.xls or *.xlsx). This method also applies to updating sample information.

1. Download a sample list template from the Projects and Samples view in Clarity LIMS.
2. Open the sample list template.
   By default, the template contains the following information:
   - <TABLE HEADER> and <SAMPLE ENTRIES> tags (red/purple text)
     The import process requires these identifying tags. Do not edit them.
   - Column headers (white text on blue background)
     These headers must reference the names of the fields containing the information to capture for a sample. If editing the column headers or creating additional headers, make corresponding changes to the fields in Clarity LIMS. See *Add and Configure Custom Fields* on page 146.
3. Populate the columns with the information associated with the samples.
   Enter the data into the rows between the <TABLE HEADER> and <SAMPLE ENTRIES> tags. Insert additional rows as needed.
4. Save the file and import it into a project (see *Upload and Modify Samples* on page 16).
   If the sample list specifies a container name that does not exist in Clarity LIMS, the system creates the container.

Requirements

- The sample list must be in *.xls or *.xlsx format.
- In the sample list, the column header names must match the default fields in Clarity LIMS.
- The following column header names cannot be changed: Sample/Name, Container/Name>, and Sample/Well Location.
- The following columns must be populated: Sample/Name and any sample-level custom fields that the system administrator requires.
- By default, import up to a maximum of 3456 samples from a single sample list file. To import more than 3456 samples, divide the samples into multiple files.

Tips for Data Entry

Refer also to *Batch Sample Import* on page 18.

- Enter dates using Excel date cell formatting.
- To preserve currency characters (eg, $), currency is best entered as a string (rather than using the Excel currency category).
- Numbers can be entered either as numeric or string values.

- If there are drop-down lists of values in Clarity LIMS, enter these exact values in the sample list.
- Container well locations are always Row:Column. The actual dimensions depend on the container type configuration.
- Excel may sometimes automatically alter values, depending on the type of data being entered.

For example, for Boolean fields such as Stored On Site? in the following table, numeric values of zero and false evaluate to FALSE whereas nonzero numeric values and true evaluate to TRUE. Other values result in an error on import.

Custom Field/Sample Material	Custom Field/Stored On Site?	Custom Field/Sample Location	Custom Field/Date Received
Tissue	1 (TRUE)	Freezer #1	06/01/2014
Serum	true (TRUE)	Freezer #1	06/01/2014
Tissue	0 (FALSE)	Fridge #2	07/15/2014
Serum	false (FALSE)	Fridge #2	07/15/2014
Tissue	yes (ERROR)	Fridge #2	07/15/2014

Configuring Sample Lists for Usability and Speed

Spreadsheet programs like Microsoft Excel contain features for increasing usability and speed when entering data. For example, the following configurations are available:

- Add drop-down lists of options that correspond to options available in Clarity LIMS. Use the Named Range and Data Validation Excel features.
- Hide header columns required by the system but not required.

The Clarity LIMS support team can create custom, efficient sample list templates.

Upload and Modify Samples

If there are many samples to process, add them to the system by uploading a Microsoft Excel spreadsheet file (*.xls or *.xlsx). Use the same method to modify information for multiple samples.

By default, a maximum of 3456 samples can be uploaded from a single sample list file. To upload more than 3456 samples, divide the samples into multiple files.

In the sample list, specify container placement and include values for standard and user-defined options and fields (for details, see *Create Sample Lists* on page 15).

Samples can be added individually in the Sample Management screen. For details, see *Sample Accessioning* on page 20.

Upload a Sample List

1. Navigate to the Projects and Samples tab.
2. In the Projects list, select a project to add samples. The Project Details area updates to show the details for the selected project.

3. Select Upload Sample List.
   If a sample list is not readily available, select the Download Example Sample List link to download a sample list template. Open the template file in Excel, populate it with the sample details, and save the file.

   > For more information, see *Create Sample Lists* on page 15.

4. In the Upload File dialog, select Choose File and browse to and open the sample list file.
5. Select Upload File.
   As part of the upload process, Clarity LIMS validates the file to make sure the custom field data it contains meet the requirements, presets, and restrictions that apply to submitted samples. If the file contains invalid data, an error message displays.
6. When the upload process completes, the samples display in the Submitted Samples list for the project.
   The Submitted Samples list allows the following actions:
   - Hover over the Information icon for a sample to view the details associated with it.
   - Modify sample details.
   - Add samples to a workflow.
   - If samples have been created in error, delete them from the sample list and the project (provided no work has been done on them). To complete this action, select the samples and select Delete.

After uploading, the submitted samples can be assigned to a workflow. When they are assigned, the samples are available for lab scientists to work on.

Modify Sample Information

1. Navigate to the Projects and Samples tab.
2. In the Projects list, select the project containing the samples to modify.
3. Select Modify Samples.
   Clarity LIMS generates a sample list containing all samples in the project and downloads it.
4. Open the file in Excel. It contains the Clarity LIMS IDs of all samples and all custom field data.
5. Update the sample information as required.
6. Return to the LIMS and upload the modified sample list. Follow the steps outlined in *Upload a Sample List* on page 16.

Rules for Modifying Sample Information

- A sample list can be uploaded/imported in which custom field values have been changed, removed, or added.
- While sample custom fields can only be updated, the sample list can contain other columns of data. The original data from the sample list does not have to be removed.
- If the system does not require the custom field, leave the cell blank or enter NULL.
  - A blank value leaves existing data in the system intact.

  - A NULL value clears any existing data in the system for that field.
- Clarity LIMS uses the information defined in the sample list (sample name, container type, and so on) and looks for matching samples in the project. If a matching sample is found, the system updates the sample with the values specified in the sample list.

Batch Sample Import

This topic provides guidelines and tips to help compile a sample list, in Microsoft Excel format, for importing into Clarity LIMS.

- Import up 3456 samples from a single sample list file. To import more than 3456 samples, divide the samples into multiple files.
- If an error is detected in the spreadsheet, the import process aborts. No sample imports until the error condition is resolved. See *Troubleshooting* on page 19.

Column Headers

Legend

- An asterisk indicates a mandatory field.
- Regular font, without an asterisk, indicates an optional field. See *Optional Fields* on page 19 for details.
- Text enclosed in angle brackets indicates a placeholder custom field name to replace with a value.
- Italicized text indicates a group of fields that depend on each other. All headers in the group must be either all present or all absent.

The following column headers can be used in the sample list:

- *Sample/Name—Specify the name of the sample. If the system has the unique sample name option enabled and there are duplicate sample names in the spreadsheet, expect an error message. The message provides information on this error condition. No sample is imported until duplicate names are resolved.
- Sample/Volume—Specify the volume of the sample.
- Container/Type—Specify the name of the container type to use for this sample. When specifying a value for this column, verify it exists in the system already. For instance, you can specify 100 well MALDI plate as a value, provided this container type is configured in the system.
- Container/Name—Specify the name of the container to place this sample. If the name does not match a container already in the system, a new container by this name (and of the specified type) is created.
- Sample/Well Location—Specify the well location for the sample. Values for this column are formatted like the following examples: A:1, B:12, or 1:10.
  The import process validates this location against the container type specified. If the location is out of range, the process rejects it. If placing a sample into an existing container, the process checks if the well location is already occupied and rejects it if occupied.

- Sample/Reagent Label—Specify the reagent label name to use for this sample. Values for this column are optional. They can exist in the system or, if the reagent label is not found, a new one is created. Only one reagent label is supported per sample via batch sample import.
- Custom Field/<Name of Custom Field>—Add a custom field instance to the sample. The name of the custom field must exist in the system. If the custom field name specified is not in the system, an error message displays.
  You can specify a value for this custom field in the remaining cells of this column. For example, if there is a custom field by the name Clinical Source, you may have a column header Custom Field/Clinical Source and a value of hospital for the sample. See *Optional Fields* on page 19 for details.
- Container/Custom Field/<Name of Custom Field>—Add a custom field instance to container. This field functions in a similar way to the sample custom field previously described, except the values must be defined on each row (per container). If not, an error message displays.

Optional Fields

Take Custom Field as an example. Its optional nature in the spreadsheet is contingent on whether a particular field is defined as optional or required in Clarity LIMS.

If there is a required custom field for a sample, there must be a column in the spreadsheet for this field. A value must be specified for it, before any sample can be imported.

Custom field values are validated against their type defined in Clarity LIMS, as follows.

- Date type—For example, if there is a custom field type of Date and the name is Completion Date, the best practice method is to have a column header Custom Field/Completion Date. The remaining values for the cells in the file should be formatted using one of the Excel date formats.
- Numeric type with a range defined—The value is first validated as a number. Then, the number is validated against the range defined in Clarity LIMS.
  - If the validation fails, error messages display.
  - No sample is imported until the value is validated.
- Custom field with values defined in a group of defaults—If a custom field is configured to have one or more values defined in a group of defaults and is only allowed to have one of these defined values, Clarity LIMS validates the value entered against the defined values.
  - If the value in the spreadsheet does not match one of the default values, validation fails.
  - If the validation fails, an error message displays. No sample is imported.

Troubleshooting

If Clarity LIMS expects certain information to be provided and this information is not included in the sample list, the samples are not imported.

Consider the following examples:

- If an option or field is mandatory, the sample list must contain a column to capture that information. The sample list must use the appropriate column title.
- If the samples must contain unique names, the sample list must not contain duplicate names or the names of samples already recorded in Clarity LIMS.
- Containers types referenced in the sample list must already be defined in Clarity LIMS. For example, 96-well plate or tube.
- The sample list must not place a sample into a container well that is already populated with another sample.
- Any custom fields referenced in the sample list must be defined in Clarity LIMS.

Sample Accessioning

The Sample Management screen allows for convenient sample accessioning. On this screen, add multiple samples to a single project or to multiple projects, and modify samples already added to the system.

There are two ways to access the Sample Management screen:

- The main menu bar, which allows for adding samples to one project or to multiple projects.
- The Project and Samples tab, which allows for adding samples to a project or modifying samples already added to a project.

Add Samples to One or Multiple Projects

1. On the main menu bar, hover over Projects and Samples tab and select Add Samples when the option displays.
2. In the Sample Management screen, select a project from the Project Name drop-down list. This selection autopopulates the fields in the Project Details area.
   - Edit the project details if necessary.
   - To upload files to the project, select Upload File.
3. In the Sample Details area, provide the following information:
   a. Enter the name of the sample.
   b. Choose a container from the drop-down list.
   c. Enter the container name.
   d. Complete any other applicable fields (mandatory fields are marked with an asterisk).

   LIMS ID (Submitted Sample), Date Submitted, and LIMS ID (Container) fields are automatically populated after the sample is saved.
4. To upload sample files, select Upload File at the bottom of the Sample Details section.
5. To add another sample, select Sample +.
   Add this sample to the same project or select a different project from the Project Name drop-down list.
6. Repeat steps 3 to 5 as required.

7. When all samples are added, select Submit Samples.
   Clarity LIMS validates, saves the samples, and returns to the Project and Samples tab.

On the Project and Samples tab, the projects with recently added samples are automatically selected.

While adding samples, note the following details:

- To view a subset of samples, remove selected samples from view. For details, see *Remove Samples from View* on page 21.
- Copy values across to adjacent samples by selecting the arrows to the left of the fields. Clarity LIMS automatically populates the Well field.
- If editing well information, make those changes last (before submitting the samples). Changes to Container, Container Name, LIMS ID (Container), and Sample Name may reorder the well locations.
- Use the paging buttons to scroll pages of samples.

Add Samples to a Selected Project

In this method, only add samples to the project selected. It is not possible to select a different project as described in the previous section of the documentation.

1. On the Project and Samples tab, select a project to add samples.
2. In the Submit Samples section, select Add Samples.
3. On the Sample Management screen, because the project has already been specified, the project details are automatically completed.
4. Follow steps 3 to 7 of the previous section to add the sample details.

Modify Samples

1. On the Project and Samples tab, select a project to add samples.
2. In the samples list, select the submitted samples to modify (derived samples cannot be modified).
3. Select Modify Samples.
4. Modify the sample and project details as required (the Project Name or Container Name fields cannot be modified).

   To avoid modifying or seeing all the samples selected, remove them from the view. See Remove Samples from View.

5. To save the changes, select Submit Samples.
6. Clarity LIMS validates the modifications, saves the samples, and returns to the Project and Samples tab.
   On the Project and Samples tab, the projects containing the modified samples are automatically selected.

Remove Samples from View

On the Sample Management screen, hovering over a sample displays a small Remove from view (X) button in the upper-right corner.

The effects of selecting this button differ depending on the circumstances.

Before Submitting a Sample

Selecting the Remove button before submitting a sample discards all sample details entered. A prompt appears to confirm this action.

After Submitting a Sample

Selecting the Remove button after submitting a sample removes the sample from the Sample Management screen. The sample is only hidden from this view. It is not removed from the system.

This is useful in the following circumstances:

- Adding numerous samples and only wanting to see a subset.
- Copying values across to nonadjacent samples

When Modifying Samples

Selecting the Remove button when modifying samples removes the sample from the Sample Management screen. The sample is only hidden from this view. It does not remove the sample from the system.

This is useful in the following circumstances:

- Multiple samples are selected on the Project Management screen, but not all of those selected needs to be seen or modified on the Sample Management screen.
- Copying values across to nonadjacent samples.

Assign and Process Samples

Samples must be assigned to an active workflow before they can be accessed and worked on from Lab View.

1. On the main menu, navigate to the Projects and Samples tab.
2. In the Projects list, select the project containing the desired samples.
3. In the Samples and Workflow Assignment area, the Submitted Samples and Derived Samples tabs list all the samples included in the project. Select the tab that lists the desired samples. If no work has been performed on the samples, no derived samples are listed.
4. In the chosen samples list, select the samples to be assigned to a workflow. Use the following methods to select or deselect samples:
    - Select a group to select all samples in the group (the button label changes to Deselect Group).
    - Expand the group and select samples to add them individually. Use Shift + select to select multiple adjacent samples or Ctrl + select to select multiple nonadjacent samples.
    - To deselect samples, select them or select Deselect Group to deselect all samples in the group.
5. When finished selecting samples, select Assign To Workflow and select the desired workflow from the drop-down list.

The list displays all the workflows that are currently active in the system.

6. In the samples list, a label displays showing the samples that are now assigned to a workflow. Select the X inside a label to remove that sample from the workflow.
   In the Workflows area on the right, the number of samples assigned to the workflow displays. Select the X in the upper-right corner to remove all samples from the workflow.
7. Repeat steps 3 to 6 to assign other samples to workflows, as required.
8. Assigned samples now display in Lab View, in the Available Work area, listed under the first protocol step of the selected workflow.
   To locate samples in the queue quickly, filter on the sample name.

By default, anyone signed in can remove or unassign samples from a workflow, provided no work has been recorded (or is in progress) in that workflow for those samples. However, this role-based permission is configurable. If the samples have recorded protocol steps or are in progress in the workflow, they cannot be removed from it without special user permissions. For details, see *Configure Role-Based Permissions* on page 158.

Add Samples to an Existing Container

To run a step in Clarity LIMS, select a destination container type from a preconfigured list in the Ice Bucket screen. Then, proceed to the Record Details screen where you scan the barcode of a new container to add it to Clarity LIMS.

However, you may sometimes want to place samples into an existing container with a barcode that has already been entered into Clarity LIMS. Adding samples to an existing container is easily achieved in the Ice Bucket screen.

1. In Lab View, open the step containing the samples to place into an existing container.
2. Select the samples and add them to the Ice Bucket.
3. On the Ice Bucket screen in the Container Options panel, select the desired container type from the Destination Container drop-down list.
4. In the Find Existing Container field, type the name or Clarity LIMS ID of the container in which to place the samples. While typing, Clarity LIMS presents a filtered list of containers with matching names or Clarity LIMS IDs. Select the appropriate container from the list.
5. Select Begin Work to proceed to the Record Details screen.

Remove Samples from a Queue

Occasionally, you must remove samples from a workflow queue in Clarity LIMS. Only administrator users can perform this operation.

1. In Clarity LIMS, open the step containing the samples to remove.
2. Select one or more samples, expand the Options drop-down list and select Remove.

The Options drop-down list is available to administrator users only.

If necessary, complete the following actions:

1. Search for the samples in Clarity LIMS.

2. Requeue them for a previous step.

Requeue and Rework Samples

To requeue and rework samples, specific role-based permissions are required. For details, see *Configure Role-Based Permissions* on page 158.

Requeueing Samples for a Step

Occasionally, a sample must be rerun through a particular step. For example, there may have been a technical error in the lab. More sequencing may be needed at the end of a workflow if there are not enough samples.

To solve this problem, return samples to the queue and repeat the step.

There are several ways to requeue samples:

- Search for the step with samples to requeue, view all samples that have completed this step, and choose the ones to requeue.
- Search for a specific sample to requeue.

Requeue Samples from a Completed Protocol Step

1. In the header, select Search.
2. Select Protocol Step from the drop-down list of search categories, type the step to search for, and press the Enter key.
   Type the complete step name or part of it followed by an asterisk.
3. In the search results list, select the arrow to the right of the step name to show details for all the samples that have been run through the step.
4. Select Requeue to requeue samples as required.

Requeue a Specific Sample

1. Select Sample from the drop-down list of search categories, type the sample name to search for, and press the Enter key.
2. Expand the search results details to view all the steps performed on the sample and select Requeue to return the sample to the queue for the required step.

Reworking Samples from a Previous Step

In addition to requeueing samples for the same step, you can also rework samples from a previous step. For example, an action is needed if there is an insufficient quantity of a particular sample to meet the required target concentration level.

1. In the Assign Next Steps screen, select the next step drop-down list, select Rework from an earlier step.
2. All the steps performed on the sample are listed, up to and including the current step. Select the required step and select OK.

Clarity LIMS takes the upstream sample from the selected step and places it back in the queue for the selected step, so it can be reworked from that point in the workflow.

3. The Rework from <step name> option is reflected in the next steps field.
4. The sample no longer advances in the workflow, but the sample is now found in the queue for the selected rework step.

> If a sample has been flagged for manager review, the manager can select Rework from an earlier step directly from the Review Samples screen.

Manually Move Samples to the Next Step

Usually, samples move through the system according to the sequence of protocols and steps defined in a workflow.

However, sometimes samples are moved into the next step manually.

For example, suppose you must delete a step from a particular protocol. If there are samples queued for the step, they are not able to delete it. In this case, you can move the samples forward into the next step and proceed with the step deletion (see *Configure Protocols* on page 98).

1. In Clarity LIMS, open the step containing the samples to move.
2. Select one or more samples, expand the Options drop-down list and select Move.
   The samples move into the subsequent step in the protocol.

Next Step Selection and Sample Routing

In Clarity LIMS, the outcome of the next step selection for sample outputs depends on whether those outputs are derived samples, pools, or derivatives.*Step Output: Derived Sample* on page 25

The following tables summarize the expected results when choosing next steps for these three output types.

Step Output: Derived Sample

Resolution Option	Input Result	Output Result
Next Step	Remains in workflow, but not queued for any steps	Queued for next step in the protocol
Mark Complete (last step in protocol, not last protocol in workflow)	Remains in workflow, but not queued for any steps	Queued for first step in next protocol
Mark Complete (last step in last protocol in workflow)	No longer in the workflow	No longer in the workflow
Repeat This Step	Requeued for same step	No longer in the workflow
Remove from Workflow	No longer in the workflow	No longer in the workflow

Resolution Option	Input Result	Output Result
Request Review	In progress for same step	In progress for same step, but not in any queues
Rework from Earlier Step	Queued for specified earlier step	No longer in the workflow
Complete and Repeat (not last step in protocol)	Requeued for same step	Queued for next step in the protocol
Complete and Repeat (last step in protocol, not last protocol in workflow)	Requeued for same step	Queued for first step in next protocol
Complete and Repeat (last step in last protocol in workflow)	Requeued for same step	No longer in workflow

Step Output: Pool

Resolution Option	Input Result	Output Result
Next Step	Remains in workflow, but not queued for any steps	Queued for next step in the protocol
Mark Complete (last step in protocol; not last protocol in workflow)	Remains in workflow, but not queued for any steps	Queued for first step in next protocol
Mark Complete (last step in last protocol in workflow)	No longer in the workflow	No longer in the workflow
Repeat This Step	Requeued for same step	No longer in the workflow
Remove from Workflow	No longer in the workflow	No longer in the workflow
Request Review	In progress for same step	In progress for same step, but not in any queues
Rework from Earlier Step (option not available for pooled output)	Not applicable	Not applicable
Complete and Repeat (not last step in protocol)	Requeued for same step	Queued for next step in the protocol
Complete and Repeat (last step in protocol; not last protocol in workflow)	Requeued for same step	Queued for first step in next protocol

Resolution Option	Input Result	Output Result
Complete and Repeat (last step in last protocol in workflow)	Requeued for same step	No longer in workflow

Step Output: Derivative

Resolution Option	Input Result	Output Result
Next Step	Remains in workflow, but not queued for any steps	Queued for next step in the protocol
Mark Complete (last step in protocol; not last protocol in workflow)	Remains in workflow, but not queued for any steps	Queued for first step in next protocol
Mark Complete (last step in last protocol in workflow)	No longer in the workflow	No longer in the workflow
Repeat This Step	Remains in workflow but not in any of its queues	Replicates requeued for replication step
Remove from Workflow	No longer in the workflow	No longer in the workflow
Request Review	In progress for same step	In progress for same step, but not in any queues
Rework from Earlier Step (this same step)	Requeued for same step	No longer in workflow
Rework from Earlier Step (another previous step)	Requeued for specified step	No longer in workflow
Complete and Repeat (not last step in protocol)	Requeued for same step	Queued for next step in the protocol
Complete and Repeat (last step in protocol; not last protocol in workflow)	Requeued for same step	Queued for first step in next protocol
Complete and Repeat (last step in last protocol in workflow)	Requeued for same step	No longer in workflow
Store for Later (only for replicates)	Remains in workflow	Not in any queue

Store Sample Aliquots for Later Use

When working on a step, you can create multiple aliquots of each sample, move one aliquot to the next step in the workflow, and store the others for later use.

Create and Store for Later Use

1. Add samples to the Ice Bucket.
2. In the Ice Bucket, create the required number of sample aliquots.
   - To create the same number of aliquots for all samples, select the number of derivatives to create and select Apply All. (The number adjacent to each sample updates automatically.)
   - To create a different number of aliquots for each individual sample, adjust the number adjacent to each sample.
   - In the Assign Next Steps screen, all the sample aliquots are listed.
3. To store an aliquot for later use, select Store for later from the next step drop-down list.

All aliquots of a sample cannot be stored. Advance at least one aliquot of each sample to the next step in the workflow. If not, an error message displays.

Resume Workflow on Stored Aliquots

1. In the Search drop-down list, select Sample, type the sample name, and press the Enter key.
   In the search results, all the sample aliquots are listed.
2. Select a sample aliquot to expand the details.
3. To resume work on the stored aliquot, select Resume Workflow.
   A prompt appears to confirm this step.
4. Select Confirm.
   After it is confirmed, the search results update and the sample are shown as queued for the next step in the workflow. In Lab View, the sample aliquot is now ready to be worked on.

Modify Completed Step Details

To modify the information captured on the Record Details screen of a completed step, the CanEditCompletedSteps permission is required. This functionality allows for modifications to correct errors and/or bad data.

The CanEditCompletedSteps permission is not assigned to any user roles by default. A Clarity LIMS administrator must explicitly assign the permission to each user who requires it. See the *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158 sections for details.

> Signature is not enforced again when editing completed steps. For recommended best practice, the role with CanEditCompletedSteps permission should be the same role that electronically signs off on steps. See *Rules and Constraints* on page 31 for details.

Users who have been assigned the CanEditCompletedSteps permission see an Edit button on the Assign Next Steps screen of completed steps. Selecting this button takes them to the Record Details screen, where they may modify certain step details.

The following table lists and describes the step details that can be modified:

Step Details	Description
Reagent lots	The reagent lots that were originally used when executing the step can be removed and new ones can be added. However, at least one lot must be selected. Reagent lots of any status (Pending, Active, Archived) can be used. Archived and expired lots can be selected.

Step Details	Description
Instruments	A new instrument can be selected. At least one instrument must be used. Instruments of any status (Active, Archived, Expired) can be used. Archived instruments can be selected.
Step custom fields	Step custom fields can be modified with the same constraints as when the step was originally executed. For example, read-only fields are still read-only and required fields are still required.

Step Details	Description
Sample table custom fields	Sample table custom fields can be modified with the same constraints as when the step was originally executed. For example, read-only fields are still read only and required fields are still required. The QC flag can be changed.
Files	Existing files can be removed and new files can be uploaded. Files that are script generated cannot be modified.

Rules and Constraints

To ensure the integrity of data, the following rules and constraints are in place when editing a completed step:

- Only steps that were completed in Clarity LIMS v5.1 and later are editable. If the system is upgraded to Clarity LIMS v5.1 or later, steps that were completed in a previous version cannot be edited.
- Steps that were executed using the API cannot be edited.
- If the configuration of a completed step changes after the step was run, it cannot be modified. This constraint includes any changes made to the protocol or workflow in which the step is included.
  - The automations enabled on the step.
  - The automation triggers configured on the step.
- An automation cannot be rerun on a completed step. The details of the automation command line cannot be viewed.
- Manager review/escalation comments on completed steps cannot be edited.
- The eSignature is not enforced again when editing completed steps. The eSignature from the original step execution is retained. There is not a prompt for a new signature when editing the step.

Modify a Completed Step

1. On the Assign Next Steps screen of the completed step, select Edit (upper-right corner).
   A prompt displays to confirm the desire to proceed and edit the step details.
2. Select Yes to confirm.
   The Record Details screen displays.
3. Modify the step details as required.
4. Review your changes and select Save.

Search

With Clarity LIMS v6.1 or later, there are two ways to search for items:

Basic Search—Searches the entire system or within a specific category, like samples, projects, containers, and protocol steps.

Advanced Search—Locates information stored in the system using specific criteria that cannot be defined in Basic Search.

Basic Search

Basic Search is used to search the entire system or search within the following categories:

- Samples
- Projects
- Containers
- Protocol steps

Keywords

Type a complete keyword or search term, or part of the term followed by an asterisk. Search terms are not case-sensitive.

The results include all samples, containers, projects, and protocol steps that contain the search term.

Search the Entire System

1. Select Search.
2. In the drop-down Search category list, select All. Type a search term into the adjacent field and press the Enter key.
3. At the left of the Search results windows, the Category Results panel summarizes the search results and groups them by category.
4. In the Search results list, the following actions are available:
   - Hover over the information icon to view more information.
   - Select on links to drill down further into the data.

Search for Samples

When searching for a particular sample, you may want to:

- View a list of all steps that have been performed on a specific sample.
- See which in-progress steps involve a specific sample.
- Determine which steps used a particular derived sample.
- Return a sample to the queue for a particular step, so that the step can be repeated or requeued (refer to *Requeue and Rework Samples* on page 24).

Search Keywords

When searching for samples, type the keyword or term to search for into the Search box.

Search on the following information, as it relates to a sample:

Search Keyword	Applies To	Notes
Sample name	Derived and submitted samples	
Derived sample custom fields	Derived samples	
Submitted sample custom fields	Derived and submitted samples	
Container information, container custom fields	Derived and submitted samples	Searchable information includes container name, container type, and well information.

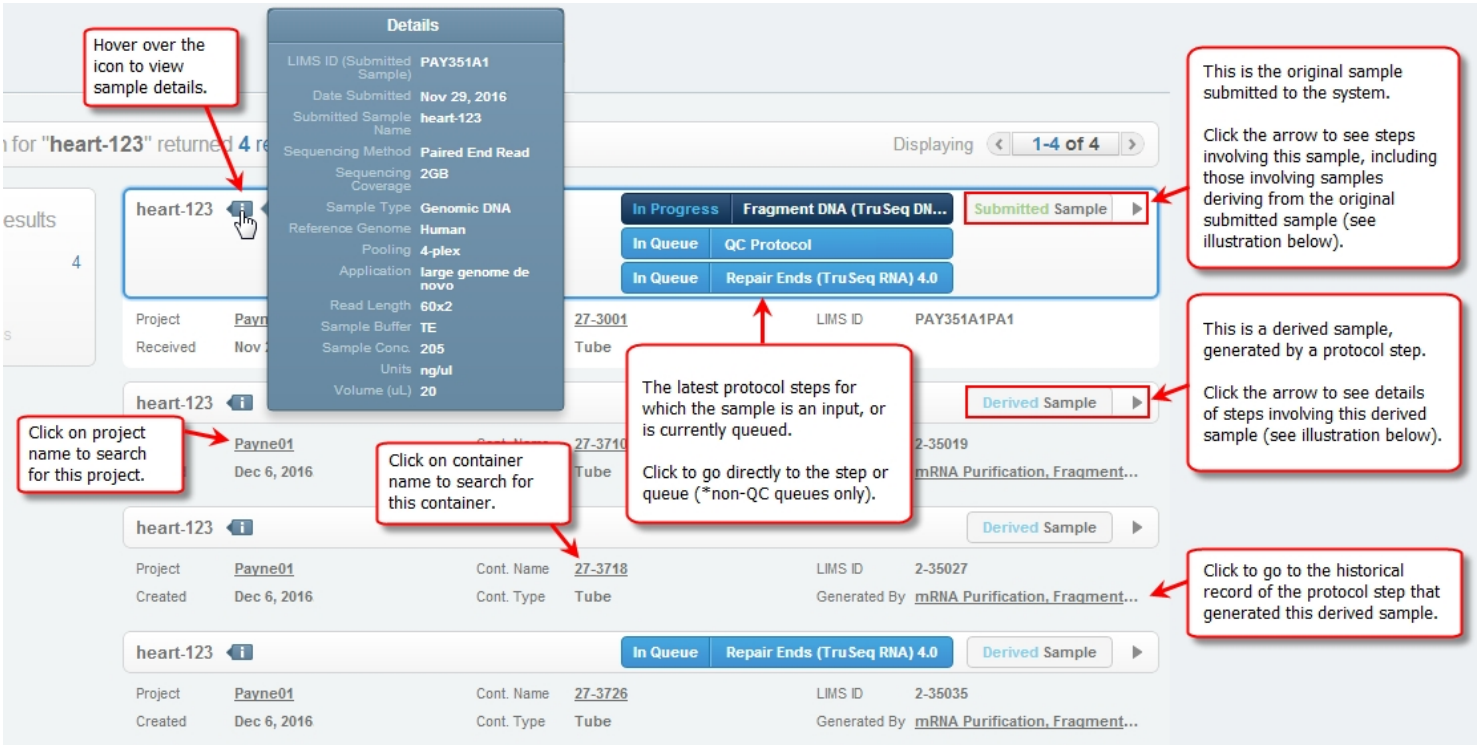
Search Keyword	Applies To	Notes
Project information, project custom fields	Derived and submitted samples	Searchable information includes project name, project owner, and account name.
Workflow name	Derived and submitted samples	Search on a workflow name to find the samples included in that workflow.

Search for a Sample

1. Select Search.
2. In the drop-down Search category list, select Sample. Type a search term into the adjacent field and press the Enter key.
   You can type the complete keyword or part of the keyword followed by an asterisk.
   For example, the search can be performed on the complete sample name (eg, heart-123). However, a keyword followed by an asterisk (eg, heart*) could also be used. The results return all samples whose name include the keyword.

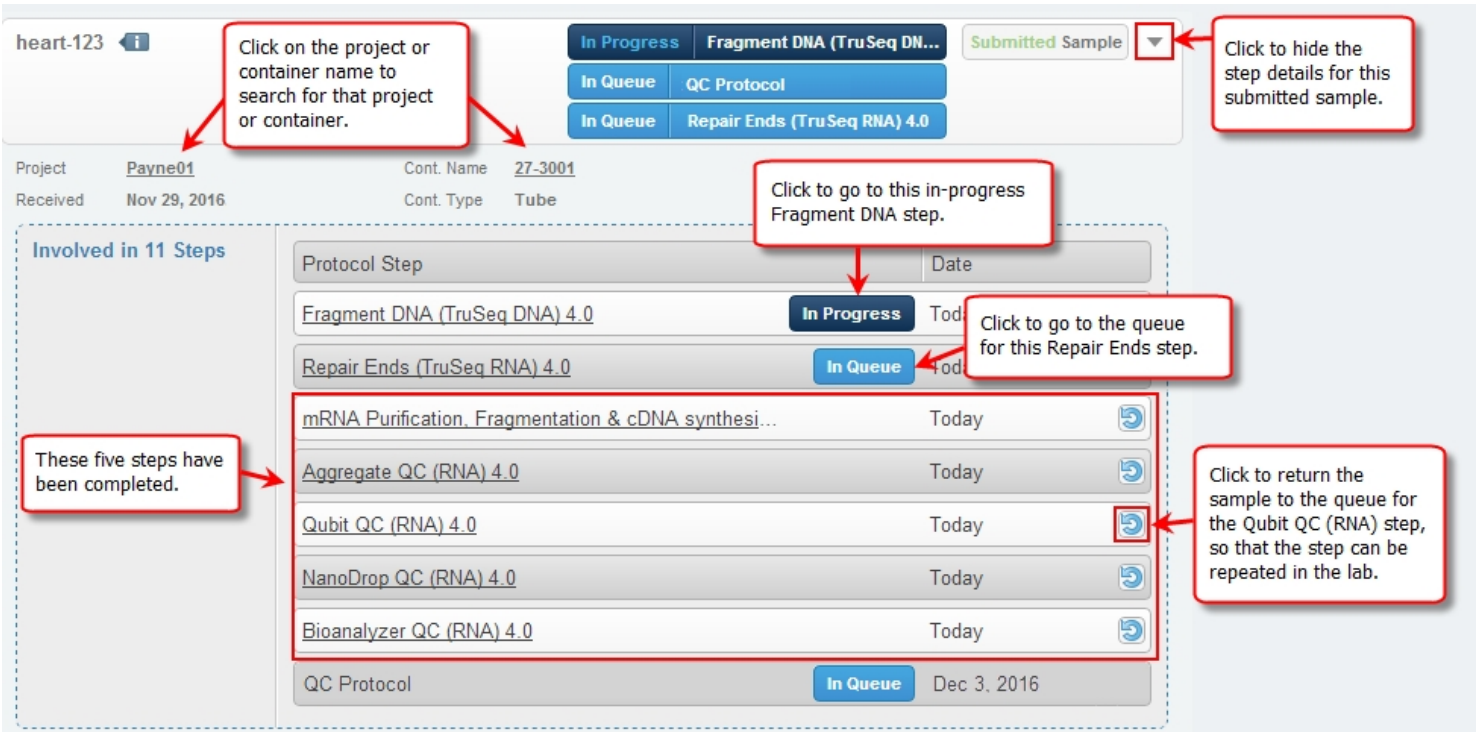
From the sample Search results list, view more information about the sample, including all steps in which it is involved and/or queued.

These options differ depending on whether the sample is a submitted sample or a derived sample.



In QC protocols, you cannot go directly to the queue for a specific step, because all steps share a queue.

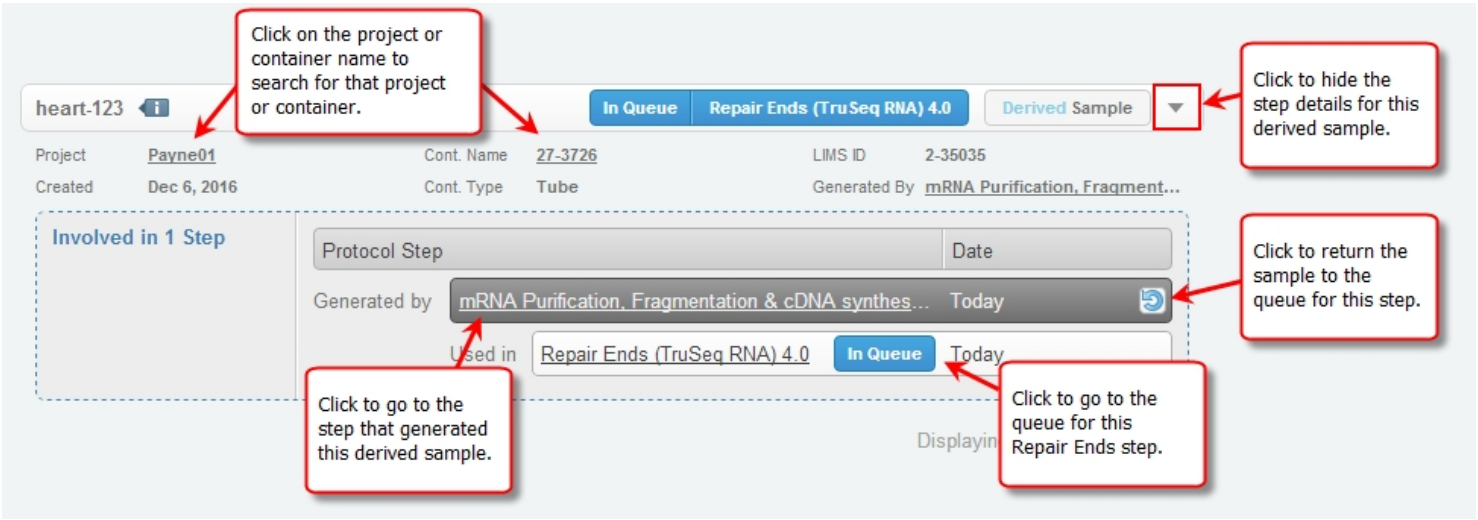
View Submitted Sample Details



Repeated steps display in the sample details search results.

For example, in the previous illustration, suppose that the sample was requeued for the Qubit QC step and the step was repeated. The next time a sample is searched, the step is listed twice.

View Derived Sample Details



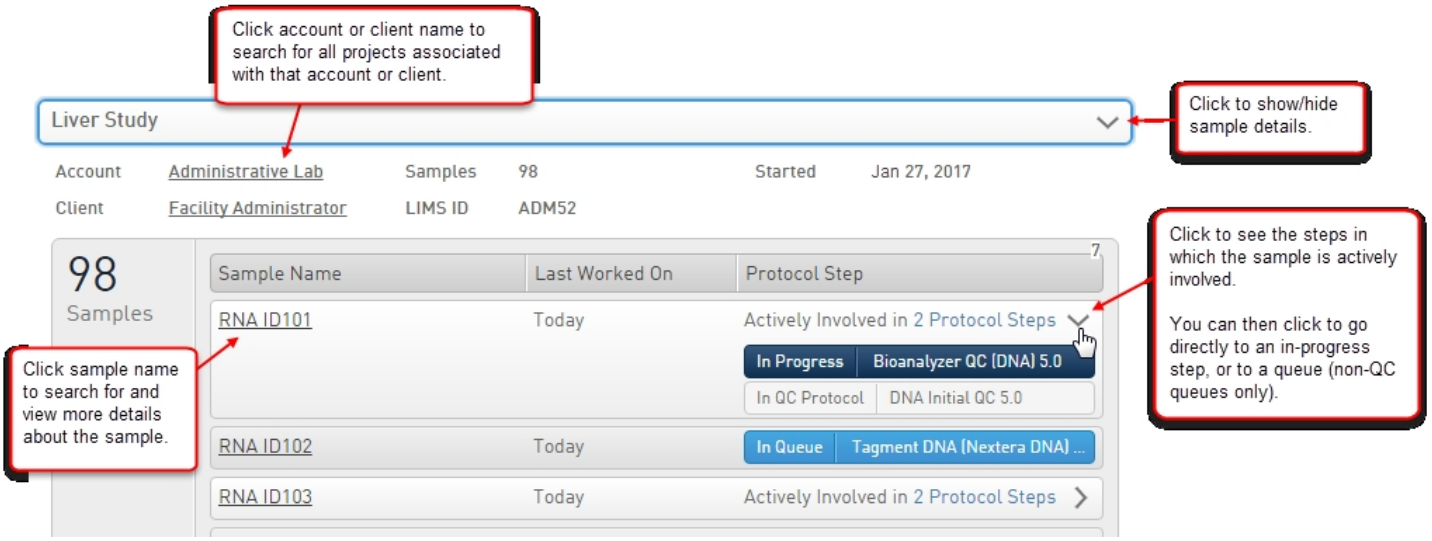
Search for Projects

Searching within the Project category allows you to drill down and quickly find the following project details:

- The account and client associated with a specific project.
- The number of samples included in a project.
- The current project status. For example, at what stage in the workflow samples are currently located and what has been completed.

Search for a project as follows.

1. Select Search.
2. In the drop-down Search category list, select Project. In the adjacent field, type the project name and then press the Enter key.
3. Type the complete project name or part of it followed by an asterisk.
4. From the Search results list, view more information about the project.
   For example, the following search results show that the Liver Study project was started on January 27, 2017 and contains 98 samples. The account and client associated with the project are also shown.



Expanding the sample details shows a list of all the steps in which the project samples are actively involved.

In QC protocols, users cannot go directly to the queue for a specific step, because all steps share a queue.

Search for Containers

Search within the Container category to search for a specific container by name (Clarity LIMS ID) or quickly find all containers of a certain type in the lab. From the search results returned, the following information can be determined:

- Which samples are in the container(s).
- Which projects are associated with the sample(s) in the container(s).
- What was the last step performed on the sample(s) and who performed it.

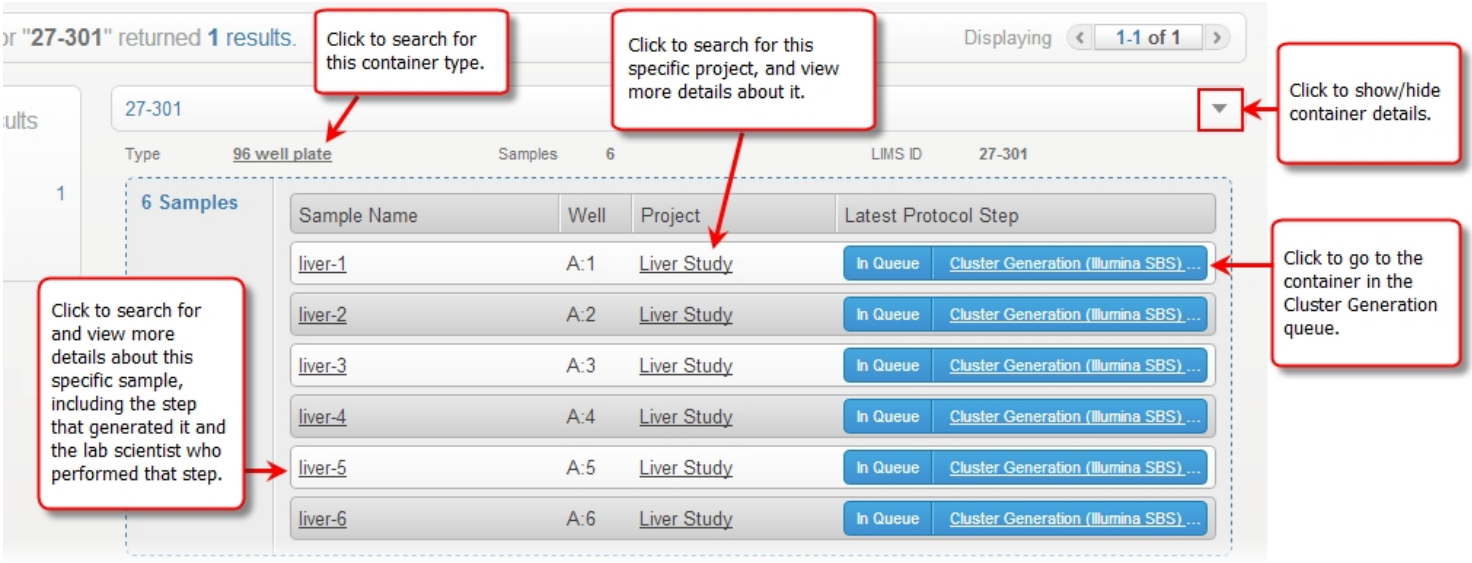
Search for a container as follows.

1. Select Search.
2. In the drop-down Search category list, select Container. In the adjacent field, type the container name and then press the Enter key.
   Type the complete container name/Clarity LIMS ID or part of the name followed by an asterisk.

From the search results list, you can view more information about the container and the sample(s) it contains.

For example, the following search results show numerous details:

- Clarity LIMS ID 27-301 belongs to a 96 well plate.
- The plate contains six samples from the Liver Study project.
- These samples are currently in the queue for the Cluster Generation step.



Search for Steps

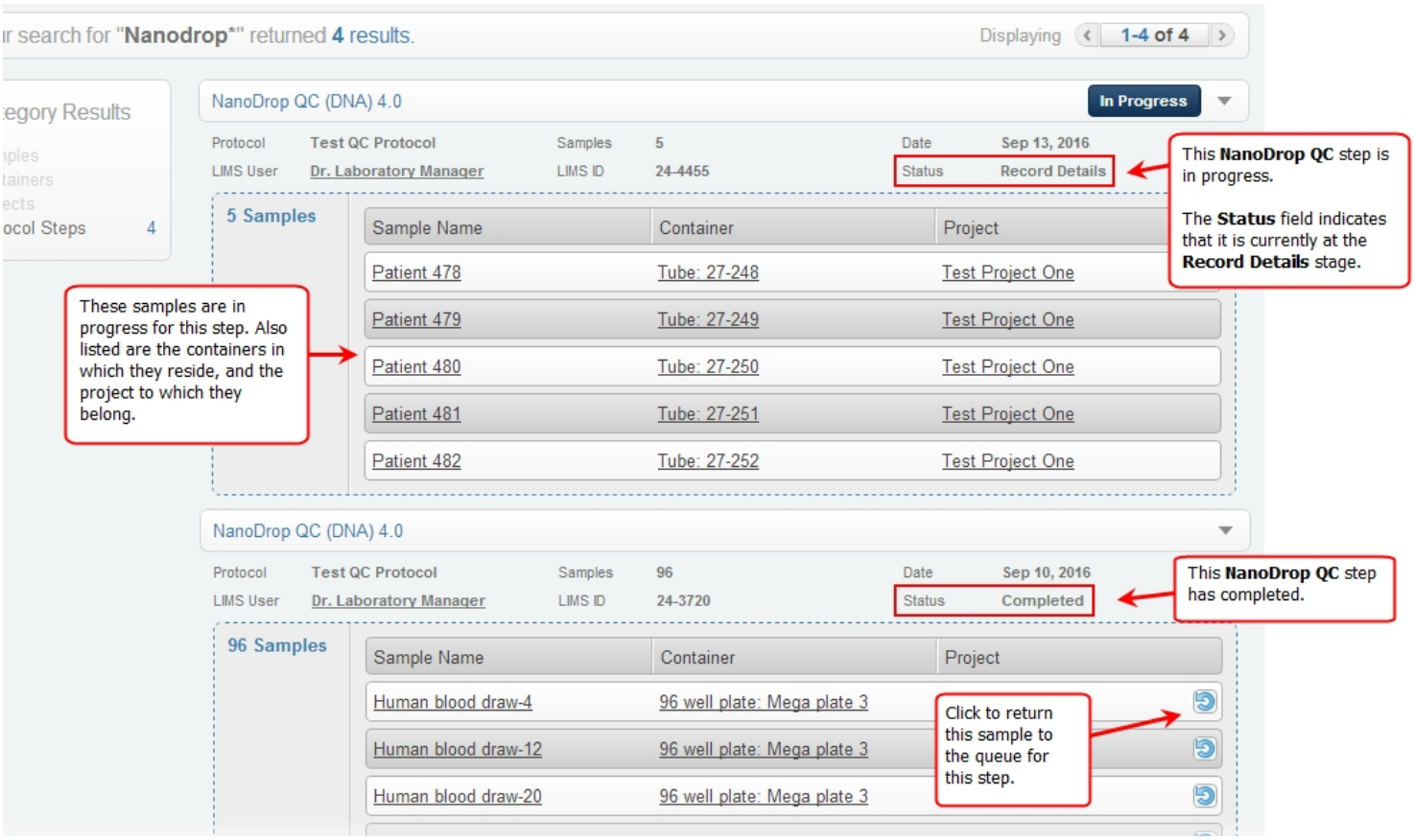
Restrict a search to protocol steps to determine how many steps of a particular type are currently in progress or completed.

Search for a Step

1. Select Search.
2. In the drop-down Search category list, select Protocol Step. In the adjacent text box, type the step name and press the Enter key.
   You can type the complete step name or part of it followed by an asterisk.

The search results list provides at-a-glance information, such as the status of each step, the date the step was started, the user who ran the step, and the number of samples contained within the step.

Various options for drilling down further into the data are provided.



Search for Steps Associated with a User

1. Select Search.
2. In the drop-down Search category list, select Protocol Step. In the adjacent field, type all or part of the user name to search for and press the Enter key.

The Search results returned will list all of the in-progress and completed steps associated with the user.

Advanced Search (Clarity LIMS v6.1 or later)

The Advanced Search function is included in Clarity LIMS v6.1 or later. Advanced Search allows you to search for specific criteria and create relationships that are used to locate information stored in the system. You can use Advanced Search to build detailed search strings (including grouped and nested strings). These search strings provide the search engine with precise instructions on what to look for in the system.

Access Advanced Search

You can use the search toolbar to select Advanced Search from the drop-down list. This selection takes you to the Advanced Search page. You can also access the Advanced Search page directly at `/clarity/advanced-search`.

Users with Read-Only permissions cannot perform a search using Advanced Search. If a user with Read-Only permissions must use Advanced Search, enable access as follows.

1. Locate the file on the server (`/opt/gls/clarity/tomcat/current/lib/activity-management-ui-config.groovy`). Create a backup of the file before proceeding.
2. Open the file and add the following code:

```
// To grant Advanced-search access to Readonly user
readonly.allowUrlMap = [
[post: ['/clarity/api/advanced-search']]
]
```

3. Restart Clarity LIMS.

Create Search Strings

The query builder panel enables you to create detailed search strings that are used within the following categories:

- Sample
- Project
- Container
- Step
- File

The panel is on the right side of the Advanced Search page.

Create search strings as follows.

1. From the query builder panel, select a category from the Search drop-down list.
2. Select Add to add one or more search conditions to the selected category.
   If a search condition has other conditions following it, an AND/OR operator is displayed. A search condition contains the following components:
   - Constraining Entity
   - Field
   - Constraint
   - Constraint Value

   Each of these conditions has an available drop-down list option (except for Constraint Value). Constraint Value can be either a field or a date picker.
3. To remove a condition, select Delete (X) to the right of the condition.

Grouping Controls

Use grouping controls to group search conditions by selecting the Show Grouping Controls checkbox. When these controls are enabled, select the checkboxes next to the conditions, and then select Group to group them together. The conditions and groups must be adjacent to each other.

The Query Preview field uses the numbers of each condition to display your search string. To separate the conditions, select the checkbox within the group, then select Ungroup.

Use Undo and Redo Operations

The Undo and Redo operations record the state of a search string when you perform one of the following operations:

- Add
- Delete
- Group
- Ungroup
- Clear all groups

When you select Undo, the string returns to the state before the last operation. When you select Redo, the string reverts to the state after the Undo operation.

Advanced Search Result Table

After you perform a search, a table shows the results. This table displays the first 500 returning results by default. Use the Configuration Property tool to change the default display.

To export the search results, select Export (down arrow) to the right of the table. Filters applied to the table are not preserved in the exported search results.

Save Query

The Save Query operation is enabled after a search is completed using a search string. You can use the Save Query panel to save search strings as follows.

1. Select Save Query.
2. Enter a descriptive name for the search string.
3. Select Save.

The new search query shows in the Save Query panel and can be used in future searches.

View, Modify, or Delete a Saved Query

- To view a saved query, select the query from the Saved Query panel.
  The Query Builder panel shows the conditions and details of the selected search query.
- To modify the search query, select the applicable conditions and edit them.
  When you update a saved query, an EDITED label displays to the left of the query name.
- To delete a saved query, select Delete (trash bin) to the left of the query.

Share or Import a Saved Search Query

- To share a saved query, select Share (right arrow) next to the applicable query in the Saved Query panel.
  A text file is downloaded that contains the selected query details.
- Import a saved search query as follows.
  a. Select Import Query.
  b. Browse for the text file and select Open.
  The query builder panel shows the details of the imported search query.
  c. After performing a search with the imported query, select Save Query.
  d. Enter a descriptive name for the search query.
  e. Select Save.
  The imported search query shows in the Saved Query panel and can be reused in future searches.

Genealogy View

Genealogy view is an interactive and hierarchical view of the history of an experiment processed through Clarity LIMS. A genealogy starts with a submitted sample and progresses with nodes nested beneath it. Information is displayed in a hierarchy and shows parent - child relationships between these nodes. For example, a derived sample may be an input to a step that produces derived sample outputs. This sample output is then input to the next step in the workflow.

Genealogy can be used to:

- View submitted samples and derived samples, on each step the samples pass through.
- Troubleshoot and view the outcome and possible continuous outcomes of each step, including the indented children steps nested within their parent steps.
- View QC flags relating to sample measurements.
- View custom fields for items in the genealogy.
- View and download files.
- View and print summary reports.

Generate a Genealogy

1. On the Projects & Samples screen, or using the search toolbar, navigate to a sample.
   – Projects & Samples screen: Select a project. All samples in the selected project are listed in the Samples & Workflow Assignment section at the bottom of the screen.
   – Search toolbar: Select Search, then select Sample from the drop-down list . Type a search term into the adjacent field and press the Enter key. You can type the complete search term, or part of it followed by an asterisk. (For details, see *Searching for Samples*.)
2. Select the sample to open the search results page.

If using the search toolbar, the search results page lists submitted samples, derived samples, and measurements that match the search criteria.

3. Select the genealogy icon next to the submitted sample name.
   Selecting a derived sample genealogy icon opens a partial genealogy. This provides information from the selected derived sample onwards. A partial genealogy does not show how the selected derived sample was produced, or provide any information about the original submitted sample.

Genealogy Node Types

Genealogy starts with a submitted sample, and progresses with additional nodes (steps, derived samples, custom fields, and/or measurements) nested beneath it.

- **Steps**—may be parent or child nodes. Most often, they are parent nodes with child nodes that are derived samples or measurements. The nodes for steps do not contain an icon.
  - **Parent nodes**—produce nested child nodes. Select the plus icon to expand the nested child nodes.
  - **Child nodes**—listed beneath parent nodes. Select the step minus icon to nest the child nodes beneath the parent node.
- **Submitted samples**—listed at the top of a complete genealogy (not listed with a partial genealogy). Cannot be a child node.
- **Derived samples**—denoted by an Erlenmeyer flask icon, these nodes contain partial genealogies. Can be parent or child nodes.
- **Custom fields**—denoted by an 'i' information icon, these nodes are created by parent nodes with custom field entries. Can be parent or child nodes.
- **Measurements**—denoted by a 'paper file' icon, these nodes represent measurements (typically produced by a QC step). Measurement nodes may also serve as file placeholders. Can be parent or child nodes, but do not produce child nodes.

Customize Genealogy View

Genealogy view can be customized to show or hide specific nodes.

Show/Hide Parent/Child Nodes

Select the plus icon next to a parent node to show the nested hierarchy of child nodes. The plus icon changes to a minus icon.

Inversely, select the minus icon next to a parent node to hide the nested child nodes. Child nodes with identical indentation are siblings.

Show/Hide Custom Fields Nodes

By default, the genealogy lists parent custom fields nodes, but hides the child nodes. To expand the child custom fields nodes, select Show All Custom Fields from the pulldown menu in the top-right corner. Select Hide All Custom Fields to return to the previous view.

Show/Hide Files Nodes

Some steps produce numerous measurements and file placeholder nodes. By default, the genealogy lists all file placeholder nodes.

- Select Hide All Files from the drop-down menu to hide all placeholders and child nodes.
- Select Show Available Files to limit the view to file place holders with attached files.
- Select Show All Files to return to the default view.

Additional Information

Genealogy lists additional information in the following areas:

Information Box

The genealogy information box contains additional information useful to the user.

View Step Information

Select the blue hyperlink text associated with a step name to launch the step screen and view detailed step information in a new browser tab.

Download Attached Files

Select the blue hyperlink text associated with a measurement node name, or a file placeholder node name, to download an attached file.

XML View

Select the blue hyperlink text listed in the LIMS ID column to open a new browser tab, and view the XML representation of the node in the API (requires API access).

QC Flags

Measurement nodes produced by steps that pass required thresholds are denoted by QC flag icons (listed under the QC flag column). To ensure they are visible when child nodes are hidden, QC flags are always shown on the parent measurement node rather than the child node.

Terms and Definitions

The following table defines the terms used in Clarity LIMS and related documentation.

Refer to *Understanding API Terminology (LIMS v5 and later)* in the *API & Database* documentation.

Account	Not fully supported in Clarity LIMS v5.x and later. Support is planned for a future release. A workaround is to create an account quickly from the Projects and Samples screen. An organization with which the facility conducts business. Includes account address, client names, and other information. Associate clients with their applicable account (see Client). ℹ In Clarity LIMS v2.1, the term labs was replaced with accounts. However, the API resource is still called lab.
Aggregation	See QC Aggregation.
Analyte	See Derived Sample. As of Clarity LIMS v5.0, this term is deprecated. However, the API resource is still called analyte.
Artifact	A generic term for an item at the beginning of a step generated by an earlier step. A derived sample or measurement is a type of artifact. ℹ In the Clarity LIMS user interface, the term artifact has been replaced with derived sample or measurement. However, the API resource is still called artifact.
Automation	Used to trigger scripts from the Clarity LIMS user interface. An automation can be configured for steps and for derived samples.
Automation worker	A software component that runs automation. May be installed on the same server as Clarity LIMS or on several other machines that all draw from the queues of one Clarity LIMS instance.
Batch processing	Operations performed on more than one object at a time. For example, adding multiple samples to the system, rather than adding them individually.
BClarity LIMS	The main web client used by lab scientists, lab managers, and system administrators to complete the following tasks: • Access information about the work currently underway in the lab. • Create projects and upload samples. • Record work completed in the lab. • View project and sample status. • Create and configure workflows, protocols, and steps. • Create and configure automation. • Create and custom fields and presets. • Create and configure instruments, reagent kits and lots, reagent labels, and control samples.

Client	An individual within the laboratory, or an external individual who works with the laboratory, who is directly associated with a project in Clarity LIMS. In the Clarity LIMS user interface, the term contact has been replaced with client. However, the API permission is still called contact.
Cloud hosted deployment	Clarity LIMS deployed with Illumina automation scripts to the Illumina Amazon AWS environment.
Collaborator	Clarity LIMS user role assigned to external customers or other individuals who submit samples to Clarity LIMS.
Contact	See Client.
Custom field (formerly UDF)	A field that Clarity LIMS administrators can add to the interface to collect information for a sample (or group of samples), master step, step, client, account, or container. For example, the administrator may wish to add a field to record whether a sample is toxic or safe to handle.
Derived sample	A sample that was generated (output) by a step. All derived samples trace back to submitted samples. By default, a step generates one derived sample. Configure some step types to output multiple derived samples (also referred to as derivatives)
Derivative	One of multiple samples generated by a step. See Derived Sample.
External Program Integration Plug-in (EPP)	See Automation. As of Clarity LIMS v5.0, this term is deprecated. However, some of the API documentation may still refer to EPP.
EPP node	See Automation worker. As of Clarity LIMS v5.0, this term is deprecated. However, some of the API documentation may still refer to EPP node.
Export	To copy a file and place it on the hard disk drive or in another piece of software.
File placeholder (formerly shared ResultFile)	A placeholder configured on a step that is replaced by a file at a run time. The file may be automatically generated or manually uploaded.
Group of defaults	A collection of prepopulated master step fields that define values for step data at run time. This eliminates the need to manually enter and make sure that information is recorded correctly every time a step is run. Groups of defaults are configured on the Custom Fields > Master Step Fields tab.
Import	To bring a file into Clarity LIMS and attach it to a placeholder or step.

Index	See Reagent Label and Label Group.
Input	An item that is consumed, processed, or analyzed by a step.
Label Also referred to as Reagent Label	Also referred to as reagent type, index, or molecular barcode. Add a label group for each reagent category used in the lab, and then add labels to the groups. Each label represents a reagent type within the group/category. See also Label Group.
Label group	A reagent category. Add a label group for each reagent category used in the lab then add labels to the groups. Each label represents a reagent type within the group or category. See also Label.
LIMS ID	A unique identifier assigned to all assets (samples, projects, containers, steps, and so on) in Clarity LIMS. • IDs are assigned in a nondecreasing sequence. • To prevent duplicate IDs being created by different applications in the suite in a race condition, each application allocates a group of IDs to itself when more are needed (currently in chunks of 50, which is not configurable). Therefore, Clarity LIMS IDs of sequentially uploaded samples, for example, may not have sequential Clarity LIMS IDs. • We reserve the right to change the algorithm that generates Clarity LIMS IDs in future versions of Clarity LIMS. It is not suggested to assume that IDs are sequential. Instead, consider using a custom field and a script to set a sequential number.
Master step (formerly process type)	A technique or procedure performed on a sample. To be considered a master step in Clarity LIMS, the technique/procedure must be created and configured as such, and must have an input (not all steps have an output). Master steps are created and configured on the Lab Work configuration screen. These master steps act as templates from which individual steps are created and configured.
Measurement (formerly ResultFile)	Data that is generated during a step for each sample input to the step. Measurements can either be data written to measurement fields and/or files attached to the step inputs.
On premise deployment	Clarity LIMS deployed to your on-premise server or another non-Illumina cloud hosted environment, such as your own Amazon AWS environment.
Parse	The process of analyzing an input file and displaying it in Clarity LIMS.
Plug-in	A software component or module that adds functionality to a software program.
Preset	See Group of Defaults. As of Clarity LIMS v5.0 this term is deprecated.
Process	See step. As of Clarity LIMS v5.0, this term is deprecated. However, the API resource is still called process.

Process type	See Master step. As of Clarity LIMS v5.0, this term is deprecated. However, the API resource is still called process.
Project	Clarity LIMS uses projects as the basis for all work performed in the system. A project stores the information about the user who created it, the account and client with which they are associated, samples submitted to the project, significant dates, associated files, and so on. When adding samples to Clarity LIMS, they must add them to a project.
Protocol	In Clarity LIMS, a protocol is a set of steps that must be performed in a specific sequence, as part of a lab workflow.
QC aggregation	QC aggregation refers to a configured step that assembles sample QC measurements, evaluates them based on priority, determines overall QC results, and then assigns QC flags.
Queue	Queues allow the grouping of a collection of samples that are all waiting to be processed at a specific stage (protocol) in the lab workflow.
Reagent label	See Label.
Replicate(s)	See Derivative. As of Clarity LIMS v5.0, this term is deprecated.
Resultfile	See Measurements and File Placeholders. As of Clarity LIMS v5.0, this term is deprecated. However, some of the API documentation may still refer to ResultFile outputs.
Researcher	A role that can be assigned to a user in Clarity LIMS. Typically, the researcher role is assigned to laboratory scientists who use Clarity LIMS to manage and record their work as samples are processed in the lab.
Step	A lab procedure that has been configured and included as part of a protocol. All steps have a master step as their foundation.
Step type	In Clarity LIMS, steps and master steps are categorized based on the requirements and goals of the step, its inputs, and its outputs. For details, see *About Step Types and Outputs* on page 62.
Submitted sample	The original sample that is added to a project in Clarity LIMS.
Timestamp	The dates and times associated with a file.
User	An individual within the laboratory or an external individual who works with the laboratory and has access to the Clarity LIMS system. Because each step performed in Clarity LIMS is associated with a user, you can use this feature to track work through the lab.
User-defined field (UDF)	See Custom Fields. As of Clarity LIMS v5.0, this term is deprecated. However, the API resource is still called UDF and some API documentation may still refer to UDFs.
Workflow	A set of protocols arranged in a sequence that corresponds to how work is performed in the lab.

Configuration Restrictions

Use the Lab Work configuration screen to model the workflows, protocols, and steps used in the lab.

Workflow and Protocol Restrictions

- Empty protocols cannot be added to a workflow. The protocol must include steps.
- Empty workflows cannot be activated. However, empty workflows can be saved in the pending state.
- Modify a workflow only while it remains in the pending state. You cannot rename a protocol included in an active or archived workflow.
- Delete a workflow only while the workflow remains in the pending state. You cannot delete active or archived workflows.
- A protocol cannot be removed from an active or archived workflow.
- A protocol cannot be deleted from an active or archived workflow.
- A protocol cannot be added to an active or archived workflow.
- Protocols cannot be reordered within an active or archived workflow.

Step Restrictions

- Steps in a protocol cannot be added, reordered, or deleted in an active or archived workflow.
- Settings saved as part of the master step configuration cannot be configured at step level. On the step configuration form, these settings display with a Locked icon.
- The master step can be changed, providing the new master step is of the same step type. The list of master steps is filtered to show valid options.
- If you remove configured settings from a master step, the settings on the derived steps revert to their default values unless doing so would leave the step in an unworkable state. For example, the last container from a step cannot be removed. Exceptions to this 'revert to default' rule are noted where applicable.

Master Step Restrictions

- A master step cannot be deleted if it is used to generate a step that is in an active or archived workflow.
- A master step cannot be deleted if it has already been used to create one or more steps. First, delete the step, and then delete the master step. In this case, the Delete button is disabled.

For Research Use Only. Not for use in diagnostic procedures.

- After a step type has been chosen and saved as part of a master step configuration, it cannot be change.

Custom Field Restrictions

- A master step field cannot be deleted if it has been assigned a value, or is in use in a step. If a step derived from the master step with which the field is associated has been started.
- A custom field no longer displays if deleted in the LIMS interface; however, its information is retained in the database for historical purposes.
- If the field name specified is the same as a field that has been deleted, the new field is created and the conflicting field name is renamed in the database.
- A custom field cannot be deleted on a global field object or master step with the same name as an existing field on that object/master step. For example, if a global field is created called 'Description' on the Account object, another global field cannot be created called 'Description' on the Account object. However, a 'Description' field on the Project object can be created.

Step Automation Restrictions

- Multiple automations with the same name cannot be enabled on a master step, even if the automations are configured differently.
- Two automations can have the same name as long as they are unique in some other way. For example:
  - channel name is unique, or
  - command line is unique, or
  - run-program-per-eventvalues (available in the API only) are unique

Attached files and associated master steps are ignored in these comparisons.

Configuration Restrictions

Use the Lab Work configuration screen to model the workflows, protocols, and steps used in the lab.

Workflow and Protocol Restrictions

- Empty protocols cannot be added to a workflow. The protocol must include steps.
- Empty workflows cannot be activated. However, empty workflows can be saved in the pending state.
- Modify a workflow only while it remains in the pending state. You cannot rename a protocol included in an active or archived workflow.

For Research Use Only. Not for use in diagnostic procedures.

- Delete a workflow only while the workflow remains in the pending state. You cannot delete active or archived workflows.
- A protocol cannot be removed from an active or archived workflow.
- A protocol cannot be deleted from an active or archived workflow.
- A protocol cannot be added to an active or archived workflow.
- Protocols cannot be reordered within an active or archived workflow.

Step Restrictions

- Steps in a protocol cannot be added, reordered, or deleted in an active or archived workflow.
- Settings saved as part of the master step configuration cannot be configured at step level. On the step configuration form, these settings display with a Locked icon.
- The master step can be changed, providing the new master step is of the same step type. The list of master steps is filtered to show valid options.
- If you remove configured settings from a master step, the settings on the derived steps revert to their default values unless doing so would leave the step in an unworkable state. For example, the last container from a step cannot be removed. Exceptions to this 'revert to default' rule are noted where applicable.

Master Step Restrictions

- A master step cannot be deleted if it is used to generate a step that is in an active or archived workflow.
- A master step cannot be deleted if it has already been used to create one or more steps. First, delete the step, and then delete the master step. In this case, the Delete button is disabled.
- After a step type has been chosen and saved as part of a master step configuration, it cannot be change.

Custom Field Restrictions

- A master step field cannot be deleted if it has been assigned a value, or is in use in a step. If a step derived from the master step with which the field is associated has been started.
- A custom field no longer displays if deleted in the LIMS interface; however, its information is retained in the database for historical purposes.
- If the field name specified is the same as a field that has been deleted, the new field is created and the conflicting field name is renamed in the database.

For Research Use Only. Not for use in diagnostic procedures.

- A custom field cannot be deleted on a global field object or master step with the same name as an existing field on that object/master step. For example, if a global field is created called 'Description' on the Account object, another global field cannot be created called 'Description' on the Account object. However, a 'Description' field on the Project object can be created.

Step Automation Restrictions

- Multiple automations with the same name cannot be enabled on a master step, even if the automations are configured differently.
- Two automations can have the same name as long as they are unique in some other way. For example:
  - channel name is unique, or
  - command line is unique, or
  - run-program-per-eventvalues (available in the API only) are unique

Attached files and associated master steps are ignored in these comparisons.

Lab Work Overview

Configure the workflows, protocols, steps, and master steps used in the lab on the Lab Work configuration screen.

To access the Lab Work configuration screen, the Configuration:update permission is required. Without this permission, the Lab Work tab is not visible.

By default, only the administrator role has the Configuration:update permission. For more on user roles and permissions, refer to *User Roles* and *Configure Role-Based Permissions*.

To view and configure lab work components:

1. On the main menu, select Configuration.
2. Select the Lab Work tab.
   The main navigation panel lists the workflows, protocols, steps, and master steps configured in Clarity LIMS. From here, complete the following actions as needed:
   - View the relationships between workflows, protocols, steps, and master steps.
   - View workflow, protocol, step, and master step configuration in the form beneath the navigation panel.
   - See the status of workflows (pending, active, or archived).
   - Add and modify workflows, protocols, steps, and master steps.
3. Select a workflow, protocol, step, or master step to view related configuration items in the other lists.
   Selecting a protocol highlights the following items:

For Research Use Only. Not for use in diagnostic procedures.

- All workflows that include the selected protocol are highlighted.
- All steps in the selected protocol are highlighted.
- All master steps from which the steps are derived are highlighted.

Selecting a workflow highlights the following items:

- All protocols in the workflow, which display sequentially at the top of the Protocols list.
- All steps in those highlighted protocols.
- All master steps from which the highlighted steps are derived.

Zoom out in the browser to maximize the number of items visible in the lists. Drag the lower edge of the panel to see more list items.

Versioning Components in Clarity LIMS

The sections below provide two best practice strategies for versioning lab work components in Clarity LIMS.

Strategy A

The following table summarizes Strategy A versioning rules for workflow items.

Entity	In Test Environment	In Production Environment
Master Step	Not versioned with a number	Not versioned with a number
Protocol Step	Not versioned with a number	Not versioned with a number
Protocol	Versioned with Prod version.Test version	Not versioned with a number
Workflow	Versioned with Prod version.Test version.Revision	Versioned with Prod version

Example Workflow and Components

Workflow A	Protocol A	Step A
		Step B
		Step C
	Protocol B	Step D
		Step E

For Research Use Only. Not for use in diagnostic procedures.

		Step F
	Protocol C	Step G

Scenario 1: Create New Test Workflow

Assumption: You create a workflow in the Test environment.

Recommendation:

- The workflow does not yet exist in the Production environment. Production version is 0.
- As this is the first version in the Test environment, version the workflow and protocols as 0.1, but not the steps / master steps. Test version is 0.1.

Results:

Workflow A - 0.1	Protocol A - 0.1	Step A
		Step B
		Step C
	Protocol B - 0.1	Step D
		Step E
		Step F
	Protocol C - 0.1	Step G

Scenario 2: Replace Step B

Assumption: You made a configuration error in Step B and need to replace it.

Recommendation:

1. Rename Step B to *Step B – deprecated*.
2. Recreate Step B with new configuration.
3. Rename Protocol A – 0.1 to *Protocol A – 0.1 – deprecated*.
4. Recreate Protocol A, naming it *Protocol A – 0.2*.
5. Archive Workflow A – 0.1.
6. Rebuild Workflow A. For the workflow name (version number), use the number of the most recently created protocol—in this case, Workflow A – 0.2.

Results:

Workflow A - 0.2	Protocol A - 0.2	Step A

		Step B
		Step C
	Protocol B - 0.1	Step D
		Step E
		Step F
	Protocol C - 0.1	Step G

Scenario 3: Replace Step E

Assumption: You made a configuration error in Step E and need to replace it.

Recommendation:

1. Rename Step E to *Step E – deprecated*.
2. Recreate Step E with new configuration.
3. Rename Protocol B – 0.1 to *Protocol B – 0.1 – deprecated*.
4. Recreate Protocol B, naming it *Protocol B – 0.2*.
5. Archive Workflow A – 0.2.
6. Rebuild Workflow A. For the version number, use the number of the most recently created protocol. In this case, because version 0.2 of the workflow already exists, name it *Workflow A – 0.2.1* to indicate the first revision of 0.2.

Results:

Workflow A - 0.2.1	Protocol A - 0.2	Step A
		Step B
		Step C
	Protocol B - 0.2	Step D
		Step E
		Step F
	Protocol C - 0.1	Step G

Scenario 4: Replace Step C

Assumption: You made a configuration error in Step C and need to replace it.

Recommendation:

1. Rename Step C to *Step C – deprecated*.

For Research Use Only. Not for use in diagnostic procedures.

2. Recreate Step C with new configuration.
3. Rename Protocol A – 0.2 to *Protocol A – 0.2 – deprecated*.
4. Recreate Protocol A, calling it *Protocol A – 0.3*.
5. Archive Workflow A – 0.2.1.
6. Rebuild Workflow A, naming it with the largest number of its protocols—in this case *Workflow A – 0.3*.

Results:

Workflow A - 0.3	Protocol A - 0.3	Step A
		Step B
		Step C
	Protocol B - 0.2	Step D
		Step E
		Step F
	Protocol C - 0.1	Step G

Scenario 5: Move Workflow to Production Environment

Assumption: The workflow is ready to be moved from the Test environment to the Production environment.

Recommendation:

1. Slice the workflow and its components out of the Test environment using the config-slicer tool.
2. Rename the workflow in the XML-based slice to be version 1.
3. Rename the protocols in the XML-based slice, removing version numbers.
4. Slice the workflow into the Production environment.

Results:

Workflow A - 1	Protocol A	Step A
		Step B
		Step C
	Protocol B	Step D
		Step E
		Step F
	Protocol C	Step G

For Research Use Only. Not for use in diagnostic procedures.

Scenario 6: Remove Step C

Assumption: Step C is no longer required.

Recommendation in Test:

1. Rename Protocol A – 0.3 to Protocol A – 0.3 – deprecated.
2. Recreate Protocol A, calling it Protocol A – 0.4.
3. Archive Workflow A – 0.3.
4. Rebuild Workflow A, naming it with the largest number of its protocols—in this case Workflow A – 0.4.

Recommendation in Production:

1. Slice the workflow and its components out of the Test environment using the config-slicer tool.
2. Rename the workflow in the XML-based slice to be 2.
3. Rename the protocols in the XML-based slice removing version numbers.
4. Slice the workflow into the Production environment.

Results in Test:

Workflow A – 0.4	Protocol A – 0.4	Step A
		Step B
	Protocol B – 0.2	Step D
		Step E
		Step F
	Protocol C – 0.1	Step G

Results in Production:

Workflow A – 2	Protocol A	Step A
		Step B
	Protocol B	Step D
		Step E
		Step F
	Protocol C	Step G

For Research Use Only. Not for use in diagnostic procedures.

Strategy B

The following table summarizes Strategy B versioning rules for workflow items.

Entity	In Test Environment	In Production Environment
Master Step	Versioned with a number	Versioned with a number
Protocol Step	Versioned with a number	Versioned with a number
Protocol	Versioned with Major version.Minor Version	Versioned with Major version.Minor version
Workflow	Versioned with Major version.Minor version.Revision (if necessary)	Versioned with Prod version.Test version.Revision (if necessary)

Example Workflow and Components

Workflow A	Protocol A	Step A
		Step B
		Step C
	Protocol B	Step D
		Step E
		Step F
	Protocol C	Step G

Scenario 1: Revise Test Workflow

Assumption: You have revised a test workflow, but it is likely to undergo several iterations before it goes live.

Recommendation:

- As the workflow does exist in Production, with version 1, this new version becomes 2.
- As this is the first version in Test, version everything as 2.1.

Results:

Workflow A - 2.1	Protocol A - 2 .1	Step A - 2 .1
		Step B - 2.1

For Research Use Only. Not for use in diagnostic procedures.

		Step C - 2.1
	Protocol B - 2.1	Step D - 2.1
		Step E - 2.1
		Step F - 2.1
	Protocol C - 2.1	Step G - 2.1

Scenario 2: Replace Step B

Assumption: You have made a mistake in configuration and need to replace Step B.

Recommendation:

1. Recreate Step B with new configuration, leading to version 2.2.
2. Rename Protocol A – 2.1 to *Protocol A – 2.1 – deprecated*.
3. Recreate Protocol A, naming it *Protocol A – 2.2*.
4. Archive Workflow A – 2.1.
5. Rebuild Workflow A, naming it with the largest number of its protocols, in this case *Workflow A – 2.2*.

Results:

Workflow A - 2.2	Protocol A - 2 .2	Step A - 2 .1
		Step B - 2.2
		Step C - 2.1
	Protocol B - 2.1	Step D - 2.1
		Step E - 2.1
		Step F - 2.1
	Protocol C - 2.1	Step G - 2.1

Scenario 3: Replace Step E

Assumption: You have made a mistake in configuration and need to replace Step E.

Recommendation:

1. Recreate Step E with new configuration, leading to version 2.2.
2. Rename Protocol B – 2.1 to *Protocol B – 2.1 – deprecated*.
3. Recreate Protocol B, naming it *Protocol B – 2.2*.
4. Archive Workflow A – 2.2.

For Research Use Only. Not for use in diagnostic procedures.

5. Rebuild Workflow A, naming it with the largest number of its protocols. As version 2.2 of the workflow already exists, and this is the first revision of the workflow, the new workflow name is *Workflow A – 2.2.1*. This indicates that it is the first revision of 2.2.

Results:

Workflow A - 2.2.1	Protocol A - 2 .2	Step A - 2 .1
		Step B - 2.2
		Step C - 2.1
	Protocol B - 2.2	Step D - 2.1
		Step E - 2.2
		Step F - 2.1
	Protocol C - 2.1	Step G - 2.1

Scenario 4: Replace Step C

Assumption: You have made a mistake in configuration and need to replace Step C.

Recommendation:

1. Recreate Step C with new configuration, leading to version 2.2.
2. Rename Protocol A – 2.2 to *Protocol A – 2.2 – deprecated*.
3. Recreate Protocol A, naming it *Protocol A – 2.3*.
4. Archive Workflow A – 2.2.1.
5. Rebuild Workflow A, naming it with the largest number of its protocols—in this case *Workflow A – 2.3*.

Results:

Workflow A - 2.3	Protocol A - 2 .3	Step A - 2 .1
		Step B - 2.2
		Step C - 2.2
	Protocol B - 2.2	Step D - 2.1
		Step E - 2.2
		Step F - 2.1
	Protocol C - 2.1	Step G - 2.1

For Research Use Only. Not for use in diagnostic procedures.

Scenario 5: Move Workflow to Production Environment

Assumption: The workflow is ready to be moved from the Test environment to the Production environment.

Recommendation:

1. Slice the workflow and its components out of the Test system using the config-slicer tool.
2. Slice the Workflow into the Production environment.

Results:

Workflow A - 2.3	Protocol A - 2 .3	Step A - 2 .1
		Step B - 2.2
		Step C - 2.2
	Protocol B - 2.2	Step D - 2.1
		Step E - 2.2
		Step F - 2.1
	Protocol C - 2.1	Step G - 2.1

Scenario 6: Remove Step C

Assumption: Step C is no longer required.

Recommendation in Test:

1. Rename Protocol A – 2.3 to *Protocol A – 2.3 – deprecated*.
2. Recreate Protocol A, calling it *Protocol A – 2.4*.
3. Archive Workflow A – 2.3.
4. Rebuild Workflow A, naming it with the largest number of its protocols—in this case *Workflow A – 2.4*.

Recommendation in Production:

1. Slice the Workflow and its components out of the Test system using the config-slicer tool.
2. Slice the Workflow into the Production system.

Results:

Workflow A - 2.4	Protocol A - 2 .4	Step A - 2 .1
		Step B - 2.2
	Protocol B - 2.2	Step D - 2.1

For Research Use Only. Not for use in diagnostic procedures.

		Step E - 2.2
		Step F - 2.1
	Protocol C - 2.1	Step G - 2.1

Best Practice Configuration

The best practice method for creating and configuring lab work components in Clarity LIMS is as follows.

1. Create and configure master steps.
2. Create and configure protocols.
3. Create and configure steps, adding them to the appropriate protocols, and using the master steps created in step 1 as templates.
4. Create and configure workflows, adding required protocols.

While these are the recommended steps, you can create protocols first, or create workflows and add the protocols later. However, before creating a step, you must select the protocol in which to add the step, and the master step on which to base its configuration.

Overview of Steps and Master Steps

In Clarity LIMS, steps and master steps are techniques or procedures that are performed on a sample. They are the building blocks of the lab work.

Think of master steps as starting points to create the individual steps that are run in the lab.

- The master step <--> step relationship is one to many:
  - Each step is derived from a master step.
  - A master step may be used as the foundation for multiple steps.
- All steps are derived from a master step and inherit any properties configured on the master step.
- If you configure properties at the step level, those properties only apply to that particular step.

To understand how properties set on the master step propagate down to the step level, refer to *Rules for Propagation of Master Step Properties* on page 67.

To access the Lab Work tab and configure workflows, protocols, steps, and master steps, the Configuration:update permission is required. By default, only the Administrator role has this permission. For details, refer to *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

For Research Use Only. Not for use in diagnostic procedures.

About Step Types and Outputs

In Clarity LIMS, steps are categorized by type, where each type is based on the requirements and goals of the step, and the outputs generated by the step. Some step types have unique interfaces and properties designed to perform specific tasks, such as adding reagent labels or pooling samples.

The step type is set on the Master Step Settings configuration form, and all steps inherit the step type of the master step on which they are based. (To understand the relationship between master steps and steps, refer to *Overview of Steps and Master Steps* on page 61.)

The step type is also displayed on the Step Settings configuration form, but as a read-only property.

Step Inputs and Outputs

All step types must have a submitted sample or derived sample input, and may generate either derived sample outputs, measurement outputs, or no outputs.

Keep in mind that only one output type is permitted. A step cannot generate both a derived sample and a measurement output. The type of step you choose determines which output generation options display. For example:

- Selecting the Standard step type only displays settings for derived sample generation.
- Selecting the Standard QC step type only displays settings for measurement generation.
- Selecting the No Outputs step type only displays settings for no output generation.

Downstream Functionality

The type of step you choose also enables or disables certain functionality downstream. For example:

- Selecting the Pooling step type displays the Pooling screen when the step is run, allowing the ability to create pools of samples. Choosing this step type allows you to configure the number of aliquots used to generate the pools.
- Selecting the Add Labels step type displays the Add Labels screen when the step is run, allowing the ability to configure reagent label format options.

Rules and Constraints

- When creating a master step, you must choose a step type.
- When you have saved a master step configuration:
  - Step type cannot be changed.
  - The number of outputs generated can be adjusted, or switch from a fixed number to a variable number (Standard, Standard QC, Add Labels, Pooling, Analysis step types).

Step Types

The following step types are available in Clarity LIMS:

Standard

Standard steps can have a fixed or variable ratio of samples entering the step to derived samples being generated from the step. After saving, you can switch between fixed and variable.

Default step output: By default, this step type generates one derived sample for every sample tracked in the step.

Setting	Options for This Step Type	Default	Description
Derived sample generation	Fixed – For every sample that enters the step, a fixed number of derived samples are generated.	Fixed value set to 1, configurable	The number of derived samples generated is fixed. The number cannot be changed when running the step.
	Variable – For every sample that enters the step, a variable number of derived samples are generated at run time.		The number of derived samples generated can be set. This option displays on the Ice Bucket screen.

Downstream functionality: Choosing this step type disables the Pooling and Add Labels screens. Derived sample outputs require placement.

Example steps of this type: Library Normalization, Fragment DNA

Standard QC

Standard QC steps may be included in QC protocols, and may also be included as inline QC steps in other protocol types.

Standard QC steps generate sample measurements, which can have a Fixed or Variable ratio of samples entering the step to measurements being generated.

Default step output: By default, this step type generates one measurement for every sample tracked in the step.

Setting	Options for This Step Type	Default	Description
Measurement generation	Fixed – For every sample that enters the step, a fixed number of derived samples are generated.	Fixed value set to 1, configurable	The number of derived samples generated is fixed. The number cannot be changed when running the step.
	Variable – For every sample that enters the step, a variable number of measurements are generated at run time.		The number of derived samples generated can be set. This option displays on the Ice Bucket screen.

Downstream functionality: Choosing this step type disables the Pooling and Add Labels screens. You may configure a QC step to display or not display the Placement screen.

Example steps of this type: Bioanalyzer QC, NanoDrop QC, Qubit QC

No Outputs

The No Outputs step type does not generate any outputs. You can use this step type for sorting steps or for aggregate QC steps.

Default step output: This step type does not generate any outputs. (This is not configurable.)

QC aggregation is the final step in a QC protocol. This step aggregates the data from the previous Standard QC steps to determine the overall quality of the samples. At the end of the step, samples either pass QC and proceed to the next protocol, or fail QC and are rerun or removed from the workflow.

- At least one aggregate QC step is required in QC protocols.
- At a minimum, one Standard QC step must be run before QC aggregation can occur.

To use a No Outputs step type for QC aggregation, enable QC flags on the Record Details milestone. Refer to *Record Details Milestone* on page 93.

Setting	Options for This Step Type	Default	Description
Measurement generation	None - For every sample that enters the step, 0 measurements are generated.	None (not configurable)	No measurements are generated and cannot be change this at run time.

For Research Use Only. Not for use in diagnostic procedures.

Downstream functionality: Choosing this step type disables the Pooling, Placement, and Add Labels screens.

Example steps of this type: Aggregate QC (DNA), Aggregate QC (RNA), Aggregate QC (Library Validation)

Add Labels

This step type is used to apply a reagent label (or molecular barcode) to each sample entering the step. It may be run on multiple tubes and on multiple plates. Running an Add Labels step allows for a permanent reagent label to be added to each sample. The label data appears while running the step, in a new column in the Sample Data table on the Record Details screen.

Add Labels steps generate derived samples, which can have a Fixed or Variable ratio of samples entering the step to derived samples being generated.

Default step output: By default, this step type generates one labeled derived sample for every sample that enters the step.

Setting	Options for This Step Type	Default	Description
Derived sample generation	Fixed– For every sample that enters the step, a fixed number of labeled derived samples is generated.	Fixed value set to 1, configurable	The number of derived samples generated is fixed. The number cannot be changed when running the step.
	Variable– For every sample that enters the step, a variable number of labeled derived samples is generated at run time.		The number of derived samples generated can be set. This option displays on the Ice Bucket screen.

Downstream functionality: Choosing this step type disables the Pooling screen and enables the Add Labels screen.

Example steps of this type: Add Multiple Reagents, Adenylate Ends and Ligate Adapters, PCR Amplification.

Pooling

This step type allows for multiple samples to be pooled into a single sample/container for sequencing efficiency. The number of pools is determined while running the step. Samples typically have a label, which is used to differentiate each sample at the demultiplexing stage.

Pooling steps generate pools that are created from a Fixed or Variable number of aliquots.

Default step output: By default, for every sample that enters the step, one aliquot is used to generate pools.

Setting	Options for This Step Type	Default	Description
Aliquot generation	Fixed – For every sample that enters the step, a fixed number of aliquots is used to generate pools.	Fixed value set to 1, not configurable	The number of aliquots used to generate pools is fixed, and displays on the Pooling screen and cannot change this value when running the step.
	Variable – For every sample that enters the step, a variable number of aliquots is used to generate pools at run time.		The number of aliquots used to generate pools can be set. This option displays on the Ice Bucket screen.

Downstream functionality: Choosing this step type disables the Add Labels screen and enables the Pooling screen.

- The number of pools is determined on the Pooling screen.
- By default, users are prevented from pooling samples without labels or with identical labels. You can modify this on the Pooling Settings configuration screen.

Example steps of this type: Pool Samples

Analysis

Analysis steps allow data to be manipulated by scripts, for example, they may be used to trigger secondary analysis or import data post analysis.

Analysis steps behave similarly to Standard QC steps and generate sample measurements. They can have a Fixed or Variable ratio of samples entering the step to measurements being generated.

Default step output: By default, this step type generates one measurement for every sample that enters the step.

Setting	Options for this step type	Default	Description
Measurement generation	Fixed– For every sample that enters the step, a fixed number of measurements are generated.	Fixed value set to 1, configurable	The number of measurements generated by the step is fixed. and cannot be changed this when running the step.
	Variable– For every sample that enters the step, a variable number of measurements are generated at run time.		The number of measurements generated can be set. This option displays on the Ice Bucket screen.

For Research Use Only. Not for use in diagnostic procedures.

Downstream functionality: Choosing this step type disables the Pooling, Placement, and Add Labels screens.

Example steps of this type: Sample History Report, Process Summary Report

Demultiplexing

This is essentially an Analysis step that deals specifically with labeled samples. It separates pools of samples based on the label assigned to those samples.

Demultiplexing steps have a Fixed ratio of samples entering the step to measurements being generated.

Default step output: By default, this step type generates one measurement for every sample that enters the step.

Setting	Options for this step type	Default	Description
Measurement generation	Fixed– For every sample that enters the step, a fixed number of measurements are generated.	Fixed value set to 1, not configurable	The number of measurements generated by the step is fixed. This is not configurable and cannot be change it when running the step.

Downstream functionality: Because samples are placed automatically by a script configured on the step, choosing this step type disables the Placement screen. Choosing this step type also disables the Pooling and Add Labels screens.

Example steps of this type: BCL Conversion and Demultiplexing.

Rules for Propagation of Master Step Properties

In Clarity LIMS, all steps are derived from a master step and inherit any properties configured on the master step.

The rules for how properties set on the master step propagate down to the step level apply to all properties. Those configured on the Master Step Settings configuration form and those configured on the step milestones.

- By default, master step properties are not set (values are null). Therefore, by default, the property settings do not propagate down to the derived steps. This means that you can set, or not set, the property freely at the step level.
- If you set a property on the master step, that property is locked (a Locked icon displays) at the step level, and cannot be modified.

In some situations, you can add to or reorder a locked property at the step level, but you can never remove the property. For example, on the Step Settings form:

For Research Use Only. Not for use in diagnostic procedures.

- You can add and reorder the column headers that display in the Sample table, even if some of those column headers are set on the master step.
- You cannot remove column headers that are set on the master step.

Master Step Property Propagation Rules

When you add a master step property setting, the setting is also added to all steps derived from that master step.

When you update a master step property setting, the setting is also updated on all steps derived from that master step. This overrides any previous values that had been applied at the Protocol Step level.

When you remove a master step property setting, the setting is also removed from all steps derived from that master step. There are a few exceptions to this rule where appropriate defaults must be applied to keep the step in a valid, workable state.

The following table summarizes what happens at the step level when a property setting is removed from the master step.

Property	Configured on Form	What Happens at Step Level
Reagent kits	Master Step/Step Settings	Removed. No defaults set.
Instrument types	Master Step/Step Settings	Removed. No defaults set.
Automation trigger	Master Step/Step Settings	Reverts to default - Button (manually triggered)
Sample grouping	Queue, Ice Bucket, Placement milestones	Reverts to default - Group by Containers
Well sort order	Queue, Ice Bucket, Record Details milestones	Reverts to default - Row
Sample fields display	Queue, Ice Bucket, Placement, Record Details milestones	No action - the last fields that were configured to display remain there.

For Research Use Only. Not for use in diagnostic procedures.

Property	Configured on Form	What Happens at Step Level
Destination containers	Placement milestone	Reverts to default - uses the Container Type specified in the 'OutputContainerType' Process Type Attribute if set, and Tube otherwise. (If Tube has been deleted from the system, then the first single-well Container Type in the system is used.) Removing the last destination container also removes the ability to set placement on the Master Step (you only have the option to turn on the placement screen if there is at least one multi-well container).
Destination containers on a QC Step	Placement milestone	Reverts to default - No placement
Placement pattern	Placement milestone	Reverts to default - Row
Skip alternating rows, Skip alternating columns.	Placement milestone	Reverts to default - No
Label groups	Add Labels milestone	Reverts to default - First group configured in LIMS (first by creation date, not by name)
Step data heading	Record Details milestone	Reverts to default - Step Data
Default group of defaults	Record Details milestone	Removed. No defaults set.
Step fields display	Record Details milestone	Removed. No defaults set.
Step field order	Record Details milestone	Reverts to default - Vertical
File attachment method	Record Details milestone	Reverts to default - Manual
eSignature	Record Details milestone	Reverts to default - Off
Sample details heading	Record Details milestone	Reverts to default - Sample Table

For Research Use Only. Not for use in diagnostic procedures.

Property	Configured on Form	What Happens at Step Level
Sample display default	Record Details milestone	Reverts to default - Collapse
Enable QC flags	Record Details milestone	Reverts to default - No
File Column Display	Record Details milestone on QC Steps	Reverts to default - Show
File Attachment Method	Record Details milestone on QC Steps	Reverts to default - Manual

For details on configuring step and master step property settings, refer to *Configure Master Steps and Steps* on page 70.

To configure each milestone, milestone, refer to *Configure Step Milestones* on page 79.

Configure Master Steps and Steps

Clarity LIMS includes preconfigured steps and master steps designed to support established lab processes. You can create additional steps and master steps to represent the procedures that are specific to your lab. There are two approaches:

- Create steps based on the preconfigured master steps. The steps you create inherit the properties of the configured master steps, and you can then set additional properties on the steps themselves.
- Create master steps, and then use them as the foundations on which to create your steps.

You can add the steps to protocols and workflows so that lab scientists can work with them in Lab View.

To access the Lab Work tab and configure steps and master steps, the Configuration:update permission is required. By default, only the Administrator role has this permission. For details, refer to *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

View Master Steps and Steps

The Lab Work screen provides an at-a-glance view of all steps and master steps configured in the LIMS, along with the protocols and workflows in which they are included.

1. On the main menu, select Configuration.
2. On the LIMS configuration screen, select the Lab Work tab.
   The Workflow, Protocol, Step, and Master Step navigation panel displays. This lists the workflows, protocols, steps, and master steps configured in the LIMS.
3. In the Master Steps list, select a master step to highlight it:
   - The Steps list updates, highlighting the steps derived from the selected master step.

For Research Use Only. Not for use in diagnostic procedures.

If multiple steps are derived from the same master step, the Master Steps list includes duplicate rows, each mapping to a different step, and each representing the same master step. All of these rows are highlighted.

- The Protocols list updates, highlighting all the protocols that contain the highlighted steps.
- The Workflows list updates, highlighting all workflows that include the highlighted protocols.

4. In the Steps list, select a step to highlight it: The Master Steps list updates, highlighting the master step on which the selected step is based.
   If multiple steps are derived from the same master step, the Master Steps list includes duplicate rows, each mapping to a different step, and each representing the same master step. All of these rows are highlighted.
   - The Protocols list updates, highlighting the protocol that contains the selected step.
   - The Workflows list updates, highlighting all of the workflows that include the highlighted protocols.

   Below the main navigation panel, the step and master step configuration forms display.
5. Select these tabs to switch between the forms and see which settings are configured on the step and which are configured on the underlying master step.

Master Step and Step Configuration Settings

Table 1 shows which settings must be configured on the master step and which may be configured on the master step or on the step.

Settings configured on the master step are locked at the step level. On the step configuration form, these settings display with a Locked icon.

Table 1 Table 1: Master Step and Step Settings

Setting	Configured on	Notes
Step type	Master step	
Output generation	Master step	
Output naming convention	Master step	
Automation	• Automations are enabled on the master step • Automation triggers may be set on master step or step.	
Instrument types	Master step or step	

For Research Use Only. Not for use in diagnostic procedures.

Setting	Configured on	Notes
Control types	Master step or step	
Reagent kits	Master step or step	
Step milestones	Master step or step	Some milestone settings must be configured on the master step.
Label groups	Master step or step	Refer to *Add Labels Milestone* on page 92.
Label uniqueness	Master step	Refer to *Pooling Milestone* on page 88.
Step file placeholders	Master step	Refer to *Record Details Milestone* on page 93.

Add a Master Step

1. On the Lab Work configuration screen, in the upper-right corner of the Master Steps list, select Add.
2. Below the main navigation panel, the master step configuration form displays.
3. To begin, type a name for your new master step.
4. Configure the settings for this master step - refer to *Configure a Master Step* on page 72, below.
5. Select Save to save your master step configuration.

When adding a master step, keep the following in mind:

- Each step is created from a master step. You can create multiple steps from the same master step.
- Any settings you configure on the master step are inherited by all steps derived from that master step.

To understand how properties set on the master step propagate down to the step level, refer to *Rules for Propagation of Master Step Properties* on page 67.

Configure a Master Step

The following sections describe the settings available when configuring a master step. Note the following:

- Any settings saved as part of the master step configuration cannot be configured at step level. On the step configuration form, these settings display with a Locked icon.
- Some settings may be configured at the step level, as indicated in Table 1.
- The master step configuration form does not show the default setting values (this includes toggle switches).

For Research Use Only. Not for use in diagnostic procedures.

Step Type

Step types are configured on master steps.

Steps are categorized by step type, where each type is based on the requirements and goals of the step, and the output generated by the step (derived samples, measurements, or aliquots).

The step type is set on the master step, and all steps inherit the step type of the master step on which they are based. After you have chosen a step type and have saved it as part of a master step configuration, you cannot change it.

- If you are not sure which step type to choose, review *About Step Types and Outputs* on page 62.
- To understand the relationship between master steps and steps, refer to *Overview of Steps and Master Steps* on page 61.

The step type you choose determines which step milestones are available for configuration.

Output Generation

Configured on master step.

A step may generate a derived sample output, a measurement output, an aliquot output, or no output.

The type of step you choose determines which output generation options are available. Usually, you may choose to keep the default setting or modify the output generation configuration.

For details on the output generation options available for each step type, refer to *About Step Types and Outputs* on page 62.

Output Naming Convention

Configured on master step.

By default, the name of the outputs generated by a step follows the naming pattern of the inputs to the step.

You can use tokens to configure the naming convention so that it resolves to other unique attributes of the output. These tokens function as placeholders that are replaced with actual values at run time. For example, for the Standard step type, the default naming convention resolves to the value of the {InputItemName} token.

The following table lists the default naming conventions for each of the step types.

Table 2 Table 2: Default Naming Conventions for Step Types

Step type	Default Naming Convention Token	Naming Convention Preview
Standard	{InputItemName}	Input Sample
Standard QC	{InputItemName}	Input Sample

Step type	Default Naming Convention Token	Naming Convention Preview
Aggregate QC	None - Aggregate QC steps do not produce outputs.	Not applicable
Add Labels	{InputItemName}-{AppliedReagentLabels}	Input Sample-N701-N501 (TAAGGCGA-TAGATCGC)
Pooling	{PoolName}	Pool #1
Analysis	{InputItemName}	Input Sample
Demultiplexing	{InputItemName} (FASTQ reads) {AppliedReagentLabels}	Input Sample (FASTQ reads) N701-N501 (TAAGGCGA-TAGATCGC)

The Tokens list provides a list of tokens you can use to configure the naming convention. For descriptions and examples, refer to *Derived Sample Naming Convention Tokens*.

To add a token:

1. Copy the token you want to use from the Tokens list and paste it into the Naming Convention field. If using multiple tokens, add a space between each entry.
2. Below the Naming Convention field, you can see a preview of how one or more tokens resolve. Some runtime-specific items, such as dates and times, do not preview exactly as they resolve at run time.

Automation

Automations are enabled on master step. Automation triggers may be set on master step or step.

A master step can be configured to update sample fields, assign QC flags, generate files, and submit files and command-line parameters to third-party programs, using automations and the Rapid Scripting API.

When you have configured an automation, you can enable it on one or more master steps and set its trigger location and style.

You can enable automations on master steps in two configuration areas of the LIMS:

- On the Automations tab, when adding/configuring an automation.
- On the master step configuration form.

After it is enabled on a master step, the automation becomes available for use on all steps derived from that master step.

You can set the trigger location and trigger style for an automation on the master step, or on the steps derived from that master step:

For Research Use Only. Not for use in diagnostic procedures.

- On the master step—In this case, all steps derived from the master step inherit the automation and the trigger settings.
- On the steps derived from the master step—In this case, all steps inherit the automation from the master step, but you can configure different trigger settings for each step, if necessary.

To enable an automation on a master step, you must have first configured the automation on the Automation tab. For details, refer to *Add and Configure Automations* on page 135.

To enable an automation on a master step:

1. In the Automation section, click the Automation configuration screen link.
   The Automation configuration screen opens, with the Step Automation tab active.
2. In the Automation Use section, select inside the Enable on the Master Steps field and select the master step on which to enable the automation. (If you make a mistake, select the X button to remove a master step from the field.)
3. Select Save.
4. Return to the master step configuration form. The automations are listed alphanumerically by name.

To set an automation trigger on a master step (or step):

1. In the Trigger Location drop-down list, select the stage of the step at which to enable the automation.
   - The list displays all available stages of the step from which the automation can be triggered.
   - Only valid options for the step are displayed, for example, the Pooling option only displays on Pooling steps, the Step Setup option only displays for steps on which the Step Setup screen is enabled.
   - To ensure sequence of execution, only one automation can be associated with each trigger location.
2. In the Trigger Style drop-down list, select how to initiate the automation. For example, automatically on entry to or exit from the screen or manually when a button is selected on the screen.
   The trigger location and style are saved with the automation configuration.
3. Repeat steps 1 and 2 to configure triggers for each automation added.
4. Save the automation configuration.

Instrument Types

Configured on master step or step

You can specify the instrument/equipment types that may be used in a step. You can do this on the master step or at the step level. At run time, on the Record Details screen, the lab scientist selects from a list of instruments/equipment of that type.

To enable an instrument/equipment type on a master step or step, you must have first added the instrument type to the system. Refer to *Add and Configure Instruments* on page 112.

For Research Use Only. Not for use in diagnostic procedures.

Note also that instrument type/master step configuration is bidirectional - when adding an instrument type, you can select master steps to associate with that instrument type.

To enable an instrument type on a master step (or step):

1. In the Instrument Types section, select Add.
2. At the right of the screen, a list of instrument/equipment types displays. Select one or more instrument/equipment types and select the checkmark button.
   The instrument/equipment types are added to the master step/step configuration.
   - If necessary, you can remove an instrument type by clicking the X button.
   - Step configuration form only: You can reorder instrument types by dragging and dropping them. The order is reflected on the step Record Details screen, in the Instrument selection drop-down list.
3. Save the master step/step.

Reagent Kits

Configured on master step or step

You can specify the reagent kits that may be used in a step. You can do this on the master step or at the step level.

Configuring reagent kits on the step/master step enables reagent lot tracking on the Record Details screen at run time.

To enable a reagent kit on a master step or step, you must have first added the reagent kit to the system. Refer to *Add and Configure Reagent Kits and Lots* on page 118.

Note also that reagent kit/master step configuration is bidirectional—when adding a reagent kit, you can select master steps to associate with that kit.

To enable a reagent kit on a master step (or step):

1. In the Reagent Kits section, select Add.
2. At the right of the screen, a list of reagent kits displays. Select one or more kits and select the checkmark.
   The reagent kits are added to the master step/step configuration.
   If necessary, you can remove a reagent kit by clicking the X button.
3. Save the master step/step.

Control Types

Configured on step

You can specify the control types that may be used in a step. This is done at the step level.

Selected controls are then available to add to the Ice Bucket when running the step.

For Research Use Only. Not for use in diagnostic procedures.

To enable a control type on a step, you must have first added the control type to the system. Refer to *Add and Configure Controls* on page 127.

Note also that control type/step configuration is bidirectional—when adding a control type, you can select the steps to be associated with it.

To enable a control type on a step:

1. In the Control Types section, select Add.
2. At the right of the screen, a list of control types displays. Select one or more control types and select the checkmark.
   The control types are added to the step configuration.
3. Remove a control type by clicking the X button.
4. Save the step.

Step Milestones

Configured on master step or step

When running samples through steps in the LIMS, each screen displayed represents a specific stage, or 'milestone' of the step.

Some screens display on all steps, while others only display on certain step types.

For more on milestones, and instructions on configuring milestone settings, refer to *Configure Step Milestones* on page 79

Add a Step

When adding steps to the LIMS, first select a protocol to include the new step, and a master step on which to base it. The new step inherits all settings configured on the master step.

To add a new step:

1. On the Lab Work configuration screen, in the Protocols list, select the protocol in which to add the new step.
2. In the upper-right corner of the Steps list, select Add.
   Below the main navigation panel, the step configuration form displays.
3. Type a name for the new step.
4. In the adjacent Master Steps list, select the master step upon which to base the new step.
   If creating a step within a QC protocol, the Master Steps list only displays master steps that are Standard QC and Aggregate QC step types.
5. Select Save (this button is not enabled until a master step is selected).
6. In the Protocols list, select the protocol again.
7. The step added displays at the top of the Steps list.

For Research Use Only. Not for use in diagnostic procedures.

- The '1' indicates that this is the first step in the protocol. (QC protocol steps are not numbered as they are typically not sequential.)
- In the Master Steps list, the master step upon which the step is based is also highlighted.

8. Repeat steps 1–5 to add more steps to the protocol.
   - To delete a step, select it and select Delete.
   - To reorder steps within the protocol, drag and drop them.
9. Select Save.
   To drag and drop on a mobile or touch-screen device, touch and hold the item you wish to drag. After a moment, the item appears to lift off the page and its color changes to white. You can then drag the item and drop it into its new position.

You can configure the order in which the protocol steps are run, and the method used to assign and run 'next steps.' Refer to *Configure Protocols* on page 98 and refer to the *Configuring next steps* section.

Configure a Step

On the step configuration form:

- Any settings that were configured on the master step are locked. On the step configuration form, these settings display with a Locked icon.
- You can configure settings that were not configured on the master step. These settings only apply to the step.
- Settings not configured on the master step typically use the default value at the step level, unless those settings are configured on the step.

If not locked on the master step, the following settings can be configured at the step level.

- Automation triggers
- Instrument types
- Reagent kits
- Control types
- Step Milestones

Modify Master Steps and Steps

1. In the Master Steps list, select the master step you would like to modify.
2. Make your changes and select Save.

When modifying master steps and steps, keep the following in mind:

- You can change the master step on which a step is based, providing the new master step is of the same step type. The list of master steps is filtered to show valid options.

For Research Use Only. Not for use in diagnostic procedures.

- If you remove configured settings from a master step, those settings on the derived steps revert to their default values, except if this would leave the step in an unworkable state. For example, you cannot remove the last container from a step. Exceptions to this revert to default rule are noted where applicable.
- If you rename a step, the Recent Activities list in Lab View continues to display the name of the step as it was when the step was run. This is because the step name in this case is derived from the activity record.

Delete Master Steps and Steps

1. In the Master Steps list, select the master step to delete.
2. On the master step configuration form, select Delete.

When deleting master steps and steps, keep the following in mind:

- You cannot delete a step if it is included in an active or archived workflow.
- You cannot delete a master step if it is used to generate a step that is in an active or archived workflow.
- You cannot delete a master step if it has already been used to create one or more steps. First delete the step, and then delete the master step.

Configure Step Milestones

Milestones are the various stages of a step that are presented to lab users as they run samples through steps in Clarity LIMS.

This section explains the relationship between milestones, master steps, and steps; shows how to access milestone configuration settings; and provides an overview of each milestone.

Milestones and Step Types

Some screens (such as the Queue, Ice Bucket, and Record Details screens) display on all steps, while others only display on certain step types.

For example, the Pooling milestone only displays on steps of the Pooling type and the Add Labels screen only displays on steps of the Add Labels type. On all other step types, those milestones are disabled on both the master step and step configuration forms.

The following table shows the milestones that are available for display for each step type. For more information on step types, refer to *About Step Types and Outputs* on page 62.

For Research Use Only. Not for use in diagnostic procedures.

Table 3 Milestones Displayed for Step Types

Step Type	Queue	Ice Bucket	Step Setup*	Pooling	Placement	Add Labels	Record Details
Standard	✓	✓	✓		✓		✓
Standard QC	✓	✓	✓		✓		✓
Aggregate QC	✓	✓	✓				✓
Add Labels	✓	✓	✓		✓	✓	✓
Pooling	✓	✓	✓	✓	✓		✓
Analysis	✓	✓	✓				✓
Demultiplexing	✓	✓	✓				✓

*While the Step Setup screen is available for display on all step types, it is optional and does not display by default. To enable the Step Setup screen, you must first add file placeholders on the master step. For details, refer to the *Step Setup Milestone* on page 86.

Configuring Milestones

You can configure milestone settings on the master step and step configuration forms.

When switching between the step and master step configuration forms while viewing or editing a milestone, you are returned to the parent step/master step form. You need to select the milestone name again to open its settings form.

Similarly, if you wish to return to the step or master step settings form, select the parent master step or step tab.

To configure a milestone:

- Select it to open its settings form.

When configuring milestones on master steps and steps, consider the following details:

- Milestone settings configured on the master step remain locked on all steps derived from the master step. In this scenario, the milestone displays on the step configuration form with a Locked icon, indicating that these settings are not configurable at the step level.
- If you configure a list of items at the master step level—for example, expanded view fields, instrument types, reagent kits—the order in which they are listed on the master step is overwritten by the order set at the step level. Set the order of any list at the step level. This includes the order of the Sample table column headers.

For Research Use Only. Not for use in diagnostic procedures.

- If you remove configured settings from a master step, those settings on the related steps revert to their default values. The exception is if this would leave the step in an unworkable state. For example, you cannot remove the last container from a step. Exceptions to this 'revert to default' rule are noted where applicable.
- Settings configured at the step level only apply to that particular step.

To understand how properties set on the master step propagate down to the step level, refer to the *Rules for Propagation of Master Step Properties* on page 67.

Queue Milestone

When running samples through a step, the first screen that displays is the Queue screen. This screen provides a sample table to select samples to be placed into the Ice Bucket, reserving them for use.

The following components of the Queue Sample table are configurable on the Queue Settings form:

- The Sample table column headers
- The Sample table expanded view fields
- Default grouping and well sort order of Sample table

Configure Sample Table Column Headers

On the Queue Settings form, configure the column headers that display in the Sample table, and the order in which they display.

Note the following:

- No default column headers are configured at the master step level.
- When configuring column headers on a new step, several default column headers will display. You can remove these, but the table must have at least one field remaining (this may be set on either the master step or the step).

Add a Column Header

1. On the Queue Settings form, in the Sample Table section, select Add.
2. At the right of the screen, a list of fields displays, grouped by Measurement, Derived Sample, Submitted Sample, Container, and Project.
   These are the groups of custom fields configured on the Custom Fields > Global Fields configuration screen.
3. Select the arrows to expand the groupings and view the fields within each group.
4. Select one or more fields, and then select the checkmark to add them to the Sample Table area. Select fields individually, Shift + select to select multiple adjacent fields, or Ctrl + select to select multiple nonadjacent fields.

For Research Use Only. Not for use in diagnostic procedures.

As you add column headers, you may notice that the display changes from a horizontal to a vertical layout. This is an indication that you have exceeded the recommended optimum width of the table. You may want to consider removing some fields.

5. Save your changes

> While there is no limit to the number of column headers that can be added to the Sample table, we recommend a maximum of six columns. As more columns are added, each becomes narrower and this can make the heading text difficult to read.

Remove a Column Header

1. Select the X button that displays beneath (or next to, if fields are listed vertically) the column header you want to remove.
2. Save your changes.

Reorder Column Headers

1. Select a column header and then drag it into its new position.
2. Save your changes.

> To drag and drop on a mobile or touch-screen device, touch and hold the item you wish to drag. After a moment, the item will appear to lift off the page and its color will change to white. You can then drag the item and drop it into its new position.

Configure Sample Table Expanded View Fields

Expanded view fields are hidden by default in the Sample table. These fields contain additional details about the samples in the queue. At run time, choose to display these details by clicking the Show/Hide Details button.

On the Queue Settings form, in the Expanded View Fields section, you can select additional fields to add to the body of the Sample table.

Note the following:

- No default expanded view fields are configured at the master step or the step level.
- If expanded view fields are configured at the master step level, they display as locked at the step level and cannot be removed. You can modify the order in which the locked fields display.
- Expanded view fields are available for display in multiple milestone screens. The configuration options set in each milestone are specific to that milestone. You may choose to configure the expanded view fields differently in other milestones.

Add Expanded View Fields

1. In the Expanded View Fields section, select Add.

2. At the right of the screen, a list of fields displays. These are the groups of custom fields configured on the Custom Fields > Global Fields configuration screen. Any fields already included in the Expanded View Fields list do not display in the list.
3. Select the arrows to expand the groupings and view the fields within each group.
4. Select one or more fields, and then select the checkmark to add them to the Expanded View Fields list. Select fields individually, Shift + select to select multiple adjacent fields, or Ctrl + select to select multiple nonadjacent fields.
5. Save your changes.

Remove Expanded View Fields

1. Select the X that displays next to the field you want to remove.
2. Save your changes.

Reorder Expanded View Fields

1. Select a field and then drag it into its new position.
2. Save your changes.

Configure Sample Table Defaults

On the Queue screen, samples are grouped by Container and sorted by well Row by default.

On the Queue Settings form, in the Defaults section, you can modify these settings if necessary.

Set Default Sample Grouping

1. In the Sample Grouping drop-down list, select your preferred default sample grouping option.
2. You can choose to group by:
   - The project (in which samples belong.
   - The container (in which the samples are currently located).
   - The submitted sample (from which the samples originated).
   - The previous step (the samples have undertaken).
3. Save your changes.

Set Well Sort Ordering

1. Select the Well Sort Order toggle switch to set the default well sort ordering to Column (A1, B1, C1, and so on) or Row.
2. Save your changes.

Ice Bucket Milestone

Samples move from the Queue into the Ice Bucket, where they are reserved for use for 30 minutes. The Ice Bucket screen displays for all step types. It comprises a Sample table that displays information about the samples entering the step.

The following components of the Ice Bucket screen are configurable on the Ice BucketSettings form:

- The Sample table column headers
- The Sample table expanded view fields
- Default grouping and well sort order of Sample table

Configure Sample Table Column Headers

On the Ice Bucket Settings form, configure the column headers that display in the Sample table, and the order in which they display.

Note the following:

- No default column headers are configured at the master step level.
- When configuring column headers on a new step, several default column headers will display. You can remove these, but the table must have at least one field remaining (this may be set on either the master step or the step).

Add a Column Header

1. On the Ice Bucket Settings form, in the Sample Table section, select Add.
2. At the right of the screen, a list of fields displays, grouped by Measurement, Derived Sample, Submitted Sample, Container, and Project.
   These are the groups of custom fields configured on the Custom Fields > Global Fields configuration screen.
3. Select the arrows to expand the groupings and view the fields within each group.
4. Select one or more fields and then select the checkmark to add them to the Sample Table area. Select fields individually, Shift + select to select multiple adjacent fields, or Ctrl + select to select multiple nonadjacent fields.
5. As you add column headers, you may notice that the display changes from a horizontal to a vertical layout. This is an indication that you have exceeded the recommended optimum width of the table, and you may want to consider removing some fields.
6. Save your changes.

> While there is no limit to the number of column headers that can be added to the Sample table, we recommend a maximum of six columns. As more columns are added, each becomes narrower and this can make the heading text difficult to read

For Research Use Only. Not for use in diagnostic procedures.

Remove a Column Header

1. Select the X button that displays beneath (or next to, if fields are listed vertically) the column header you want to remove.
2. Save your changes.

Reorder Column Headers

1. Select on a column header and then drag it into its new position.
2. Save your changes.

> To drag and drop on a mobile or touch-screen device, touch and hold the item you wish to drag. After a moment, the item will appear to lift off the page and its color will change to white. You can then drag the item and drop it into its new position.

Configure Sample Table Expanded View Fields

Expanded view fields are hidden by default in the Sample table. These fields contain additional details about the samples in the Ice Bucket. At run time, choose to display these details by clicking the Show/Hide Details button.

On the Ice Bucket Settings form, in the Expanded View Fields section, you can select additional fields to add to the body of the Sample table.

Note the following:

- No default expanded view fields are configured at the master step or the step level.
- If expanded view fields are configured at the master step level, they display as locked at the step level and cannot be removed. However, you can modify the order in which the locked fields display.
- Expanded view fields are available for display in multiple milestone screens. However, the configuration options set in each milestone are specific to that milestone; you may choose to configure the expanded view fields differently in other milestones.

Add Expanded View Fields

1. In the Expanded View section, select Add.
2. At the right of the screen, a list of fields displays. These are the groups of custom fields configured on the Custom Fields > Global Fields configuration screen (see the Adding and Configuring Custom Fields article in the Custom Fields section of the LIMS Documentation).
3. Select the arrows to expand the groupings and view the fields within each group.
4. Select one or more fields and then select the checkmark button to add them to the Expanded View Fields list. You can select fields individually, Shift + select to select multiple adjacent fields, or Ctrl + select to select multiple nonadjacent fields.

For Research Use Only. Not for use in diagnostic procedures.

5. Save your changes.

Remove Expanded View Fields

1. Select the X button that displays next to the field you want to remove.
2. Save your changes.

Reorder Expanded View Fields

1. Select on a field and then drag it into its new position.
2. Save your changes.

Configure Sample Table Defaults

By default in the Ice Bucket screen, samples are grouped by Container and sorted by well Row.

On the Ice BucketSettings form, in the Defaults section, you can modify these settings if necessary.

Set Default Sample Grouping

1. In the Sample Grouping drop-down list, select your preferred default sample grouping option. You can choose to group by:
   - The project (in which samples belong)
   - The container (in which the samples are currently located)
   - The submitted sample (from which the samples originated)
   - The previous step (the samples have undertaken)
2. Save your changes.

Set Well Sort Ordering

1. Select the Well Sort Order toggle switch to set the default well sort ordering to Column (A1, B1, C1, and so on.) or Row.
2. Save your changes.

Step Setup Milestone

The Step Setup screen is an optional screen. By default, it does not display at run time.

This screen lets you provide the lab scientist running the step—and provide Clarity LIMS—with access to files before samples are placed. You can then configure step automations that parse these files and use the information to place samples into destination containers, based on the result file specifications.

If you enable the display of the Step Setup screen (you can enable it on any step type), it displays immediately after the Ice Bucket screen.

The Step Setup Settings screen allows you to do the following:

For Research Use Only. Not for use in diagnostic procedures.

- Add file placeholders that will be populated at run time. Configure these on the master step.
- After you have added file placeholders, you can then enable the display of the Step Setup Settings screen at run time. You can configure this on the master step or the step. However, as with all master step settings, if you enable the screen on the master step, it displays on all steps derived from that master step.
- Configure the attachment method for each file added—manual or automatic. You may configure this on the master step or the step.

To enable the Step Setup screen, you must first configure one or more file placeholders on the master step.

Add a File Placeholder

1. On the Lab Work tab, in the Master Steps list, select the master step on which you would like to configure the file placeholders.
2. Select the Step Setup milestone.
3. In the File Placeholders section, select Add.
4. Type a name for the file placeholder.
5. [Optional] You can copy and paste tokens from theTokens list into the name field. For details, refer to *Derived Sample Naming Convention Tokens*.
6. Enter instructional text.

Set the Attachment Method

To set the attachment method, select the Attachment toggle switch to set the file attachment method.

If you set the attachment method to Auto, configure a step automation to generate and attach the file. For details, refer to *Add and Configure Automations* on page 135.

Remove a File Placeholder

To remove a file placeholder, select the X button.

Enable the Step Setup Screen

1. On the Lab Work tab, in the Master Steps or Steps list, select the master step or step on which you would like to configure Step Setup file placeholders.
2. Select the Step Setup milestone.
3. At the top of the Step Setup Settings screen, select the toggle switch to enable the Step Setup screen. The screen now displays at run time.

When the Step Setup screen is enabled, it becomes available for selection as an automation trigger location. If you configure an automation trigger location on the Step Setup screen, the Step Setup screen cannot be disabled.

For Research Use Only. Not for use in diagnostic procedures.

Pooling Milestone

When you create a step and choose the Pooling step type, the Pooling milestone is enabled. When running the step, the Pooling screen allows the lab scientist to create pools of samples.

The following components of the Pooling screen are configurable on the Pooling Settings form.

- Enable and disable label uniqueness to control whether samples with the same labels, or no labels, may be pooled together. This must be configured on the master step.
- Configure defaults for sample grouping and well sort order. You can configure these settings at the master step or step level.

Configure Label Uniqueness

1. Select the Label Uniqueness toggle switch to turn label uniqueness on and off.
   - When Label Uniqueness is On (default setting), samples with the same labels cannot be pooled together.
   - When Label Uniqueness is Off, samples with the same label or no labels may be pooled together.
2. Save your changes.

Configure Pooling Screen Defaults

On the Pooling screen, by default samples are:

- Grouped by Container
- Sorted by well Row (A1, A2, A3, and so on)
- Placed by Column (A1, B1, C1, and so on)

You can modify these settings if necessary.

Set Default Sample Grouping

1. In the Sample Grouping drop-down list, select your preferred default sample grouping option. You can choose to group by:
   - The project (in which samples belong)
   - The container (in which the samples are currently located)
2. Save your changes.

Set Well Sort Ordering

1. Select the Well Sort Order toggle switch to set the default well sort ordering to Column (A1, B1, C1, and so on) or Row (A1, A2, A3, and so on).

2. Save your changes.

Placement Milestone

The Placement screen is used for QC steps and for steps that generate derived samples. When the screen displays at run time, it allows manual placement of samples into the destination container.

Note the following:

- In tube-only workflows, the Placement screen is disabled by default and samples are automatically placed. This is true for all step types, except Add Labels steps, in which a tube rack Placement screen displays to allow for manual placement of samples.
- In the following step types, no sample placement occurs. The Placement screen is disabled and it does not display at run time. Analysis steps
  - Aggregate QC steps
  - Standard steps where derived sample generation is set to None.

The Placement Settings form allows for the following configuration.

- Turn off the Placement screen and have samples placed automatically into corresponding wells of the destination container (source and destination containers must be the same).
- Disable the Placement screen so that it does not display at run time and cannot be viewed. You can only do this on QC steps where no sample placement is required—ie, where samples remain in the same container throughout the step. The step cannot have destination containers configured.
- Configure the destination containers that are permitted on the step.
- Configure the sample placement defaults—grouping, well sort order, placement pattern, and whether to skip alternate rows/columns in the container.

Configure Display of the Placement Screen

When the Placement Screen toggle switch is enabled, the Placement screen displays at run time. The lab scientist manually places samples into the destination container.

To turn off the Placement screen:

- Select the toggle switch to turn off the Placement Screen and enable autoplacement of samples.
- At run time, bypass the Placement screen. If necessary, the user can return to the screen (by selecting its tab) to view placement details.

When the Placement Screen is disabled, the milestone label changes to Auto-Placement. However, if the source and destination containers are not of the same type, Clarity LIMS determines that autoplacement cannot occur and reenables manual placement so that samples can be placed.

For Research Use Only. Not for use in diagnostic procedures.

Configure Destination Containers

Destination containers are the containers into which samples are placed at run time. These containers display to the user in a drop-down list on the Ice Bucket screen. The selected container is then used to set up the subsequent Placement screen.

Before You Begin

When creating a step that supports placement, keep the following details in mind:

- By default, any destination containers configured on the master step are added to the step.
- If the master step does not have a destination container set, and the step is not a QC step, then the Tube container type is added by default. If no such container type exists, the first 'tube-like' (eg., single well) container, and that failing, the first container type available, is associated to the step.
- Destination containers configured at the master step level display as locked at the step level - you cannot remove them from the step. However, you can modify the order in which the locked containers display in the drop-down list.

Also note the following:

- Destination containers configured at the master step level display as locked and cannot be removed at the step level. However, you can modify the order in which the locked containers display in the drop-down list.
- To add destination containers to a step, you must have first configured those containers on the Containers configuration screen. Refer to *Add and Configure Containers* on page 131.
- You can add, reorder, and remove containers freely, but you must choose at least one container if your step type requires placement (either via autoplacement or via manual placement during run time).
- If the container is a tube or other single well container that is treated like a tube, an Autoplace label displays on the container, to inform you that the Placement screen does not display at run time. This behavior is controlled by a toggle switch that displays on the Containers configuration screen when configuring single-well containers. (The exception to this is for Add Labels steps, which display a tube rack Placement screen for placing samples into tube-like containers.)

Add a Destination Container

1. In the Destination Containers section, select Add.
2. At the right of the screen, a list of container types displays. These are the containers configured on the Containers configuration screen.

For Research Use Only. Not for use in diagnostic procedures.

3. Select one or more containers and then select the checkmark button to add them to the Destination Containers list. You can select containers individually, Shift + select to select multiple adjacent fields, or Ctrl + select to select multiple nonadjacent fields.
4. Save your changes.

To add destination containers to a step, you must have first configured those containers on the Containers configuration screen. Refer to *Add and Configure Containers* on page 131.

Remove a Destination Container

1. Select the X button that displays next to the container you want to remove. (you cannot remove the last container from a step.)
2. Save your changes.

Reorder Destination Containers

1. Select a container and then drag it into its new position.
2. Save your changes.

To drag and drop on a mobile or touch-screen device, touch and hold the item you wish to drag. After a moment, the item appears to lift off the page and its color changes to white. You can then drag the item and drop it into its new position.

Configure Placement Screen Defaults

On the Placement screen, by default samples are:

- Grouped by Container
- Sorted by well Row (A1, A2, A3, and so on).
- Placed by Column
- Placed into all container wells - no rows or columns are skipped.

You can modify these settings if necessary.

Set Default Sample Grouping

1. In the Sample Grouping drop-down list, select your preferred default sample grouping option. You can choose to group by:
   - The project (in which samples belong)
   - The container (in which the samples are currently located)
2. Save your changes.

For Research Use Only. Not for use in diagnostic procedures.

Set Well Sort Ordering

1. Select the Well Sort Order toggle switch to set the default well sort ordering to Column (A1, B1, C1, and so on) or Row (A1, A2, A3, and so on).
   The well sort ordering configured here is also applied to the Add Labels screen.
2. Save your changes.

Set the Placement Pattern

1. Select the Placement Pattern toggle switch to set the default placement pattern to either Column, Row, or Same Shape.
2. Save your changes.

Skip Alternating Rows/Columns

1. Select the Skip Alternating Rows or Skip Alternating Columns toggle switch to skip alternate rows or columns in the destination container when samples are placed.
2. Save your changes.

Add Labels Milestone

When you create a step and choose the Add Labels step type, the Add Labels milestone is enabled. When running the step, the Add Labels screen allows the lab scientist to add a reagent label (also known as index or molecular barcode) to each sample.

Note the following:

- To add a label group to a step, you must have first configured the label group on the Consumables > Labels configuration screen. Refer to *Add and Configure Labels and Label Groups* on page 122.
- When you create an Add Labels step, the first label group configured in the system is added to the step automatically.
- There must be at least one label group defined on either the master step or the step.
  - You cannot remove the last label group from the step/master step.
  - You cannot remove label groups added on the master step from the step.
- Label groups are listed in alphanumeric order. The order is not modifiable.
- The well sorting setting configured on the *Placement Milestone* on page 89 is also applied to the Add Labels screen.

Label groups are the only configurable components on the Add Labels Settings form.

Add a Label Group

1. On the Add Labels Settings form, in the Label Groups section, select Add.

2. At the right of the screen, the Label Groups list displays.
   These are the label groups configured on the Consumables > Labels configuration screen (refer to *Add and Configure Labels and Label Groups* on page 122).
3. Select one or more label groups and then select the checkmark to add them to the Label Groups area. Select groups individually, Shift + select to select multiple adjacent fields, or Ctrl + select to select multiple nonadjacent groups.
   The selected label groups are added to the list.
4. Save your changes.

Delete a Label Group

1. To remove a label group, select its X button.

Remember that there must be at least one label group defined on either the master step or the step.

You cannot remove the last label group from the step/master step - the X button does not display.

Record Details Milestone

The Record Details screen is where data are tracked on the step at run time. It includes information about the step, files generated by or uploaded to the step, e-Signature sign-off (if enabled), and information about the samples in the step.

The following components of the Record Details screen are configurable on the Record Details Settings form:

- The step-level information (step data) tracked on the step. You can also change the heading of the step data section, and set a default value for the Group of Defaults configured on the master step.
- Step file placeholders for files that is attached to the step at run time, and their attachment method.
- The sample-level information tracked and displayed in the Sample table
- Electronic signatures - this panel only displays if you have enabled the clarity.eSignature.enabled property.

Configure Step Data

The Step Data section of the Record Details screen allows you to track and display step-level data at run time, specifically the master step fields associated with the step.

On the Record Details Settings form, you can configure the following:

- The heading that displays at the top of the section.
- The default value for the Group of Defaults that displays in the upper-right corner of the screen.
- The step data fields that display, and the order and layout in which they display.
  Note the following:
  - The default heading is 'Step Data Table'.

For Research Use Only. Not for use in diagnostic procedures.

- You are not required to set a default value for the Group of Defaults.
- You are not required to add master step fields or multiline text fields.
- When step fields and/or multiline text fields are added, they are arranged vertically by default.
- As you configure the step data, the Preview area on the right updates to show you how the configuration displays at run time on the Record Details screen.

Multiline text fields are much wider than step fields and always display below them on the Record Details screen. For this reason, they are configured separately.

- Groups of defaults and master step fields are defined on the Custom Fields > Master Step Fields configuration screen. For details, refer to *Add and Configure Custom Fields* on page 146.

Change the Step Data Heading

1. In the Step Data Heading field, type your preferred heading.
2. Save your changes.

Select a Default Group of Defaults

1. Expand the Group of Defaults drop-down list and select the group of defaults you would like to use.
2. Save your changes.

Select the Master Step Fields to Display

1. In the Master Step Fields section, select Add.
2. At the right of the screen, the step fields that are configured on the master step are listed.
3. Select a field and then select the checkmark button to add it to the Display Step Fields list. Select fields individually, Shift + select to select multiple adjacent fields, or Ctrl + select to select multiple nonadjacent fields. After you have added a field, it is removed from the list on the right.
4. If necessary, you can reorder fields by clicking and dragging them into position.
   On the right, the preview area updates to show you how the fields display at run time.
5. Save your changes.

Select the Multiline Text Fields to Display

1. In the Multiline Text Fields section, select Add.
2. At the right of the screen, any multiline fields that are configured on the master step are listed.
3. Select a field and then select the checkmark button to add it to the Multiline Text Fields list. Select fields individually, Shift + select to select multiple adjacent fields, or Ctrl + select to select multiple nonadjacent fields. After you have added a field, it is removed from the list on the right.
4. If necessary, reorder fields by clicking and dragging them into position. On the right, the preview area updates to show you how the fields display at run time.

For Research Use Only. Not for use in diagnostic procedures.

5. Save your changes.

Set Field Order

1. Select the Field Order toggle switch to determine whether step fields are arranged horizontally or vertically, and the tab order of the fields. Multiline fields are not included in the field order and always display below the step field columns.
   The preview area updates to show you how the fields display at run time.
2. Save your changes.

Configure Step File Placeholders

Configuring file placeholders allows you to attach sample measurement files to a step at run time. For example, you may want to attach an instrument input files or sample sheets, a QC measurement file, a log file, run report, or lab tracking form. Files may be manually uploaded or automatically generated and attached using a script. The default attachment method is manual attachment.

Note the following:

- Configure step file placeholders on the master step. You cannot configure or modify these at the step level. A lock icon on the Step Settings form indicates this.
- Create a placeholder for each file to be attached.
- Configure the attachment method—Manual or Auto, at the master step or the step level. If the attachment method is set on the master step, it cannot be changed at the step level (lock icon displays on the Step Settings form).
- The default attachment method is Auto.
- In the Sample Table section, if the File Column Display is set to Hide, the Attachment toggle switch is set to Auto and is disabled. To manually attach files in the Sample table, the column must be visible.
- The attachment method applies to the shared sample measurement files generated. If you need to set the attachment method for individual files generated for each sample, you can use the API to do this. For more information, refer to the *API & Database* documentation.

Add a Step File Placeholder

1. On the Lab Work tab, in the Master Steps list, select the master step on which you would like to configure file placeholders.
2. Select the Record Details milestone.
3. In the Step File Placeholders section, select Add.
4. Type a name for the file placeholder. You can copy and paste tokens into the name, if necessary. For details, refer to *Derived Sample Naming Convention Tokens*.

For Research Use Only. Not for use in diagnostic procedures.

Set the Attachment Method

1. On the Master Step Settings form or Step Settings form, select the Attachment toggle switch to determine whether files are to be attached manually or automatically by a script.
2. Save your changes.

Configure the Sample Table

At the bottom of the Record Details form, the Sample Table section lets you view and track data on your samples at run time.

On the Record Details Settings screen, you can configure the following components of the Record Details screen Sample table:

- The table heading. (Default table heading is 'Sample Table'.)
- The display of the QC flags field (when this field is enabled, mark samples with a QC pass or fail flag.
- The default display of the Sample table listing. The default view is Collapsed - for faster loading time of the sample list.
- The table columns that display in the Sample table, and the order in which they display.
  - The File Options Column and the File Attachment Method toggle switch only display on the Record Details Settings screen on steps that generate measurements. These settings allow you to choose if you want to display a column for sample files and choose how these files are attached to the step (manually or automatically).

Note the following:

- You can enable QC flags on any step type that allows you to mark a sample with a pass or fail flag.
- By default, QC flags are enabled on Standard QC steps. This setting is locked and cannot be changed.
- By default, QC flags are disabled on Analysis steps. This setting is locked and cannot be changed.
- Enable QC flags on a No Outputs step to use the step for QC aggregation.
- Sample groupings are collapsed by default to optimize screen loading time, but can also be expanded by default.
- If the step generates measurements, Sample File Options display. These allow you to choose if you want to view a column for Sample Files and choose how these files are attached (manually or automatically).
- When configuring the Sample table:
  - No default column headers are configured at the master step level.

For Research Use Only. Not for use in diagnostic procedures.

- When configuring column headers on a new step, several default column headers display. You can remove these; however, the table must have at least one field remaining (this may be set on either the master step or the step).
- The Sample table displays in multiple milestone screens. However, the configuration options set in each milestone are specific to that milestone; you may choose to configure other milestone Sample tables differently. The unique aspect of the Record Details Sample table is that the derived sample and submitted sample fields can be written to (according to their respective step type).

Change the Sample Table Heading

1. In the Table Heading field, type your preferred heading.
2. Save your changes.

Enable/Disable QC Flags

1. Select the Enable QC Flags toggle switch to enable or disable the QC column in the Sample table.
   - When enabled, the QC column displays and must be written to - each sample must be assigned either a QC pass or QC fail flag.
   - When disabled, the QC column does not display.
2. Save your changes.

Set the Default Display for the Sample Table Fields

1. Select the Sample Display Default toggle switch to set the default sample display to Expand or Collapse.
2. Save your changes.

Add Sample Table Columns

1. In the Table Columns section, select Add.
2. At the right of the screen, a list of fields displays, grouped by Measurement, Derived Sample, Submitted Sample, Container, and Project.
   These are the groups of custom fields configured on the Custom Fields > Global Fields configuration screen.
3. Select the arrows to expand the groupings and view the fields within each group.
4. Select one or more fields and then select the checkmark button to add them to the Table Columns area. Select fields individually, Shift + select to select multiple adjacent fields, or Ctrl + select to select multiple nonadjacent fields.
5. As you add column headers, you may notice that the display changes from a horizontal to a vertical layout. This is an indication that you have exceeded the recommended optimum width of the table, and you may want to consider removing some fields.

For Research Use Only. Not for use in diagnostic procedures.

6. Save your changes.

While there is no limit to the number of column headers that can be added to the Sample table, we recommend a maximum of six columns. As more columns are added, each becomes narrower and this can make the heading text difficult to read.

Remove a Column Header

1. Select the X button that displays beneath (or next to, if fields are listed vertically) the column header you want to remove.
2. Save your changes.

Reorder Column Headers

1. Select on a column header and then drag it into its new position.
2. Save your changes.

To drag and drop on a mobile or touch-screen device, touch and hold the item you wish to drag. After a moment, the item appears to lift off the page and its color changes to white. You can then drag the item and drop it into its new position.

Configure eSignatures

The eSignatures Review configuration panel displays on the Record Details Settings screen only if the clarity.eSignature.enabled property is enabled. For details on setting this property, refer to *Configure Electronic Signatures* on page 180.

If the panel is enabled, you can configure electronic signatures (e-signatures) on a step or master step. This means that samples in the step cannot move forward (Next Steps button is disabled) until an e-signature has been entered with the appropriate role-based permission.

As with all other step settings, if you enable e-signatures on a master step, the setting displays with a Locked icon and is enabled on all steps derived from that master step.

Configure Protocols

Clarity LIMS includes preconfigured protocols, each containing a series of steps through which a sample must pass. You can create custom protocols, adding steps that represent the steps that are run in your lab. You can then add the protocols to workflows so that lab users can work with them in Lab View.

Use the Lab Work configuration screen to view, add, and configure the protocols used in the lab. For an overview of this screen, refer to *Lab Work Overview* on page 51.

To access the Lab Work tab and configure protocols, the Configuration:update permission is required. By default, only the Administrator role has this permission. For details, refer to *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

View Protocols

1. On the main menu, select Configuration.
2. Select the Lab Work tab.
   The Workflows, Protocols, Steps, and Master Steps navigation panel displays.
3. In the Protocols list, select a protocol to highlight it:
   - The Workflows list updates, highlighting the workflows that contain the selected protocol.
   - The Steps list updates, highlighting the steps included in the selected protocol.
   - The Master Steps list updates, highlighting the master steps on which the highlighted steps are based.
4. Below the main navigation panel, review the protocol configuration form.
   This displays the name of the protocol and its settings.

Protocol Settings

The Protocol Settings area captures important information about the protocol—the date it was created, the date it was last modified, and other settings that determine how the protocol is used in the lab. The following table summarizes these settings.

Setting	Configuration options	What it means in the lab
QC Protocol?	QC protocols comprise a series of QC steps.	All steps share queue of samples. Samples do not move sequentially from step to step. Instead, they appear available/unavailable for a particular step based on configured filtering criteria.
	Non-QC protocols typically comprise a series of non-QC steps. However, you can include a QC step as part of a Non-QC protocol.	Each step has its own queue of samples. Samples move sequentially through the steps, until they have completed all steps in the protocol.
Protocol Type	Sample Prep Library Prep Sequencing Data Analysis Sample Analysis Other	See Non-QC protocol information in previous row.

For Research Use Only. Not for use in diagnostic procedures.

Setting	Configuration options	What it means in the lab
Show in Lab View?	No	These protocols are hidden for both lab scientists and administrators in Lab View and are therefore not available for use in the lab. These protocols are only visible to administrative users in the configuration area.
	Yes	These protocols are displayed in Lab View and can be used by lab scientists to perform their work in the lab.
Capacity	The sample capacity of the protocol. This depends on the number of lab scientists in your facility, and the number of samples they can work with at any given time.	The Capacity setting controls the highlighting on the Overview and Projects dashboards, allowing you to see at a glance which protocols are approaching or exceeding sample capacity.

Add Protocols

When adding and configuring protocols, note the following details:

- When adding steps to a protocol, reordering steps, or removing steps from a protocol, changes are autosaved. You do not need to select Save after every modification.
- When configuring next steps, you must select Save to save your changes.

To add a protocol:

1. On the Lab Work configuration screen, in the upper-right corner of the Protocols list, select Add. Below the main navigation panel, the protocol configuration form displays.
2. To begin, type a name for the new protocol.
3. Select the settings for this protocol (for details, refer to Protocol settings):
    - Select whether this is a QC or Non-QC protocol.
    - Select the Protocol Type:

    a. If you are adding a QC protocol, this automatically is set to QC.

    b. If you are adding a Non-QC protocol, select the type from the drop-down list.

    c. In the Capacity field, enter the sample capacity of this protocol.
4. [Optional] To temporarily hide the protocol from Lab View, use the Show in Lab View? slider. Change the setting to No.

For Research Use Only. Not for use in diagnostic procedures.

5. Select Save. The new protocol displays at the bottom of the Protocols list. You can move it to a different position in the list by dragging and dropping.
   To drag and drop on a mobile or touch-screen device, touch and hold the item you wish to drag. After a moment, the item appears to lift off the page and its color changes to white. You can then drag the item and drop it into its new position.

You can also copy a protocol and then modify the copy for use in other workflows. Refer to *Copy Protocols* on page 109.

Add Steps to Protocols

This section provides an overview of the step creation process. For detailed information on steps and master steps, and step-by-step instructions for configuring them, refer to *Configure Master Steps and Steps* on page 70.

To add a step to a protocol:

1. In the Protocols list, select the protocol.
2. In the upper-right corner of the Steps list, select Add.
   Below the main navigation panel, the step configuration form displays.
3. Type a name for the new step.
4. In the adjacent Master Step list, select the master step upon which to base the new step.
5. Select Save (this button is not enabled until you have selected a master step).
6. In the Protocols list, select the protocol again.
   - The step you added displays at the top of the Step list.
   - If this is a non-QC protocol, a 1 is in front of the step name, indicating that this is the first step in the protocol.(QC steps are not numbered as they are typically not sequential.)
   - In the Master Step list, the master step upon which the step is based is also highlighted.
7. Repeat steps 1–5 to add more steps to the protocol.
   - To delete a step, select it and select the Delete.
   - To reorder steps within the protocol, simply drag and drop them.

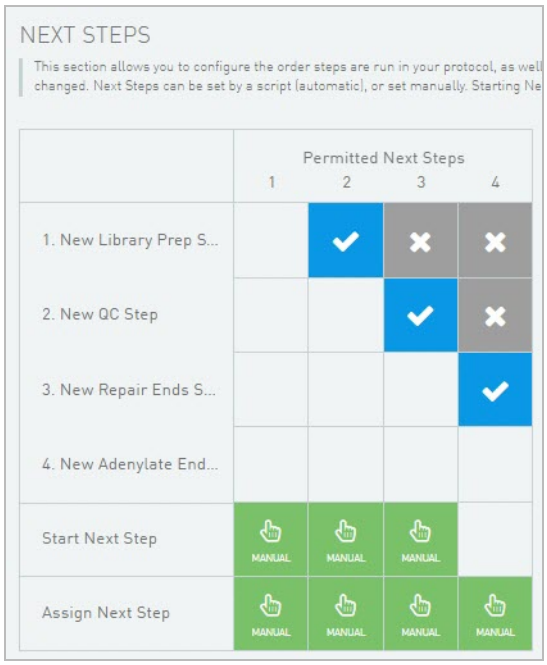
   To drag and drop on a mobile or touch-screen device, touch and hold the item you wish to drag. After a moment, the item appears to lift off the page and its color changes to white. You can then drag the item and drop it into its new position.
8. Select Save.

You can now configure the order in which the steps are run, and the method used to assign and run 'next steps.' Refer to Configure next steps.

For Research Use Only. Not for use in diagnostic procedures.

Configure Next Steps

When configuring non-QC protocols, the protocol configuration form includes a Next Steps table. This allows you to configure the sequence in which steps are run in the protocol. This table does not display for QC protocols, because the steps in a QC protocol are typically not sequential.



In the table:

- Each row represents a numbered step in the protocol.
- Each column represents a 'permitted next step' for each of the numbered steps.
- The cells at each row/column intersection indicate which steps are potential permitted next steps for the step represented in that row.
  - If there is an icon in the cell (an X or a checkmark), the step represented by that column may be selected or deselected as a permitted next step.
  - Previous and current steps cannot be selected as permitted next steps, and are shown as nonselectable cells.
- The bottom two rows determine whether the next steps are started and assigned manually or automatically. Manual is the default setting.

To configure next steps

1. In the Next Steps table, select a cell to select (or deselect) one or more permitted next steps.
2. In the Start Next Step and Assign Next Step rows, select a cell to switch between Manual and Automatic.

For Research Use Only. Not for use in diagnostic procedures.

To assign a next step automatically, you also need to configure an automation and add it to the step. For details, refer to *Add and Configure Automations* on page 135.

Configure QC Filters

When configuring QC protocols, the protocol configuration form includes a QC Filters section. This section lets you configure QC logic to make sure that only certain samples are queued for each QC step. Typically, QC protocols contain multiple nonsequential steps that culminate in a QC aggregation step.

QC filters are composed of two drop-down lists.

The first list refers to the QC flag assigned at run time:

- Passed means that a pass QC flag was assigned to the sample at run time.
- Failed means that a fail QC flag was assigned to the sample at run time.
- Did not pass means that the sample did not run, or received a fail QC flag, at run time.
- Did not fail means that the sample did not run, or received a pass QC flag, at run time.

The second list refers to the master steps from which the steps are derived:

- All master steps used in the protocol are included in the list. Together, these form a statement (for example, Failed Bioanalyzer).
- Each statement may be followed by an'AND', which allows you to create an additive statement.
- Statements are separated by an'OR', which allows you to create mutually exclusive statements.
- Together, these AND/OR statements create the QC filter logic for a given step.

For example:

You may want the NanoDrop QC queue to show samples that have not passed NanoDrop QC (ie, they did not run, or received a fail QC flag), and that have passedBioanalyzer QC.

- If the procedures dictate that all samples must have passed Bioanalyzer QC and NanoDrop QC, use an 'AND' statement to ensure samples are not queued for a QC aggregation step unless they have passed both of these steps.
- If your lab procedures dictate that all samples must have passed Bioanalyzer QC or NanoDrop QC, use an 'OR' statement to ensure samples are not queued for QC aggregation unless they have passed one of these steps.

Modify Protocols

You may want to rename a protocol, or add or reorder steps. Some modifications are only permitted if the protocol is not included in an active or archived workflow.

We recommend that you do not modify or delete the preconfigured protocols without first consulting the Clarity LIMS Support team.

To modify a protocol:

1. In the Protocols list, select the protocol.
2. Make your changes and select Save.

Note the following details:

- You can rename protocols in pending, active, and archived workflows.
- For non-QC protocols, you can modify the protocol type. For example, you can change a Sample Prep protocol to a Library Prep protocol.
- You can choose to hide or show the protocol in Lab View.
- You cannot change a QC protocol to a non-QC protocol, and vice versa.
- You cannot add, reorder, or delete steps if the protocol is included in an active or archived workflow.

Delete Protocols

To delete a protocol:

1. In the Protocols list, select the protocol.
2. On the protocol configuration form, select Delete.

Note the following details:

- You cannot delete a protocol if it is included in an active or archived workflow. In this case, the Delete button is not enabled.
- If you delete a protocol, the steps it contains, and the master steps on which those steps were based are not deleted.

Configure Workflows

After protocols are created and configured, add them to workflows that represent how samples move through your lab.

In Clarity LIMS, use the Lab Work configuration screen to view, add, and configure the workflows used in the lab. For an overview of this screen, refer to *Lab Work Overview* on page 51.

To access the Lab Work tab and configure workflows, the Configuration:update permission is required. By default, only the Administrator role has this permission. For details, refer to *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

View Workflows

The Lab Work screen provides an at-a-glance view of all workflows configured in the LIMS, along with the protocols and steps they contain. You can quickly see which workflows are active, which are archived, and which do not yet have protocols assigned to them.

To view workflow details:

1. On the main menu, select Configuration.
2. Select the Lab Work tab.
   The Workflows, Protocols, Steps, and Master Steps navigation panel displays. This presents alphabetically sorted lists of all workflows, protocols, steps, and master steps configured in the LIMS.
3. In the Workflows list, select a workflow to highlight it.
   - The Protocols list updates to show all protocols included in the workflow. These are highlighted and displayed sequentially at the top of the list. A dashed line separates these workflow protocols from the comprehensive list of all protocols in the system.
   - The Steps list updates, highlighting the steps included in the highlighted protocols.
   - The Master Steps list updates, highlighting the master steps on which the highlighted steps are based.

   You can also select a protocol, step, or master step to view the related workflows.
4. Below the main navigation panel, review the workflow configuration form. This displays the name of the workflow and its status.

The following table provides an overview of each status setting and describes the implications of each.

For Research Use Only. Not for use in diagnostic procedures.

Status	What It Means in the Lab	Configuration Implications
Active	• These workflows are currently in use - or available for use - in the system. • Samples can be assigned to these workflows so that lab scientists can work on them in Lab View.	• Active workflow cannot be modified or deleted. • Protocols in an Active workflow cannot be reordered. • Protocols in an Active workflow can be modified or deleted, and modify their steps. • Active workflow can be made unavailable for use by changing its status to Archived. Samples that are currently queued or in progress for the workflow can complete it, but new samples cannot be added. • When a workflow in Active state is saved, it can only transition to the Archived state.
Pending	• These workflows have not yet been activated. • These workflows are not available for use in the lab. • These workflows do not display in Lab View. • Samples cannot be added to these workflows from the Projects and Samples screen.	• Pending workflows can be modified, for example, by renaming them, or by adding, modifying, or removing, modifying protocols. • Pending workflows can be activated.

For Research Use Only. Not for use in diagnostic procedures.

Status	What It Means in the Lab	Configuration Implications
Archived	• These workflows are currently not in use in the system. • These workflows do not display in Lab View. • Samples cannot be added to these workflows from the Projects and Samples screen. • Samples that are currently queued or in progress for an Archived workflow can complete it.	• After a workflow is saved in Archived state, it can only transition to the Active state. • An Archived workflow cannot be modified or deleted. • In an Archived workflow, protocols cannot be reordered.

Add Workflows

The following section shows how to add a workflow to the LIMS and add protocols to it. When configuring workflows, keep the following in mind:

- You are not required to add protocols immediately. If you prefer, you can create empty Pending workflows and assign protocols to them later.
- You can only activate a Pending workflow if it contains at least one protocol.
- When adding protocols to a workflow, reordering protocols within a workflow, or removing protocols from a workflow, your changes are autosaved. You do not have to select Save after every modification.
- You cannot add empty protocols to a workflow. The protocol must include steps.

To add a new workflow:

1. On the Lab Work configuration screen, in the upper-right corner of the Workflow list, select Add.
2. Below the main navigation panel, the workflow configuration form displays.
3. To begin, type a name for your new workflow.
4. Select Save.
   The workflow is saved in a Pending state, and displays in the Workflow list of the main navigation panel.

To add protocols to a workflow:

1. In the Workflow list, select the workflow.

For Research Use Only. Not for use in diagnostic procedures.

2. In the Protocol list, locate the first protocol to include and select Add.

The protocol is added to the workflow and displays at the top of the Protocol list. The 1 indicates that this is the first protocol in the workflow.

3. Repeat step 2 until you have added all required protocols to the workflow.
   - To remove a protocol from the workflow, select its Remove button.
   - Drag and drop to reorder protocols within the workflow.
     - To drag and drop on a mobile or touch-screen device, touch and hold the item you wish to drag. After a moment, the item appears to lift off the page and its color changes to white. You can then drag the item and drop it into its new position.
   - To view or modify a protocol, select the protocol to display its configuration form below the main navigation pane.
4. You can now save the workflow as a Pending workflow.
   - or -
   Select Activate to use this workflow immediately.

   After you activate a workflow, you cannot modify or delete it.

Modify and Activate Pending Workflows

1. On the Lab Work configuration screen, in the Workflow list, select the Pending workflow to modify or activate.
2. Make your changes and select Save to save the workflow as a Pending workflow.
   -or-
   Select Activate to change the workflow status to Active and begin using the workflow.

When modifying or activating workflows, keep the following in mind:

- You cannot activate empty workflows.
- You can only modify a workflow while it remains in the Pending state. That is:
  - You cannot add a protocol to an Active or Archived workflow.
  - You cannot remove a protocol from an Active or Archived workflow.
  - You cannot rename or reorder protocols in an Active or Archived workflow.
  - You cannot delete protocols included in Active or Archived workflows.

Archive and Reactivate Workflows

While you cannot delete workflows after they have been activated, you can archive them. This makes them temporarily unavailable for use in the lab. You can reactivate an Archived workflow at any time.

To archive a workflow:

1. On the Lab Work configuration screen, in the Workflow list, select the Active workflow to archive.

For Research Use Only. Not for use in diagnostic procedures.

2. In the Workflow Settings area, select Archive. Select Save.

To reactivate an archived workflow:

1. On the Lab Work configuration screen, in the Workflow list, select the Archived workflow to reactivate.
2. In the Workflow Settings area, select Activate. Select Save.

Delete Workflows

1. On the Lab Work configuration screen, in the Workflow list, select the pending workflow to delete.
2. On the workflow configuration form, select Delete.
3. Confirm the workflow deletion:
   - To proceed with the deletion, select Delete.
   - To cancel the deletion, select Cancel.

You can only delete a workflow while the workflow remains in the Pending state. You cannot delete Active or Archived workflows.

Copy Protocols

After you have added and configured a protocol, you can copy it and then modify the copy for use in other workflows. This is useful if you have multiple protocols with similar base configuration, as it saves you having to recreate each one from scratch.

To access the Lab Work tab and configure protocols, the Configuration:update permission is required. By default, only the Administrator role has this permission. For details, refer to *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

When you copy a protocol, all of its steps are also copied—along with any step-level fields, automations, reagents, controls, and instruments configured on those steps.

You can also create copies of the master steps, or you can reuse the same master steps.

- Copying master steps does copy step-level fields.
- Reusing master steps does not copy step-level fields.
- If a copied master step has custom field default values that refer to other steps within the protocol, update those values to refer to the copied steps. Refer to *Update Custom Field Defaults on Copied Master Steps* on page 110.

Copy a Protocol and Its Steps

1. On the main menu, select Configuration.
2. On the LIMS configuration screen, select the Lab Work tab.
3. In the main navigation panel, in the Protocols list, select the protocol to copy.

4. Below the navigation panel, select Copy.
5. The Copy Protocol Options dialog opens. This dialog provides two options:
   - Append name with—This option lets you specify text to be appended to the protocol name (default is _copy). This text also is appended to the copied step names, and to the master step names if you also choose to copy those. Note: Copied step-level field names do not have the text appended.
   - Copy Master Steps?—This option lets you choose to reuse the same master steps (this is the default behavior), or create copies of the master steps.
   - Selected an option and then select Continue to copy the protocol and steps.
6. The copied protocol displays in the Protocols list, and is selected along with its related steps and master steps.
   Below the navigation panel, the protocol configuration form displays. You can work with the protocol and its steps just as you would with any other protocol/steps in the system.

Update Custom Field Defaults on Copied Master Steps

If you have configured a custom field default on the master step you are copying, and the default value refers to the name of another step within the protocol, you must update that default value on the copied master step, so that it refers to the appropriate step in the copied protocol. The default values are not automatically updated to refer to the copied step names.

Similarly, if you have configured a script or logic that uses custom field defaults that refer to another step within the protocol, you must update those default values on the copied master step.

For example, in a QC protocol:

- The Aggregate QC step has various 'Copy Task' UDFs defined - eg, Copy Task 1 - Source Step and Copy Task 2 - Source Step.
- The values of these fields are determined by other QC steps within the protocol.
- The script that is configured on the QC Aggregate step references those QC step names, locates the specified custom field values from the steps, and uses them to determine QC results.

If the QC protocol is copied, the copy of the master step on which the Aggregate QC step is based must be updated so that the custom field default values refer to the appropriate steps within the protocol.

Consumables

Consumables are the instruments, reagents, containers, and other equipment used in the lab. Configure these items in Clarity LIMS and associate them with specific master steps. When the steps are run in the LIMS, the consumables used are recorded.

For Research Use Only. Not for use in diagnostic procedures.

The Instruments Configuration Screen

Add the instruments and equipment used in your lab to Local Analysis Software, and associate these items with specific steps. When running steps in the LIMS, lab scientists can record the instruments and equipment used.

All users logged into the LIMS can access the Instruments configuration screen. However, what they are allowed to do in this screen is determined by their user permissions.

By default, only the Administrator role has the Configuration:update permission. For more on user roles and permissions, see *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

ClarityLogin Permission Access

- View instrument types, but not add, edit, or delete them.
- Add new instruments to existing instrument types.
- Edit and delete instruments.
- Reactivate archived / expired instruments.

Configuration:update Permission Access

All actions from ClarityLogin permission access, plus:

- Add instrument types.
- Edit and delete instrument types.

Access the Instruments Configuration Screen and View Existing Instruments

1. On the main menu, select Configuration.
2. On the LIMS configuration screen, select the Consumables tab, and then select Instruments.
3. All configured instrument types and instruments are listed in the Instrument Types area on the left.
   - Active instruments are grouped by instrument type and have ther software name and version displayed. Select the arrows to expand and collapse the groups.
   - Archived instruments display in a separate group at the bottom of the list.

   For more on active and archived instruments, refer to *Instrument Status* on page 114.
4. Select an instrument or instrument type to view its details on the right.

The Instruments Configuration Screen

Add the instruments and equipment used in your lab to Local Analysis Software, and associate these items with specific steps. When running steps in the LIMS, lab scientists can record the instruments and equipment used.

All users logged into the LIMS can access the Instruments configuration screen. However, what they are allowed to do in this screen is determined by their user permissions.

By default, only the Administrator role has the Configuration:update permission. For more on user roles and permissions, see *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

ClarityLogin Permission Access

- View instrument types, but not add, edit, or delete them.
- Add new instruments to existing instrument types.
- Edit and delete instruments.
- Reactivate archived / expired instruments.

Configuration:update Permission Access

All actions from ClarityLogin permission access, plus:

- Add instrument types.
- Edit and delete instrument types.

Access the Instruments Configuration Screen and View Existing Instruments

1. On the main menu, select Configuration.
2. On the LIMS configuration screen, select the Consumables tab, and then select Instruments.
3. All configured instrument types and instruments are listed in the Instrument Types area on the left.
   - Active instruments are grouped by instrument type and have ther software name and version displayed. Select the arrows to expand and collapse the groups.
   - Archived instruments display in a separate group at the bottom of the list.

   For more on active and archived instruments, refer to *Instrument Status* on page 114.
4. Select an instrument or instrument type to view its details on the right.

Add and Configure Instruments

This section describes how to add and configure the instruments and equipment used in your lab, and associate these items with master steps.

When adding instruments to Clarity LIMS, there are two main steps involved:

1. Add a new instrument type (Configuration:update permission required).
2. Select an instrument type and then add a new instrument of that type. You cannot add an instrument without first selecting an instrument type.

When initially setting up the system, add all the instrument types used in the lab. For example, HiSeq 3000, 2100 Bioanalyzer, NanoDrop 2000. Any logged in user can then add specific instruments to each type.

Add a New Instrument Type

1. On the main menu, select Configuration.
2. On the configuration screen, select the Consumables tab, then select Instruments.
3. On the Instruments configuration screen, select New Instrument Type.
4. In the Instrument Type Details area, complete the following required information:
   - Enter the name of the type of instrument or equipment you are adding.
   - In the Vendor drop-down list, select an existing vendor from the list, or select Create new and type the new vendor name into the field. After you create a vendor, it is added to the list and can then be selected when creating other instrument types.
   - In the Instrument Type Use area, select inside the Enable on the Master Steps field.
   - In the drop-down list that displays, select one or more master steps on which to enable this instrument type.
   - To remove a step from this field, select the X to the left of the step name.

   The instrument type is made available for use on all steps that are created from the selected master steps. When running those steps in the LIMS, the appropriate instrument can be selected from the Record Details screen. This configuration is bidirectional - when configuring a master step, you can select instrument types to associate with that master step.
5. Select Save.
   The new instrument type displays in the Instrument Types area. The ' zero instruments ' label indicates that no instruments of this type have yet been added.

Add a New Instrument

1. On the Instruments configuration screen, in the Instrument Types area, select the appropriate instrument type.
2. Select New Instrument.
3. In the Instrument Details area, enter the details for this instrument.
   - Instrument Name: Enter the name of the instrument. (This is the only required field.)
   - Serial number: Enter the serial number of the instrument, or other instrument-specific information.
   - Expires: Select the expiry date (or calibration date) of the instrument or equipment.

   Valid dates are the current date or any date in the future.
   After an instrument has been saved, a label displays next to this field. The label shows the number of days, and then hours, remaining before the instrument expires, or warns that the instrument has expired.
   The LIMS automatically archives the instrument when the expiry date is reached (refer to *Instrument Status* on page 114).

For Research Use Only. Not for use in diagnostic procedures.

- Software Name: Enter the name of the instrument software.
- Software Version: Enter the instrument software version number.

4. Select Save.
   In the Instrument Types area, the new instrument is nested under its instrument type.
5. To create another instrument of the same type, select Add Another New Instrument.
   When creating instruments, note the following:
   - A LIMS ID is automatically assigned to the instrument.
   - The instrument record Created date is automatically populated.
   - The instrument record Modified date is automatically populated; this field keeps track of any changes made to the instrument details.
   - By default, the instrument status is set to Active. Refer to *Reactivate an Archived Instrument* on page 116.

Instrument Status

The instrument Status toggles between Active and Archived. By default, when adding a new instrument, its status is Active.

Active instruments:

- These instruments are in use, or available for use, in your lab workflows; they can be selected by lab users as they record work for a protocol step.
- Users may edit the details of Active instruments.

Archived instruments:

- These instruments are not currently in use in lab workflows (for example, they may be expired or under repair), and are not available for selection by lab users working in the LIMS.
- When the expiry date for an instrument has passed, the LIMS automatically archives the instrument.
- The details of Archived instruments are read-only. They may be viewed, but not edited.
- Archived instruments are listed together in a single Archived Instruments group (no subgrouping by type), at the bottom of the Instrument Types area. If an archived instrument is reactivated, it once again displays under its respective instrument type.

Edit Instrument Types and Instruments

When editing instrument types and instruments, keep the following in mind:

- Only users with the Configuration:update permission type can edit instrument types.
- Changes made to an instrument type, or to any instruments of that type, are reflected on all future steps on which the instrument type is enabled.

- Steps that have already been run are not affected by changes made to instrument types or instruments.

Edit an Instrument Type

1. On the Instruments configuration screen, in the Instrument Types area, select an instrument type. The Instrument Type Details area displays the details for the selected instrument type.
2. Edit the details as required.
3. Select Save.

Edit an Instrument

1. On the Instruments configuration screen, in the Instrument Types area, expand the instrument type group that contains the instrument to be edited.
2. Select the instrument.
3. The Instrument Details area displays the details for the selected instrument. Edit the details as required.
4. Select Save.

Delete Instrument Types and Instruments

When deleting instrument types and instruments, keep the following details in mind:

- To delete instrument types, the Configuration:update permission is required.
- When deleting an instrument type, all instruments of that type are also deleted and are no longer available for selection on steps.
- You cannot delete an instrument type if any instruments of that type are in use.
- You cannot delete an instrument if that instrument has been used in a step.

Delete an Instrument Type

1. On the Instruments configuration screen, in the Instrument Types area, select the instrument type to delete.
2. Select Delete.
3. Confirm the deletion.

Delete an Instrument

1. On the Instruments configuration screen, in the Instrument Types area, expand the instrument type group that contains the instrument to be deleted.
2. Select the instrument to delete.
   The instrument details display on the right.

For Research Use Only. Not for use in diagnostic procedures.

3. Select Delete.
4. Confirm the deletion. The instrument is deleted and is no longer available for selection on steps.

Reactivate an Archived Instrument

1. In the Instrument Types area, expand the Archived Instruments section and select the instrument to reactivate.
2. If the instrument has not expired, select Activate.
3. If the instrument has expired, reset the expiry date to a date in the future, and then select Activate.
4. Select Save.
   In the Instrument Types area, the reactivated instrument displays under its instrument type. The instrument may now be selected when running steps.

The Reagents Configuration Screen

Add the reagent kits and lots used in the lab to Clarity LIMS and enable them for use on specific steps. When lab scientists run samples through a step, they can record the reagent lots used.

All users logged into Clarity LIMS can access the Reagents configuration screen. However, their user permissions determine what they are allowed to do in this screen.

By default, only the Administrator role has the Configuration:update permission. For more on user roles and permissions, see *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

ClarityLogin Permission Access

- View reagent kits but not add, edit, or delete them (all fields are read-only and New Reagent Kit, Delete, Cancel, and Save buttons do not display).
- View the details of a reagent kit, including the steps on which it is enabled.
- Add new reagent lots to existing kits.
- Edit reagent lot details.
- Archive and reactivate reagent lots.
- Delete reagents.

Configuration:update Permission Access

All actions listed in ClarityLogin, plus:

- Add new reagent kits.
- Edit reagent kit details.
- Archive and reactivate reagent kits.
- Delete reagent kits.

Access the Reagents Configuration Screen & View Existing Reagent Kits and Lots

1. On the main menu, select Configuration.
2. On the configuration screen, select the Consumables tab and then select Reagents.
   All reagent kits configured in the system are listed in the Reagent Kits list on the left.
   - Active kits are listed alphabetically.
   - Archived kits display in a separate group at the bottom of the list.

   For more on active and archived kits, refer to *Reagent Kit and Lot Status* on page 119.
3. Hover over On <n> steps to view the steps that have been configured to record lot numbers for each reagent kit.
4. Select an arrow to expand a reagent kit and view the related lot details, expiry dates, and status.
5. Select a reagent kit to view details.

The Reagents Configuration Screen

Add the reagent kits and lots used in the lab to Clarity LIMS and enable them for use on specific steps. When lab scientists run samples through a step, they can record the reagent lots used.

All users logged into Clarity LIMS can access the Reagents configuration screen. However, their user permissions determine what they are allowed to do in this screen.

By default, only the Administrator role has the Configuration:update permission. For more on user roles and permissions, see *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

ClarityLogin Permission Access

- View reagent kits but not add, edit, or delete them (all fields are read-only and New Reagent Kit, Delete, Cancel, and Save buttons do not display).
- View the details of a reagent kit, including the steps on which it is enabled.
- Add new reagent lots to existing kits.
- Edit reagent lot details.
- Archive and reactivate reagent lots.
- Delete reagents.

Configuration:update Permission Access

All actions listed in ClarityLogin, plus:

- Add new reagent kits.
- Edit reagent kit details.
- Archive and reactivate reagent kits.

- Delete reagent kits.

Access the Reagents Configuration Screen & View Existing Reagent Kits and Lots

1. On the main menu, select Configuration.
2. On the configuration screen, select the Consumables tab and then select Reagents.
   All reagent kits configured in the system are listed in the Reagent Kits list on the left.
   - Active kits are listed alphabetically.
   - Archived kits display in a separate group at the bottom of the list.

   For more on active and archived kits, refer to *Reagent Kit and Lot Status* on page 119.
3. Hover over On <n> steps to view the steps that have been configured to record lot numbers for each reagent kit.
4. Select an arrow to expand a reagent kit and view the related lot details, expiry dates, and status.
5. Select a reagent kit to view details.

Add and Configure Reagent Kits and Lots

This section describes how to add and configure the reagent kits and lots used in your lab, and enable them for use on specific master steps.

Enabling kits on steps makes them available for use in the lab. When running those steps, the reagent lots used are recorded

When a new reagent kit is added, it is not a requirement to enable it on a step. It can be enabled at any time.

Reagent kit/step configuration is bidirectional. Enable a reagent kit on a step in the following situations:

- When adding reagents on the Reagents configuration screen (described in this section).
- When configuring a master step or step. For details, refer to *Configure Master Steps and Steps* on page 70.

The Configuration:update permission is required to add new reagent kits to Clarity LIMS.

Add a New Reagent Kit

1. On the main menu, select Configuration.
2. On the configuration screen, select the Consumables tab, then select Reagents.
3. On the Reagents configuration screen, select New Reagent Kit.
4. Type a name for the reagent kit. This name displays in queues of steps on which use of the reagent kit is enabled.
5. Enter details for the reagent kit to help with future reordering:
   - Supplier: Enter the commercial vendor name.

- Cat. #: Enter the catalog number.
- Website. Enter the website of the commercial vendor. When viewing details for the reagent kit, select the link to open the web page in a new browser window.
- In the Reagent Kit Use section, the status of the new kit is set to Active. This status means that it is available to be used in the lab (after it is enabled on steps).

6. Select Save to add the new reagent kit.
   The new kit displays in the Reagent Kits list.

Enable a Reagent Kit on a Step

1. On the Reagents configuration screen, in the Reagent Kits list, select the kit to enable on steps.
2. In the Reagent Kit Use area on the right, compete the following actions:
   - Select a protocol from the drop-down list. Type the first few letters of the protocol to filter the list.
   - In the adjacent list, select the step on which to enable the reagent kit.
   - Enable the control on additional steps, if necessary.
3. Select Save.
   The Reagent Kits list now indicates that the kit has been enabled on the selected steps.

Add a Reagent Lot

1. On the Reagents configuration screen in the Reagent Kits list, select the kit for which you would like to add a new lot.
2. Below the Kit Details in the Lots area, select New Lot.
3. In the Lot Details area, enter the lot name.
4. [Optional] Enter additional details about the lot, such as the lot number and expiry date.
   - Specify a storage location and add notes about the reagent lot. For example, use this field to note why a lot is being archived).
   - Clarity LIMS automatically populates the LIMS ID and Created and Modified dates.
5. Select Save.
   The new lot displays in the Reagent Kits list.

By default, when a new lot is added, the status is Pending. The Status of Reagent Lot slider at the bottom of the Lot Details area controls the lot status.

Reagent Kit and Lot Status

The status of a reagent kit may be Active or Archived. The status of a reagent lot may be Pending, Active, or Archived.

For Research Use Only. Not for use in diagnostic procedures.

Note the following details about reagent kit status:

- Active reagent kits are in use, or are available for use, in the lab workflows. By default, when a new kit is added, the status is saved as Active.
- Archived reagent kits are kits that are not currently in use, or available for use, in the lab workflows. Configuration details for archived kits are saved, so reactivation is easy.

Archived kits are listed at the bottom of the main Reagent Kits list in the Archived Reagent Kits group.

Note the following details about reagent lot status:

- Active reagent lots are in use, or are available for use, in the lab. Select the active reagent lots as they record work for a step.
- Pending reagent lots have been ordered but not yet received in the lab. They are not available for selection by lab users running steps in Clarity LIMS. By default, when a new lot is added, the status is saved as Pending.
- Archived reagent lots have typically expired or been used up. They are not available for selection by lab users. Note the following information:
  - When the expiry date for a lot has passed, Clarity LIMS automatically archives the lot.
  - Archived lots that have passed their expiry date cannot be reactivated.
  - Archived lots display in an Archived Reagent Lots group within the Reagent Kit details list.

Activate and Archive Reagent Kits and Lots

Archive or Reactivate a Reagent Kit

1. In the Reagent Kits list, select the kit to be archived or reactivated.
2. In the Reagent Kit Use area on the right, select Archived / Active.
3. Select Save.

Activate or Archive a Reagent Lot

1. In the Reagent Kits list, select the kit containing the lot to be activated or archived.
2. At the bottom of the Lot Details area on the Status of Reagent Lot slider, select Active / Archived.
3. Select Save.

Delete Reagent Kits and Lots

1. In the Reagent Kits list, select the reagent kit or lot to delete.
2. In the Kit Details/Lot Details area on the right, select Delete.

When deleting reagent kits and lots, keep the following in mind:

- Only reagent kits and lots that have not been used in a step can be deleted.

- If a kit or lot has been recorded in a step, or is being used in a step, it cannot be deleted. The Delete button is not enabled.

The Labels Configuration Screen

Add a label group for each reagent category used in your lab, and then add labels to the groups. Each label represents a reagent type (or molecular barcode) within the group/category.

Select the label groups to be used in the step when configuring the properties of steps generated from an Add Labels master step type.

To access the Labels configuration screen, the Configuration:update permission is required. Users who do not have this permission do not see the Labels option displayed under the Consumables tab.

By default, only the Administrator role has the Configuration:update permission. For more on user roles and permissions, see *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

Configuration:update Permission Access

- View existing label groups and labels and their details.
- Add new label groups and labels.
- Edit and delete label groups.
- Edit and delete labels.

Access the Labels Configuration Screen and View Label Groups

1. On the main menu, select Configuration.
2. On the LIMS configuration screen, select the Consumables tab, and then select Labels.
3. All label groups configured in the system are listed alphabetically in the Label Groups area on the left.
    - Each label group corresponds to a reagent category that exists in the system.
    - Each label group displays a count of the labels (reagent types) present in that particular group.
    - Select a label group to view its details on the right.

The Labels Configuration Screen

Add a label group for each reagent category used in your lab, and then add labels to the groups. Each label represents a reagent type (or molecular barcode) within the group/category.

Select the label groups to be used in the step when configuring the properties of steps generated from an Add Labels master step type.

To access the Labels configuration screen, the Configuration:update permission is required. Users who do not have this permission do not see the Labels option displayed under the Consumables tab.

By default, only the Administrator role has the Configuration:update permission. For more on user roles and permissions, see *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

Configuration:update Permission Access

- View existing label groups and labels and their details.
- Add new label groups and labels.
- Edit and delete label groups.
- Edit and delete labels.

Access the Labels Configuration Screen and View Label Groups

1. On the main menu, select Configuration.
2. On the LIMS configuration screen, select the Consumables tab, and then select Labels.
3. All label groups configured in the system are listed alphabetically in the Label Groups area on the left.
   - Each label group corresponds to a reagent category that exists in the system.
   - Each label group displays a count of the labels (reagent types) present in that particular group.
   - Select a label group to view its details on the right.

Add and Configure Labels and Label Groups

This section describes how to add and configure label groups (reagent categories) and labels (reagent types or molecular barcodes), and enable them for use on specific master steps.

Add Label Groups and Labels

When adding label groups and labels to the LIMS, there are several main steps involved:

1. Add a new label group.
2. Then, to add labels to the group:
   - Download a template label list (Microsoft® Excel® file) from the Labels configuration screen.
   - Add reagent type details to the downloaded template.
   - Upload the completed label list.

Add a New Label Group

1. On the main menu, select Configuration.
2. On the configuration screen, select the Consumables tab and then select Labels.
3. On the Labels configuration screen, select New Label Group.
4. In the Label Group Details area, enter the name of the label group you are adding.

- Numeric names are not permitted.
- Duplicate names are not permitted.
- You may use the name of a previously deleted label group.

5. Select Save.
   - The new label group is listed in the Label Groups list. Because there are no labels in the group, no count displays.
   - The Upload Label List and Download Label List buttons display in the Label Group Details area.

Add Labels to a Label Group

1. On the Labels configuration screen, in the Label Groups list, select the label group to which you want to add labels.
2. In the Label Group Details area, select Download Label List to download the template.
3. Open the template in Excel. It has two example label entries containing the following information:
   - Group Name (column A): Prepopulated with the name of the label group you selected in the LIMS.
   - Label ID (column B): No information is provided in this column as it is populated by the LIMS.
   - Label Name (column C): Provides examples of label name (reagent type) formats.
   - Sequence (column D): Provides examples of sequence properties of theIndex special type of the reagent type. Dual-indexes may be used, separated by a hyphen.
4. To complete your label list, add new rows between the <LABEL ENTRIES> opening and </LABEL ENTRIES> closing tags and enter reagent label information into these rows:
   - Group Name: (Required on upload) Enter the name of the label group (reagent category) into which you are adding labels.
   - Label ID: Leave this column empty. It is populated by the LIMS when you upload your completed label list.
   - Label Name: (Required on upload) Enter the names of the reagent labels (reagent types) you would like to add to the LIMS, using one of the example formats.
   - Sequence: (Optional on upload) Enter the index sequence of the Index special type of the reagent type, for example, "ATCACG." You may enter dual-indexes, separated by a hyphen.
5. Save your label list file.
   - Return to the Labels configuration screen, select Upload Label List and upload your completed labels list. If there are errors in the list, the upload does not complete. Refer to *Label List Upload Error Conditions* on page 125.
   - In the Label Groups list, the label count shows the number of labels in the group.

For Research Use Only. Not for use in diagnostic procedures.

Edit and Delete Label Groups

When editing/deleting label groups, keep the following in mind:

- The only item you can change directly in the LIMS is the label group name.
- To make changes to the labels within the group, you must upload a modified label list. See *Edit and Delete Labels* on page 124.
- Deleting a label group does not affect historical run data. This information is preserved in the LIMS.

Edit a Label Group

1. On the Labels configuration screen, in the Label Groups list, select the label group you would like to edit.
2. Select inside the Name field and enter the new name.
3. Select Save.

Delete a Label Group

1. On the Labels configuration screen, in the Label Groups list, select the label group you would like to delete.
2. In the Label Group Details area, select Delete.
3. Confirm the deletion.

Edit and Delete Labels

When editing and deleting labels (reagent types), keep the following in mind:

- Changes you make to a label are reflected on all future steps on which the label is applied.
- Steps that have already been run are not affected by changes you make to labels. The labels are mapped to samples in the run and historical run data are preserved.

Edit Labels

1. On the Labels configuration screen, in the Label Groups list, select the label group containing the labels you would like to edit.
2. Download the existing label list from the Labels configuration screen.
3. Edit the downloaded label list. Note the following:
   - If adding new labels to the label group, the modified label list must also include the rows for the existing labels.
   - If modifying existing labels, the modified label list must also include the rows for labels that you are not modifying.
   - If you omit rows from the label list, these labels are deleted.

- Upload the modified label list. Refer to *Label List Upload Error Conditions* on page 125.

Delete Labels

1. On the Labels configuration screen, in the Label Groups list, select the label group containing the labels you would like to delete.
2. Download the existing label list from the Labels configuration screen.
3. Edit the downloaded label list, removing the rows containing the labels you would like to delete.
4. Upload the modified label list. Refer to *Label List Upload Error Conditions* on page 125.

Label List Upload Error Conditions

When uploading a label list, the following conditions result in an error:

- One or more of the four headers (Group Name, Label ID, Label Name, Sequence) is missing or misspelled.
- Attempting to rename a label to the same name as an existing label within any label group.
- Attempting to rename a label to the same name as an existing label—even if you are also renaming the other label at the same time.
- Adding a label with the same name as another label within any label group.
- Attempting to edit a label without providing the Label ID.
- Providing labels for the wrong group. That is, the Group Name column does not match the name of the label group into which you are uploading labels.
- Providing a sequence for a reagent that does not have the 'Index' special type.

The Controls Configuration Screen

Controls behave like special samples that can be enabled at specific points in your workflows. However, unlike samples, controls do not need to belong to a project and do not have to be assigned to a workflow.

Add the control samples used in the lab to Clarity LIMS, and enable them for use on steps. When running a step on which control samples are enabled, the lab scientist can add those control samples to the Ice Bucket.

All users logged into the LIMS can access the Controls configuration screen. However, their user permissions determine what they are allowed to do in this screen.

By default, only the Administrator role has the Configuration:update permission. For more on user roles and permissions, see *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

ClarityLogin Permission Access

- View the list of controls but not add, edit, or delete them (all fields are read-only and New Control, Delete, Cancel, and Save buttons do not display).
- View the details of a control, including the steps on which it is enabled.

Configuration:update Permission Access

All actions listed in ClarityLogin, plus:

- Add new controls
- Modify controls
- Delete controls

Access the Controls Screen and View Controls

1. On the main menu, select Configuration.
2. On the configuration screen, select the Consumables tab and then select Controls.
3. In the Control Samples area on the left:
   - Active control samples are listed alphabetically. These controls are in use, or are available for use, in the lab.
   - Archived control samples are listed in a separate group at the bottom of the list. These controls are not currently available for use in the lab.
   - For both active and archived controls, the number of steps on which a control is enabled is displayed. Hover over the label to see a list of the steps and the protocols that include those steps.
4. Select a control sample to view its details on the right.

The Controls Configuration Screen

Controls behave like special samples that can be enabled at specific points in your workflows. However, unlike samples, controls do not need to belong to a project and do not have to be assigned to a workflow.

Add the control samples used in the lab to Clarity LIMS, and enable them for use on steps. When running a step on which control samples are enabled, the lab scientist can add those control samples to the Ice Bucket.

All users logged into the LIMS can access the Controls configuration screen. However, their user permissions determine what they are allowed to do in this screen.

By default, only the Administrator role has the Configuration:update permission. For more on user roles and permissions, see *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

ClarityLogin Permission Access

- View the list of controls but not add, edit, or delete them (all fields are read-only and New Control, Delete, Cancel, and Save buttons do not display).
- View the details of a control, including the steps on which it is enabled.

Configuration:update Permission Access

All actions listed in ClarityLogin, plus:

- Add new controls
- Modify controls
- Delete controls

Access the Controls Screen and View Controls

1. On the main menu, select Configuration.
2. On the configuration screen, select the Consumables tab and then select Controls.
3. In the Control Samples area on the left:
   - Active control samples are listed alphabetically. These controls are in use, or are available for use, in the lab.
   - Archived control samples are listed in a separate group at the bottom of the list. These controls are not currently available for use in the lab.
   - For both active and archived controls, the number of steps on which a control is enabled is displayed. Hover over the label to see a list of the steps and the protocols that include those steps.
4. Select a control sample to view its details on the right.

Add and Configure Controls

This section describes how to add and configure the control samples used in the lab and enable them for use on specific master steps.

There is no limit to the number of controls you can create or the number of steps on which you can enable a control. When adding a new control, you are not required to enable it on a step. You can do this action at any time.

Control sample/step configuration is bidirectional. Enable a control sample on a step in the following situations:

- When adding control samples on the Controls configuration screen (described in this section).
- When configuring a step (refer to *Configure Master Steps and Steps* on page 70).

Add a New Control

1. On the main menu, select Configuration.
2. On the configuration screen, select the Consumables tab, then select Controls.
3. On the Controls configuration screen, select New Control.
4. Type a name for the control sample. This name displays in queues of steps on which controls are enabled. This field is the only required field.
5. [Optional] Enter additional details for the control sample:
   - Supplier—Enter the commercial vendor name. If this control sample was made in the lab, enter in-house.
   - Cat. #—Enter the catalog number.
   - Website—Enter the website of the commercial vendor. If it is an in-house control, enter the URL of the internal web page that contains details of the in-house control. When viewing details for the control sample, lab scientists can select the link to open the web page in a new browser window.
6. In the Control Use section, note the following defaults:
   - The status of the new control is set to Active.
   - The new control is not flagged as a single step only control.
7. Select Save.
   The new control displays in the Control Samples list.

Enable a Control on a Step

Enabling controls on steps makes them available for use in the lab.

To enable a control sample on a step, complete the following steps:

1. On the Controls configuration screen in the Control Samples list, select the control to enable on steps.
2. In the Control Use area, select the protocol that includes the step on which you want to enable the control. Type the first few letters of the protocol to filter the list.
3. In the adjacent list, select the step on which you want to enable the control.
4. Enable the control on additional steps, if necessary.
5. Select Save.
   The Control Samples list now indicates that the control has been enabled on a step. Hovering over the On 1 step label displays a popup that shows the protocol and step involved.

Control Status

The status of a control may be Active or Archived.

For Research Use Only. Not for use in diagnostic procedures.

- Active controls are controls that are in use or available for use in the lab workflows.
- Archived controls are controls that are not currently available for use in the lab workflows.
  - Lab users do not see archived controls when initiating steps.
  - Configuration details for archived controls are saved, so it is easy to reactivate them.

In the Control Samples list, archived controls are listed in their own group. Select the arrow to expand the list and view control details.

Single Step Only Controls

Single step only controls do not progress in workflows. When completing a step, lab users do not need to select a Next Step for these controls.

Use this option to represent single-use, disposable samples such as QC standards, molecular weight ladders, and blanks.

Archive and Reactivate Controls

Archive a Control

1. In the Control Samples list, select the control to archive.
2. On the Status of Control slider, select Archived.
3. Select Save.

Reactivate an Archived Control

1. In the Control Samples list, expand the archived control group and select the control to be activated.
2. On the Status of Control slider, select Active.
3. Select Save.

Delete Controls

When deleting controls, keep the following details in mind:

- You can only delete control samples that have not been used in a step.
- If a control sample has been recorded in a step, or is currently being used in a step, you cannot delete it. The Delete button is not enabled.

To delete a control:

1. On the Controls configuration screen in the Control Samples list, select the control to delete.
2. In the Control Sample Details area on the right, select Delete.

The Containers Configuration Screen

Clarity LIMS is a container-based system requiring that samples reside in a container at every step of a workflow. Add the types of containers used in your lab to Local Analysis Software and enable them for use on specific steps.

When running a step in the LIMS, the lab scientist scans in the container barcode and proceeds to the Ice Bucket screen. In the Ice Bucket, the output container types that can be used in the step are listed.

To access the Containers configuration screen, the Configuration:update permission is required. Users who do not have this permission do not see the Containers option displayed under the Consumables tab.

By default, only the Administrator role has the Configuration:update permission. For more on user roles and permissions, see *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

Configuration:update Permission Access

- View existing container types and their details (number of rows and columns, numeric/alphabetic naming, unavailable wells.)
- Edit the details of container types.
- Delete container types.
- Add new container types.

Access the Containers Configuration Screen and View Containers

1. On the main menu, select Configuration.
2. On the configuration screen, select the Consumables tab, then select Containers.
   All containers configured in the system are listed alphabetically in the Containers area on the left.
3. Select a container to view its details on the right.

The Containers Configuration Screen

Clarity LIMS is a container-based system requiring that samples reside in a container at every step of a workflow. Add the types of containers used in your lab to Local Analysis Software and enable them for use on specific steps.

When running a step in the LIMS, the lab scientist scans in the container barcode and proceeds to the Ice Bucket screen. In the Ice Bucket, the output container types that can be used in the step are listed.

To access the Containers configuration screen, the Configuration:update permission is required. Users who do not have this permission do not see the Containers option displayed under the Consumables tab.

By default, only the Administrator role has the Configuration:update permission. For more on user roles and permissions, see *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

For Research Use Only. Not for use in diagnostic procedures.

Configuration:update Permission Access

- View existing container types and their details (number of rows and columns, numeric/alphabetic naming, unavailable wells.)
- Edit the details of container types.
- Delete container types.
- Add new container types.

Access the Containers Configuration Screen and View Containers

1. On the main menu, select Configuration.
2. On the configuration screen, select the Consumables tab, then select Containers.
   All containers configured in the system are listed alphabetically in the Containers area on the left.
3. Select a container to view its details on the right.

Add and Configure Containers

This section describes how to add and configure the containers used in your lab, and enable them for use on specific master steps.

When adding a new container to the LIMS, you are adding a container type (ie, a tube, a 96 well plate, a flow cell). When the container barcode is scanned, an instance of that container type is added.

Add a Container Type

1. On the main menu, select Configuration.
2. On the configuration screen, select the Consumables tab, then select Containers.
3. On the Containers configuration screen, select New Container.
4. In the Container Details area, enter the name of the container type you are adding. This is the only required field. When you have entered a name, the Save button becomes available.
5. [Optional] Specify the details of the rows and columns in the container:
   - In the Number fields, enter the number of rows and columns in the container.
   - Use the Naming toggle to specify whether the rows and columns have Alphabetic or Numeric labels.
   - For numeric rows and columns, use the Start at field to specify the number at which the row/column labels start.
6. [Optional] If you enter 1 in both row and column Number fields, an additional Yes/No toggle setting displays, asking Do you want to skip the placement screen?
   - Yes—The LIMS does not display the placement screen when the step is run. It automatically places the samples into the container.

For Research Use Only. Not for use in diagnostic procedures.

- No—The placement screen displays samples that need to be manually placed into the single well.

7. [Optional] List any unavailable wells (ie, wells in which samples must not be placed). Specify these in a comma-separated format, for example, A:1, A:2, A:3, A:4.
   Note the following:
   - If you switch between Numeric and Alphabetic rows/columns, the list of unavailable wells updates to reflect the change.
   - If you change the Start at number for numeric rows/columns, the list of unavailable wells updates to reflect the change.
   - If you specify an invalid unavailable well, or change the dimensions of the container such that one or more of the specified unavailable wells becomes invalid, the List unavailable wells field turns red.
   - The Save button is only available when all specified unavailable wells are valid.
8. Select Save.

Specify Unavailable Wells

To prevent lab users from placing samples in specific wells of a container, list the unavailable wells in a comma-separated list. Each well must be listed individually. You cannot enter a range.

Wells that are marked as unavailable are shown with a dashed line border in the sample placement screen. If a sample is placed into an unavailable well, a Destination is unavailable error message displays.

Edit Container Type Details

1. On the Containers configuration screen, in the Containers list, select a container type.
   The Container Details area displays the details for the selected container type.
2. Edit the details as required.
3. Select Save.

When editing container type details, keep the following in mind:

- To view and edit container types, the Configuration:update permission is required.
- Changes made to a container type are reflected on all future steps on which that container type is enabled.
- Steps that have already been run are not affected by changes made to container type details.
- When a container type has been used, its row, column, and unavailable wells settings are not editable.

For Research Use Only. Not for use in diagnostic procedures.

Delete Container Types

1. On the Containers configuration screen, in the Containers list, select a container.
   The container details display on the right.
2. Select Delete.
3. Confirm the deletion.The container is no longer be available for selection on steps.

When deleting container types, keep the following in mind:

- To delete container types, the Configuration:update permission is required.
- Container types cannot be deleted if an instance of that container type is in use, or has been used, in a step.

Automations Configuration Screen

To access the Automation configuration screen, the Configuration:update permission is required. Users who do not have the Configuration:update permission do not see the Automation tab.

By default, only the Administrator role has the Configuration:update permission. For more on user roles and permissions, see *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

Configuration:update Permission Access

- View existing automations and their details
- Edit automation details
- Delete automations
- Add new automations

Access the Automation Configuration Screen and View Existing Automations

1. On the main menu, select Configuration.
2. On the configuration screen, select the Automation tab.
3. On the Automation Configuration Screen, select one of the following tabs:
   - Step Automation
   - Project Automation
   - Derived Sample Automation

   All step, project, and derived sample automations configured in the system are listed alphabetically on their respective tab.
4. Select an automation to view its details in the Automation Details area on the right.
   In the Automation Details area, the following information is available:
   - The automation name.

For Research Use Only. Not for use in diagnostic procedures.

- Channel Name: The channel used for the automation (for more information, refer to *Automation Channels* in the Clarity LIMS API documentation section).
- Command Line: The command line that is run when the automation is triggered.
- Tokens list: A list of parameters that can be used in the command-line string.
- Automation Use: The master step on which the automation is enabled (applies to step automations only.
- Template Files: One or more files that are referenced in the command-line string and used to generate a file at run time (refer to *Template Files Associated with Automations* on page 141).

Tokens

The Derived Sample Automation, Project Automation, and Step Automation tabs include a collapsible Tokens list.

This list is context-sensitive. Its contents differ depending on the tab being viewed. Copy and paste tokens from these lists directly into the Command Line field.

Automations Configuration Screen

To access the Automation configuration screen, the Configuration:update permission is required. Users who do not have the Configuration:update permission do not see the Automation tab.

By default, only the Administrator role has the Configuration:update permission. For more on user roles and permissions, see *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

Configuration:update Permission Access

- View existing automations and their details
- Edit automation details
- Delete automations
- Add new automations

Access the Automation Configuration Screen and View Existing Automations

1. On the main menu, select Configuration.
2. On the configuration screen, select the Automation tab.
3. On the Automation Configuration Screen, select one of the following tabs:
   - Step Automation
   - Project Automation
   - Derived Sample Automation

All step, project, and derived sample automations configured in the system are listed alphabetically on their respective tab.

4. Select an automation to view its details in the Automation Details area on the right.
   In the Automation Details area, the following information is available:
   - The automation name.
   - Channel Name: The channel used for the automation (for more information, refer to *Automation Channels* in the Clarity LIMS API documentation section).
   - Command Line: The command line that is run when the automation is triggered.
   - Tokens list: A list of parameters that can be used in the command-line string.
   - Automation Use: The master step on which the automation is enabled (applies to step automations only.
   - Template Files: One or more files that are referenced in the command-line string and used to generate a file at run time (refer to *Template Files Associated with Automations* on page 141).

Tokens

The Derived Sample Automation, Project Automation, and Step Automation tabs include a collapsible Tokens list.

This list is context-sensitive. Its contents differ depending on the tab being viewed. Copy and paste tokens from these lists directly into the Command Line field.

Add and Configure Automations

You can create three types of automations in Clarity LIMS: step automations, project automations, and derived sample automations.

- Step automations—Actions that are triggered when running samples through a step. Configure them to be triggered automatically (at the start/end of the step, or when a particular screen is entered or exited), or manually (when selecting a button on the Record Details screen). The automations are enabled on the master step, but the trigger points are configured at the master step or step level.
- Project automations—Actions that users can run on submitted samples, directly from the Projects & Samples screen. For example, you might configure an automation that gives the ability to assign the samples to a workflow.
- Derived sample automations—Actions that users can run on derived samples, directly from the Projects dashboard. For example, you could configure an automation that gives the ability to queue selected samples for a new workflow. In this case, the automation would trigger a custom script created for this purpose.

For Research Use Only. Not for use in diagnostic procedures.

Before You Begin

- Step automations are reusable. After you have created an automation, you can enable it on multiple master steps.
- If you intend the automation to be triggered manually, the name you choose for the automation is used to name the button that initiates it from the LIMS interface.
- Two step automations can have the same name as long as they are unique in some other way. For example:
  - channel name is unique, or
  - command line is unique, or
  - run-program-per-event values are unique (available in the API only)

  Attached files and associated master steps are ignored in these comparisons.
- Two project automations cannot have the same name, regardless of the uniqueness of channel name and command line.
- You cannot enable multiple automations with the same name on a master step, even if the automations are configured differently.

Add a Step Automation

1. On the main menu, select Configuration.
2. On the configuration screen, select the Automation tab.
3. On the Step Automation tab, select New Automation.
4. In the Automation Details area, complete the required fields:
   - Type a name for the new automation.
   - In the Channel Name field, enter the channel to be used for this automation (for more information, refer to *Automation Channels* in the Clarity LIMS API documentation section).
   - In the Command Line field, enter the command line to be run when the automation is triggered. Copy/paste tokens from the Tokens list, as required. For details, refer to *Step Automation Tokens* in the Clarity LIMS API documentation section.
5. [Optional] Enable automation on steps:
   - In the Automation Use section, select inside the Enable on these Master Steps field and select the master step on which to enable the automation. (Note that this configuration is bidirectional—when configuring a master step, you can select automations to associate with that master step.)

   If necessary, you can:
   - Repeat this process to enable the automation on multiple steps.
   - Select the X button to remove a step from the field.

For Research Use Only. Not for use in diagnostic procedures.

6. Select Save.
   The new step automation is now available to be configured on the selected master steps.

Attach Template Files to Step Automations

The Automations configuration screen includes a Template Files section that allows for the upload of a template file to an automation. Reference the file in the automation command line and use it to generate a file that is attached to the step—typically a sample sheet file that can be used to start the instrument run.

A token for the template file is automatically added to the Tokens list. When included in the command line, the token is replaced with the absolute path of the template file at run time.

Downloadable sample sheet template files are available for several Illumina instrument integrations. For details on modifying the example template for the needs of your lab, refer to the *Lab Instrument Tool Kit* section of the Clarity LIMS Integrations and Tool Kits documentation.

To attach a template file:

1. In the Template Files section, select Upload File.
2. In the Upload File dialog, select Choose File, and then browse to and select the appropriate template file.
3. Select Upload. The file is attached to the automation and listed in the Template Files section. When upload is complete, a new dynamic token is added to the Tokens list.
4. In the Command Line field:
   - Include a script that generates the output file.
   - Provide the template file token as a script parameter. You can copy and paste the token directly from the Tokens list. At run time, the token is replaced with the absolute path of the file.
5. Select Save.
   In the Step Automation list, an icon indicates that a file is attached.
   If necessary, you can:
   - Repeat this process to attach additional files to the automation.
   - Select the X button to remove the file from the automation.

You can also attach template files to automations via the API, using the files endpoint. For details, refer to the Clarity LIMS API documentation.

Add a Derived Sample Automation

1. On the Derived Sample Automation tab, select New Automation.
2. In the Automation Details area, complete the required fields:
   - Type a name for the new automation.

For Research Use Only. Not for use in diagnostic procedures.

- In the Channel Name field, enter the channel to be used for this automation (for more information, refer to *Automation Channels* in the Clarity LIMS API documentation section).
- In the Command Line field, enter the command line to be run when the automation is triggered. Copy/paste tokens from the Tokens list, as required. For details, refer to *Derived Sample Automation Tokens* in the Clarity LIMS API documentation section.
- Select Save.

The new derived sample automation is added to the Derived Sample Automations list, and is now available to be run on derived samples from the Projects dashboard.

The following examples show how derived sample automations can be used in the lab.

Example 1: Requeue Samples

In this example, when the Requeue Samples automation is run, the following occurs:

- The custom script, requeue.py, is initiated. (This script is used for illustrative purposes only and is not provided with Clarity LIMS.)
- The command-line parameters are interpreted by the automation worker node, and their values are provided to the script.
- The selected samples are requeued.

1. On the Projects dashboard, run the automation on selected derived samples.
2. As the script runs, the status is reported back.

Refer also to The Projects Dashboard, *Run Automations on Derived Samples* on page 12.

Example 2: User Input

This example shows the configuration of an automation named User Input X, which includes a {user input} token in the command line. (For details, refer to *Step Automation Tokens* in the Clarity LIMS API documentation section.

1. On the Projects dashboard, run the automation on selected derived samples.
2. A custom script called custom_script.sh is initiated.
3. The script prompts for a value to be entered for the input_x parameter.
4. The command-line parameters are interpreted by the automation worker node, and their values—along with the user-supplied input_x value—are provided to the script.
5. The script runs.

Add a Project Automation

1. On the Project Automation tab, select New Automation.
2. In the Automation Details area, complete the required fields:
   - Type a name for the new automation.
   - In the Channel Name field, enter the channel to be used for this automation (for more information, refer to *Automation Channels* in the Clarity LIMS API documentation section).
   - In the Command Line field, enter the command line to be run when the automation is triggered. Copy/paste tokens from the Tokens list, as required. For details, refer to *Project Automation Tokens* in the Clarity LIMS API documentation section.
   - Select Save.

The new project automation is added to the Project Automations list, and is now available to be run on submitted samples from the Projects & Samples screen.

For Research Use Only. Not for use in diagnostic procedures.

Edit an Automation

1. On the Automation Configuration screen, select one of the following tabs:
   - Step Automation
   - Project Automation
   - Derived Sample Automation
2. In the list of automations on the left, select the automation to edit.
3. Make your changes and select Save.

When editing step automations, keep the following in mind:

- Changes you make to a step automation are reflected on all future steps on which that automation is enabled.
- Steps that have already been run are not affected by changes you make to a step automation.

Delete an Automation

1. On the Automation configuration screen, select one of the following tabs:
   - Step Automation
   - Project Automation
   - Derived Sample Automation
2. In the list of automations on the left, select the automation to delete.
3. Select Delete.

Information about deleted automations is saved in the Clarity LIMS database for historical purposes. However, there is no way to restore a deleted automation for use in Clarity LIMS.

Copy Custom Fields from Step Input to Output

Use an automation with the copyUDFs script and to copy custom fields from a step input to a step output. This example uses the Library Normalization master step, and shows how to copy the Concentration field from the step input samples to the output samples.

To copy a custom field from step input to output:

1. On the Lab Work configuration screen, select the Automation tab, then select the Step Automation tab.
   - Add a new automation.
   - Name the automation and enter the channel name.
   - In the Command Line field, copy the following command, replacing the { } placeholders with your own information:

```
bash -c "/opt/gls/clarity/bin/java -jar /opt/gls/clarity/extensions/ngs-common/v5/EPP/ngs-extensions.jar script:copyUDFs -u {username} -p {password} -i {processURI:v3:http} -f Concentration"
```

- In the Automation Use section, enable the automation on the desired master step (this example uses the Library Normalization master step).
- Save the automation.

2. Return to the Lab Work configuration screen and select the Lab Work tab. In the Master Steps list, select the master step on which you enabled the automation.
3. In the Automation section, the new automation is listed. Configure as follows:
   - Trigger Location: Record Details
   - Trigger Style: Automatic upon entry

Automation triggers can be configured at the master step or the step level. If configured on the master step, the trigger settings are locked on all steps derived from that master step.

4. On the Record Details milestone of the same master step, add the Concentration derived sample field to the Sample Table table.
   You can add it as an expanded view field or as a column header (for details, refer to *Record Details Milestone* on page 93
5. Save your changes.
   At run time:
   - When the Record Details screen is entered, the automation are automatically triggered.
   - The copyUDFs script runs and copies the Concentration field values from the step input samples to the output samples.

Template Files Associated with Automations

Old Method (all versions)

Under the old method, template files must be saved to a folder accessible to the automation worker node. Typically /opt/gls/clarity/customextensions/folderName/templateFileName.

If a script needs a template file, the file is specified by including its full path in the syntax that invokes the script.

Advantages

A single template file might be associated with many automations. If the template file needs a minor update, the update can be made in one place. You do not need to update the individual automations.

Disadvantages

Creating a template file is typically an iterative process: create the file, run the script, examine the output, tweak the template file, run the script, examine the output, tweak the template file, and so on.

The file must live on the server to be accessed by the script. Therefore, the developer needs access to the server filesystem—or must go through a trusted party to get the file to the server. This process inhibits rapid development and testing.

New Method (Clarity LIMS v5.1 and later)

As of Clarity LIMS v5.1, template files can (optionally) be attached directly to an automation via the GUI.

Advantages

The iterative process—create file, run script, examine output, tweak template file, run script, examine output, and so on— is much faster because the template file can be replaced via the GUI in a matter of seconds.

If the workflow is being validated, the validator can download and inspect the template file directly from the GUI. There is no need to gain access to the server filesystem.

Disadvantages

Because a single template file is associated with a single automation, a template file with common contents can be duplicated and associated with many automations. If the template needs modification, it must be modified in many places.

When configuration that involves template files is migrated from one Clarity LIMS system to another using the config-slicer tool, the template files themselves are not migrated. After the config-slicer has done its work, the administrator must update the automations in the Clarity LIMS GUI, reuploading and associating the template files. If these steps are not done correctly, the syntax invoking the scripts breaks because the required files are not present on the destination system.

Because a template file is associated with a specific automation, the system allows for multiple automations associated with template files that all have the same name for the template file. While this configuration is not a problem in itself, it can cause problems. For example, if converting from the new method to the old method, you might have multiple template files with the same name but different contents. These files cannot be copied to /opt/gls/clarity/customextensions/ because they overwrite each other. Instead, each one needs to be placed in a distinct folder: /opt/gls/clarity/customextensions/folderName/. (See later why you might want to convert from new method to old.)

Template files can be easily edited and overwritten by an administrator. This interaction might be undesirable in a validated environment. It might be safer if the templates files are harder to reach, and thus not available for inadvertent modification.

Which Method to Use

We recommend that you use a combination of both methods, as follows.

Use the embedded template while developing the template. During this process, having the template file easily available for editing is helpful. After the template is finalized, move it to the server and adjust the automation command line to use the server path/filename instead of the file token.

This method allows for easy, iterative testing and precise traceability for production work. This method also facilitates reliable migrations involving the config-slicer tool and coordinated movement of associated /customextensions/ files.

Config-slicer does not currently migrate automations that need template files without additional manual manipulation after the configuration migration. Regardless of method, you must manipulate the system manually to complete the migration of the template files.

Custom Fields Configuration Screen

In Clarity LIMS, custom fields are used to record information about a step, sample, or other LIMS component.

The default configuration includes both global and master step fields. You can add additional fields to meet the needs of your lab, and display those fields to the user at run time (refer to *Configure Step Milestones* on page 79).

- Global fields—Apply to the whole LIMS system. You can use these fields to record measurements and information about measurements, submitted samples, derived samples, accounts, containers, projects, and clients.
- Master step fields apply to the master step on which they are configured, and are inherited by all steps derived from that master step.

To access the Custom Fields configuration screen, the Configuration:update permission is required. Users who do not have this permission do not see the Custom Fields tab.

By default, only the Administrator role has the Configuration:update permission. For more on user roles and permissions, see *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

Configuration:update Permission Access

- View custom fields.
- Add new custom fields.
- Edit custom fields.
- Delete custom fields.

Access the Custom Fields Configuration Screen and View Existing Custom Fields

1. On the main menu, select Configuration.
2. On the LIMS configuration screen, select the Custom Fields tab.
3. On the Custom Fields configuration screen, select the Global Fields or Master Step Fields tab.
   All global fields and master step fields configured in the system are listed on their respective tab, and are organized into groups.
   - Global fields are grouped by object—Measurement, Derived Sample, Submitted Sample, Account, Container, Project, and Client.
   - Global field groups are sorted by the number of fields each contains, starting with the group that contains the most fields. Groups with the same number of fields are sorted alphabetically.
   - Master step fields are grouped by master step.
   - Master step field groups are sorted alphabetically.
4. Select a group header to expand the list of fields it contains.

Each list item includes the name of the custom field and an icon to convey its field type (refer to *Field Types and Additional Options* on page 147).

Note the following additional details:

- An asterisk (*) displays if the custom field is Required.
- Secondary icons display if the custom field is Read-Only or a Dropdown list.

  To maximize the number of field name characters displayed, the asterisk and secondary icons are hidden in smaller viewports (between 766 px and 875 px).

- Select a field to view its details in the Field Details area on the right (refer to *Field Details* on page 147).
- If viewing master step fields, there is also a Group of Defaults section. Select a group to see the fields and their prepopulated values. For details, refer to *Configure Groups of Defaults* on page 151.

Custom Fields Configuration Screen

In Clarity LIMS, custom fields are used to record information about a step, sample, or other LIMS component.

The default configuration includes both global and master step fields. You can add additional fields to meet the needs of your lab, and display those fields to the user at run time (refer to *Configure Step Milestones* on page 79).

- Global fields—Apply to the whole LIMS system. You can use these fields to record measurements and information about measurements, submitted samples, derived samples, accounts, containers, projects, and clients.
- Master step fields apply to the master step on which they are configured, and are inherited by all steps derived from that master step.

For Research Use Only. Not for use in diagnostic procedures.

To access the Custom Fields configuration screen, the Configuration:update permission is required. Users who do not have this permission do not see the Custom Fields tab.

By default, only the Administrator role has the Configuration:update permission. For more on user roles and permissions, see *User Roles* on page 157 and *Configure Role-Based Permissions* on page 158.

Configuration:update Permission Access

- View custom fields.
- Add new custom fields.
- Edit custom fields.
- Delete custom fields.

Access the Custom Fields Configuration Screen and View Existing Custom Fields

1. On the main menu, select Configuration.
2. On the LIMS configuration screen, select the Custom Fields tab.
3. On the Custom Fields configuration screen, select the Global Fields or Master Step Fields tab.
   All global fields and master step fields configured in the system are listed on their respective tab, and are organized into groups.
   - Global fields are grouped by object—Measurement, Derived Sample, Submitted Sample, Account, Container, Project, and Client.
   - Global field groups are sorted by the number of fields each contains, starting with the group that contains the most fields. Groups with the same number of fields are sorted alphabetically.
   - Master step fields are grouped by master step.
   - Master step field groups are sorted alphabetically.
4. Select a group header to expand the list of fields it contains.

Each list item includes the name of the custom field and an icon to convey its field type (refer to *Field Types and Additional Options* on page 147).

Note the following additional details:

- An asterisk (*) displays if the custom field is Required.
- Secondary icons display if the custom field is Read-Only or a Dropdown list.

  To maximize the number of field name characters displayed, the asterisk and secondary icons are hidden in smaller viewports (between 766 px and 875 px).

- Select a field to view its details in the Field Details area on the right (refer to *Field Details* on page 147).
- If viewing master step fields, there is also a Group of Defaults section. Select a group to see the fields and their prepopulated values. For details, refer to *Configure Groups of Defaults* on page 151.

For Research Use Only. Not for use in diagnostic procedures.

Add and Configure Custom Fields

Configure custom fields to record information about a step, sample, or other Clarity LIMS component.

For example, you can:

- Use global fields to capture sample measurements and track information about projects.
- Use master step fields to record instrument settings and other details about a specific step.
- Configure automation scripts that populate custom fields or perform calculations at run time.
- Create groups of defaults—collections of prepopulated master step fields that eliminate the need for manual input of values at run time and make sure that the correct information is always recorded.

When adding custom fields, keep the following in mind:

- You cannot save a custom field until you have entered a name and selected a field type.
- You cannot create a custom field on a global field object or master step with the same name as an existing field on that object/master step. For example, if you have a created a global field called 'Description' on the Account object, you cannot create another global field called 'Description' on the Account object. However, you can create a 'Description' field on the Project object.
- If the field name you specify is the same as a field that has been deleted, the new field is created and the conflicting field name is renamed. Deleted fields do not display in the LIMS interface, but are saved in the database.

Add a Custom Field

1. On the main menu, select Configuration.
2. On the configuration screen, select the Custom Fields tab.
3. On the Custom Fields configuration screen, select the Global Fields or Master Step Fields tab.
4. In the header of the global field object or master step for which you want to add a new field, select Add.
5. In the Field Details area, complete the required fields:
   a. Type a name for the field.
   b. Select the appropriate field type. See sections below for details.
6. Set the required field options:
   - Required: If this field must be filled in, set this option to Yes. Otherwise, set to No.
   - Read only: If you do not want the user to edit the field value at run time, set to Yes. To allow editing of the field at run time, set to No
7. The Field Options and Additional Options reflect the field type selected:

For Research Use Only. Not for use in diagnostic procedures.

- Default (for nondrop-down field types only): If you would like to set a default value, enter the value here.
- Dropdown Items (for drop-down field types only):

To set a default item, add this value first and set the Set as Default toggle switch to Yes. You can only set the first item as the default, and you cannot reorder items after you have added them.

- Repeat to add more items to the list.
- To remove a list item, select the X button.
- If you do not specify any drop-down items, or if you specify only one item and set it as the default value, upon save, the field converts to its equivalent nondrop-down type and custom entries are enabled.
- Select Add and enter the first list item.

8. Complete other options, as required. See sections below for details.
9. Select Save. The new custom field is added to the bottom of the fields list. It is now available to be displayed on master step and/or step milestone screens.

Field Details

For any field selected, the Field Details area displays the following information:

- The field name.
- The global field object (Derived Sample shown here), or the master step, with which the field is associated.
- The field type.
- The field options, that is, whether the field is:
  - Required—If set to Yes, the field must be filled in.
  - Read only—If set to Yes, the field cannot be edited at run time.
- The default value for the field, if set.
- For drop-down field types:
  - The Default option is replaced with a Dropdown Items list.
  - The first list item may be set as the default value for the field.

Additional options may also display, as described below. These differ depending on the field type. For example, the Range From and To fields only display for Numeric field types.

Field Types and Additional Options

The following table describes the field types available for custom fields, and the additional options that apply to each type.

For Research Use Only. Not for use in diagnostic procedures.

Table 4 Custom Field Types and Additional Options

Field Type	Field Description	Additional Options
Text	Field in which to type a line of text. Field length is only limited by the database field used to store it. PostgreSQL limit - 1 Gb, Oracle limit - 4000 characters.	Not applicable
Numeric	Field in which to type a number.	• Range From, To • Decimal Places Displayed
Hyperlink	Field containing a link to a website URL. Select the link to open the URL in a web browser.	None
Text Dropdown	Field in which to select from a list of predefined text options.	• Custom Entries • Dropdown Items
Numeric Dropdown	Field in which to select from a list of numbers.	• Custom Entries • Dropdown Items • Range From, To • Decimal Places Displayed
Hyperlink Dropdown	Field in which to select from a list of website URLs. Select a link to open the URL in a web browser.	• Custom Entries • Dropdown Items
Multiline Text	Field in which to type multiple lines of text.	Not applicable
Toggle Switch	A field to toggle between Yes and No values.	• None Set (Default) • Yes • No

For Research Use Only. Not for use in diagnostic procedures.

Field Type	Field Description	Additional Options
Date	A calendar tool to select a date.	Not applicable

Toggle Switch Field Types

The Toggle Switch field type renders as a toggle switch on the Record Details screen.

Configuration options:

- Default value configured as Yes or No: When the screen displays, Yes or No is selected by default. User can select Yes or No.
- Default value configured as None Set: When the screen displays, neither Yes nor No is selected. User selects a value.
- Required: The field may be configured as a required field, even if the default value is None Set. When the user enters the screen, neither Yes nor No is selected, but a value must be selected.

Additional Options Usage

The following table explains how to use the additional options associated with the Numeric, Numeric Dropdown, Text Dropdown, and Hyperlink Dropdown field types.

Table 5 Field Types Additional Options Usage

Additional Options	Usage
Range From, To	Use to define the range within which numeric values must fall. At run time, the user is prevented from entering a number outside of the defined range.
Decimal Places Displayed	Use to specify the number of decimal places to display in a numeric field. This value is used for display purposes only. The field stores the value as input by the user or script.
	Note: If the user edits the value of a Numeric field (or gives the field focus by selecting inside it), the value that displays— including the number of decimal places, is written to the database, overwriting the existing value. For this reason, we recommend that you increase the number of decimal places to display to ensure sufficient precision.
Dropdown Items	Use to create a list of options to select at run time.

For Research Use Only. Not for use in diagnostic procedures.

Additional Options	Usage
Custom Entries	Use to control whether or not the user may enter a value at run time. If set to No, a value from the predefined drop-down list must be selected. If set to Yes, a value must be entered into the field.

Edit and Delete Custom Fields

This section describes how to edit and delete custom fields.

Edit Custom Fields

1. On the Custom Fields configuration screen, select the Global Fields or Master Step Fields tab.
2. Expand the global field object group or master step containing the field to edit.
3. Select the field.
4. Make your changes and select Save.

When editing custom fields, keep the following in mind:

- You cannot modify the field type, unless you are changing a drop-down field type to its equivalent nondrop-down type or vice versa. For example, you can change a Numeric Dropdown field to a Numeric field, or a Text field to a Text Dropdown field.
- If you convert a drop-down field type to its equivalent nondrop-down type, Clarity LIMS removes all nondefault list values and enables custom entries upon saving. If a default drop-down option was set, it becomes the default for the nondrop-down field.

Delete Custom Fields

1. On the Custom Fields configuration screen, select on the Global Fields or Master Step Fields tab.
2. Expand the global field group or master step containing the field you would like to delete.
3. Select the field and select Delete. Confirm the deletion.

When deleting custom fields, keep the following in mind:

- You cannot delete a master step field if it has been assigned a value, or is in use in a step—that is, if a step derived from the master step with which the field is associated has been started.
- If you delete a custom field, it no longer displays in the LIMS interface. However, its information is saved in the database for historical purposes.
- You cannot restore a deleted field for use in the LIMS, but you can create a field with the same name. The original deleted field is renamed in the database.

Reorder Global Fields

You cannot reorder master step fields on the Custom Fields configuration screen. This configuration is instead available on the Record Details milestone. For details, refer to the *Configure Step Data* on page 93 section of the *Record Details Milestone* on page 93 topic.

However, you can reorder global fields by simply clicking and dragging them into position.

To drag and drop on a mobile or touch-screen device, touch and hold the item you wish to drag. After a moment, the item appears to lift off the page and its color changes to white. You can then drag the item and drop it into its new position.

The order is reflected in various places in the LIMS interface, for example:

- Submitted sample global field ordering is reflected on the Sample Management screen, in the Sample Details section.
- Project global field ordering is reflected on the Project Details screen (on the Custom Fields tab) and on the Sample Management screen (in the Project Details section).

Configure Groups of Defaults

Groups of defaults are collections of prepopulated master step fields. Using these eliminates the need for lab scientists to manually enter field values each time they run the step, and makes sure that the correct information is recorded every time a step is run.

When you have added groups of defaults to a master step:

- They become available for selection when you create a step based on the master step.
- When running a step in Clarity LIMS, if the step has one or more groups of defaults configured, these steps display in a drop-down list in the upper-right corner of the Record Details screen. Select the desired group of defaults and the LIMS populates the step fields with the corresponding values.
- If you have configured a default group of defaults, those values automatically populate the step fields.

Add a Group of Defaults

1. On the Custom Fields configuration screen, select the Master Step Fields tab.
2. Expand the master step on which to configure a group of defaults.
3. Below the configured master step fields, in the Group of Defaults section, select Add.
4. In the Group of Defaults area on the right, the fields associated with the master step display.
   - Name the group of defaults.
   - Populate each field with the value to set for the group of defaults.
5. Select Save.

6. [Optional] When configuring the Record Details milestone for a step, if the related master step has one or more groups of defaults configured, you can select a default group to display.
7. [Optional] Reorder groups of defaults by clicking and dragging them into position.
   To drag and drop on a mobile or touch-screen device, touch and hold the item you wish to drag. After a moment, the item appears to lift off the page and its color changes to white. You can then drag the item and drop it into its new position.
   The order is reflected in the drop-down list that displays at the top of the Record Details screen.

User Management

The User Management configuration screen allows for viewing and managing users, clients, and accounts.

- Users are the individuals who have access to the Clarity LIMS interface. Because each step in Clarity LIMS is associated with a user, you can make use of user profiles to track the work moving through your lab. While users are associated with the steps they perform as part of a project, they are not directly associated with that project—unless they are assigned as the project client.
- Clients are directly associated with projects in Clarity LIMS. When you create a project, you must associate it with a client. Clients differ from users in that they are not able to log in and access the Clarity LIMS web interface. They are typically external collaborators or customers who submit samples to the lab.
- Accounts must be directly associated with projects, users, and clients that are created in Clarity LIMS.

Viewing user/client/account details, and adding, modifying, and deleting users/clients/accounts are role-based permissions. For more information, refer to *Configure Role-Based Permissions* on page 158

Add and Manage Users and Clients

This section describes how to add and manage users and clients in Clarity LIMS.

When creating users, keep the following in mind:

- The username must be unique among active users in the system. This is validated when you save the user details.
- If the username is already associated with an existing user, an error message displays and you are not be able to save the new user profile.
- All users must provide their email address and reset their password upon upgrading their software to v5.4 (or later).

Add a User

1. From the main menu, select Configuration.
2. Select User Management.
3. From the Users tab, select New User.
4. In the User Details area, complete the following required information:
   - Enter the first name and last name of the user.
   - Select inside the Account field and select a user account from the drop-down list.
   - Enter an email address for the user.
   - Enter a unique username for this user.
5. Select inside the Role field to display a drop-down list of roles:
   - Select the role to assign to this user.
   - To remove a role from this field, select the X to the left of the role name.
6. [Optional] Enter a title, phone number, and fax number for the user.
7. Select Save.
   An invitation email is automatically sent to the user. This email includes the login screen URL and information on how to set the login password. You may resend the login instructions email at any time (refer to *Modify User Details* on page 153).
   The user displays in the Users list.
8. [Optional] By default, the status of a new user is set to Active, which means that they can log in to Clarity LIMS. To temporarily prevent a user from logging in, change this setting by selecting Archived. (Refer to also *Manage User Access* on page 156.)

Users cannot log into Clarity LIMS unless they have been assigned a username and have set a password. Once logged in, they can modify some of their user details. Refer to *Update Profile and Reset Password* on page 155.

Modify User Details

1. From User Management, select the Users tab.
2. Select the user to modify.
3. In the User Details area, modify the details as required. If you change the username, a password reset email is sent automatically to the user.
4. Select Login and Password to access the following options:
   - Send login instructions—Choose this option to re-send the user the login screen URL and information on how to set their login password.

- Reset password—Choose this option to send the user a link that allows them to reset their login password (refer to *Manage User Access* on page 156).

5. Select Save.

Delete a User

1. From User Management, select the Users tab.
2. Select the user to delete.
3. In the User Details area, select Delete.

When deleting users, keep the following in mind:

- You cannot delete a user if that user has logged in to Clarity LIMS.
- You cannot delete a user if that user is associated with a project (eg, the user is the project client).
- Deleting a user removes them from Clarity LIMS. You may instead prefer to archive the user or temporarily remove their access to the system. For details, refer to *Manage User Access* on page 156.

Add and Modify Clients

When adding new clients, each client must be a unique entry in the LIMS.

To add a client:

1. From User Management, select the Clients tab.
2. Select New Client.
3. In the Client Details area, complete the following required information:
   - Enter the first name and last name of the client.
   - Select inside the Account field and select the client account from the drop-down list.
   - Enter the client email address.
4. [Optional] Enter client title, phone number, and fax number.
5. Select Save.
   The user displays in the Clients list, under their account name.

To modify client details:

1. From User Management, select the Clients tab.
2. Select the client to modify.
3. In the Client Details area, modify the details as required.
4. Select Save.

Delete a Client

A client cannot be deleted if that client is associated with a project.

For Research Use Only. Not for use in diagnostic procedures.

1. From User Management, select the Clients tab.
2. Select the client to delete.
3. In the Client Details area, select Delete.

Add and Manage Accounts

Accounts are the organizations with which a facility conducts business.

In the Clarity LIMS Projects and Samples screen, select the existing account from the Account drop-down list to associate projects and samples with it.

To create a new account, type directly into the Account field.

For Clarity LIMS v6.2 and later, you can also create a new account through the Accounts section of the User Management tab that is under Configuration.

Add a New Account

1. From Configuration, select the User Management tab.
2. Select the Accounts tab.
3. In the Account Details area, select New Account.
4. Type a name for the account and complete any other applicable fields (eg, Billing Address).
5. Select Save.

Modify Account Details

1. From Configuration, select the User Management tab.
2. Select the Accounts tab.
3. In the Accounts list, select the account that you want to modify.
4. In the Account Details area, update the fields that need to be modified.
5. Select Save.

Delete an Account

1. From Configuration, select the User Management tab.
2. Select the Accounts tab.
3. In the Accounts list, select the account that you want to delete.
4. Select Delete.
   You cannot delete an account that is associated with a user or project.

Update Profile and Reset Password

After signing into Clarity LIMS, you can update some of the details associated with your profile, including your password, email address, and profile photo.

If the user is an LDAP account, then you cannot update the profile in Clarity LIMS.

If you forget your password and are unable to sign in, request a password reset from the Sign In screen.

Update User Profile

1. In Clarity LIMS, at the right of the menu bar, select your username and then select Profile.
2. The Profile page opens, displaying the details associated with your user profile.
3. On this page, you can:
   - Change your password.
   - Change your email address.
   - Upload an image to associate with your profile.

Manage User Access

This section describes two tasks that Clarity LIMS administrators are often required to perform:

- Temporarily prevent a user from logging in by archiving the user.
- Email a link to a user that allows them to reset their Clarity LIMS password.

While Clarity LIMS does not enforce password changes, for best practice and security, we recommend that user passwords are changed frequently.

Archive a User

1. On the main menu, select Configuration.
2. Select User Management.
3. Select the Users tab to see a list of all current active and archived users in the system, categorized by role.
4. Select the user to archive.
   The details for the selected user display in the User Details area on the right. The Status slider displays the current status of the user.
5. Select Archived to temporarily archive the user.
6. Select Save.

By default, every new user created in Clarity LIMS is an active user and can sign in to Clarity LIMS with their username and password.

Reset a User Password

For best practice and security, we recommend that user passwords are changed frequently.

1. On the main menu, select Configuration.

2. Select User Management.
3. Select the Users tab to see a list of all current active and archived users in the system.
4. Select the user whose password is to be reset.
   The details for the selected user display in the User Details area on the right.
5. Select Login and Password and select Reset password.
   This sends the user a link that allows them to reset their password.

The Send login instructions option sends the user the following information:

- The URL for the login screen.
- Instructions on how to set their login password.
- This email is sent automatically when a new user is created, but you may occasionally need to resend it.

User Roles

Clarity LIMS users are assigned roles. These roles control permissions and the ability to:

- Access certain Clarity LIMS features.
- Perform certain actions.
- Sign in to the Clarity LIMS interfaces.

The following sections describe the default permissions of the four primary user roles. Some user role permissions are configurable (refer to *Configure Role-Based Permissions* on page 158).

System Administrator and Facility Administrator

By default, both the System Administrator and Facility Administrator user roles have access to:

- All configuration areas of the Clarity LIMS web interface, allowing them to:
  - Add and configure workflows, protocols, and steps.
  - Add consumables—reagents, controls, instruments, reagent labels, containers.
  - Add and configure custom fields.
  - Add and configure automations.
- Supervisory and lab management functions in the Clarity LIMS web interface, allowing them to:
  - Review escalations.
  - Remove samples from workflows.
  - Move samples into the next step in a workflow.
  - Access the Overview and Projects dashboards.
- User management, allowing them to:
  - Create, modify, and delete user accounts.

  - Modify user roles and permissions.
  - Approve access requests from external collaborators.

Researcher

The Researcher role is typically assigned to the laboratory scientist. By default, individuals who are assigned this user role are able to:

- Log in to Clarity LIMS.
- Access Lab View.
- Manage and work with samples contained in all projects in the system.
- Edit their own user profiles—ie, they can change their own passwords and other profile information.
- Access three Consumables configuration areas: Reagents, Controls, and Instruments, and do the following.
  - View reagent kits and add new reagent lots to those kits (researchers cannot create reagent kits).
  - View controls.
  - View instrument types and add new instruments to those instrument types (researchers cannot create instrument types).
  - Reactivate expired (archived) instruments by resetting the expiration date.

Collaborator

The Collaborator role is assigned to external collaborators who interact with Clarity LIMS using the LabLink Interface.

The Collaborator role is supported in v5.3 and later. It is not supported in v5.0.x to v5.2.x.

An external person can request a user ID through LabLink. By default, when the request is approved by an administrator, the collaborator is able to:

- Sign in to LabLink.
- Create, view, and delete projects. (Collaborators are automatically given full permissions to projects they create.)
- Submit samples to projects, and delete samples from projects.

By default, collaborators do not have access to the main Clarity LIMS web interface.

Configure Role-Based Permissions

Manage the permissions of the System Administrator, Facility Administrator, Researcher, and Collaborator user roles to restrict or allow the following actions:

- Sign in to Clarity LIMS.
- Sign in to the API.

- View and interact with certain features of the interface.
- Perform certain actions in the interface.
- [Clarity LIMS v6.1] View and restrict any actions in the interface.

Command-Line Permissions Tool

Role-based permissions are controlled through the permissions-tool.jar tool, at /opt/gls/clarity/tools/permissions/.

For assistance with running the command-line permissions tool, contact the Illumina Support team.

Functionality includes the following commands:

- listRoles—List all roles in the system.
- describeRole—List names and descriptions of all permissions in the system.
- createRole—Create a role.
- showSummary—List permissions assigned to each role in the system.
- listPermissions—List permissions assigned to a specific role.
- assignPermission—Assign a permission to a role.
- removePermission—Remove a permission from a role.

The permissions-tool.jar tool function names and property names are case-sensitive. If you type the incorrect case, your command or property cannot be understood.

There can be a delay (up to 20 minutes) before changes to some API-related permissions take effect.

Supported Commands

listRoles

List all user roles in the system:

```
java -jar permissions-tool.jar -a <apiUri> -u <username> -p <password> listRoles
```

describeRole

Show permissions for a specific role:

```
java -jar permissions-tool.jar -a <apiUri> -u <username> -p <password>
describeRole <rolename>
```


For Research Use Only. Not for use in diagnostic procedures.

createRole

Create a role:

```
java -jar permissions-tool.jar -a <apiUri> -u <username> -p <password>
createRole <rolename>
```

showSummary

Show assigned permissions for all roles:

```
java -jar permissions-tool.jar -a <apiUri> -u <username> -p <password>
showSummary
```

listPermissions

List names and descriptions of all permissions:

```
java -jar permissions-tool.jar -a <apiUri> -u <username> -p <password>
listPermissions
```

assignPermission

Assign a permission to a role (the example assigns permission to create controls):

```
java -jar permissions-tool.jar -a <apiUri> -u <username> -p <password>
assignPermission <rolename> Controls:create
```

[Clarity LIMS v6.1] Assign a permission to a role (the example assigns read-only permission to a role):

```
java -jar permissions-tool.jar -a <apiUri> -u <username> -p <password>
assignPermission <rolename> RoleOnly
```

Refer to Supported permissions.

removePermission

Remove a permission from a role (the example removes permission to create controls):

```
java -jar permissions-tool.jar -a <apiUri> -u <username> -p <password>
removePermission <rolename> Controls:create
```

Refer to Supported permissions.

Usage

```
java -jar permissions-tool.jar -a <apiUri> -u <username> -p <password> <command>
[<args>]
```

Options

-a	--apiUri	REST API base URI (ends with "/api/<version>/") Must be completed as: http://<servername>/api/v2/
-p	--password	LIMS password (required)
-u	--username	LIMS sign-in username (required)

Supported Permissions

The sections below list LIMS permissions and actions, and the user roles to which each permission/action is assigned by default.

By default, System Administrators and Facility Administrators have all permissions listed.

Permission: AdministerLabLink

The default role with AdministerLabLink permission is Administrator. This permission is added to the existing System Administrator & Facility Administrator roles.

The Collaborator role is based on the existing Collaborator role in LabLink v1.0.

Note: The existing Researcher role does not have the new permission and behaves similarly to the LabLink Collaborator role.

Action	Permission Required	System Administrator and Facility Administrator	Collaborator
Sign in to LabLink	CollaborationsLogin action	Yes	Yes
Manage Project	Projects create, read, update.	Yes	Yes
Manage Sample	Samples create, read, update.	Yes	Yes
Manage User	Users create, read, update.	Yes	No
Manage Configuration	Configuration update	Yes	No
View the Configuration page	AdministerLabLink	Yes	No

Action	Permission Required	System Administrator and Facility Administrator	Collaborator
View the User Management page	AdministerLabLink	Yes	No

Permission: ClarityLogin

Default roles with this permission: Administrator, Researcher

Allows:	Result of denied permission
• Sign in to BaseSpace LIMS • Access Lab View and Projects and Samples screen • Access Consumables > Reagents configuration tab; view, edit, and delete reagent lots; add lots to existing kits. • Access Consumables > Controls configuration tab and view control details • Access Consumables > Instruments configuration tab; add, edit, delete, and activate instruments; view instrument types.	Sign In screen • Sorry, you do not have permission to sign in to Clarity LIMS.

Permission: APILogin

Default roles with this permission: Administrator

Allows:	Result of denied permission
• Access LIMS Rest API	Sign In screen • 403 Forbidden error via http://host/api/*

Permission: Project

Default roles with these permissions: Administrator, Researcher, Collaborator

Action	Allows:	Result of denied permission
• create	• Create project • Modify project details • Modify project custom fields	Projects and Samples • New Project button hidden • View project details (read-only) Note: No permission is needed to upload files to a project

For Research Use Only. Not for use in diagnostic procedures.

Action	Allows:	Result of denied permission
• update	• Modify project details	Projects and Samples • Save button disabled (if delete is permitted) • Button menu hidden (if delete is not permitted) • View project details (read-only)
• delete	• Delete project containing no samples. • Delete project containing samples (also requires Sample:delete permission)	Projects and Samples • Delete button disabled (if update is permitted) • Button menu hidden (if update is not permitted)

Permission: Sample

Default roles with these permissions: Administrator, Researcher, Collaborator

Action	Allows:	Result of denied permission
• create	• Submit/add samples • Upload sample list • Download sample list example • Modify samples.	Projects and Samples • Submit Samples title hidden • Download Example Sample List link hidden • Upload Sample List button hidden • Add Samples button hidden • Modify Samples button renamed Download List • Modify <n> Samples button hidden (sample list) Sample Management • Sample + button hidden
• update	• Modify samples.	Projects and Samples • Modify Samples button renamed Download List

For Research Use Only. Not for use in diagnostic procedures.

Action	Allows:	Result of denied permission
The Sample:update permission is automatically granted to roles that have the Sample:create permission at the time of migration to Clarity LIMS v5.x. If you have removed create permissions from any default role, the role does not acquire the update permission.		
• delete	• Delete a submitted sample on Projects and Samples screen, provided no work has been performed on the sample. • Delete a submitted sample in API, provided no work has been performed on the sample.	Projects and Samples • Delete button hidden • 403 Forbidden error via http://host/api/sample

Permission: Controls

Default roles with these permissions: Administrator

Action	Allows	Result of denied permission
• create	• Create control samples.	Controls • New Control button hidden • View control sample details (read-only)
• update	• Modify control samples. • Archive control samples (requires both update and delete permissions)	Controls • Save button disabled (if delete is permitted) • Button menu hidden (if delete is not permitted) • View control sample details (read-only)
• delete	• Delete control samples. • Archive control samples (requires both update and delete permissions)	Controls • Delete button disabled (if update is permitted) • Button menu hidden (if delete is not permitted) • Archived toggle disabled

For Research Use Only. Not for use in diagnostic procedures.

Action	Allows	Result of denied permission
Users with ClarityLogin permission can access the Consumables > Controls tab and view control sample details (read only).		

Permission: ReagentKit

Default roles with these permissions: Administrator

Action	Allows	Result of denied permission
• create	• Create reagent kits	Reagents • New Reagent Kit button hidden • View reagent kit details (read-only)
• update	• Modify reagent kits • Archive reagent kits (requires both update and delete permissions)	Reagents • Save button disabled (if delete is permitted) • Button menu hidden (if delete is not permitted) • View kit details (read-only - except for Status)
• delete	• Delete reagent kits • Archive reagent kits (requires both update and delete permissions)	Reagents • Delete button disabled (if update is permitted) • Button menu hidden (if delete is not permitted) • Archived toggle disabled
Users with ClarityLogin permission can access the Consumables > Reagents tab. They can also view, edit, and delete reagent lots, and add lots to existing kits. No additional ReagentKit permissions are required.		

Permission: Role

Default roles with these permissions: Administrator

For Research Use Only. Not for use in diagnostic procedures.

Action	Allows	Result of denied permission
• read	• View client (researcher/contact) details, including details such as username and roles in API • View users and clients (contacts) on Users and Clients screen	• 403 Forbidden error via http://host/api/roles
• create	• Create user roles.	• 403 Forbidden error via http://host/api/roles
• update	• Modify existing user roles. • Add/remove user role permissions	• 403 Forbidden error via http://host/api/roles
• delete	• Delete user roles.	• 403 Forbidden error via http://host/api/roles

APILogin permission is required for role management. All users with ClarityLogin permissions can view and edit their own user details (except for assigning/removing roles).

[Clarity LIMS v6.1] Permission: Read-Only

Default roles with this permission: Not applicable. You can assign this permission to any role.

At least one System Administrator must be available to reconfigure user roles. Therefore, we recommend that you do not assign the Read-Only permission to the default Administrator and API users.

Action	Allows
• read	• View project and sample details on the Projects & Samples screen • View lab activities, in-progress steps, and steps that are ready to be worked on in Lab View

Permission: User

Default roles with these permissions: Administrator

Action	Allows	Result of denied permission
• read	• View users and clients on Users and Clients screen • View client details, including details such as username and roles in API	• 403 Forbidden error via http://host/api/researchers
• create	• Create users and clients on Users and Clients screen (User:update permission is required to assign permissions to the user) • Send login instructions and password reset emails on Users and Clients screen (either this action or User:update is required) • Create clients in API. • Create user credentials and assign roles in API.	Users and Clients • New User button hidden • View user details (read-only) • 403 Forbidden error via http://host/api/researchers
• update	• Update users and clients on Users and Clients screen • Send sign in instructions and password reset emails on Users and Clients screen (either this action or User:create is required) • Modify client details in API. • Assign role to user in API. • Remove role from user in API.	• Save button disabled (if delete is permitted) • Button menu hidden (if delete is not permitted) • View user/client details (read-only) • 403 Forbidden error via http://host/api/researchers
• delete	• Delete users and clients on Users and Clients screen. • Delete a client and associated user in API.	• Delete button disabled (if update is permitted) • Button menu hidden (if delete is not permitted) • 403 Forbidden error via http://host/api/researchers

In the LIMS user interface, the term 'contact' has been replaced with 'client.' However, the API still uses the permission Contact.

All users with ClarityLogin permission can view and edit their own user details (except for assigning/removing roles).

Permission: Contact

Default roles with these permissions: Administrator

For Research Use Only. Not for use in diagnostic procedures.

Action	Allows	Result of denied permission
• read	• View clients on Users and Clients screen • View client details in API	• 403 Forbidden error via http://host/api/researchers
• create	• Create clients on Users and Clients screen. • Create clients in API. Contact:update permission is required to assign permissions to clients.	• New Client button hidden • View client details (read-only) • 403 Forbidden error via http://host/api/researchers
• update	• Update client details on Users and Clients screen. • Update client details in API. • Assign role to/remove role from client.	• 403 Forbidden error via http://host/api/researchers This permission does not affect the display of clients in Project and Samples and Sample Accessioning screens.
• delete	• Delete clients on Users and Clients screen. • Delete clients in API. Clients with associated user details cannot be deleted.	• Delete button disabled (if update is permitted) • Button menu hidden (if delete is not permitted) • 403 Forbidden error via http://host/api/researchers

In the LIMS user interface, the term 'contact' has been replaced with 'client.' However, the API still uses the permission Contact.

Users with ClarityLogin permission can view and edit their own client and user details.

Clients can edit their own details (except for assigning/removing roles) without having update permission.

Permission: Process

Default roles with these permissions: Administrator

Action	Allows	Result of denied permission
• read	• View master steps	• 403 Forbidden error via http://host/api/process
• create	• Create master steps.	• 403 Forbidden error via http://host/api/process

For Research Use Only. Not for use in diagnostic procedures.

Action	Allows	Result of denied permission
• update	• Modify master steps.	• 403 Forbidden error via http://host/api/process

In the LIMS user interface, the term 'process' has been replaced with 'master step.' However, the API still uses the permission Process.

Permission: OverviewDashboard

Default roles with this permission: Administrator

Action	Allows	Result of denied permission
• read	• Access the Overview Dashboard	• No Dashboards button

Permission: Configuration

Default roles with this permission: Administrator

Action	Allows	Result of denied permission
• update	• Manage all configuration in the LIMS interface (ClarityLogin permission is also required) • Manage configuration in API (APILogin permission is also required)	• 403 Forbidden error via any URI that begins with http://host/api/configuration.

Permission: ReQueueSample

Default roles with this permission: Administrator, Researcher, Collaborator

Allows	Result of denied permission
• Requeue a sample in sample search. • Requeue a sample in container search.	Sample and Container Search • Requeue button hidden.

Permission: SampleWorkflowAssignment

Default roles with this permission: Administrator, Researcher, Collaborator

For Research Use Only. Not for use in diagnostic procedures.

Allows	Result of denied permission
• Assign sample to workflow from Projects and Samples screen.	Sample Management • Sample cannot be dragged into workflow widgets. • Workflow selection widget hidden • Workflow lozenge Remove button hidden • Delete workflow button hidden.

Permission: RemoveSampleFromWorkflow

Default roles with this permission: Administrator

Allows	Result of denied permission
• Remove sample from queue. • Remove sample from workflow.	Sample Management • Remove from this queue option hidden (if Move to next step is permitted) • Options button hidden (if Move to next step is not permitted)

Permission: MoveToNextStep

Default roles with this permission: Administrator

Allows	Result of denied permission
• Move sample to next step in workflow	Sample Management • Move to the next step option hidden (if Remove from this queue is permitted) • Options button hidden (if Remove from this queue is not permitted)

Permission: SampleRework

Default roles with this permission: Administrator

Allows	Result - permission granted
• Rework a sample from a previous step.	Sample Management • In Select the next step of the sample drop-down list, Rework from an earlier step option displays. • On Protocol Step Results screen, a button displays to allow the sample to be reworked from an earlier step.

For Research Use Only. Not for use in diagnostic procedures.

Permission: ReviewEscalatedSamples

Default roles with this permission: Administrator

Allows	Result - permission granted
• Review escalated samples.	Sample Escalation • Enter Review Comment box enabled.

Permission: ESignatureSigning

Default roles with this permission: Administrator

Allows	Result of denied permission
• Sign an eSignature on step completion.	Record Details • Error message in e-Signature popup

Permission: CanEditCompletedSteps (LIMS v5.1 and later)

Default roles with this permission: None

Allows	Result - permission granted
• Edit button when viewing a completed step. • Select button to edit completed step details on Record Details screen.	Assign Next Steps. • Edit button displays. Record Details • After clicking Edit button, Record Details fields are editable, as applicable/permitted.

Modifications are limited to what is available on the Record Details screen for the step.

Details such as sample placement or routing cannot be modified.

Only steps completed after upgrading to LIMS v5.1 can be edited. Steps completed in v5.0 or earlier cannot be edited.

Steps that were executed using the Process API cannot be edited.

For details, refer to *Modify Completed Step Details* on page 28.

Automated QC Overview

The Clarity LIMS automated QC system is configurable. This allows administrators to determine which QC master steps and steps are required for aggregation, the criteria to apply to each master step/step, and the field values to be copied up to aggregation.

The following features are provided:

- Preconfigured protocols for DNA Initial QC and RNA Initial QC that include master step templates for Bioanalyzer, NanoDrop, Qubit, PicoGreen, CaliperGX, TapeStation, and Aggregate QC.
- Custom field-based storage of key QC results for both automated and spreadsheet-based manual storage.
- Custom field-based criteria (Source Data Field, Operator, and Threshold Value) for QC steps that allow for automatic assignment of QC flags triggered on the storage of a QC result file.
- QC protocol filter configuration that allows you to determine to which QC step samples are queued and which must be completed before aggregation can occur.
- Automated aggregation of QC results and assignment of QC flags, from individual step right up to the sample undergoing QC, with the option of using custom field-based configuration to update Concentration (and other fields) from a particular QC result.
- Easy access to individual sample QC measurements and flags, allowing you to review results, see the criteria evaluated, and the resulting QC flags assigned.
- Excel-based log files, attached to the aggregation step, clearly show the criteria evaluated, the resulting QC flag assigned, and which individual QC test results were used to update the custom field values on the sample undergoing QC.

Remove QC Steps

Clarity LIMS includes preconfigured RNA Initial QC, DNA Initial QC, and Library Validation QC protocols, each containing a sequence of steps. You can modify these protocols, and remove steps that your lab does not use.

1. On the main menu, select Configure.
2. On the LIMS configuration screen, select the Lab Work tab.
   The Workflows, Protocols, Steps, and Master Steps navigation panel displays.
3. In the Protocols list, select the protocol you want to modify.
   The Steps list updates, highlighting the steps included in the selected protocol.
4. To delete a step, select it and select Delete.

You cannot remove a step if it contains samples that are currently in progress, or if there are samples queued for it.

In this scenario, you must move the samples before proceeding with the deletion. Refer to *Manually Move Samples to the Next Step* on page 25.

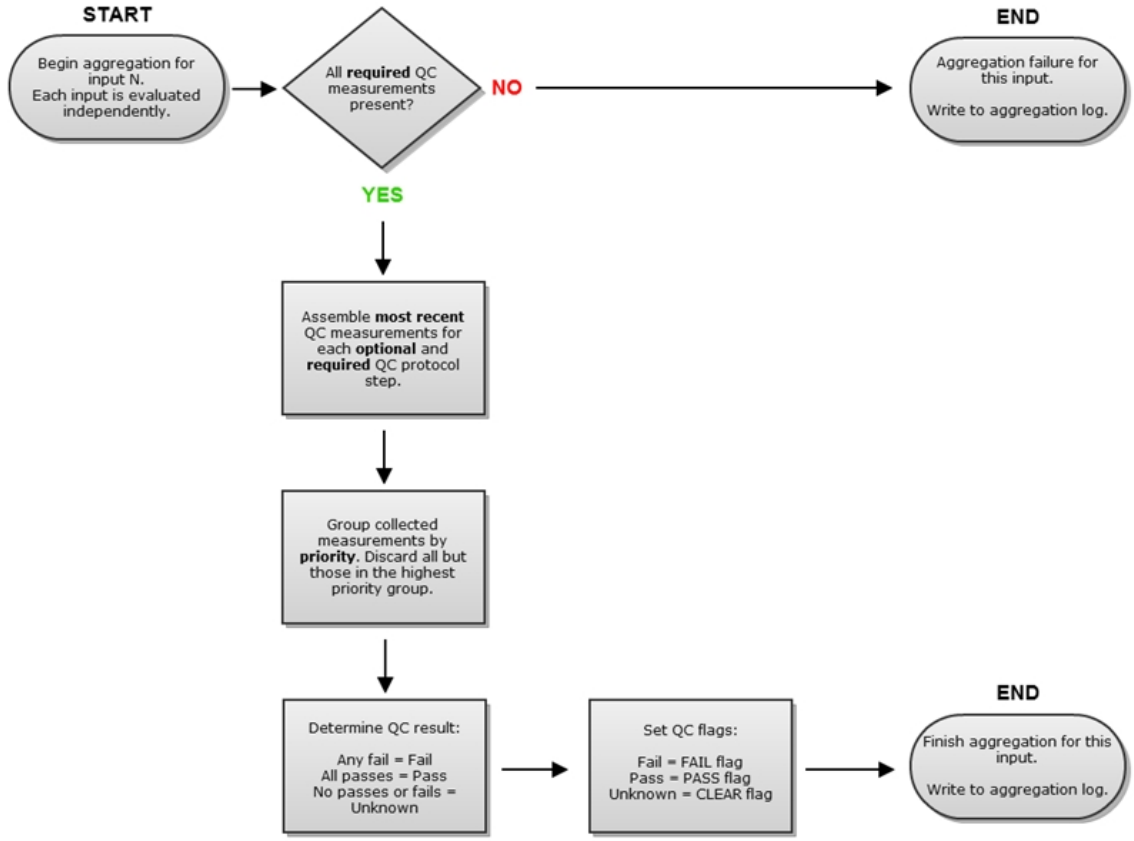
Configure Master Step Fields for QC Aggregation

In the default BaseSpace Clarity LIMS configuration, the Aggregate QC step aggregates the results of all QC steps in the protocol—if they are available.

If a step has been removed from a QC protocol, it is ignored and aggregation still occurs for the remaining steps. No error is generated.

QC Aggregation Logic

The following flowchart shows the logic behind the default configuration of QC aggregation.



Often, this default configuration is acceptable and there is no need to make any changes. However, you can configure alternate QC master step field values that overwrite these defaults. For example, you may want to:

- Make a particular step required for aggregation.
- Increase the priority of the results of a particular step—a step whose results are considered more accurate, for example.
- Make one/both of the changes listed, and then lock down values so that users cannot modify them.

Aggregation Master Step Fields

The Aggregate QC master step includes a master step field for each QC step to be considered for aggregation.

The value for the QC master step field may be one of two values:

- Use if available—If the QC step was run for a sample, its value is used in the aggregation calculation. If the QC step was not run, it is ignored.
- Required—The step is required for aggregation. If it has not been run for a sample, the QC value cannot be calculated and aggregation does not proceed.

The default setting for all QC steps is Use if available.

Aggregation Priority

The Required and Use if available master step field values can have an additional (Priority n) suffix.

To be an acceptable value, the value for 'n' may be any value between 1–99, where 1 is the highest priority and 99 is the lowest priority. Master step fields without a priority value defined are assigned a priority of 99.

The default priority value for all QC steps is (Priority 5).

If sample measurements exist for multiple QC steps, all of which have been assigned the same level of priority (as is the case in the default system) the QC flags are evaluated such that any failure results in an overall fail flag for QC aggregation.

Sometimes, however, a particular QC technology may be considered more accurate and you may want its results to take precedence.

For example, a lab may run Bioanalyzer and NanoDrop QC steps on all samples. If one of these steps results in a QC fail, a PicoGreen assay is run on the failed sample and its result is then considered more accurate. In this case, set Bioanalyzer and NanoDrop at priority 5 and PicoGreen at priority 3.

All QC aggregations are logged in an Excel workbook log file and attached to the Aggregate QC step.

Subsequent invocations of the aggregation script results in a new sheet being created in the workbook, in the first sheet position. This new sheet automatically becomes the active sheet.

Configuring Alternate Master Step Fields for QC Aggregation

The best practice method for configuring alternate master step field values for QC aggregation is to create a group of defaults. The fields defined in the group overwrite the default configuration values.

For details, refer to *Add and Configure Custom Fields* on page 146.

The aggregate QC script treats any custom field that does not begin with 'Copy' as a priority master step field. Therefore, you are restricted from adding fields that are not priority fields. Any new priority fields must contain default values of Required and Use if available.

If you do not want lab scientists to be able to manually edit a master step field value, lock it down by setting the Custom Entries toggle switch to No. At run time, the lab scientist must select a value from the predefined drop-down list.

Configure QC Evaluation Criteria

In the default Clarity LIMS system, each QC master step has two sets of QC evaluation criteria defined. These are displayed in the Record Details screen when the QC step is run.

Each set of criteria comprises three master step fields: Source Data Field, Operator, and Threshold Value.

When the QC protocol step is run, the lab scientist selects from the prepopulated drop-down lists of Source Data Field and Operator values, and then types a numeric value into the Threshold Value field.

You may want to restrict the values available for selection from the Source Data Field and Operator lists, or set default criteria values that cannot be changed.

The best practice method for configuring the criteria used to evaluate QC protocol steps is to create a group of defaults. The master step fields defined in the group overwrite the default configuration values.

For details, refer to *Configure Groups of Defaults* on page 151.

Copy Master Step Fields

In the default Clarity LIMS system, when QC aggregation is executed, the Record Details screen allows lab scientists to (optionally) select one or two master step field values to be copied up from a QC protocol step.

Generally, this is a concentration value.

If necessary, you can specify the master step field values to be copied.

The best practice method of setting master step fields to be copied up to aggregation is to create a group of defaults. For details, refer to *Configure Groups of Defaults* on page 151.

Setting QC master step fields to copy up to aggregation is an optional step. If you do not require this feature, leave the default system as is. Note also that if the Copy task fields are left empty, no values are copied up and no errors are generated. Similarly, if you specify a QC step that has not been run or a field that contains no value, no errors are generated.

Queue Performance and Usability

The Queue screen lists the samples that are queued for a step, and provides a table from which samples are selected for placement into the Ice Bucket.

By default, samples listed in the Sample table are grouped by container. Groups are collapsed by default and can be expanded as required by selecting the arrows.

Lab scientists can also choose to group samples by project, submitted sample, or previous step.

Performance and Usability

In the past, some performance and usability issues were encountered when viewing large data sets in the Queue screen. Clarity LIMS now includes performance enhancements that speed up the Sample table loading time, allowing users to more quickly interact with the data.

Clarity LIMS development teams measured the performance for various samples that are queued for a step with the Time to Interactive (TTI) metric. This metric defines the time it takes for a page to become fully interactive and for functionality to start working (eg, selecting, scrolling, and so on). The metric numbers vary based on the following information:

- Server specification.
- Amount of data stored on the server database.
- Client hardware specifications and the browser type used to access Clarity LIMS.
- Network conditions between the server and client.

Performance Test Setup

The following table shows the server and client specifications used for the performance test.

The different client types are used to demonstrate the different setups.

Table 6 Performance Test Specifications

Hardware	Specification	Additional Notes
Server	3.1 GHz Intel Xeon Platinum processor (8-core) 32 GB RAM Oracle Linux v8.8 PostgreSQL 15.2 database	The server database is loaded with the following information: • 200,000 submitted sample records • 2,000,000 derived sample records • 500 projects
Client A	3.1 GHz Intel Xeon Platinum processor (8-core) 32 GB RAM	Access Clarity LIMS within the same network in the lab.
Client B	2.3 GHz Intel Core i9 (8-core) 32 GB RAM	Access Clarity LIMS on the cloud. The VPN access and different network region setup results in high network latency and demonstrates the worst case for performance.

For Research Use Only. Not for use in diagnostic procedures.

Performance Test Results

The following tables show the results of two performance tests conducted on a Clarity LIMS system on which performance enhancements had been implemented. In both tests, samples were grouped by container.

The tables show how the usability rating changes as the number of samples in the queue increases.

Test 1: Container = Tube

Table 7 Test 1 Performance Results

Number of Samples	Response Time (seconds) - Client Type A	Response Time (seconds) - Client Type B
1000	2.0	4.5
3000	2.5	5.0
7000	3.5	6.5
10,000	5.0	7.5
15,000	7.0	10.5
20,000	9.0	12.5

Test 2: Container = 96 well plate

Table 8 Test 2 Performance Results

Number of Samples	Response Time (seconds) - Client Type A	Response Time (seconds) - Client Type B
1000	2.0	4.5
3000	3.0	5.5
7000	5.0	7.5
10,000	7.0	9.5
15,000	9.5	12.5
20,000	12.5	15.0

Demultiplexing API Endpoint Performance

The demultiplexing API endpoint is an extension of the existing artifact endpoint. This endpoint demultiplexes artifacts recursively to all individual derived samples that they represent.

For more information, refer to the *API & Database* documentation.

Performance and Usability

In the past, some may have experienced performance and usability issues when demultiplexing large data sets. Clarity LIMS now includes the demultiplexing API endpoint, resulting in performance enhancements that speed up demultiplexing and allow quicker interaction with the data.

While acknowledging that usability is subjective, the Clarity LIMS product and development teams have established usability ratings based on criteria that measure how lab scientists must wait before they can interact with a feature on the screen. These criteria also allow for the comparison of performance and usability across the various screens of Clarity LIMS.

In the following table:

- Successful user interaction means that a feature can begin to be interacted with (ie, it can be selected, scrolled, moved, and so on).
- Numbers are provided for guidance only, and differ depending on the RAM and CPU speed of the computer used to view the page.

Usability Rating	Criteria
Good	A successful user interaction (data load) in ~ 2 seconds
Reasonable	A successful user interaction (data load) in ~ 6 seconds
Acceptable	A successful user interaction (data load) in ~ 9 seconds
Degraded	A successful user interaction (data load) in ~ 20 seconds
Unusable	A subjective limit to usability

Performance Test Results

The following table shows how the usability rating changes as the number of samples in the pool undergoing demultiplexing increases.

Usability Rating	# Samples
Good	2200–2400
Reasonable	3400–3600
Acceptable	4600–5800
Degraded	7200–7400

Audit Trail

Clarity LIMS provides Audit Trail, a robust data-tracking system that allows for tracking of the following:

- All user activity (ie, who did what, and when).
- Every action that is written to the database.

Audit Trail has two capture systems, Event Log and Detail Log.

- Event Log—Records familiar BaseSpace Clarity LIMS user actions and presents this information in a format that is easy to read and understand.
- Detail Log—Records exacting information about changes resulting from actions recorded in the Event Log. This includes both updated values and previous values.

Enabling Audit Trail may result in a small performance hit due to the overhead of writing the entries to the database. It is recommended that you periodically archive the Audit Trail database so that it does not become too large.

Audit Trail is enabled by default.

Note that the Audit Trail feature is available to Enterprise customers only. To enable, validate, or disable audit trail on your Clarity LIMS cloud instance, contact Illumina Technical Support for assistance.

Customize the Term Used for Projects

You can configure an alias for the short and long, singular, and plural forms of the term Project, as displayed in the Clarity LIMS interface.

Renaming is achieved by configuring the following properties, using the omxprops-ConfigTool.jar tool at:

```
/opt/gls/clarity/tools/propertytool
```

Properties

- clarity.alias.project.short.singular—The short term for Project
- clarity.alias.project.short.plural—The short term for Projects
- clarity.alias.project.full.singular—The full term for Project
- clarity.alias.project.full.plural—The full term for Projects

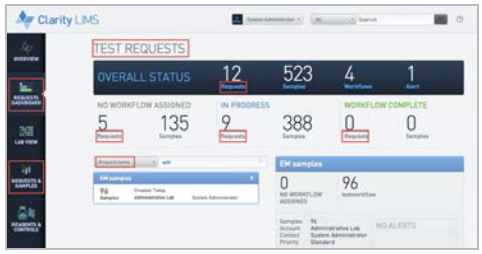
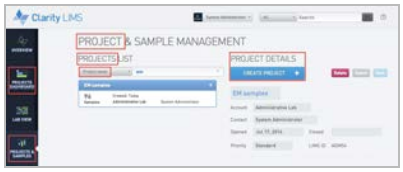
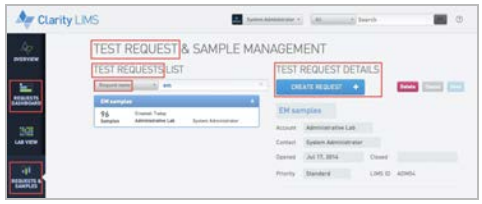
Rules for Alias

- clarity.alias.project.short.singular—Maximum of eight characters.
- clarity.alias.project.short.plural—Maximum of nine characters.
- If multiple words are used, capitalize each word (eg, Test Requests).
- Short form singular and plural aliases are truncated to eight characters and nine characters respectively. An ellipsis is used to indicate truncation.

How This Affects the Clarity LIMS Interface

In the following screenshots, the full aliases are set to Test Requests and the short aliases to Requests.

Select images to view larger size.

Default	Alias Configured
Projects Dashboard 	Test Requests Dashboard 
Project and Sample Management 	Test Request and Sample Management 

Configure Electronic Signatures

Clarity LIMS provides the ability to configure a step such that it requires sign-off by electronic signature (eSignature) before it can be completed.

- Steps that have eSignature enabled display an eSignature enforcement button on the Record Details screen, and require valid eSignature credentials (username and password) to be entered.
- Next Steps cannot be viewed until these credentials have been entered with eSignature signing permission.
- Until the step has been completed, any changes made to the step will again require an eSignature sign off.
- All eSignature events, successful or not, are recorded with the step and in the audit trail.

Who Can Sign

Permission to sign an eSignature is a role-based permission. For details, refer to *Configure Role-Based Permissions* on page 158.

By default, lab scientists cannot sign off on their own work.

Configuration Tool and Properties

eSignature enforcement is achieved by configuring the eSignature.Enabled and eSignature.RequiresDifferentReviewer properties, using the omxprops-ConfigTool.jar tool at:

```
/opt/gls/clarity/tools/propertytool
```

- eSignature.Enabled
  - Description: Enables/disables eSignature for step execution
  - Default value: false
  - Result: By default, eSignature enforcement on step execution is not enabled.
- eSignature.RequiresDifferentReviewer
  - Description: Determines whether the eSignature must be provided by someone other than the person executing the step.
  - Default value: true
  - Result: By default, if eSignature.Enabled is set to "true", the eSignature must be provided by someone other than the person executing the step.

To change the default settings for eSignature enforcement, contact the Clarity LIMS Support team for assistance.

Configuring Steps to Require an eSignature

When eSignature is globally enabled, you can enable/disable eSignature requirement for any step.

This setting is available on the Record Details milestone in master step/step configuration (accessible from the Lab Work configuration screen). For details, refer to *Record Details Milestone* on page 93.

By default, eSignature is enabled for steps.

When eSignature is enabled for a step:

- The Record Details screen shows the eSignature button and the Next Steps button is disabled.
- Selecting eSignature opens a dialog that requires valid eSignature credentials to be entered. Before proceeding to the next step, another user with the permission to sign eSignatures must sign in to the system and sign the eSignature.
- After valid eSignature credentials have been entered, the Next Steps button is enabled.
  Hovering over the eSignature button displays a tooltip showing who signed the step and when.

For Research Use Only. Not for use in diagnostic procedures.

About LabLink

LabLink is a sample submission portal that is part of Clarity LIMS. LabLink allows end users of the lab (ie, principal investigators, clinicians, external labs) to submit samples to the lab for processing. By allowing end users to submit samples through LabLink, the lab benefits in the following ways:

- Save time and avoid manual errors during sample accessioning by automatically receiving submitted sample information in Clarity LIMS.
- Easily configure LabLink to include sample submission templates and supplementary materials (ie, shipping instructions). End users of the lab use these materials during the sample submission process.
- Provide progress updates and publish files to end users of the lab.

Sign In to LabLink

To sign in to LabLink, open the LabLink URL associated with the Clarity LIMS instance for the lab.

On the Sign In screen, the following actions are available:

- Sign in to LabLink with a user ID and password.
- Request a user ID by selecting Request for a User ID.
- Request to reset a password by selecting Forgot Password?.
- Reset a password after multiple failed sign-in attempts.

Requesting a LabLink User ID

To request a LabLink user ID, complete the following steps:

1. On the Sign In screen, select Request for a User ID.
   The Request A New User ID form displays.
2. Complete the request form, which includes the following fields:
   - First Name
   - Last Name
   - Title [optional]
   - Email Address
   - Submitting Lab Name
3. Select the I agree with the above disclaimer and I'm not a robot checkboxes.
4. Select Request User ID.
   A User ID Requested success messages displays.

When a user ID request is submitted for approval or denial, an email notification can also be sent to the LabLink administrator. This feature is not active by default. Contact Support to activate this feature. Refer to *Create Projects and Add Samples* on page 183

Resetting the LabLink Password

LabLink passwords can be reset at any time. After multiple failed sign-in attempts, consider resetting the password.

If accessing LabLink through Lightweight Directory Access Protocol (LDAP), contact the on-site administrator to reset a password. LDAP users are denoted in the Type column of the Users tab.

To reset a LabLink password, complete the following steps:

1. On the Sign In screen, select Forgot password?.
   The Reset Password screen displays.
2. Enter the user ID or email address that was used to register.
3. Select the I'm not a robot checkbox.
4. Select Submit.
   A password reset email is sent.
5. Select the link provided in the email to access the Reset Password screen.
6. Enter the new password in the New Password and Confirm New Password fields. The new password must satisfy the following requirements:
   - Contain at least 12 characters
   - Contain at least one special character (# $ % ? ! @, etc.)
   - Contain at least one number
   - Contain at least one lowercase letter
   - Contain at least one uppercase letter
7. Select Reset Password.

When upgrading Clarity LIMS software to v5.4 (or later), you must provide an email address and reset your password.

Create Projects and Add Samples

The Projects tab is the landing page that displays after signing in to LabLink. The view of the Projects tab differs between administrators and collaborators:

- LabLink administrators—the Projects tab displays all projects submitted to the lab.
- Collaborators—the Projects tab displays only the projects submitted to the lab by the current collaborator.

To create a project and submit sample, go to the Projects tab and select Create.

The Create A New Project guided sample submission form displays. This form includes the following steps:

Step 1: Project Information

Enter general information for the project, as follows.

1. Enter the project name.
2. [Optional] Enter project notes for the lab.
3. Select Continue.

> By default, the Project Name and Project Notes fields are always shown. Other project fields can display, depending on the configuration of custom fields by the lab.

Step 2: Upload Samples

In this step, upload a sample submission document containing sample information for the lab.

> Download a sample submission document template from the Resource Materials tab (the lab administrator uploads the templates). Populate the template with the sample information.

1. Select Browse Document and locate the sample submission document. Select Open to upload the document.
2. After the document has been added, LabLink validates the headers and fields. If the headers and fields are not valid, error messages display.
3. After successfully uploading a document, a list of fields populated with sample information displays for review.
   - If the sample information is incorrect, replace the existing document by selecting Replace.
   - If the sample information is correct, select Continue.

Step 3: Upload Additional Documents

In this step, upload additional documents to share with the lab regarding this project. Skip this step if additional documents are not needed.

1. [Optional] Select Browse Documents and locate the document to be shared with this project submission. Select Open to upload the document.
2. Upload additional documents or select Continue.

Step 4: Review Project

In this step, review a summary of the project and uploaded documents before submitting the project and samples to the lab.

If the lab has configured a disclaimer for sample submission, the disclaimer is available for review.

1. After reviewing, select all required checkboxes.
   The Submit Project button becomes available.
2. Select Submit Project.
3. After the project has been successfully created and submitted to the lab, a confirmation message displays.
4. [Optional] Select View Confirmation to print an overview of the submitted samples.
   The Project Submission Confirmation page opens in a new tab. The page includes an overview of project information, lines for a signature and date of signature, and a list of all samples submitted.

This page can be printed and shipped to the lab with the submitted samples.

About Project Status

Once submitted, all projects are associated with one of the three following status types:

- Pending—The lab has not started processing the samples (or samples have not been received).
- Open—The lab has received the samples and the samples are being processed.
- Closed—The lab has completed processing the samples (or the lab has decided to close the project).

These three status types correlate to the status shown in Clarity LIMS. By changing the status of the project in Clarity LIMS, the status automatically changes in LabLink.

After samples are submitted to the lab, the project is listed with a Pending status until the lab changes the status in Clarity LIMS.

Search for and View Projects

To search for projects or samples in LabLink, enter a term in the search box and select one of the following criteria:

- Projects—The search is performed on all projects.
- Sample—The search is performed on all samples.

To view a single project, select a project in the project list.

Project Overview

By selecting a single project, the project opens in the Project Overview tab.

The Project Overview tab contains an overview of the project and options to complete the following actions:

- View / Add Notes—Select this link to view or add notes. All notes are tracked in this view with date and time. The latest note is included at the top of the list.

For Research Use Only. Not for use in diagnostic procedures.

The LabLink administrator uses this link to add notes. The latest note is shown as part of the project list in the Project tab.

- View Confirmation—Select this link to open the Project Submission Confirmation page in a new tab.
- Upload Documents—Select this button to add additional documents for the lab.

Samples

The Samples tab lists all samples submitted for a particular project. In this tab, 10 samples display at a time.

The LabLink administrator configures the visible columns in the Configuration tab. If the lab has configured the tab to provide progress updates, the Progress column is updated. Refer to *Publishing Progress* on page 187.

The submitted sample information can be modified in Clarity LIMS. Any changes in Clarity LIMS automatically update in LabLink.

For example, a LabLink user enters a paired end for the sequencing read type, but it should be single. A Clarity LIMS user can change this field in Clarity LIMS. The field automatically changes in LabLink.

Results and Documents

The Results and Documents tab displays two lists of documents.

- Project Documents
  - Any documents uploaded.
  - Download these documents to view.
- Sample Results and Documents
  - Any results or documents uploaded by the lab. To upload files, refer to *Publishing Files* on page 187.
  - Download these result files and documents to view.

Publishing Files and Progress

The lab carrying out the processing/assaying of the samples can publish the following, and make them available to collaborators:

- Files that are attached to steps and derived samples.
  Examples include the following use cases:
  - Publishing an image of an electropherogram for a sample that failed Bioanalyzer QC.
  - Publishing small files such as AB1 files that result from Capillary Electrophoresis sequencing.

> It is not recommended to publish large NGS or microarray derived data (such as FASTQ or VCF files) through LabLink. Although technically possible, BaseSpace Sequence Hub works much better for these large files.

- Custom fields that are defined and populated on samples in Clarity LIMS. For example, a field that tracks the progress of the samples.

Publishing Files

The only way to publish a file is by using the Clarity LIMS API. To publish documents to LabLink, run a custom script in Clarity LIMS at the end of a step.

For example, at the end of a Bioanalyzer QC step, if individual electropherogram images are available, they may be published and made available immediately in LabLink. See the API & Database documentation for an example script that publishes files to LabLink.

Files published to LabLink are available under the Results and Documents tab of a LabLink project, in the Sample Results and Documents section.

The Sample Results and Documents section of the page has three elements for each row:

- Document Name—The name of the file that has been stored in Clarity LIMS and published.
- Sample Name—The name of the sample associated with the published file.
- Download Link—Select this link to download a copy of the file from LabLink.

For example, if all samples in a project participate in a step, publishing a file associated with that step causes the file to also be associated with all samples in that step.

Publishing a step-level file may have undesired consequences. Imagine a single step that was run on samples from two separate LabLink projects. If that step includes a step-level file that is published, it is available to both LabLink projects.

Depending on the contents of the file, publishing might lead to one collaborator seeing sample data that relates to another collaborator.

> Only publish step-level files if they are associated with samples in a single LabLink project.

Publishing Progress

The lab can publish custom fields that are defined and populated on samples in Clarity LIMS. Collaborators in LabLink can then see these custom fields.

This functionality depends on how Clarity LIMS is configured. For example, assume that the sample-level custom field called Progress should be visible in Clarity LIMS.

1. Define the Progress custom field in Clarity LIMS, including field type, field options, and additional options.
2. Make the Progress custom field visible in LabLink.

a. Navigate to the Custom Fields screen from the Configuration menu.
b. Select the Progress checkbox for the field to be visible in LabLink.

3. When samples are first submitted to LabLink, the Progress field is empty.
4. When the lab receives the samples, they may set the Progress field to have the Awaiting QC value for all samples in the project.
5. When the samples have completed the QC steps, the lab may update the Progress field with different values depending on the success or failure of QC.
6. As the samples move through the workflow, lab technicians update the Progress field as required. These updates provide the collaborator with insight into what is happening in the lab, on a per-sample basis. You can configure a script that automatically updates the Progress field, eliminating the need for manual updates by lab technicians. For example, configure the following automation command line that uses Clarity LIMS Lab Logic Toolkit to update the Progress field.

```
bash -l -c "/opt/gls/clarity/bin/java -jar /opt/gls/clarity/extensions/ngs-
common/v5/EPP/ngs-
extensions.jar -i {stepURI:v2:http} -u {username} -p {password}
script:evaluateDynamicExpression - t
true -h false -exp '\
submittedSample.::Progress:: = ::Awaiting QC::; \
' -log {compoundOutputFileLuid0}"
```

If the value of the Progress field is long, it may be truncated in LabLink. However, the full value can be obtained by hovering the mouse over the truncated value.

Widening the browser window may show more of the field, but truncation may still occur.

Email Notifications for Notes

Project notes are made through the Project Overview tab. Sample notes are made through the project Sample tab.

When this feature is active, LabLink sends an email notification if a new project note or sample note is created.

The email notification is sent to the owner of the project/sample or to the distribution list configured in properties (lablink.admin.email), depending on who saved the note.

- Notes saved by the project/sample owner produce email notifications sent to the distribution list.
- Notes saved by anyone other than the project/sample owner produce email notifications sent to the project/sample owner.

Project note email notifications contain a link to the project details Project Overview page. Sample note email notifications contain a link to the project details Sample page.

This feature is not active by default. To receive email notifications for notes, send a request to the Support team.

For Research Use Only. Not for use in diagnostic procedures.

Configuration

The Configuration tab is only available to LabLink administrators. This tab consists of the following sections:

- Resource Materials
- Custom Fields
- Disclaimers
- Contact Us

If there are any configuration errors, a red dot appears on the Configuration tab and the section that requires attention.

Resource Materials

In LabLink, there are two types of resource materials:

- Sample submission templates
- Supplementary documents

The administrator can manage these resource materials to assist end users of the lab during the sample submission process. LabLink allows the admin to upload up to 20 resource materials.

To add new templates or documents, a LabLink administrator can use the following steps:

1. Select Create.
2. Provide a name and description for the document.
3. Select the resource type.
4. Upload the resource file.

By selecting the resource type, the document is added to the appropriate location on the Resource Material tab.

Custom Fields

The Custom Fields section of the Configuration tab displays all custom fields that have been configured in Clarity LIMS for projects and submitted samples.

A LabLink administrator can choose to display custom fields by selecting the checkbox next to the custom field.

- The project custom fields display during the sample submission process.
- The sample custom fields display on the Samples tab.
- The client custom fields display during the create new user and request a new user ID processes.

For Research Use Only. Not for use in diagnostic procedures.

Disclaimer

The Disclaimer section allows the LabLink administrator to manage the disclaimers that display for the following processes:

- Requesting a new user ID
- Creating a project for sample submission

Select Edit to modify the disclaimer text. The character limit is 4096 for each disclaimer.

Contact Us

The Contact Us section allows the LabLink administrator to manage the contact us information that displays for the end users of the lab. Select Edit to modify the contact us information.

LabLink Users

The Users tab is only available for LabLink admins. This tab displays a list of pending requests and all users. If there are any pending requests, a red dot appears on the Users tab.

In the All Users section, only approved users display. The account status for each user shows as Active or Deactivated.

Review User Request

Pending requests require a LabLink admin to approve or deny the request. To approve or deny the request, complete the following steps:

1. Select the name of the pending request.
   A Review User Request window displays with the option to approve or deny.
2. Approve or deny the pending request.
   - To approve, update any of the prepopulated fields and provide a user ID. When all fields are correct, select Approve and an email is sent to the requester stating that the request has been approved.
   - To deny, select Deny and provide the reason for the denial. After entering in the reason, select Deny and an email is sent to the requester with the reason for denial.

Deactivate a User

To deactivate a user, edit the user information as follows:

1. Select the name of a user.
   The User Information screen displays.
2. Select Edit.
3. Deselect the Active checkbox (under Account Status) to deactivate the user.

For Research Use Only. Not for use in diagnostic procedures.

4. Save changes.

Create a New User

Create a new user from the Users tab:

1. Select Create.
   The Create A New User screen displays.
2. Define the user information, which includes the following fields:
   - First Name
   - Last Name
   - Title [optional]
   - Phone Number
   - Email Address
   - User ID
   - Role
   - Submitting Lab Name (Account).
3. Select Create.

Roles and Permission

LabLink offers the following two roles:

- An admin role grants access to all submitted projects and samples, resources materials, users, configuration, and the Contact Us tab. The LabLink admin role is equivalent to a system administration role.
- A collaborator role grants access to the submitted projects and samples from that user, available resource materials, and the Contact Us tab. The collaborator role in LabLink does not grant access to Clarity LIMS.

All users with a collaborator role in Clarity LIMS appear in the LabLink All Users list.

Resource Materials & Contact Us

The Resource Materials tab provides LabLink users with resource materials from the lab. The lab can upload different types of resources from the Configuration tab. There are two types of resource materials:

- Sample Submission Templates—Templates that can be used to submit samples. Each template contains headers and custom fields that are required for each sample.
- Supplementary Materials—Documents that can be used as part of the sample submission process.

The Contact Us tab provides LabLink users with information on how to contact the lab. The lab can update this information through the Configuration tab.

For Research Use Only. Not for use in diagnostic procedures.

Administration

This section provides information and instructions to support Clarity LIMS and administration tasks. Topics covered include database cleanup, LDAP integration, logging, and password management. Instructions for working with the Config Slicer tool and for troubleshooting Automation Worker nodes are also provided. If you require assistance with Clarity LIMS administration, contact the Clarity LIMS Support Team.

Creating Encrypted Passwords

Saving passwords in encrypted format is recommended. Use the omxprops to do this action.

To encrypt a password, use the following command:

```
# java -jar /opt/gls/clarity/tools/propertytool/omxprops-ConfigTool.jar
encryptPassword <password>
```

This command returns a text string resembling the following example:

```
RqHL5XpY0NStVRjd+BngRQ==
```

Set the encrypted password by enclosing the text string in the `ENC()` wrapper.

Consider the following examples:

- When setting an encrypted password in a configuration file:

```
rabbitmq.password=ENC(RqHL5XpY0NStVRjd+BngRQ==)
```

- When using the property tool to set an encrypted password:

```
# java -jar /opt/gls/clarity/tools/propertytool/omxprops-ConfigTool.jar set -y
ftp.password 'ENC(RqHL5XpY0NStVRjd+BngRQ==)'
```

- Using `ENC()` is not needed when setting the password in Automation Worker:

```
informaticsClientTarget.sftpPassword=RqHL5XpY0NStVRjd+BngRQ==
```

Using Clarity LIMS with your LDAP Server

If you use, or would like to use, an LDAP server to consolidate directory services, it is possible to integrate LDAP with Clarity LIMS.

The Clarity LIMS LDAP solution allows for the following features:

- Username and password authentication against LDAP to govern access to Clarity LIMS.
- Ongoing unidirectional synchronization of user information (such as first name, last name, title, phone, fax, and email) from LDAP to Clarity LIMS. For example, if your telephone number is changed in the LDAP directory, the information is pushed down to Clarity LIMS, keeping contact information current.

For Research Use Only. Not for use in diagnostic procedures.

- Automated unidirectional provisioning of user accounts from LDAP to Clarity LIMS. For example, adding a user to a particular group within the LDAP directory automatically results in a local account with LDAP authentication being added to Clarity LIMS.

Providing Information about your LDAP Implementation

Our Field Application Specialist (FAS) team meets with you to discuss the current LDAP implementation. In preparation for this meeting, collect the following information:

- The type of provisioning to use for synchronizing Clarity LIMS with LDAP (automatic or manual).
- A list of the LDAP attributes the current system uses to record the following user properties: first name, last name, title, phone number, fax number, and email address.

When integrating Clarity LIMS with LDAP, the LIMS database and the LDAP directory remain as separate and distinct entities.

Supported LDAP servers

Clarity LIMS is tested with the following LDAP servers:

- ApacheDS 1.5 and later
- Microsoft Active Directory (Windows Server 2003 or later)
- OpenLDAP 2.3.35 and later

Access and Changes

While user provisioning and authentication are handled with LDAP, a Clarity LIMS system administrator completes the following steps:

1. Determine the level of access required.
2. Modify the user account within Clarity LIMS to provide that access.

After an LDAP integration with Clarity LIMS is established, all changes to user profiles must be made from the LDAP server.

Provisioning Users

Only automatic user provisioning is available.

With automatic user provisioning, Clarity LIMS users are created automatically by a provisioning tool that periodically synchronizes the LDAP server with the LIMS.

To make use of the LDAP directory services, Clarity LIMS maps to specific LDAP attributes within a defined schema.

However, the directory structure used can vary among installations. Our Field Applications Specialist (FAS) team work with you to complete the following items:

For Research Use Only. Not for use in diagnostic procedures.

- Analyze a specific LDAP solution and directory organization or assist with the selection and initial configuration of an LDAP service.
- Discuss the user elements that to synchronize between the LDAP service and Clarity LIMS systems.
- Configure LDAP to connect to your Clarity LIMS systems.

Caching User Authentication Results from your LDAP Server

User authentication is handled in Clarity LIMS.

In previous versions of Clarity LIMS, a few customers reported slow response time for the REST API when using LDAP users for authentication. As of Clarity LIMS v5.2.x / v4.3.x, the REST API response time has improved by introducing a new feature that caches user authentication results through a new property (api.session.timeout).

To make use of the new feature, do the following actions:

- Make sure that api.session.timeout property is set.
- Include the HTTP Connection and Authorization request headers and session cookie in the HTTP request.

Setting the api.session.Timeout Property

Stored in the Clarity LIMS database table, the `api.session.timeout` property allows you to specify how long a user session should persist, after they have been authenticated.

This property is set during installation or upgrade of Clarity LIMS. The default value is 5 minutes.

If necessary, update the value using the `omxprops-ConfigTool.jar` tool at the following location:

```
/opt/gls/clarity/tools/propertytool
```

For example:

```
$ java -jar /opt/gls/clarity/tools/propertytool/omxprops-ConfigTool.jar
set -y api.session.timeout '15'
```

For this configuration to take effect, stop and restart Tomcat:

```
service clarity_tomcat stop
service clarity_tomcat start
```

Including the HTTP Authorization Request Header and Session Cookie

To persist user authentication, the HTTP request must contain the following HTTP request headers:

- Request HeaderConnection: Keep-Alive
  - Authorization: Basic <credentials>

The HTTP request headers are required for the initial request and for any subsequent request to get a valid JSESSIONID. Additional scenarios are described in the following table.

To make sure that a valid authenticated session is provided if the cookie in the request has expired, also provide the following JSESSIONID cookie:

- CookieJSESSIONID=<a valid JSESSIONID from the initial request>

The following table lists the various combinations of HTTP Authorization request header and JSESSIONID cookie and their expected result. It assumes that the HTTP Connection request header is provided for all scenarios.

Clarity LIMS version	Authorization	JSESSIONID	Expected Result
v5.0.x and v5.1.x	Present	Absent	Open API performs the user authentication depending on whether the account is in the database or LDAP server, and responds with requested resources.

For Research Use Only. Not for use in diagnostic procedures.

Clarity LIMS version	Authorization	JSESSIONID	Expected Result
v5.2.x and later, and v4.3.x	Present	Present (Valid)	Open API does not perform the user authentication and responds with requested resources.
	Present	Present (Invalid)	Open API performs the user authentication depending on whether the account is in the database or LDAP server, and responds with requested resources.
	Absent	Present (Valid)	Open API does not perform the user authentication and responds with requested resources.
	Absent	Present (Invalid)	Open API responds with HTTP Status 401 - Unauthorized.
	Absent	Absent	Open API responds with HTTP Status 401 - Unauthorized.

Using the LDAP Checker Tool

This section explains how to use the LDAP Checker tool a script (`ldap-checker.jar`) that checks and reports on an LDAP configuration. Instructions for use are also provided in the `README.txt` file that accompanies the tool.

The ldap-checker script is included with the Clarity LIMS installation and is available at the following location:

`/opt/gls/clarity/tools/ldap-checker`

The ldap-checker script performs numerous checks of the LDAP configuration and reports on any incorrect items found.

For Research Use Only. Not for use in diagnostic procedures.

Script Properties

Point the script to one or more files containing (at a minimum) the database connection properties. Alternatively, set these properties from the command line.

The script loads properties from the following sources and in the following order:

1. Any JDBC properties files specified with `-f` (see the table for options).
   If multiple properties files specify the same property, the last file is used.
2. Any Java system properties specified on the command line using `-D<propertyName>=<propertyValue>`.
   Properties specified on the command line are only checked if they do not appear in the properties files.
3. The properties table in the database.
   The properties table is only checked if the same property is not already specified in the properties file or on the command line.

After the script has the basic database connection properties, it loads further settings from the corresponding Clarity LIMS database.

The following JDBC properties are required:

- jdbc.driverClassName
- jdbc.url
- jdbc.username
- jdbc.password

Options:

-f	--files <f>	Property files to process
-h	--help	Show usage information
-u	--users <u>	Usernames to check

Run the Script

1. Change to the directory containing ldap-checker tool:

```
/opt/gls/clarity/tools/ldap-checker
```

2. Run the script. To specify a properties file, use the following example:

```
java -jar ldap-checker-<version>.jar -f database.properties
```

Example Properties File

The tool includes an example `database.properties` file. This example shows a properties file that is specified with the `-f` option.

The following options are available:

- Edit this file and use it.
- Point the tool to another file that contains the required properties:

```
<jboss>/server/default/conf/<propertiesfile>
```

- Provide properties on the command line, using `-D`.

  For example:

```
-Djdbc.url=<url to properties file>
```

Examples

Example 1: Using SSL

Specify and provide the path to the keystore:

```
java -Djavax.net.ssl.trustStore=/path/to/keystore -jar ldap-checker-
<version>.jar -f database.properties
```

Example 2: Checking Users

To check a set of specific users (even those users that have not been provisioned), use the following script:

```
java -jar ldap-checker-<version>.jar -u usertocheck -f database.properties
```

Overriding Properties

To override properties that are typically loaded from the properties table, use command-line system properties or one or more properties files.

Using system property (`-D` options must be specified before the `-jar` option):

```
java -Djavax.net.ssl.trustStore=/path/to/keystore -Dldap.managerPass=mypassword
-jar ldap-checker-<version>.jar -u usertocheck -f database.properties
```

Using multiple properties files:

```
java -jar ldap-checker-<version>.jar -u usertocheck -f database.properties
custom-ldap.properties
```

In this example, `Custom-ldap.properties` might resemble the following:

```
ldap.managerDn=CN=GLS Admin,CN=Users,DC=gls,DC=lan ldap.managerPass=mypassword
```

Receiving & Decrypting SaaS Backup Data

If necessary, the Clarity LIMS Support team can provide a backup of your Clarity LIMS data. The data are contained in an encrypted file, which can be downloaded from a secure SFTP server.

To receive the backup data file, provide the Clarity LIMS Support team with a GNU Privacy Guard (GPG) public key.

For instructions on generating a GPG public key, see the following documentation:

- For Microsoft® Windows®, refer to *Creating a Certificate* on the Gpg4win Compendium website.

For Research Use Only. Not for use in diagnostic procedures.

- For Linux® or Mac®, refer to *Generating a New GPG Key* on the GitHub website.

After the Clarity LIMS Support team has received the GPG public key, they do the following actions:

- Create a backup file encrypted with the key.
- Place the backup file on the LIMS SFTP server at sftp.clarity-lims.com.
- Provide a username and password so you can access your data. The backups are added to the FTP server weekly.

After downloading the backup file, there are several tools available to decrypt the data.

- For Windows, use the gpg4win tool. For details, refer to the Gpg4win Compendium website.
- For Mac/Linux, use the GPG command on the command line. For details, refer to *Encrypting and Decrypting Documents* on the GNU Privacy Handbook website.

About Config Slicer

The Config Slicer tool is used to move small incremental configuration changes, contained in a configuration set, between Clarity LIMS systems. For example, it moves changes between a test system and a production system.

This configuration tool provides granular export/import functionality that allows the management of configurations that support experimental workflows.

Use this tool to back up, copy, deploy, and restore configuration sets. By making small incremental changes, make sure that the modifications made to the production system are minimal.

Review the following key concepts:

- Configuration set—This item may be created by the Clarity LIMS Support team or by the customer. It comprises the items (know as entities) that are added to a Clarity LIMS system to allow for customization for a particular scientific experiment or workflow. The Illumina NGS Extensions Package is a good example. Refer to *Supported Entities* on page 201.
- Configuration manifest file—This text file determines the configuration set to be exported from a system. The manifest file does not contain the actual configuration data. It only drives the extraction of configuration from a system.
- Configuration package file—This XML file contains the top-level entities selected by the configuration manifest file, plus any related child entities. For example, for process types, it includes process type UDFs, process templates (protocols), and output UDFs.

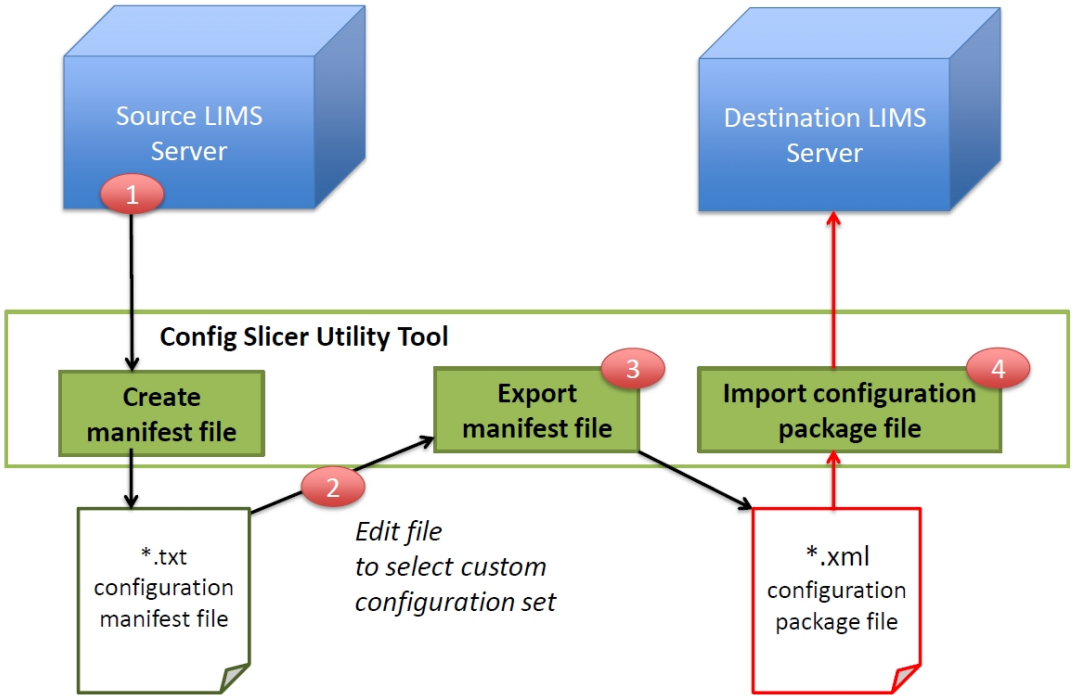
Config Slicer Export/Import Process Overview

The Config Slicer tool uses an export/import process to transfer configuration sets from a source to a destination server. This process breaks down into the following tasks:

1. On the source Clarity LIMS server, use the Config Slicer tool to create a configuration manifest file.
2. Edit the manifest file so that only the required custom configuration set is preserved.

For Research Use Only. Not for use in diagnostic procedures.

3. Use the Config Slicer tool to export the edited manifest file to a configuration package file.
4. On the destination Clarity LIMS server, use the Config Slicer tool to import the configuration package file into the system.



A configuration package file can be imported into multiple systems. Use this feature to create and import multiple custom configuration sets, such as the Illumina TruSeq integration. This functionality also provides the Clarity LIMS Support team with a scalable way to keep up with constantly changing protocols.

Supported Entities

A configuration set comprises the entities added to a Clarity LIMS system that allow for customization of the system for a particular scientific experiment or workflow. The following entities are currently supported by the Config Slicer tool:

- Sample UDFs and UDTs
- Container UDFs and UDTs
- Project UDFs and UDTs
- Artifact groups (experiments)
- Reagent types
- Control types

For Research Use Only. Not for use in diagnostic procedures.

- Reagent kits
- Process types (any configured processes – for example, Pool Samples and Add Multiple Reagents)
  - Process UDFs and UDTs
  - Output UDFs
- Process templates - UDFs, UDTs, and parameter strings only (other entities such as instruments and researchers are not supported)
- Protocols
- Workflows

When performing custom manifest generation by workflow, protocol, or process type, the following entities are not exported: Sample, Container, Project UDTs, and UDFs for Project. Account (Lab) and Client (Researcher) UDFs are never exported by config slicer. These are known issues.

Config Slicer does not export/import nonstep automation, nor does it preserve the order of protocols.

Tools and Requirements

When working with Config Slicer on the Clarity LIMS application server, there are no additional prerequisites. The latest version of the `config-slicer.jar` file is installed as part of Clarity LIMS on the Clarity LIMS server. In a default installation, find the file in the following location:

```
/opt/gls/clarity/tools/config-slicer
```

To work with Config Slicer on a machine other than the Clarity LIMS server, do the following:

1. Make sure that Java is installed.
2. Copy the `/opt/gls/clarity/tools/config-slicer` directory, and its contents, from the Clarity LIMS server to the machine.
   The config-slicer directory and the config-slicer package should contain the following:
   - `config-slicer-<version>.jar`
   - `libs` subdirectory (which includes all the libraries referenced by `config-slicer-<version>.jar`, including `groovy-all-2.4.8.jar`)
   - `upgrade-config-slice.jar`

About Config Slicer

The Config Slicer tool is used to move small incremental configuration changes, contained in a configuration set, between Clarity LIMS systems. For example, it moves changes between a test system and a production system.

This configuration tool provides granular export/import functionality that allows the management of configurations that support experimental workflows.

Use this tool to back up, copy, deploy, and restore configuration sets. By making small incremental changes, make sure that the modifications made to the production system are minimal.

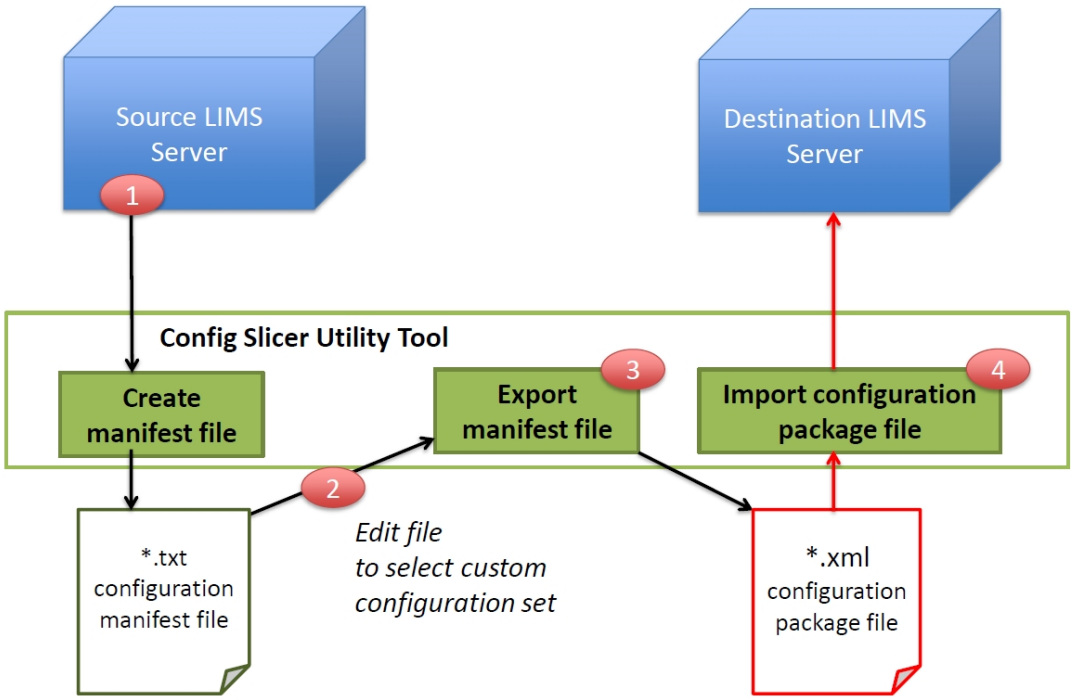
Review the following key concepts:

- Configuration set—This item may be created by the Clarity LIMS Support team or by the customer. It comprises the items (know as entities) that are added to a Clarity LIMS system to allow for customization for a particular scientific experiment or workflow. The Illumina NGS Extensions Package is a good example. Refer to *Supported Entities* on page 204.
- Configuration manifest file—This text file determines the configuration set to be exported from a system. The manifest file does not contain the actual configuration data. It only drives the extraction of configuration from a system.
- Configuration package file—This XML file contains the top-level entities selected by the configuration manifest file, plus any related child entities. For example, for process types, it includes process type UDFs, process templates (protocols), and output UDFs.

Config Slicer Export/Import Process Overview

The Config Slicer tool uses an export/import process to transfer configuration sets from a source to a destination server. This process breaks down into the following tasks:

1. On the source Clarity LIMS server, use the Config Slicer tool to create a configuration manifest file.
2. Edit the manifest file so that only the required custom configuration set is preserved.
3. Use the Config Slicer tool to export the edited manifest file to a configuration package file.
4. On the destination Clarity LIMS server, use the Config Slicer tool to import the configuration package file into the system.



For Research Use Only. Not for use in diagnostic procedures.

A configuration package file can be imported into multiple systems. Use this feature to create and import multiple custom configuration sets, such as the Illumina TruSeq integration. This functionality also provides the Clarity LIMS Support team with a scalable way to keep up with constantly changing protocols.

Supported Entities

A configuration set comprises the entities added to a Clarity LIMS system that allow for customization of the system for a particular scientific experiment or workflow. The following entities are currently supported by the Config Slicer tool:

- Sample UDFs and UDTs
- Container UDFs and UDTs
- Project UDFs and UDTs
- Artifact groups (experiments)
- Reagent types
- Control types
- Reagent kits
- Process types (any configured processes – for example, Pool Samples and Add Multiple Reagents)
  - Process UDFs and UDTs
  - Output UDFs
- Process templates - UDFs, UDTs, and parameter strings only (other entities such as instruments and researchers are not supported)
- Protocols
- Workflows

When performing custom manifest generation by workflow, protocol, or process type, the following entities are not exported: Sample, Container, Project UDTs, and UDFs for Project. Account (Lab) and Client (Researcher) UDFs are never exported by config slicer. These are known issues.

Config Slicer does not export/import nonstep automation, nor does it preserve the order of protocols.

Tools and Requirements

When working with Config Slicer on the Clarity LIMS application server, there are no additional prerequisites. The latest version of the `config-slicer.jar` file is installed as part of Clarity LIMS on the Clarity LIMS server. In a default installation, find the file in the following location:

```
/opt/gls/clarity/tools/config-slicer
```

To work with Config Slicer on a machine other than the Clarity LIMS server, do the following:

1. Make sure that Java is installed.

For Research Use Only. Not for use in diagnostic procedures.

2. Copy the `/opt/gls/clarity/tools/config-slicer` directory, and its contents, from the Clarity LIMS server to the machine.
   The config-slicer directory and the config-slicer package should contain the following:
   - `config-slicer-<version>.jar`
   - `libs` subdirectory (which includes all the libraries referenced by `config-slicer-<version>.jar`, including `groovy-all-2.4.8.jar`)
   - `upgrade-config-slice.jar`

Managing Configurations with Config Slicer

Command-Line Options and Usage

Refer to *Import/Export Modes* on page 212 and *Guidelines and Semantics for Creating Manifest Files* on page 211.

Option	Description
-a,--apiuri <apiuri>	The Clarity LIMS REST API base URI (ends in /api) (or --server must be provided)
-k,--package <package file>	File to be imported from or exported to (Required if operation is import, importAndOverwrite*, export, or validate). If file is not local, a full path is required.
-f,--force <force> *	Force update without prompt when running in importAndOverwrite mode (Optional)
-m,--manifest <manifest>	Manifest file (Required if operation is export or example). If file is not local, a full path is required.
-o,--operation <operation>	The operation mode for the Config Slicer tool. Options are import, export, validate, example, importAndOverwrite, and custom (Required)
-p,--password <password>	In Clarity LIMS REST API:
-pr,--protocols <protocols>	The protocols to include in the custom manifest (Optional)
-pt,--processTypes <processTypes>	The process types to include in the custom manifest (Optional)
-s,--server <server>	The Clarity LIMS REST API server (or --apiuri must be provided)

For Research Use Only. Not for use in diagnostic procedures.

Option	Description
-S,--Strict	Strict mode for import (fail fast - default mode is best-effort) (Optional)
-u,--username <username>	The Clarity LIMS REST API username (Required)
-w,--workflows <workflows>	The workflows to include in the custom manifest (Optional)

* The importAndOverwrite option lets Config Slicer update existing configuration, rather than creating a configuration. This option is only available in Clarity LIMS 3.4.

Usage

```
-o  <import|importAndOverwrite|export|validate|example|custom> [-m <manifest file>] [-k <package file>] [-w <workflows>] [-pr <protocols>] [-pt <process types>] [ -s <server> | -a <API root URI> ] -u <username> -p <password>
```

EXPORT: Creating a Configuration Package File

Prerequisites

- Created and validate a configuration set on the source server.
- Have access to the Config Slicer tool and the `libs` subdirectory.

Step 1: Create Configuration Manifest File

Create *Simple manifest file:* on page 206 or *Custom manifest file:* on page 207.

Simple manifest file:

1. On the source server, copy and paste following code to the command line. Edit the variables (version, server IP address, username, password, and manifest file name) to match those items in the system.

```
java -jar config-slicer-<version>.jar -o example -s <server> -u <username> -p <password> -m <manifest-filename>
```

   A command with the variables filled in might look like this:

```
java -jar config-slicer-3.0.13.jar -o example -s glsserver -u admin -p glspass -m goldenconfig.txt
```

2. This step produces a manifest file containing information about the entire system configuration. For best practice, copy this file and rename the copy in a way that reflects the configuration (we'll use `newconfiguration.txt` for this example). Use the copied file for the next steps.

For Research Use Only. Not for use in diagnostic procedures.

A manifest file is used as an intermediary step to produce an XML configuration package file.

The manifest file is only relevant to the data that exists in the system at the time it is created. Discard it after creating the configuration package file or save the manifest file for historical auditing purposes. It can provide a record of a known working configuration set on a particular system.

Custom manifest file:

To create a manifest file for only specific workflows, protocols, or process types, follow the steps outlined previously, using `-o custom` instead of `-o example`.

- When using this operation provide additional parameters (`-w`, `-pr`, and/or `-pt`), specify the exact entities for which to create a manifest.
  - For example:

```
java -jar config-slicer-<version>.jar -o custom -s <server> -u <username> -p
<password>
-m <manifest-filename> -w <workflow name> -pr <protocol name> -pt <process-type
name>
```

- Specifying every option is not required. It is also possible to specify more than one of each kind. For example, create a manifest file for a workflow with the following command:

```
java -jar config-slicer-3.0.13.jar -o custom -s glsserver -u admin -p glspass
-m workflowManifest.txt -w 'Nextera DNA for HiSeq'
```

- Or for two protocols like so:

```
java -jar config-slicer-3.0.13.jar -o custom -s glsserver -u admin -p glspass
-m protocolsManifest.txt -pr 'DNA Initial QC' -pr 'Nextera DNA Library Prep'
```

- Or for two process types and a protocol with this command:

```
java -jar config-slicer-3.0.13.jar -o custom -s glsserver -u admin -p glspass
-m processTypesManifest.txt -pt 'Blood Extraction' -pt 'Qubit QC (DNA) 4.0' -pr
'Illumina SBS (HiSeq GAIIx)'
```

Step 2: Edit Manifest File

The next step is to edit the manifest file, removing unnecessary information and preserving only the custom configuration to import into the destination system.

Example 1: In this example, everything is deleted from the manifest file, except for the two new process types to export.

```
# Selection for ProcessTypes
unit.ProcessTypes=\
Illumina Sequencing,\
BCL Conversion and Demultiplexing
```

Example 2: In this example, the manifest file contains definitions for some new reagent types:

```
# Selection for ReagentTypes
```


For Research Use Only. Not for use in diagnostic procedures.

```
unit.ReagentTypes=\
Index 1 (ATCACG),\
Index 2 (CGATGT),\
Index 3 (TTAGGC),\
Index 4 (TGACCA),\
Index 5 (ACAGTG),\
Index 6 (GCCAAT),\
Index 7 (CAGATC),\
Index 8 (ACTTGA),\
Index 9 (GATCAG),\
Index 10 (TAGCTT),\
Index 11 (GGCTAC),\
Index 12 (CTTGTA)
```

Step 3: Export to XML Configuration Package File

- Copy and paste the following code onto the command line. Edit the variables (version, server IP address, username, password, and manifest and package file names) as required.

```
java -jar config-slicer-<version>.jar -o export -s <server> -u <username> -p
<password>
-m <manifest-filename>.txt -k <configuration-package-file>.xml
```

- An edited command might look like the following example:

```
java -jar config-slicer-3.0.13.jar -o export -s glsserver -u admin -p glspass
-m newconfiguration.txt -k newconfiguration.xml
```

This step generates a data file in an XML format (`newconfiguration.xml` in our example) that is compliant with the Rapid Scripting API.

IMPORT: Installing a Configuration Package File

Prerequisites

- A configuration package file has been exported. This example uses a file named `newconfiguration.xml`.
- Access to the Config Slicer tool on the destination server has been granted.
- There are no in progress steps for any of the protocols that are going to be sliced in, otherwise the import of the protocol fails.

For Research Use Only. Not for use in diagnostic procedures.

Step 1: Import Configuration Package File

- On the destination server, copy and paste the following code to the command line. Edit the variables (version, package file name, server IP address, username, and password) as required.

```
java -jar config-slicer-<version>.jar -k <configuration-package-file>.xml -o
import -s <server> -u <username> -p <password>
```

- or -

```
java -jar config-slicer-<version>.jar -o importAndOverwrite -k <configuration-
package-file>.xml -s <server> -u <username> -p <password>
```

- A command with the variables filled in might look like this example:

```
java -jar config-slicer-3.0.13.jar -o import -k newconfiguration.xml -s
glsserver
-u admin -p glspass
```

- or -

```
java -jar config-slicer-3.0.13.jar -o importAndOverwrite -k newconfiguration.xml
-s glsserver -u admin -p glspass
```

About Duplicate Entities

If any of the configuration entities that are about to import, exist in the destination system, Config Slicer either logs a warning or attempts to update them. It depends on the mode being run (refer to *Import/Export Modes*).

If Clarity LIMS has maintained an internal record of deleted items, the previous information may also apply to deleted entities. This situation may occur if those entities have created outputs that currently still exist in the system.

- When running in import mode, entities that exist and are different from the version in the package have a warning and full diff logged.
- When running in importAndOverwrite mode, Config Slicer attempts to update entities that exist and are different from the version in the package.
  - In this scenario, back up configuration package containing copies of the updated entities before they were changed is saved to the directory where the configuration package is located. If that directory is not writable, the backup package is saved to the same directory as the log file.
- If the version in the package is identical to the version on the server, no errors are logged and Config Slicer considers that entity successfully imported.

To avoid changing existing configuration (which could possibly break historical data), another option is manually renaming the old entities. Add an extension or a prefix and continue with importing the new configuration package.

Step 2: Validate the Import

Use the following methods to validate whether an import has completed successfully:

Check the Import Log

For each specific type of configuration that is being imported (eg, container types, process types, workflows), Config Slicer logs a set of messages. The messages look similar to the following examples:

```
2015-01-16 18:45:13,046  INFO - Found 4 Container Types in configuration
package, importing now.
2015-01-16 18:45:13,614  INFO - Summary of Container Types:
   Newly imported:
   Container Type 'BioAnalyzer DNA 1000 Chip'
   Container Type 'BioAnalyzer DNA High Sensitivity Chip'
   Container Type 'BioAnalyzer RNA Nano Chip'
   Container Type 'BioAnalyzer RNA Pico Chip'
  Imported and updated (diffs in log): None
   Already existing and identical (no update performed): None
   Not imported (due to errors or existing entities): None
```

- Before it begins to process a specific entity, the file logs how many entities were found. Any errors or warnings about this set of entities always appear between `Found 4 $Entities` and `Summary of $Entities`.
- Every entity that is found in the configuration package always appears in the summary, in one category or another. If a scenario occurs where this isn't true, or where the initial count of entities does not match the number in the summary, something has gone wrong and a bug report should be filed.

Validate with Config Slicer

Running Config Slicer with the validate operation checks every entity in the package to see if it exists on the destination server. It reports results in a format similar to the log format shown previously.

Run the validate operation before or after importing:

- Before importing—checks if there could be any problems when importing a configuration from a package. This feature is its primary use as it makes sure that during import, "`configuration exists in package but not on server`" is not considered an error case.
- After importing—makes sure that the results are what was expected.

Example of validate output:

```
2015-01-16 15:42:31,174  INFO - Found 4 Container Types in configuration
package, validating now.
2015-01-16 15:42:31,706  INFO - Summary of Container Types:
```

```
Do not exist: None
Exist and are identical:
Container Type 'BioAnalyzer DNA 1000 Chip'
Container Type 'BioAnalyzer DNA High Sensitivity Chip'
Container Type 'BioAnalyzer RNA Nano Chip'
Container Type 'BioAnalyzer RNA Pico Chip'
Exist and are different (diffs in log): None
```

Check Configuration on the Destination Server

The ultimate test of whether configuration has imported successfully is to check the configuration on the destination server itself. Make sure it looks and behaves as expected.

Configuration can be checked either via the Configuration screen in the Clarity LIMS user interface, or via the configuration endpoints in the API.

Guidelines and Semantics for Creating Manifest Files

Top-level Entities

- To be included in a configuration package file, the top-level entities of the custom configuration set must be explicitly enumerated.
- Some of the top-level entities are discrete self-contained units and do not include other units (for example, container types, reagent types, artifact groups, and nonartifact/nonprocess type UDFs).
- Some top-level entities (process types, for example) automatically include other units (refer to *Non-Top-Level Entities* on page 211 for more information).
- For process types, only configured processes, vanilla Transfer processes, Pool Samples (since 7.5), and Add Multiple Reagents (since 7.6) processes are supported. All process type details are exportable/importable.

Non-Top-Level Entities

- Some entities are only included as part of other entities.

  For example, process templates, process type UDFs, and artifact UDFs are only included when included in a top-level process type. (The latter is a special case, given that the same artifact UDF can be used by multiple process types.)

Required Entities

- Some entities may be required by other entities. In these cases, make sure that these entities are exported/imported in the correct order.

  - For example, because process types may require the existence of a container type, create the container type first.
- Required entities are not automatically included. If they do not exist in the destination system, explicitly include them in the manifest file.
  - For example, suppose that a process type declares a particular container type as a default output plate. If that container type does not exist in the destination system, include that container type in the manifest file.

Import/Export Modes

Import modes affect the transactability of the tool, allowing it to make incremental changes if errors occur or provide an all-or-none option. For example, use the operation validate mode to determine if errors were encountered.

Best-Effort Mode

- This mode is the default import mode.
- This mode attempts to import as many units as possible. Any failures are logged, but the import operation is not interrupted.
  - For example, a failing container type import does not prevent other container types from being processed.
  - Similarly, if a process type fails import because it already exists, any UDFs and process templates for that process type are still processed.
- There is no need to enter an option for this mode.

Strict Mode

- If this mode is used, the import operation is aborted if it encounters a failure.
  - For example, if there is an API version mismatch, the operation aborts and no further imports are executed. Any changes already performed are not reverted.
- Use the `-Strict` option to enable this import mode.

Validate Mode

Use the validate operation (instead of import) to enable this mode.

This mode produces a report listing showing the following items:

- Entities that would be successfully imported because they do not exist on the target server.
- Entities that already exist on the target server and are identical.
- Entities that already exist on the target server but are different.

Validate mode can only detect a limited set of errors. For example, it can check if a particular piece of configuration already exists. If so, it checks if it is identical to the one included in the configuration package.

This information can help determine if the importAndOverwrite option is needed instead. For details, refer to *Command-Line Options and Usage* on page 205.

Example of console output:

```
2015-01-16 15:42:31,174  INFO - Found 4 Container Types in configuration
package, validating now.
2015-01-16 15:42:31,706  INFO - Summary of Container Types:
    Do not exist: None
    Exist and are identical:
        Container Type 'BioAnalyzer DNA 1000 Chip'
        Container Type 'BioAnalyzer DNA High Sensitivity Chip'
        Container Type 'BioAnalyzer RNA Nano Chip'
        Container Type 'BioAnalyzer RNA Pico Chip'
    Exist and are different (diffs in log): None
```

Example Mode

- Use this mode to generate a manifest file if the configuration to export is not tied to a specific set of workflows, protocols, or process types.
- Use the example operation (instead of import) to enable this mode.

Upgrading a Configuration Package/Manifest File for Compatibility with Config Slicer v3.0.x

If running Config Slicer v3.0.x against a configuration package or manifest file that was generated with a pre-3.0 version of Config Slicer, an error message displays.

Scenario 1: Out-of-Date Configuration Package

In this scenario, the error message resembles the following example:

```
Package was generated with an older version of config slicer incompatible with
the current version (3.0.2). Please upgrade the configuration package (java -jar
upgrade-config-slice.jar 'configuration_package.xml'), verify the results, and
try again.
```

Solution:

Upgrade the configuration package file by running `upgrade-config-slice.jar` against it.

- This jar file should be located in the same directory as Config Slicer (`/tools/config-slicer`).

- The upgrade script saves an upgraded copy of the configuration package file (to the same directory), which can be inspected and imported.

Example:

```
java -jar upgrade-config-slice.jar configuration_package.xml
```

To upgrade a manifest file at the same time, simply add it to the script as a second argument:

```
java -jar upgrade-config-slice.jar configuration_package.xml manifest.properties
```

Scenario 2: Out-of-Date Manifest File with no Corresponding Configuration Package

In this scenario, the error message resembles the following example:

```
Manifest was generated with an older version of config slicer incompatible with
the current version (3.0.2).
If you have the corresponding configuration package available the manifest can
be automatically upgraded
(java -jar upgrade-config-slice.jar configuration_package.xml 'manifest_
file.properties'). Otherwise please
regenerate the manifest with the current version of config slicer and try again.
```

Solution:

This upgrade process is a little more involved:

1. Extract the list of process types from the manifest file.
2. Format them as parameters to the Config Slicer custom manifest generation for process types. For example, assuming we extracted Process Type 1 and Process Type 2 in Step 1, the following command would be used:

```
java -jar config-slicer.jar -o custom -s localhost -u admin -p pass -pt
"Process Type 1" -pt "Process Type 2"
```

3. Run the custom manifest generation.
4. Take the list of analyte UDFs and ResultFile UDTs from the manifest file that was generated and add them to the old manifest file.
5. Add the following line of text to the top of the old manifest file:

```
ConfigSlicerVersion=3.0-compatible
```

Config Slicer Use Cases

Create a Configuration Package File for Import to Another System (or for Backup Purposes)

Use a configuration package file to copy a configuration set from one server to another or to back up a particular working configuration at a particular time.

Required steps:

1. Create a configuration manifest file.
2. Export to configuration package file.

Import (Install) a Configuration Package File on a Production or Test Server

This process involves copying a configuration set from one server to another, by importing a configuration package file.

For example, to move a configuration set to a different environment for testing or troubleshooting purposes, or copy a new configuration set (created and tested on one system) onto another system.

Required steps:

1. On the source server, create a configuration manifest file and export to a configuration package file.
2. On the destination server, import the configuration package file.

Compare Differences between a Working Configuration and a Broken Configuration

There are two approaches:

- Comparing configuration manifest files provides a way to determine if there are processes or UDFs missing from a system. The information in the manifest files only allows comparing process and UDF names, not the specific way in which a process or UDF is configured.
- Comparing configuration package files helps check how specific processes are configured. If the systems being compared are meant to be identical, this method is more appropriate to use.

Required steps:

1. On each system, create a configuration manifest file or a configuration package file.
2. Run a diff comparison on the two files.
3. Edit the broken manifest file, export it, and import the resulting configuration package file into the system to add the missing entities.

There are several tools that available to compare files:

- Meld (graphical), for Linux, port to MacOS.
- Standard Unix diff (Linux, MacOS) (use -q for a quick check).
- FileMerge (OSX with XCode installed) - /Developer/Applications/Utilities/FileMerge.app.
- WinMerge (graphical), for Windows (refer to http://winmerge.org/).

Merge the Configuration Sets from Multiple Test Systems to a Production System

Combine configuration sets from multiple systems, merge them into a single configuration package file, and then import the file into a new system.

Required steps:

1. On each source server, create and edit a configuration manifest file.

For Research Use Only. Not for use in diagnostic procedures.

2. Merge the entities from all files into a single manifest file.
3. Export the resulting file to a configuration package file.
4. On the destination server, import the merged configuration package file.

Back up and Restore a Configuration Set

Copy a configuration set to restore it on another server and use it for testing/troubleshooting purposes.

Required steps:

1. On the server containing the broken source system, create a full manifest file, containing all the Clarity LIMS system configuration.
2. Export the manifest to a configuration package file. Save file to media/disk.
3. On the target server, import the configuration package file created on the source system.

Back up and Upgrade a Configuration Set

To upgrade or add to a configuration set already installed on a server, two configuration package files are needed: one to back up the working configuration set and one containing the new updated configuration that have been created on a test server.

Required steps:

1. On the server that is getting upgraded, create a full manifest file and export this file to a configuration package file. Save this file as a backup.
2. On the test server, create a manifest file and edit it so that it only includes the entities you want to import.
3. On the server that is getting upgraded, import the configuration package file.

Deploy a New Configuration Set from Test to Production Server

Take a configuration that has been created and tested on one system/site (referred to as the source system in the following steps) and deploy it on another system/site (destination system).

As a best practice, make sure that the configuration is backed up by creating a full manifest file and exporting to a configuration package file (see Step 2). The process is also described in *Back up and Restore a Configuration Set* on page 216.

Required steps:

1. On the source system, create a configuration package file containing the tested configuration to import.
2. On the destination system, create a full manifest file and export this file to a configuration package file. Save this file as a backup.
3. On the destination system, import the configuration package file that was created in Step 1.

Troubleshooting Config Slicer

If there is an API version mismatch, Config Slicer logs a message at the beginning of an import:

```
API version mismatch - package: v2,r20 - server: v2,r21. This may result in some differences between configuration in package and on server.
```

Generally, this message is not a cause for concern.

However, if there are warnings about configuration differences during the import, changes that have been made to the API in between the package version and the server version may be responsible.

In addition, if the package being imported is from v4.x, a log message may appear at the beginning of an import:

```
Detected package is from a pre-5.0 Clarity system. The package will be upgraded to match new configuration requirements.
```

In this case, the package is upgraded and the resulting configuration is output to a folder in the same location as the package being imported. This upgraded configuration package is the v5.x representation of the v4.x configuration and can be used directly to troubleshoot error occurring on import. The updated packaged can also be imported directly.

Config Slicer Version Updates

The following changes are included in the latest release of Config Slicer (v3.0.51):

General Changes

- The entity summary is now shown after the individual differences have written to the log file, as opposed to before these differences.
- Support was dropped for the following process type attributes, which are no longer used:
  - SupportsExternalProgram
  - ShowInExplorer
  - ShowInButtonBar
  - OpenPostProcess
  - IconConstant
- Support was dropped for the show-in-tables property on Custom Fields (UDFs) because it is no longer used.
- There is now support for the new Clarity LIMS v5.x distinction between Protocol Step names and Master Step (ProcessType) names.
- It is now possible to slice in and out all the new Master Step settings added in Clarity LIMS v5.0:
  - Default Process Template
  - Instrument Types

For Research Use Only. Not for use in diagnostic procedures.

  - Container Types
  - Reagent Kits
  - Reagent Types
  - Control Types
  - Sample Fields
  - Queue Fields
  - Ice Bucket Fields
  - Step Fields
  - Step Properties
- When importing/validating a slice from 4.x into 5.x, if the package contains any Master Steps (process types) or Protocols, it is upgraded to be compatible with the new configuration available in 5.x. This process is automatic, and the updated package is written out to the directory containing the package being imported or the directory that log file is being written to. If errors occur while importing, this updated package can be manipulated directly and imported to fix them.

If upgrading the package fails, import/validation fails. In general, this failure reflects a mistake in the configuration package being imported.

Changes to Support Slicing from v4.x to v5.x

The following changes were added to support slicing between Clarity LIMS v4.x and v 5.x. All changes are saved into a new configuration package that is written to the same location as the package being sliced:

- Backwards compatibility for Protocol Step setup configuration.
- Support for updates of parent entities after both the parent and child entities have been imported.
  - This change is required for updating the defaultProcessTemplate and step-fields step properties on Master Steps. Both require that the Master Step (ProcessType), ProcessTemplate, and Master Step Custom Fields (ProcessType UDFs) exist before they can be set on the Master Step.
- Support for setting the qcProtocolStep flag on Master Steps, allowing the correct Master Step type to be displayed in the Lab Work Configuration UI. The setting is propagated up from the Protocol Step to the Master Step.

For Research Use Only. Not for use in diagnostic procedures.

> After slicing, it is recommended to examine the configuration closely for any QC Protocol Steps that previously shared a Master Step with nonQC Protocol Steps. This setting may not transfer as expected and there is potential for misconfigured Protocol Steps. In particular, if the Master Step produces measurements, and even just one child step of a Master Step has qcProtocolStep=true, then the Master Step will get qcProtocolStep=true set on it. Thus, all other steps that use that Master Step have qcProtocolStep=true, whether or not it was set before.

- Support for setting the default container on Steps and Master Steps in such a way that all behavior is maintained from 4.2.
  - If every child step of a Master Step has the default container that was defined as a permitted container on the master (through the OutputContainerType process-type-attribute), then the default is added as a permitted container on the master step.
  - If any child does not have the default container from the Master Step, then the default is removed from the Master and each child that had the container is updated so that the default is the first permitted container (and hence default).
- Extra containers and any step properties that are no longer valid on a step are migrated to new properties or removed.
- Step-setup file configuration has been moved to the Master Step and it not possible to have a different set of step-setup files on a step than are specified on the Master. The master step owns the list of files. Both the search-result-file-index attribute on each file element and the message element for each file are defined by the Master and must be duplicated on every step. When moving a 4.x configuration with step-setup files to a 5.x configuration, the following events will occur:
  - The set of all the step-setup files found on all the child steps in the slice are added to the Master Step and each child step.
  - If more than one step in the slice defines step-setup files for the same search-result-file-index, then all the messages for that search-result-file-index are concatenated by newlines.
  - The enabled attribute is set to true for the step-setup on all child steps.
  - The locked attribute is set to false for the step-setup on all child steps.
  - In the case of importAndOverwrite, the step-setup of any existing child steps for an overwritten master step is included.
- Upon validation after import, the following differences have been reconciled:
  - UDFs that differ by style only
  - missing defaultProcessTemplate
  - missing attemptAutoPlacement
  - missing autoAttachFiles
  - missing qcWithPlacement

For Research Use Only. Not for use in diagnostic procedures.

Database Cleanup Procedure

After initial user training, but before the lab starts to use Clarity LIMS in production, a database cleanup is recommended.

This process removes any projects, samples, workflows, protocols, steps, and other artifacts from the system that were created during training but are not needed for production.

Contact the Clarity LIMS Support team to schedule a time for this cleanup procedure.

In preparation for the cleanup, complete the following steps:

- Delete all unwanted custom fields and master steps.
- Set the status of all unwanted workflows to Archived. If there is an archived workflow that you want to keep, temporarily set its status to Active. Note the following:
  - Protocols that are part of an archived workflow or set of archived workflows are deleted.
  - Protocols that belong to an active or pending workflow, in addition to an archived workflow, are not deleted.

After these steps are completed, a Clarity LIMS Technical Support Analyst (TSA) helps to perform the cleanup procedure. This procedure takes approximately 15–20 minutes to complete.

Clarity LIMS Log Files

Clarity LIMS creates various log files to help with the resolution of issues. During support request investigation, the Support team may ask for the following types of log files:

- HiSeq Log File
- MiSeq Log File
- Automation Worker Log File
- Browser HTML and JavaScript Logging

HiSeq Log File

The following log file is available for Clarity LIMS HiSeq integrations:

- `HiSeqGAIntegrator.log` is a log file used to troubleshoot issues with run data, event files, and the sequencing service.

This file is located here (for v4):

```
Illumina_HiSeq/v4/SequencingService/
```

MiSeq Log File

The following log file is available for Clarity LIMS MiSeq integrations:

For Research Use Only. Not for use in diagnostic procedures.

- `MiSeqIntegrator.log` is a log file used to troubleshoot issues with run data, event files, and the sequencing service.

This file is located here (for v4):

```
/opt/gls/clarity/extensions/Illumina_MiSeq/v4/SequencingService/
```

The locations shown here are for HiSeq and MiSeq version 4. For version 5, replace v4 with v5 in the file paths.

Automation Worker Log File

Automation Worker creates history and log files and stores them on laboratory computers in the `logs` folder of the Automation Worker installation directory.

If Automation Worker is installed on a Windows machine using the program default, find the `logs` folder at the following location:

```
/opt/gls/clarity/automation_worker/node/logs
```

If Automation Worker is installed on a Linux server, find the `\logs` folder at the following location:

```
/opt/gls/clarity/automation_worker/node/logs
```

The following log files are available:

- `wrapper.log` is a log file that outputs information on the starting, running, and stopping of the Automatic Informatics service.
- `automatedinformatics.log` is a log file that outputs messages from installed plug-ins, such as automation commands and ADC directory scans.

To monitor the automatedinformatics.log, do as follows:

- Log on to the server using the glsai user ID and run the following command:

```
opt/gls/clarity/automation_worker/node/bin/automatedinformatics.wrapper.sh log
```

If the Automation Worker is installed on a server other than the Clarity LIMS server, use the appropriate user credentials.

Browser HTML and JavaScript Logging

In the web browser, if the LIMS interface does not display items/elements correctly, provide the information and error messages to theClarity LIMS Support team.

Instructions for finding error messages within the browser console are described in the following sections.

Google Chrome

To start the Chrome Console:

1. Right-click an element in the browser and select Inspect.

A panel opens within the main window in Chrome, showing the source HTML.

2. Select the Console tab. and reload the troublesome page. Any JavaScript errors are reported there. Include these errors in the Support Request ticket.

Between stages in a protocol step, errors of the following type may appear:

```
GET http://qaclarity02.gls.lan:8080/clarity/api/work/310/epp ?_dc=1375380986790
404 (Not Found)
```

Such messages are expected. The EPP trigger is checking that there is no EPP transition to fire on the page change. (These messages can be annoying for debug purposes, but feel free to include them in the Support Request ticket.)

To get the JavaScript version:

1. Open the Console as described in the previous section.
2. Go to the Network tab.
3. Select scripts from the options listed at the bottom of the tab.
   A script named isis-all.js?v=XXXXX displays.
4. Determine the version build number. (In the previous example, XXXXX represents the version build number).

FireFox

To start the FireFox Console:

1. Right-click an element in the browser and select Inspect Element.
   A panel opens within the main window in FireFox, showing the source HTML.
2. Select the Console tab and reload the troublesome page. Any JavaScript errors are reported there. Include these errors in the Support Request ticket.

Between stages in a protocol step, errors of the following type may appear:

```
GET http://qaclarity02.gls.lan:8080/clarity/api/work/310/epp ?_dc=1375380986790
404 (Not Found)
```

Such messages are expected. The EPP trigger is checking that there is no EPP transition to fire on the page change. (These messages can be annoying for debug purposes, but feel free to include them in the Support Request ticket.)

To get the JavaScript version:

1. Open up the Console as described in the previous section.
2. In the Filter Output field type isis.
   A script named `isis-all.js?v=XXXXX` appears.
3. Hover over this script with your mouse to find the V (version) build number.

For Research Use Only. Not for use in diagnostic procedures.

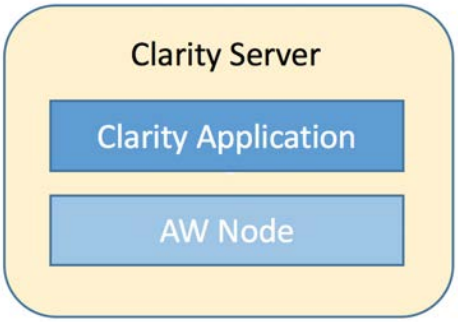
Using Log Files for Troubleshooting Purposes

If you are experiencing problems and need to submit a support request, use the following guidelines to determine which log files to send to the Clarity LIMS Support team:

- GLSInvocation*.log—Include if experiencing slowness in the application.
- server.log—Include with all support requests.
- boot.log—Include if JBoss fails to start properly (rarely needed).
- HiSeqGAIntegrator.log—Include if you are experiencing issues with run data, event files, and the sequencing service.
- MiSeqIntegrator.log—Include if you are experiencing issues with run data, event files, and the sequencing service.
- automatedinformatics.log—Include if you are experiencing problems with an integration or if a process using an EPP string does not work as expected.
- wrapper.log—Include if the Automation Worker is unable to start (rarely needed).
- Browser Console and Clarity LIMS JavaScript version—Include for any web interface display issues. A simple refresh of the browser page may resolve the issue. However, the Support team would prefer receiving the console log and JavaScript version to investigate and make product improvements.

Automation Worker Nodes

All Clarity LIMS installations include the installation of a separate component known as an Automation Worker (AW) node (formerly known as Automated Informatics (AI) node).



When writing automation-based triggers, the code invoked by an automation runs on the AW node.

While the AW node is a critical component, it typically does not require much attention. However, there are many other options that must be considered. These options include how many AW nodes a Clarity LIMS system uses, and where they are placed. This section discusses some of these options.

For Research Use Only. Not for use in diagnostic procedures.

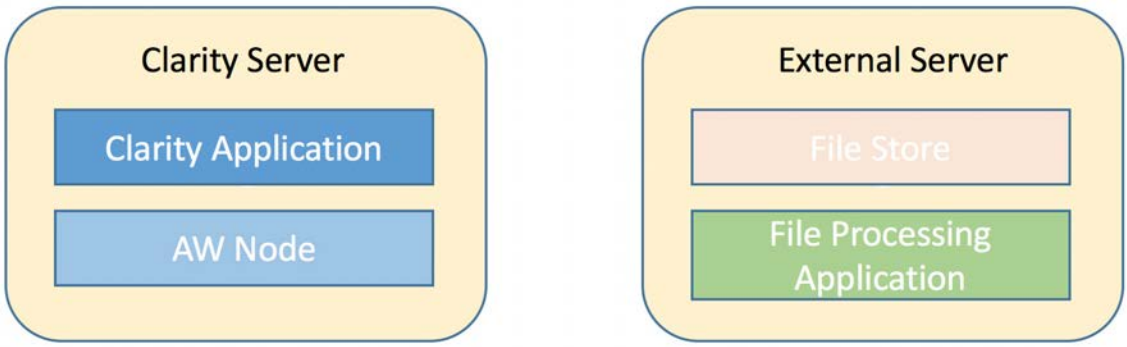
Automation Worker Nodes and Remote Computing

The AW node is installed adjacent to the Clarity LIMS application. Its original purpose was to enable remote computing.

To illustrate these features, assume that a need requires Clarity LIMS to produce a file in a specific location. The file is then processed and an action occurs.

A good example is label printing via the BarTender application. The BarTender application picks up the new file, associates it with a printer and a template, and causes a label to be printed.

The infrastructure for this file storage and processing likely occurs on a separate server from the one that contains the Clarity LIMS application and the AW node.



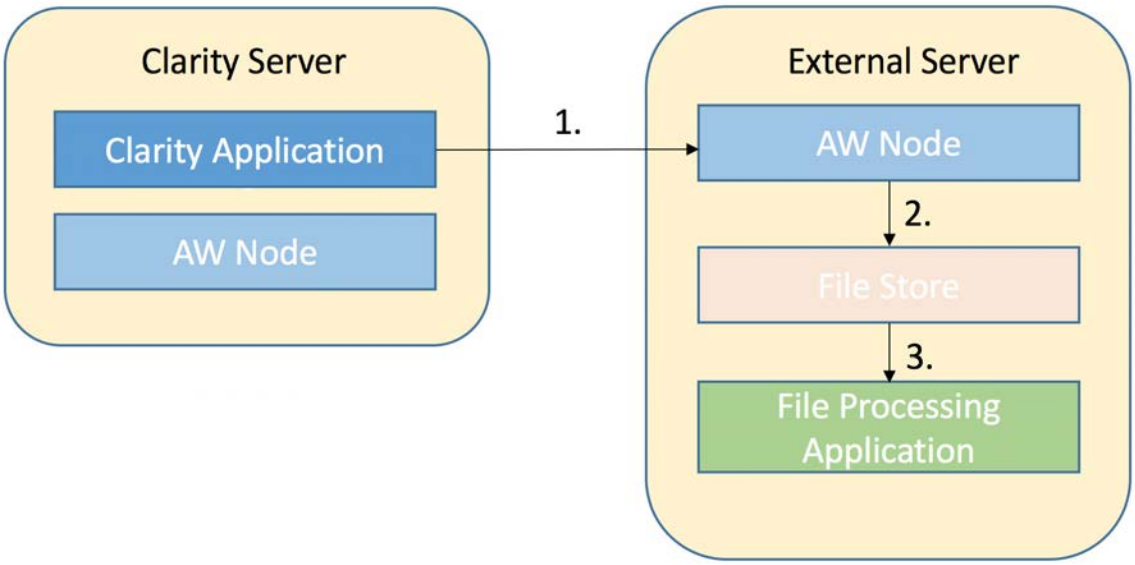
The Clarity LIMS application invokes the command to create the file on the AW node. After the file is in the file store, it is processed by the file processing application.

How does the AW node get the file to the file store, even if it is on a different server and possibly on a different network? The solution is to install an AW node on the external server.

The addition of the second AW node, which is local to the external server but remote as far as Clarity LIMS is concerned, provides a solution to the problem. This demonstrates how AW nodes can support remote computing..

1. Clarity LIMS invokes the production of the file via the remote AW node.
2. The remote AW node copies the file to the local file store.
3. The file processing application processes the file.

For Research Use Only. Not for use in diagnostic procedures.



Automation Worker Properties

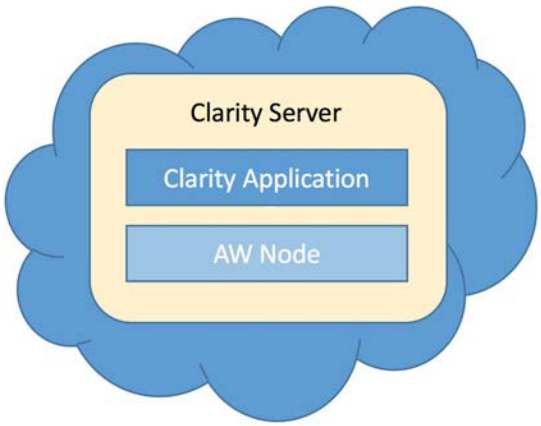
An AW node is a Java-based application and can run on most PCs/servers.

- The AW node and the Clarity LIMS application must be able to communicate through networking firewalls.
- When the Clarity LIMS application has the choice of sending the task to multiple AW nodes, the channel name property is used to determine which one receives the job. For example, the AW node installed on the Clarity LIMS server has the default channel name of limsserver. This is why you must specify the limsserver value when defining an automation command.
- When defining the automation, the following two items are defined:
  - Which command should be run by the AW node.
  - Which AW node should receive the job via the channel name property.
- Typically, for the AW node that runs on the Clarity LIMS server, the convention is to place scripts in the `/opt/gls/clarity/customextensions` folder. The log file is stored in `/opt/gls/clarity/automation_worker/node/logs/`.
- For the remote AW node, store the scripts in any folder, and choose where its log file gets stored (it is running on your hardware).
- For the external AW node to run Clarity LIMS toolkits, such as the Lab Logic or Lab Instrument toolkit, make copies of the JAR files that contain these toolkits. Place them on the external server, so the AW node can access them.
- There is no real limit to how many AW nodes you can have. Place them wherever they are needed.

For Research Use Only. Not for use in diagnostic procedures.

Automation Workers in the Cloud

Consider the AW node that is installed on the Clarity LIMS server for a cloud-based implementation.



Although cloud-based Clarity LIMS servers contain an AW node, the best practice is not to run your code on it.

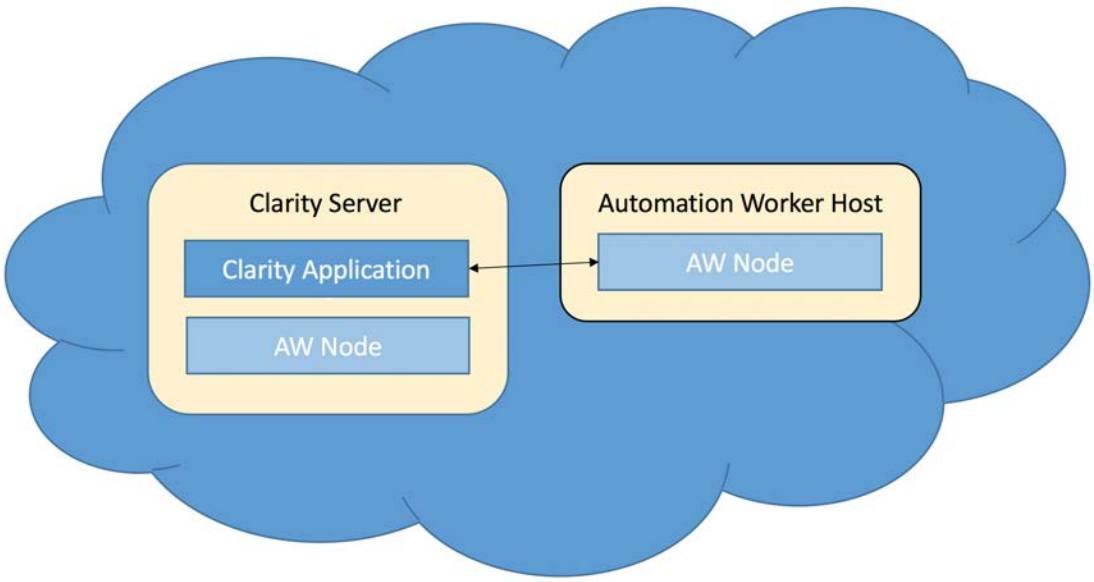
Why not? It is a question of security policies for both Illumina and our cloud-hosting provider. If we provide customers with command-line access to the AW node, we are allowing them command-line access to the Clarity LIMS server and, as a consequence, the Clarity LIMS application itself. If using Clarity LIMS in a clinical environment, this makes it more difficult to pass security and access audits.

If the Clarity LIMS instance is cloud-hosted, and you need to run custom code via an AW node, there is a solution.

You could install an AW node on your local architecture and have it interact seamlessly with Clarity LIMS, as illustrated in Figure 1. You can control access to the remote AW node, the infrastructure of the Clarity LIMS server is safely hidden behind firewalls, and security policies remain intact.

However, for some customers, part of the attraction of a cloud-based system is not having to maintain mission-critical hardware. To address this, we can offer an external AW node that does not live on local hardware but is also in the cloud.

For Research Use Only. Not for use in diagnostic procedures.



Thus, we can provide an external AW node that lives on a separate machine, known as the Automation Worker host. This Software-as-a-Service (SaaS) model gives access to only those parts of the system that require it. You can access the Automation Worker host, and its AW node can interact with Clarity LIMS. However, you cannot access the Clarity LIMS server.

Because the AW node is running on a separate machine to the Clarity LIMS server, it needs its own copy of the toolkit JAR files. For some, this feature has an additional bonus in that the Automation Worker host hardware supports Python 3 for scripting.

For customers who are cloud-based and need a true local AW node, this is not a problem. They can have an AW node in the Automation Worker host and as many local AW nodes as needed. Place them wherever they are needed.

Automation Worker Node on Windows Server

In Clarity LIMS v5.4 and later, you can install the Automation Worker Node onto the Windows server. Before you begin the installation, make sure that you have met the following requirements:

- The `clarity-aiinstaller-x-deployment-bundle.zip` file must be retrieved from the server where Clarity LIMS is installed. You can find this file at `/opt/gls/clarity/config/.templates/automation_worker/`.
- For Windows 10 users, the command prompt must be specified in the Automation command line (eg, `cmd.exe / c echo 'Hello World'`.
- If `VISTA-SETUP.bat` does not display in the installation window after Run as Administrator is selected, start the installation window as follows.
  - Launch the command prompt as an Administrator.

For Research Use Only. Not for use in diagnostic procedures.

- Change the directory where `VISTA-SETUP.bat` is located with `cd C:\<DIRECTORY>`.
- Execute the `java -jar .\GLSAutomatedInformatics-Installer.jar` command.

Install the Automated Worker Node as follows.

1. Copy the SecretUtil deployment bundle ZIP file to the remote Automation Worker node.
2. Extract the contents of the ZIP file to a folder named `secretutil`. You can add this folder to `C:\opt\gls\clarity\tools` or another location you choose.
3. Edit `vault.properties` of the file in the `conf` folder to `update application.mode` to `file`.
4. Make sure that the following System Environment Variables are set:
   - CLARITYSECRET_HOME (eg, `C:\opt\gls\clarity\tools\secretutil`)
   - CLARITYSECRET_ENCRYPTION_KEY (minimum 24 characters)
5. Using secretutil.jar, set the required secrets. For a basic installation of AutomationWorker, you must set the passwords for apiuser and glsftp using the following commands:

```
# For glsftp
java -jar C:\opt\gls\clarity\tools\secretutil\secretutil.jar -u=<secret>
app.ftp.password

# For apiuser
java -jar C:\opt\gls\clarity\tools\secretutil\secretutil.jar -u=<secret> -
n=integration apiusers\<username of the API user, e.g. apiuser>
```

6. After setting the secrets, attempt to retrieve them with the following command:

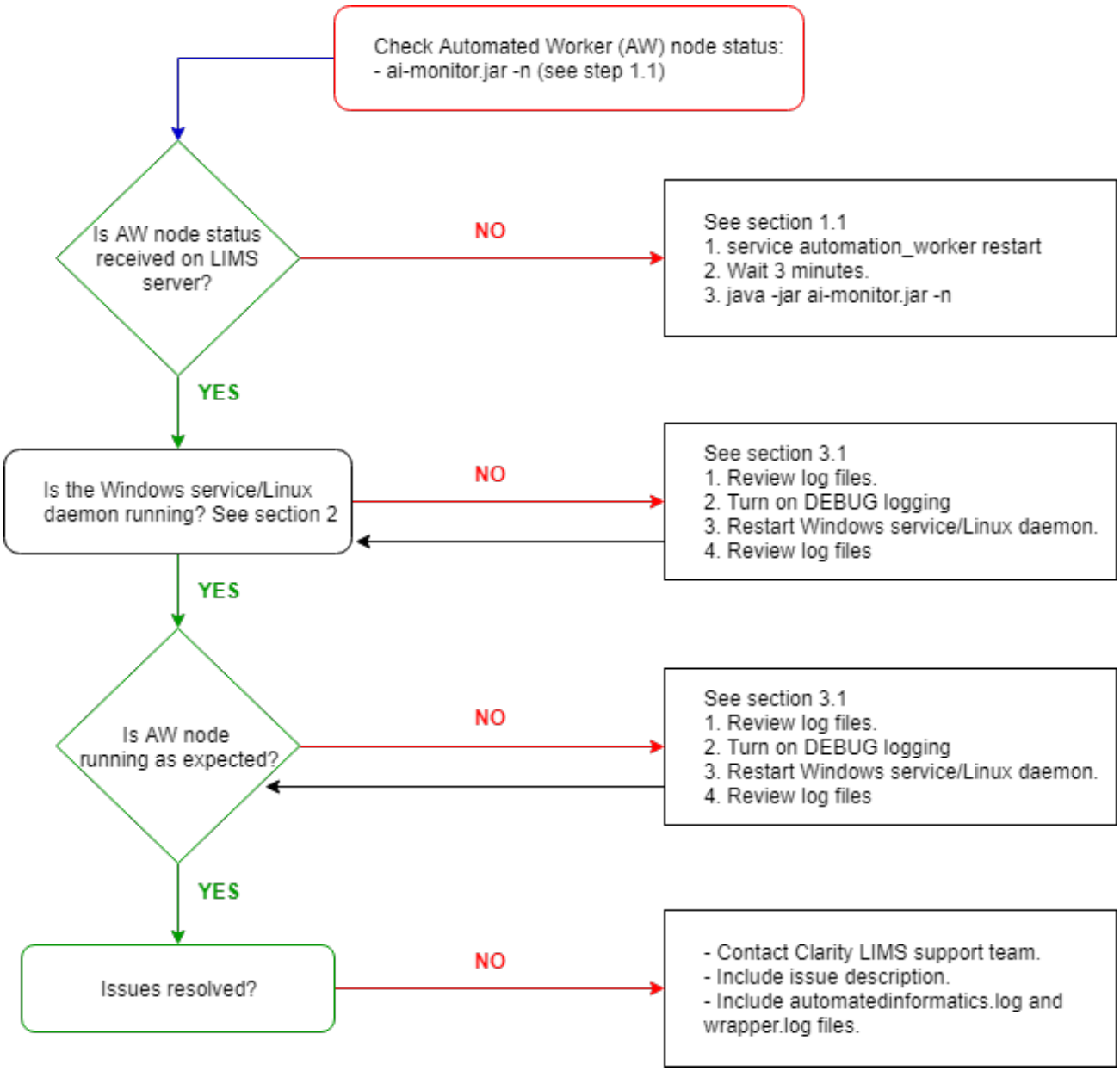
```
java -jar C:\opt\gls\clarity\tools\secretutil\secretutil.jar app.ftp.password
```

7. Restart the Automation Worker service.

Troubleshooting Automation Worker

Use the following steps to help troubleshoot the installed Automation Worker framework. A flowchart is provided as a reference.

Flowchart Reference



1. Verify Connection Between LIMS Server and Automation Worker Node

1.1 Checking the connection

The first step is to check the connection between the Clarity LIMS server and the Automation Worker node.

Use the -n option of the `ai-monitor.jar` tool script to see if the Clarity LIMSserver is currently able to communicate with the AI node.

For Research Use Only. Not for use in diagnostic procedures.

To check the status of ai-monitor.jar:

1. As the glsjboss user open a SSH session to the Clarity LIMS server.
2. Run the following command:

```
java -jar /opt/gls/clarity/tools/ai-monitor/ai-monitor.jar -u <user> -p
<password> -i <base URI> -n
```

- If the Clarity LIMS server cannot connect to any of the AI nodes the response will be as follows:

```
Listing nodes
No nodes found
Aborting
```

- In this scenario, proceed to Step 2. Verify Windows Service or Linux Daemon.
- If the Clarity LIMS server can connect to the Automation Worker nodes, the response will resemble the following:

```
Listing nodes
==========
Node: 23673@qaclarity01.gls.lan
Address: 192.168.10.88
Channel: limsserver
First update: Thu Sep 19 19:15:13 GMT 2013
Latest update: Thu Sep 19 19:22:09 GMT 2013
Release: 20190919-0708
Version: 8.6.1-SNAPSHOT
JVM: Sun Microsystems Inc. 1.6.0_45
In progress: 0 requests
```

2. Verify Windows Service or Linux Daemon

Determine if the Windows service or Linux daemon for the Automation Worker is running.

2.1 Starting and stopping the Windows service / Linux daemon

To start, stop, or restart the Windows service:

1. From the Start menu, select Run.
2. In the Open text field, type 'services.msc' and select OK.
3. In the Services dialog, locate the Automation Worker service.
4. Right-click the service and select Start, Stop, or Restart. If the service is stopped, start the service.
    - If the service is running, stop and start it again.

For Research Use Only. Not for use in diagnostic procedures.

- Wait for a minimum of three minutes, and then check if the AI node is communicating with the Clarity LIMS server by running the `ai-manager.sh` script with the status argument, as described in Step 1.

To start or stop the Automation Worker Linux daemon:

- To verify current status:

```
service automatedinformatics.wrapper.sh status
```

- To restart a running daemon:

```
service automatedinformatics.wrapper.sh restart
```

- To stop a running daemon:

```
service automatedinformatics.wrapper.sh stop
```

- To start a stopped daemon:

```
service automatedinformatics.wrapper.sh start
```

Once Started/Restarted:

- Wait for a minimum of three minutes, and then check if the AI node is communicating with the Clarity LIMS server by running the `ai-manager.sh` script with the status argument, as described in Step 1.

If the daemon is not recognized, list out the contents of the `/etc/init.d` directory and determine the exact name of the Automation Worker daemon.

The name typically contains `'automation_worker'`, but may vary—particularly if there is more than one daemon on the same Linux server, or if the Automation Worker is installed on a server other than the Clarity LIMS application server.

3. Automation Worker Log Files

Automation Worker creates history and log files and stores them on laboratory computers in the logs folder of the Automation Worker installation directory.

3.1 Reviewing Automation Worker log files

After performing the steps described above, reviewing these log files may help to determine the cause of the issue.

For details on the Automation Worker log files, and instructions on how to view them, refer to *Clarity LIMS Log Files* on page 220

3.2 Turning on debug logging

After reviewing the log files, if the cause of the issue is not evident, the next stage is to turn on debug logging. This outputs DEBUG messages to the log files.

Contact the Clarity LIMSsupport team for instructions on turning on DEBUG mode.

Review the log files to determine if the DEBUG messages help to find resolution.

After turning on debug logging, ensure that you restart the Windows service or Linux daemon.

Installation and Upgrade

This section provides information and instructions to help you install Clarity LIMS and upgrade your existing system.

In addition to installation and upgrade steps, this section also provides steps for performing the following tasks:

- Installing and configuring the Secret Utility password management tool
- Configuring your HashiCorp vault
- Changing the Clarity LIMS hostname
- Updating server passwords and database connection details
- Installing a purchased SSL/TLS certificate

For assistance with Clarity LIMS installation, contact the Clarity LIMS Support team.

Pre-Installation Requirements

Before installing Clarity LIMS, you must purchase hardware and software that meet the minimum requirements (see *Technical Overview* on page 2). Following those purchases there are several components that you must organize, install, or configure.

The following sections discuss these components, and how to install and configure them. These sections apply to on-premise customers only. Before completing the steps described, make sure that the server has the minimum requirements. See *Technical Requirements* on page 5 for details.

Before the Clarity LIMS support team can install Clarity LIMS, the items listed above must be set up and configured as described in this document. Confirm the completion of this work with the support team.

Purchase SSL / TLS Certificate

All instances of Clarity LIMS must have a purchased SSL / TLS certificate installed.

Certificate Authorities will no longer issue SSL / TLS certificates for internal server names. As a result, to obtain a certificate you must have a valid, public DNS entry for your server.

Before installing or upgrading Clarity LIMS, do the following:

1. Purchase an SSL / TLS certificate.
2. Save the certificate files on the server on which the Clarity LIMS server is installed.

3. Provide the Clarity LIMS Support team with the private key and password for the SSL / TLS certificate.

For instructions on obtaining a certificate, see *Install a Purchased SSL/TLS Certificate* on page 333.

Check SELinux Mode

Security-Enhanced Linux (SELinux) is not supported for use with Clarity LIMS. Make sure that SELinux is set to either permissive or disabled mode.

For instructions, see the following sections of the Red Hat documentation:

- 5.4.1.2 Permissive Mode
- 5.4.2 Disabling SELinux

You can find additional documentation on users at: /opt/gls/clarity/documentation/users/

Set Up Root Access to Server

Clarity LIMS is installed using industry standard RPM packaging. The Clarity LIMS support team requires root credentials to the server during the installation process.

The following sections discuss the system user accounts that the support team sets up during the installation process. It is important that you do not change these system users.

The production server must be configured in US locale.

Server-based User Accounts

During initial installation, the RPMs create the following server-based user accounts in a common group named claritylims.

- glsjboss—This user account is used for setting up and starting the Tomcat application server.
- glsai—This user account is used for setting up and starting the automation worker service.
- glsftp—This user account is configured to allow SFTP access and to redirect the home directory to the data storage area. The glsftp user account is used by Clarity LIMS clients to import and export files from the LIMS file server.

Do not manually create these user accounts.

During initial installation of the elastic search subsystem, the RPM creates the following server-based user account in the elasticsearch group.

- elasticsearch—This user account is used for setting up and starting the elastic search subsystem used by the LIMS search mechanism.

Do not manually create this user account.

During initial installation of the RabbitMQ subsystem, the RPM creates the following server-based user account in the rabbitmq group.

- rabbitmq—This user account is used for setting up and starting the RabbitMQ subsystem used by the search indexing mechanism.

Do not manually create this user account.

Set User Account Passwords

During the installation process, no default passwords are created for the glsjboss, glsai, and glsftp user accounts.

- Passwords must be set for these accounts.
- During execution of the Clarity LIMS installation script, you are prompted for the password of the glsftp user. Use the same password you set at the operating system level for this user.

You can find additional documentation on users at /opt/gls/clarity/documentation/users/.

Allow SSH Password-based Authentication

To enable SSH Password Authentication, add the following configuration to the /etc/ssh/sshd_config file:

```
Match User "glsftp"
PasswordAuthentication yes
```

Install and Configure the Database

After installing a supported database, Clarity LIMS requires certain changes to the default database configuration.

Additional tablespace names and user profiles may be needed, depending on the configuration of your system.

For more information or for assistance with your database configuration, contact the Clarity LIMS Support team.

Configure PostgreSQL Database for Use with Clarity LIMS

1. On your database server, create a Clarity LIMS user. The Clarity LIMS user must have either full rights and permissions, or the ones defined by this command:

```
CREATE ROLE clarity WITH NOSUPERUSER CREATEDB NOCREATEROLE LOGIN
```

The Clarity LIMS user must use only the public schema. Clarity LIMS does not support other schemas.

2. Create one database named ClarityDB and another named ClarityTenantLookup. Make sure that both databases are set up to receive remote connections from the Clarity LIMS application server.
3. Restart PostgreSQL.
4. Confirm the completion of these items with the Clarity LIMS Support team, and provide the following information:
   - The database user name and password for both databases.
   - The hostname/IP address of the database server.
   - The PostgreSQL port number.

Set Up Database Maintenance Tasks

To achieve optimum performance, we recommend you perform the following database maintenance tasks, using the appropriate tools and commands.

- PostgreSQL: Routinely vacuum the database. For instructions, refer to the PostgreSQL documentation.

IPv4 support

Clarity LIMS supports only IPv4.

Confirm Hostname Resolution

To access the Clarity LIMS server via DNS, make sure that the following apply:

- The server local host file /etc/hosts does not contain an entry for that hostname bound to its loopback address.
- Any hostname entries correspond to their entries in DNS.
- The command hostname -f must return the fully qualified domain name (FQDN) of the server.

For client systems:

- Users should use the FQDN when logging on to the system. Using the FQDN ensures persistence of the session ID.

Set the TimeZone (TZ) Environment Variable

Clarity LIMS requires the environment variable TZ be set on the Clarity LIMS server to your correct timezone. If the value is not configured, a default of GMT is configured by Clarity LIMS in the file /etc/profile.d/clarity.sh.

This file might update on upgrade. Any changes must be manually applied across upgrades.

Configure TCP/IP Settings

To allow proper system communication, the following ports on the Clarity LIMS server must be accessible by the LIMS clients:

- TCP/IP Port 22 (SFTP) for file transfers between the client and server
- TCP/IP Port 443 (HTTPS) for Apache proxy
- TCP/IP Port 80 (HTTP) used to forward any unknown, unsecured requests over SSL / TLS and port 443.

The following ports are required on the local Clarity LIMS server:

- TCP/IP Port 4369 for Erlang port mapping daemon (Epmd) for RabbitMQ
- TCP/IP Port 5432 for PostgreSQL database communications *
- TCP/IP Port 9009 for Tomcat
- TCP/IP Port 9200 for Elastic Search
- TCP/IP Port 9300 for Elastic Search
- TCP/IP Port 5672 for RabbitMQ
- TCP/IP Port 15672 for RabbitMQ

The database ports are configurable and might be different in your organization.

Configure Automation Worker TCP/IP Settings

Computers running an automation worker must be able to reach the Clarity LIMS server via the following ports:

- TCP/IP Port 22 (SFTP) for file transfers between the client and server
- TCP/IP Port 443 (HTTPS) for Apache proxy
- TCP/IP Port 80 (HTTP) used to forward any unknown, unsecured requests over SSL / TLS and port 443.

Configure VPN Access for Hosted Systems

To facilitate instrument integrations, a site-to-site IPSEC VPN connection can be set up between your facility and the hosted instance.

There are two ports that must be opened: 4500/udp and 500/udp.

If a VPN is required, you must provide more detailed setup information to the Clarity LIMS Support team. Upon request, the Clarity LIMS Support team will provide the additional form required to do this.

Save Apache Proxy Configuration

Clarity LIMS uses an Apache proxy and the Clarity LIMS installation process installs and configures it automatically. If the server already has an Apache proxy installed and configured, the installation process overwrites the current configuration. If that configuration is important, you must back it up before running the Clarity LIMS installation process. Any settings that are important to your organization must be reconfigured manually after an install or upgrade of Clarity LIMS.

Install and Configure HashiCorp Vault

In Clarity LIMS v6.0.0 and later, you can choose to install and configure a HashiCorp Vault to store Clarity LIMS-related passwords and secrets safely.

For more information, refer to *Configure Your HashiCorp Vault* on page 328.

Installation Procedures

This section provides instructions for installing on-premise or cloud hosted deployments of Clarity LIMS v6.0 and later. For assistance with installation steps, contact the Clarity LIMS Support team.

Installation Procedure (Clarity LIMS v6.2)

This document provides the steps required to install a new Clarity LIMS v6.2 instance to Oracle Linux/RedHat Enterprise Linux v8.8 and v8.9.

The installation procedure includes adding the Clarity LIMS repository, installing the Clarity LIMS RPM through yum commands, and configuring the installation through a series of configuration scripts.

Prerequisites

- Your system meets the requirements listed in *Technical Requirements* on page 5.
- You have installed and configured the required components. For more information, refer to *Pre-Installation Requirements* on page 232.
- You have a database user and two empty schemas on your database server. The schemas are populated during configuration.
- You have received the appropriate repository files from the Clarity LIMS Support team.
- All standard OS security updates have been applied.
- All instances of Clarity LIMS must have a purchased SSL/TLS certificate installed. Purchase the certificate before installation or upgrade. For instructions on installing purchased SSL/TLS certificates, refer to *Install a Purchased SSL/TLS Certificate* on page 333.

With the Oracle Linux/RedHat Enterprise Linux server, the following error messages can display when you perform the yum commands used to install Clarity LIMS:

```
Failed loading plugin "product-id": No module named 'urllib3'
```

```
Failed loading plugin "subscription-manager": No module named 'urllib3'
Failed loading plugin "upload-profile": No module named 'urllib3'
```

These messages do not affect the installation of Clarity LIMS. You can resolve these error messages by running the following command:

```
pip3 install urllib3==1.24.2
```

Step 1: Add the Clarity LIMS Repository

1. Using scp/sftp, WinSCP, FileZilla, PSCP, or similar, copy the repository to the following location:

```
/etc/yum.repos.d
```

2. Test the repo file with the following command:

```
yum --enablerepo=GLS_Clarity62 search ClarityLIMS-App
```

Step 2: Install Clarity LIMS

1. Run the install command:

```
yum --enablerepo=GLS_Clarity62 install ClarityLIMS-App
```

2. Type `y` to download and install the Clarity LIMS RPM core components.

The installation of Clarity LIMS creates the following three operating system users:

- glsai—User to run the Automation Worker node
- glsftp—User to access the SFTP file store
- glsjboss—Runs the application server

These users are created by the RPM installation process, and should not be created before starting the installation steps. The user home directories are created in the directory `/opt/gls/clarity/users`.

The operating system passwords for each user should be set by the root user.

Step 3: Run Configuration Scripts

1. As the glsjboss user, change directory to `/opt/gls/clarity/config/pending` with the following command:

```
cd /opt/gls/clarity/config/pending
```

2. Run the first script listed sequentially in the directory listing with the following bash command:

```
bash /opt/gls/clarity/config/pending/05_configure_claritylims_secretutil.sh
```

This script configures the Secret Utility password management tool so that secrets and passwords are accessible. It is recommended that you store application secrets in vault. If that is not possible, the configuration script supports file-based storage. For more information about the prompts, refer to *Guide to Secret Management* on page 315.

3. Run the following script:

```
bash /opt/gls/clarity/config/pending/20_configure_claritylims_platform.sh
```

4. Run the next script to initialize the database and overwrite any existing data:

```
bash /opt/gls/clarity/config/pending/26_initialize_claritylims_tenant.sh
```

> This script requires that you enter the password for the glsftp user. Entering the password does not set the password for this user.

5. If your database server is standalone or remote, update the `/opt/gls/clarity/tomcat/current/lib/activity-management-ui-config.groovy` file with the following code snippet. Substitute the `Remote DB IP` and `Remote DB Port` placeholders with the information for your server.

```
hibernate {
    isis {
        template {
            url="jdbc:postgresql://<Remote DB IP>:<Remote DB Port>/{0}"
        }
    }
}
```

> If you do not update the script, log and database connection errors can occur.

6. Change to the root user, and then run the following script in the sequence to configure RabbitMQ:

```
bash /opt/gls/clarity/config/pending/32_root_configure_rabbitmq.sh
```

7. As the root user, install the Apache proxy with the following script:

```
bash /opt/gls/clarity/config/pending/40_root_install_proxy.sh
```

Step 4: Install LabLink

LabLink v2.4 is compatible with Clarity LIMS v6.2. Before installing LabLink v2.4, make sure that a database named LabLink is created with the same database user as the Clarity LIMS database.

1. Turn off all Clarity LIMS services using the following command:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

2. Install the LabLink RPM with the following yum command. Make sure that you have the correct repo enabled:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-LabLink
```

3. As the glsjboss user, run the pending initialization script using the following command:

```
bash /opt/gls/clarity/config/pending/60_initialize_lablink.sh
```

4. Restart all Clarity LIMS services using the following command:

```
/opt/gls/clarity/bin/run_clarity.sh start
```

5. Make sure that LabLink is accessible at `https://<your-Clarity-FQDN>/lablink`.

For Research Use Only. Not for use in diagnostic procedures.

Step 5: Start the System

Clarity LIMS includes the `run_clarity.sh` script. This script starts (or stops) all Clarity LIMS services (Elasticsearch, RabbitMQ, Search Indexing, Tomcat, httpd/Apache proxy, Automation Worker) in the required order, with one command.

Run the following script as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh (start|stop|restart)
```

If an error occurs starting any service, subsequent services will not be started. Stop all services before trying to start them again.

Start the system as follows.

1. Switch to the root user.
2. Make sure that no Clarity LIMS services are running.
3. Run the script with the following start command:

```
/opt/gls/clarity/bin/run_clarity.sh start
```

4. After the script has completed, all Clarity LIMS services should be ready for use.

If any services are running, the script exits and provides a list of services to stop. In this scenario, complete the following steps:

1. Use the script with the `stop` command to stop services.
2. Open a supported browser window and make sure that you can access the Clarity LIMS client at the following URL:

```
https://<your-Clarity-FQDN>/
```

Installation Procedure (Clarity LIMS v6.1)

This document provides the steps required to install a new Clarity LIMS v6.1 instance to RedHat Enterprise Linux/CentOS 7.9 operating system (OS).

The installation procedure includes adding the Clarity LIMS repository, installing the Clarity LIMS RPM through yum commands, and configuring the installation through a series of configuration scripts.

Prerequisites

- Your system meets the requirements listed in *Technical Requirements* on page 5.
- You have installed and configured the required components. For more information, refer to *Pre-Installation Requirements* on page 232.
- You have a database user and two empty schemas on your database server. The schemas are populated during configuration.
- You have received the appropriate repository files from the Clarity LIMS Support team.
- All standard OS security updates have been applied.

- All instances of Clarity LIMS must have a purchased SSL / TLS certificate installed. Purchase the certificate before installation or upgrade. For instructions on installing purchased SSL/TLS certificates, refer to *Install a Purchased SSL/TLS Certificate* on page 333.

Step 1: Add the Clarity LIMS Repository

1. Using scp/sftp, WinSCP, FileZilla, PSCP, or similar, copy the repository to the following location:

```
/etc/yum.repos.d
```

2. Test the repo file with the following command:

```
yum --enablerepo=GLS_Clarity6 search ClarityLIMS-App
```

Step 2: Install Clarity LIMS

1. Run the install command:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-App
```

2. Type `y` to download and install the Clarity LIMS RPM core components.

The installation of Clarity LIMS creates the following three operating system users:

- glsai—User to run the Automation Worker node
- glsftp—User to access the SFTP file store
- glsjboss—Runs the application server

These users are created by the RPM installation process, and should not be created before starting the installation steps. The user home directories are created in the directory `/opt/gls/clarity/users`.

The operating system passwords for each user should be set by the root user.

Step 3: Run Configuration Scripts

1. As the glsjboss user, change directory to `/opt/gls/clarity/config/pending` as follows:

```
cd /opt/gls/clarity/config/pending
```

2. Run the first script listed sequentially in the directory listing.

```
bash /opt/gls/clarity/config/pending/05_configure_claritylims_secretutil.sh
```

This script configures the Secret Utility password management tool so that secrets and passwords are accessible. For more information about the prompts, refer to *Guide to Secret Management* on page 315.

For RabbitMQ:

- You must configure the password in Vault (vault mode) / File (file mode) before running the `configure_rabbitmq.sh` script.
- If Secret Utility is using file mode, set the RabbitMQ password as follows:

```
java -jar /opt/gls/clarity/tools/secretutil/secretutil.jar -u="password"
app.rabbitmq.password
```

Using a vault is the safer way to store application secrets. If using a vault is not possible, the configuration script supports file-based storage.

3. Run the next script in the sequence, as follows:

```
bash /opt/gls/clarity/config/pending/20_configure_claritylims_platform.sh
```

4. Run the next script to initialize the database and overwrite any existing data:

```
bash /opt/gls/clarity/config/pending/26_initialize_claritylims_tenant.sh
```

This script requires that you enter the password for the glsftp user. Entering the password does not set the password for this user.

5. If your database server is standalone or remote, update the `/opt/gls/clarity/tomcat/current/lib/activity-management-ui-config.groovy` file with the following code snippet. Substitute the `Remote DB IP` and `Remote DB Port` placeholders with the information for your server.

```
hibernate {
    isis {
        template {
            url="jdbc:postgresql://<Remote DB IP>:<Remote DB Port>/{0}"
        }
    }
}
```

If you do not update the script, log and database connection errors can occur.

6. Change to the root user, and then run the next script in the sequence to configure RabbitMQ:

```
bash /opt/gls/clarity/config/pending/32_root_configure_rabbitmq.sh
```

7. As the root user, install the Apache proxy:

```
bash /opt/gls/clarity/config/pending/40_root_install_proxy.sh
```

Step 4: Install LabLink

Before installing LabLink v2.3, make sure that a database named LabLink is created with the same database user as the Clarity LIMS database.

1. Turn off all Clarity LIMS services using the following command:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

2. Install the LabLink RPM as follows (make sure that you have the correct repo enabled):

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-LabLink
```

3. As the glsjboss user, run the pending initialization script using the following command:

```
bash /opt/gls/clarity/config/pending/60_initialize_lablink.sh
```

The script prompts for a Google reCAPTCHA URL, site key, and secret key. If you prefer not to use reCAPTCHA, leave those fields blank. If the fields are blank, LabLink does not display the reCAPTCHA. Alternatively, you can use your own reCAPTCHA accounts when configuring LabLink.

4. Restart all Clarity LIMS services using the following command:

```
/opt/gls/clarity/bin/run_clarity.sh start
```

5. LabLink should now be accessible at the following address: `https://<your-Clarity-FQDN>/lablink`

Step 5: Start the System

Clarity LIMS includes the `run_clarity.sh` script. This script starts (or stops) all Clarity LIMS services (Elasticsearch, RabbitMQ, Search Indexing, Tomcat, httpd/Apache proxy, Automation Worker) in the required order, with one command.

Run the following script as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh (start|stop|restart)
```

If an error occurs starting any service, subsequent services will not be started. Stop all services before trying to start them again.

Start the system as follows.

1. Switch to the root user.
2. Make sure that no Clarity LIMS services are running.
3. Run the script with the following start command:

```
/opt/gls/clarity/bin/run_clarity.sh start
```

4. After the script has completed, all Clarity LIMS services should be ready for use.

If any services are running, the script exits and provides a list of services to stop. In this scenario, complete the following steps:

1. Use the script with the `stop` command to stop services.
2. Open a supported browser window and make sure that you can access the Clarity LIMS client at the following URL:

```
https://<your-Clarity-FQDN>/
```

Installation Procedure (Clarity LIMS v6.0)

This document provides the steps required to install a new Clarity LIMS v6.0 instance to RedHat Enterprise Linux/CentOS 7.9 operating system (OS).

The installation procedure includes adding the Clarity LIMS repository, installing the Clarity LIMS RPM through yum commands, and configuring the installation through a series of configuration scripts.

Prerequisites

- Your system meets the requirements listed in *Technical Requirements* on page 5.
- You have installed and configured the required components. Refer to *Pre-Installation Requirements* on page 232.
- You have a database user and two empty schemas on your database server. The schemas are populated during configuration.
- You have received the appropriate repository files from the Clarity LIMS Support team.
- All standard OS security updates have been applied.
- All instances of Clarity LIMS must have a purchased SSL / TLS certificate installed. Purchase the certificate before installation or upgrade. For instructions on installing purchased SSL/TLS certificates, refer to *Install a Purchased SSL/TLS Certificate* on page 333.

Step 1: Add the Clarity LIMS Repository

1. Using scp/sftp, WinSCP, FileZilla, PSCP, or similar, copy the repository to the following location:

```
/etc/yum.repos.d
```

2. Test the repo file with the following command:

```
yum --enablerepo=GLS_Clarity6 search ClarityLIMS-App
```

Step 2: Install Clarity LIMS

1. Run the install command:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-App
```

2. Type `y` to download and install the Clarity LIMS RPM core components.

The installation of Clarity LIMS creates the following three operating system users:

- glsai—User to run the Automation Worker node
- glsftp—User to access the SFTP file store
- glsjboss—Runs the application server

These users are created by the RPM installation process, and should not be created before starting the installation steps. The user home directories are created in the directory `/opt/gls/clarity/users`.

The operating system passwords for each user should be set by the root user.

Step 3: Run Configuration Scripts

1. As the glsjboss user, change directory to `/opt/gls/clarity/config/pending` as follows:

```
cd /opt/gls/clarity/config/pending
```

2. Run the first script listed sequentially in the directory listing.

```
bash /opt/gls/clarity/config/pending/05_configure_claritylims_secretutil.sh
```

   This script configures the Secret Utility password management tool so that secrets and passwords are accessible. For more information about the prompts, refer to *Guide to Secret Management* on page 315.

   For RabbitMQ:

   - You must configure the password in Vault (vault mode) / File (file mode) before running the `configure_rabbitmq.sh` script.
   - If Secret Utility is using file mode, set the RabbitMQ password as follows:

```
java -jar /opt/gls/clarity/tools/secretutil/secretutil.jar -u="password"
app.rabbitmq.password
```

   > Using a vault is the safer way to store application secrets. If using a vault is not possible, the configuration script supports file-based storage.

3. Run the next script in the sequence, as follows:

```
bash /opt/gls/clarity/config/pending/20_configure_claritylims_platform.sh
```

4. Run the next script to initialize the database and overwrite any existing data:

```
bash /opt/gls/clarity/config/pending/26_initialize_claritylims_tenant.sh
```

   > This script requires that you enter the password for the glsftp user. Entering the password does not set the password for this user.

5. If your database server is standalone or remote, update the `/opt/gls/clarity/tomcat/current/lib/activity-management-ui-config.groovy` file with the following code snippet. Substitute the `Remote DB IP` and `Remote DB Port` placeholders with the information for your server.

```
hibernate {
    isis {
        template {
            url="jdbc:postgresql://<Remote DB IP>:<Remote DB Port>/{0}"
        }
    }
}
```

   > If you do not update the script, log and database connection errors can occur.

6. Change to the root user, and then run the next script in the sequence to configure RabbitMQ:

```
bash /opt/gls/clarity/config/pending/32_root_configure_rabbitmq.sh
```

7. As the root user, install the Apache proxy:

```
bash /opt/gls/clarity/config/pending/40_root_install_proxy.sh
```

Step 4: Install LabLink

Before installing LabLink v2.2, make sure that a database named LabLink is created with the same database user as the Clarity LIMS database.

1. Turn off all Clarity LIMS services using the following command:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

2. Install the LabLink RPM as follows (make sure that you have the correct repo enabled):

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-LabLink
```

3. As the glsjboss user, run the pending initialization script using the following command:

```
bash /opt/gls/clarity/config/pending/60_initialize_lablink.sh
```

> The script prompts for a Google reCAPTCHA URL, site key, and secret key. If you prefer not to use reCAPTCHA, leave those fields blank. If the fields are blank, LabLink does not display the reCAPTCHA. Alternatively, you can use your own reCAPTCHA accounts when configuring LabLink.

4. Restart all Clarity LIMS services using the following command:

```
/opt/gls/clarity/bin/run_clarity.sh start
```

5. LabLink should now be accessible at the following address: https://<your-Clarity-FQDN>/lablink

Step 5: Start the System

Clarity LIMS includes the `run_clarity.sh` script. This script starts (or stops) all Clarity LIMS services (Elasticsearch, RabbitMQ, Search Indexing, Tomcat, httpd/Apache proxy, Automation Worker) in the required order, with one command.

Run the following script as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh (start|stop|restart)
```

If an error occurs starting any service, subsequent services will not be started. Stop all services before trying to start them again.

Start the system as follows.

1. Switch to the root user.
2. Make sure that no Clarity LIMS services are running.
3. Run the script with the following start command:

```
/opt/gls/clarity/bin/run_clarity.sh start
```

4. After the script has completed, all Clarity LIMS services should be ready for use.

If any services are running, the script exits and provides a list of services to stop. In this scenario, complete the following steps:

1. Use the script with the `stop` command to stop services.

2. Open a supported browser window and make sure that you can access the Clarity LIMS client at the following URL:

```
https://<your-Clarity-FQDN>/
```

On Premise to Cloud Upgrade Procedures

This section provides instructions for upgrading existing on premise Clarity LIMS deployments to cloud hosted deployments. For assistance with upgrade steps, contact the Clarity LIMS Support team.

Upgrade Procedure for On Premise to Cloud Deployments

From Versions 4.2 / 4.3 / 5.0 / 5.1 / 5.2 / 6.0 / 6.1 (PostgreSQL) and 4.3 / 5.2 (Oracle) to 6.2

This section provides the steps required to upgrade an existing on-premise deployment of Clarity LIMS to a RedHat Enterprise Linux/Oracle Linux compatible Illumina cloud hosted deployment of Clarity LIMS v6.2.

For installation requirements, refer to the *Technical Requirements* on page 5.

Migration Paths

The following table shows the applicable migration paths.

From	To	Notes
PostgreSQL: • v4.2 On-premise • v5.0 On-premise • v5.1 On-premise	v6.2 Cloud	Upgrading from CentOS6 to Oracle Linux v8.8 and v8.9 (on-premise to hosted).
PostgreSQL: • v4.3 On-premise • v5.2 On-premise • v6.0 On-premise • v6.1 On-premise	v6.2 Cloud	Upgrading from CentOS7 to Oracle Linux v8.8 and v8.9 (on-premise to hosted).
Oracle: • v4.3 On-premise • v5.2 On-premise	v6.2 Cloud	Migrating from Oracle to PostgreSQL. v6.2 supports PostgreSQL only.

Prerequisites

Before Illumina can proceed with the upgrade, complete the following prerequisite steps.

For Research Use Only. Not for use in diagnostic procedures.

Provision the New Instance

Illumina provisions an instance installed with the latest qualified Oracle Linux version in the cloud.

Upgrades are only supported from Clarity LIMS versions 4.2, 4.3, 5.0, 5.1, 5.2, 6.0, and 6.1 (on-premise).

- Custom configurations: If you have made any additional configurations that are not part of the Clarity LIMS preinstallation requirements, apply these configurations to the new instance.
- Passwords: Configure all passwords to be same as the existing instance. After you have verified the new instance, you can change passwords as needed.

Verify User Account Email Addresses

Make sure that all user accounts have email addresses associated with them. User passwords must be reset after the upgrade is complete.

Install and Run the Pre-Validation Script on the Source Server

To assist with validating the system before an upgrade, install the `UpgradePreValidation` RPM on the source server.

- This RPM is installed temporarily, and provides tools to help check the system before an upgrade.
- If validation is successful, you can remove this RPM and proceed with the upgrade.

1. Install the `UpgradePreValidation` RPM. Make sure you have the correct repo enabled.
   - On the source server, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-UpgradePreValidation
```

2. [Optional] Set up Secret Utility.
   - If ClarityLIMS-SecretUtil was installed previously, run the following command to set up Secret Utility as the glsjboss user:

```
/opt/gls/clarity/config/pending/05_configure_claritylims_secretutil.sh
```

   Using a vault is the safer way of storing application secrets. If using a vault is not possible, the configuration script supports file-based storage.

   - For more information on the prompts, refer to the Configuration Script section of *Guide to Secret Management* on page 315.
3. Run the validation script.
   a. Make sure that the Clarity LIMS server is running.
   b. As the root user, run the following command:

```
bash /opt/gls/ClarityUpgradeValidation/bin/validate.sh
```

c. Review the output of the script to determine if you can proceed with the upgrade. If the script outlines any issues with the potential upgrade, review the generated log files and contact the Clarity LIMS Support team for further assistance.

4. Remove the `Pre-Validation` RPM.

> Remove the `Pre-Validation` RPM only after you confirm that you can upgrade. If you are unsure, consult the Clarity LIMS Support team.

As the root user, run the following command:

```
yum remove ClarityLIMS-UpgradePreValidation
```

Back Up the Current Database and Clarity LIMS

Archive the backup in case a rollback is required.

Before performing the backup, stop Clarity LIMS. The following command stops all Clarity LIMS components, including Automation Worker and integration services.

1. Stop Clarity LIMS:
   - On the command-line interface, run the following command as the root user:

   ```
   /opt/gls/clarity/bin/run_clarity.sh stop
   ```

2. Back up PostgreSQL database:
   On the PostgreSQL server, best practice recommends backing up the database using the pg_dump utility.
   The following example assumes the following:
   - The database server and the application server are on the same server.
   - The pg_dump utility is accessible to the glsjboss user.

   Example:
   The Postgres DBA uses the following commands to create a database backup in the glsjboss home directory. Substitute the variables as appropriate for the specific environment.
   - As the glsjboss user:

   ```
   cd ~glsjboss
   mkdir -p backups/database
   pg_dump -U database_user -b -O -Ft database_name -f
   ~glsjboss/backups/database/clarity-old_version-`date +%Y%m%d%H%M`.tar
   ```

3. Make sure that the following items, and any other files and configurations, are backed up safely:
   - crontab -l
   - custom scripts
   - OS configuration files
   - firewall rules

For Research Use Only. Not for use in diagnostic procedures.

  - network configuration
- If there are custom changes to any application configurations (to increase performance, security, etc.), restore/configure these customizations manually later by referencing the backup.
- We recommend that you back up the items into a single zip file and transfer them to the new instance.

Directories:

```
/opt/gls/clarity/users/glsftp or /home/glsftp (Clarity LIMS file store location)
/opt/gls/clarity/customextensions
/opt/gls/clarity/glscontents
```

Additional configurations:

```
rpm -qa | grep "BaseSpace\|Clarity" > clarityrpms.txt
```

Upgrade Steps

Illumina assists with the deployment of cloud-hosted Clarity LIMS instances. For more information, contact Illumina Support.

Upgrade Procedure for On Premise to Cloud Deployments

From Versions 4.2 / 4.3 / 5.0 / 5.1/ 5.2 / 6.0 (PostgreSQL) and 4.3 / 5.2 (Oracle) to 6.1

This section provides the steps required to upgrade an existing on-premise deployment of Clarity LIMS to a RedHat Enterprise Linux/CentOS compatible Illumina cloud hosted deployment of Clarity LIMS v6.1.

For installation requirements, refer to the *Technical Requirements* on page 5.

Migration Paths

The following table shows the applicable migration paths.

From	To	Notes
PostgreSQL: • v4.2 On-premise • v5.0 On-premise • v5.1 On-premise	v6.1 Cloud	Upgrading from CentOS6 to CentOS7.
PostgreSQL: • v4.3 On-premise • v5.2 On-premise • v6.0 On-premise	v6.1 Cloud	Upgrading from on-premise to Illumina cloud hosted.

For Research Use Only. Not for use in diagnostic procedures.

From	To	Notes
Oracle: • v4.3 On-premise • v5.2 On-premise	v6.1 Cloud	Migrating from Oracle to PostgreSQL. v6.1 supports PostgreSQL only.

Prerequisites

Before Illumina can proceed with the upgrade, complete the following prerequisite steps.

1. Provision the New Instance

Illumina provisions an instance installed with the latest qualified CentOS version in the cloud.

Upgrades are only supported from Clarity LIMS versions 4.2, 4.3, 5.0, 5.1, 5.2, and 6.0 (on-premise).

- Custom configurations: If you have made any additional configurations that are not part of the Clarity LIMS preinstallation requirements, apply these configurations to the new instance.
- Passwords: Configure all passwords to be same as the existing instance. After you have verified the new instance, you can change passwords as needed.

2. Verify User Account Email Addresses

Make sure that all user accounts have email addresses associated with them. User passwords must be reset after the upgrade is complete.

3. Install and Run the Pre-Validation Script on the Source Server

To assist with validating the system before an upgrade, install the UpgradePreValidation RPM on the source server.

- This RPM is installed temporarily, and provides tools to help check the system before an upgrade.
- If validation is successful, you can remove this RPM and proceed with the upgrade.

1. Install the UpgradePreValidation RPM. Make sure you have the correct repo enabled.
   - On the source server, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-UpgradePreValidation
```

2. [Optional] Set up Secret Utility.
   - If ClarityLIMS-SecretUtil was installed previously, run the following command to set up Secret Utility as the glsjboss user:

```
/opt/gls/clarity/config/pending/05_configure_claritylims_secretutil.sh
```

Using a vault is the safer way of storing application secrets. If using a vault is not possible, the configuration script supports file-based storage.

- For more information on the prompts, refer to the Configuration Script section of *Guide to Secret Management* on page 315.

3. Run the validation script.
   a. Make sure that the Clarity LIMS server is running.
   b. As the root user, run the following command:

```
bash /opt/gls/ClarityUpgradeValidation/bin/validate.sh
```

   c. Review the output of the script to determine if you can proceed with the upgrade. If the script outlines any issues with the potential upgrade, review the generated log files and contact the Clarity LIMS Support team for further assistance.
4. Remove the Pre-Validation RPM.

> Remove the Pre-Validation RPM only after you confirm that you can upgrade. If you are unsure, consult the Clarity LIMS LIMS Support team.

As the root user, run the following command:

```
yum remove ClarityLIMS-UpgradePreValidation
```

4. Back Up the Current Database and Clarity LIMS

Archive the backup in case a rollback is required.

Before performing the backup, stop Clarity LIMS. The following command stops all Clarity LIMS components, including Automation Worker and integration services.

1. Stop Clarity LIMS:
   - On the command-line interface, run the following command as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

2. Back up PostgreSQL database:
   On the PostgreSQL server, best practice recommends backing up the database using the pg_dump utility.
   The following example assumes the following:
   - The database server and the application server are on the same server.
   - The pg_dump utility is accessible to the glsjboss user.

   Example:
   The Postgres DBA uses the following commands to create a database backup in the glsjboss home directory. Substitute the variables as appropriate for the specific environment.
   - As the glsjboss user:

```
cd ~glsjboss
mkdir -p backups/database
pg_dump -U database_user -b -O -Ft database_name -f
~glsjboss/backups/database/clarity-old_version-`date +%Y%m%d%H%M`.tar
```


For Research Use Only. Not for use in diagnostic procedures.

3. Make sure that the following items, and any other files and configurations, are backed up safely:
    - crontab -l
    - custom scripts
    - OS configuration files
    - firewall rules
    - network configuration
    - If there are custom changes to any application configurations (to increase performance, security, etc.), restore/configure these customizations manually later by referencing the backup.
    - We recommend that you back up the items into a single zip file and transfer them to the new instance.

    Directories:

```
/opt/gls/clarity/users/glsftp or /home/glsftp (Clarity LIMS file store location)
/opt/gls/clarity/customextensions
/opt/gls/clarity/glscontents
```

    Additional configurations:

```
rpm -qa | grep "BaseSpace\|Clarity" > clarityrpms.txt
```

Upgrade Procedure for On Premise to Cloud Deployments

From Versions 4.2 / 4.3 / 5.0 / 5.1 / 5.2 (PostgreSQL) and 4.3 / 5.2 (Oracle) to 6.0

This section provides the steps required to upgrade an existing on-premise deployment of Clarity LIMS to a RedHat Enterprise Linux/CentOS compatible Illumina cloud hosted deployment of Clarity LIMS v6.0.

For installation requirements, refer to the *Technical Requirements* on page 5.

Migration Paths

The following table shows the applicable migration paths.

From	To	Notes
PostgreSQL: • v4.2 On-premise • v5.0 On-premise • v5.1 On-premise	v6.0 Cloud	Upgrading from CentOS6 to CentOS7.

From	To	Notes
PostgreSQL: • v4.3 On-premise • v5.2 On-premise	v6.0 Cloud	Upgrading from on-premise to Illumina cloud hosted.
Oracle: • v4.3 On-premise • v5.2 On-premise	v6.0 Cloud	Migrating from Oracle to PostgreSQL. v6.0 supports PostgreSQL only.

Prerequisites

Before Illumina can proceed with the upgrade, complete the following prerequisite steps.

1. Provision the New Instance

Illumina provisions an instance installed with the latest qualified CentOS version in the cloud.

Upgrades are only supported from Clarity LIMS versions 4.2, 4.3, 5.0, 5.1, and 5.2.

- Custom configurations: If you have made any additional configurations that are not part of the Clarity LIMS preinstallation requirements, apply these configurations to the new instance.
- Passwords: Configure all passwords to be same as the existing instance. After you have verified the new instance, you can change passwords as needed.

2. Verify User Account Email Addresses

Make sure that all user accounts have email addresses associated with them. User passwords must be reset after the upgrade is complete.

3. Install and Run the Pre-Validation Script on the Source Server

To assist with validating the system before an upgrade, install the UpgradePreValidation RPM on the source server.

- This RPM is installed temporarily, and provides tools to help check the system before an upgrade.
- If validation is successful, you can remove this RPM and proceed with the upgrade.

1. Install the UpgradePreValidation RPM (make sure you have the correct repo enabled).
   - On the source server, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-UpgradePreValidation
```

2. [Optional] Set up Secret Utility.
   - If ClarityLIMS-SecretUtil was installed previously, run the following command to set up Secret Utility as the glsjboss user:

```
/opt/gls/clarity/config/pending/05_configure_claritylims_secretutil.sh
```

Using a vault is the safer way of storing application secrets. If using a vault is not possible, the configuration script supports file-based storage.

- For more information on the prompts, refer to the Configuration Script section of *Guide to Secret Management* on page 315.

3. Run the validation script.
   a. Make sure that your Clarity LIMS server is running.
   b. As the root user, run the following command:

```
bash /opt/gls/ClarityUpgradeValidation/bin/validate.sh
```

   c. Review the output of the script to determine if you can proceed with the upgrade. If the script outlines any issues with the potential upgrade, review the generated log files and contact the Clarity LIMS Support team for further assistance.
4. Remove the Pre-Validation RPM.

Remove the Pre-Validation RPM only after you confirm that you can upgrade. If you are unsure, consult the Clarity LIMS LIMS Support team.

As the root user, run the following command:

```
yum remove ClarityLIMS-UpgradePreValidation
```

4. Back Up the Current Database and Clarity LIMS

Archive the backup in case a rollback is required.

Before performing the backup, stop Clarity LIMS. The following command stops all Clarity LIMS components, including Automation Worker and integration services.

1. Stop Clarity LIMS:
   - On the command-line interface, run the following command as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

2. Back up PostgreSQL database:
   On the PostgreSQL server, best practice recommends backing up the database using the pg_dump utility.
   The following example assumes the following:
   - The database server and the application server are on the same server.
   - The pg_dump utility is accessible to the glsjboss user.

   Example:
   The Postgres DBA uses the following commands to create a database backup in the glsjboss home directory. Substitute the variables as appropriate for the specific environment.
   - As the glsjboss user:

```
cd ~glsjboss
```


For Research Use Only. Not for use in diagnostic procedures.

```
mkdir -p backups/database
pg_dump -U database_user -b -O -Ft database_name -f
~glsjboss/backups/database/clarity-old_version-`date +%Y%m%d%H%M`.tar
```

3. Make sure that the following items, and any other files and configurations, are backed up safely:
    - crontab -l
    - custom scripts
    - OS configuration files
    - firewall rules
    - network configuration
    - If there are custom changes to any application configurations (to increase performance, security, etc.), restore/configure these customizations manually later by referencing the backup.
    - We recommend that you back up the items into a single zip file and transfer them to the new instance.

    Directories:

```
/opt/gls/clarity/users/glsftp or /home/glsftp (Clarity LIMS file store location)
/opt/gls/clarity/customextensions
/opt/gls/clarity/glscontents
```

    Additional configurations:

```
rpm -qa | grep "BaseSpace\|Clarity" > clarityrpms.txt
```

On Premise to On Premise Upgrade Procedures

This section provides instructions for upgrading an existing on premise Clarity LIMS deployment. For assistance with upgrade steps, contact the Clarity LIMS Support team.

Upgrade Procedure for On Premise to On Premise Deployments

From Versions 4.2 / 4.3 / 5.0 / 5.1 / 5.2 / 6.0 / 6.1 (PostgreSQL) and 4.3 / 5.2 (Oracle) to 6.2

This section provides the steps required to upgrade an existing on-premise deployment of Clarity LIMS to a RedHat Enterprise Linux/Oracle Linux compatible on-premise deployment of Clarity LIMS v6.2.

The installation procedure includes provisioning and configuring the new instance, and installing and then verifying the new Clarity LIMS version.

For installation requirements, refer to the *Technical Requirements* on page 5.

If you have questions about the upgrade procedure, contact the Clarity LIMS Support team.

Migration Paths

The following table shows the applicable migration paths.

From	To	Notes
PostgreSQL: v4.2 On-premise v5.0 On-premise v5.1 On-premise	v6.2 On-premise	Upgrading from CentOS6 to Oracle Linux v8.8 and v8.9.
PostgreSQL: v4.3 On-premise v5.2 On-premise v6.0 On-premise v6.1 On-premise	v6.2 On-premise	Upgrading from CentOS7 to Oracle Linux v8.8 and v8.9.
Oracle: v4.3 On-premise v5.2 On-premise	v6.2 On-premise	Migrating from Oracle to PostgresQL. v6.2 supports PostgreSQL only.

Prerequisites

Provision the New Instance

We recommend you provision an instance with similar or higher specifications to the current Clarity LIMS instance.

Note the following:

- Your system must meet the requirements listed in *Technical Requirements* on page 5
- All standard operating system (OS) security updates must have been applied.
- Upgrades are only supported from Clarity LIMS versions 4.2, 5.0, 5.1, 6.0, 6.1 and 4.3 and 5.2 (Oracle).
- The command `hostname -f` must resolve to the fully qualified domain name (FQDN) of the server. For details, refer to the *Confirm Hostname Resolution* section of *Pre-Installation Requirements* on page 232.

> Before installing Clarity LIMS on the new instance, make sure that the instance has the same FQDN as the existing production instance. If your new instance cannot have the same FQDN as the production instance, contact the Illumina Support team.

For Research Use Only. Not for use in diagnostic procedures.

Configure the New Instance

To configure the new instance, follow the instructions provided in the *Pre-Installation Requirements* on page 232 and refer to *Technical Overview* on page 2.

- Custom configurations: If you have made any additional configurations that are not part of the Clarity LIMS pre-installation requirements, apply these configurations to the new instance.
- Passwords: Configure all passwords to be same as the existing instance. After you have verified the new instance, you can change passwords as needed.

Verify the User Account Email Addresses

Make sure that all user accounts have email addresses associated with them. Users must reset their passwords after the upgrade is complete.

Install and Run the Pre-Validation Script on the Source Server

To assist with validating the system before an upgrade, install the `UpgradePreValidation` RPM on the source server.

- This RPM is installed temporarily, and provides tools to help check the system before an upgrade.
- If validation is successful, you can remove this RPM and proceed with the upgrade.

1. Install the `UpgradePreValidation` RPM (make sure you have the correct repo enabled).
   - On the source server, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-UpgradePreValidation
```

2. [Optional] Set up Secret Utility.
   - If ClarityLIMS-SecretUtil was installed previously, run the following command to set up Secret Utility as the glsjboss user:

```
/opt/gls/clarity/config/pending/05_configure_claritylims_secretutil.sh
```

     Using a vault is the safer way of storing application secrets. If using a vault is not possible, the configuration script supports file-based storage.

   - For more information on the prompts, refer to the Configuration Script section of *Guide to Secret Management* on page 315.
3. Run the validation script as follows.
   a. Make sure that the Clarity LIMS server is running.
   b. As the root user, run the following command:

```
bash /opt/gls/ClarityUpgradeValidation/bin/validate.sh
```

   c. Review the output of the script to determine if you can proceed with the upgrade. If the script outlines any issues with the potential upgrade, review the generated log files and contact the Clarity LIMS Support team for further assistance.

For Research Use Only. Not for use in diagnostic procedures.

4. Remove the `PreValidation` RPM.
   Remove the `PreValidation` RPM only after you confirm that you can upgrade. If you are unsure, consult the Clarity LIMS LIMS Support team.
   - As the root user, run the following command:

```
yum remove ClarityLIMS-UpgradePreValidation
```

Back Up the Current Database and Clarity LIMS

Archive the backup in case a rollback is required.

Before performing the backup, stop Clarity LIMS.

1. Stop Clarity LIMS:
   - On the command-line interface, run the following command as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

   This command stops all Clarity LIMS components, including Automation Worker and integration services.
2. Back up PostgreSQL database:
   On the PostgreSQL server, best practice recommends backing up the database using the pg_dump utility.
   The following example assumes the following:
   - The database server and the application server are on the same server.
   - The pg_dump utility is accessible to the glsjboss user.

   Example:
   The Postgres DBA uses the following commands to create a database backup in the glsjboss home directory. Substitute the variables as appropriate for the specific environment.
   - As the glsjboss user:

```
cd ~glsjboss
mkdir -p backups/database
pg_dump -U <database_user> -b -O -Ft <database_name> -f
~glsjboss/backups/database/clarity-old_version-`date +%Y%m%d%H%M`.tar
```

3. Make sure that the following items, and any other files and configurations, are backed up safely:
   - crontab -l
   - Custom scripts
   - OS configuration files
   - Firewall rules
   - Network configuration

   If there are custom changes to any application configurations (to increase performance, security, etc.), restore/configure these items manually later by referencing the backup.

For Research Use Only. Not for use in diagnostic procedures.

We recommend that you back up the items into a single zip file and transfer them to the new instance.

Directories:

```
/opt/gls/clarity/users/glsftp or /home/glsftp (Clarity LIMS file store location)
/opt/gls/clarity/customextensions
/opt/gls/clarity/glscontents
/etc/httpd/conf.d
/etc/httpd/sslcertificate
```

Files:

```
.pgpass
/opt/gls/pgsql/9.x/pg_hba.conf
/opt/gls/pgsql/9.x/postgresql.conf
```

Additional configurations:

```
rpm -qa | grep "BaseSpace\|Clarity" > clarityrpms.txt
```

Upgrade Steps

Install Latest Clarity LIMS on New Instance

1. Make sure that the repository file exists in the following location:

```
/etc/yum.repos.d/
```

2. As the root user, install the RPMs required on the new instance by referencing the content of `clarityrpms.txt`.
   - If you are upgrading from Clarity LIMS v4.x, some RPMs (eg, Server RPM) are now included under other RPMs.
   - Install any other required RPMs (eg, Python packages) which are not part of the Clarity LIMS setup.
   - Do not install NGS, Illumina Preset Protocols (IPP), and Sequencing RPMs during this step. You install these RPMs later in the installation process.
3. Configure and validate the new system, following the procedure outlined in the *Installation Procedure (Clarity LIMS v6.2)* on page 237.
   - When prompted for user passwords, enter the passwords used in the previous instance.
4. Stop Clarity LIMS. To do so, on the command-line interface, run the following command as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

> The following steps are only required if you are restoring from a previous instance. If you are installing in a test environment, proceed to *Verify the New Instance* on page 264 section.

Install and Configure LabLink v2.4

LabLink v2.4 is compatible with Clarity LIMS v6.2.

If upgrading from Clarity LIMS v4.x, Illumina migrates your LabLink-related data with the following exceptions:

- Sample submission templates
- Customized UI CSS
- LabLink property table configurations

Before completing the following steps, make sure that a database named lablink is created with the same database user as Clarity LIMS database.

1. Install the `LabLink` RPM. Make sure that you have the correct repo enabled.
   - On the new instance, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-LabLink
```

2. Run the pending initialization script.
   - As the glsjboss user, run the following command:

```
bash /opt/gls/clarity/config/pending/60_initialize_lablink.sh
```

3. The script prompts for a Google reCAPTCHA URL, site key, and secret key.
   - Google reCAPTCHA URL: https://www.google.com/recaptcha/
   - Google reCAPTCHA site key and secret key: View these keys from the Google reCAPTCHA Admin Console, under Settings.

   > If you prefer not to use reCAPTCHA, leave the site-key and secret-key fields blank when running the configuration script. LabLink does not display the reCAPTCHA when these fields are left blank. You can also use your own reCAPTCHA accounts when configuring LabLink.

   - To reconfigure LabLink (without initializing the database), run the following command as the glsjboss user:

```
bash /opt/gls/clarity/config/configure_lablink.sh
```

Restore Backup Onto the New Instance

1. Extract the backup zip file into a suitable location (eg, `/tmp/restore`).

   > If using Oracle database, skip the following steps 2 and 3. Contact the Clarity LIMS Support team for assistance in performing the migration from Oracle to PostgreSQL.

2. If using PostgreSQL database, the DBA imports the database dump into the new database instance. Dropping and recreating the database might be necessary. If you need to do this, use the following command:

```
dropdb -U postgres <OL8DB>
```

```
createdb -U postgres <OL8DB>
psql -U postgres -d <OL8DB> -c 'ALTER DATABASE "<OL8DB>" OWNER TO "<OL8User>"'
```

3. Restore the database exported from the previous instance.
4. Extract and restore the following directories to the same directory on the new instance:
   - Clarity LIMS file store: `/opt/gls/clarity/users/glsftp` or `/home/glsftp`
   - `/opt/gls/clarity/custom/extensions`
   - `/opt/gls/clarity/glscontents`
   - `/etc/httpd/conf.d`

   As of RedHat Enterprise Linux/Oracle Linux 8.8, Apache v2.4 is installed. There are several configuration changes in this version. You can use the new configuration, or merge your previous configuration file cautiously to the new configuration file. For details on the changes, refer to: httpd.apache.org.
5. Copy the SSL certificate files to the following location (create the directory if it does not exist):

```
/etc/httpd/sslcertificate
```

6. To configure the certificates, run the following command on the command-line interface, as the root user:

```
/opt/gls/clarity/config/installCertificates.sh
```

   For more information, refer to *Install a Purchased SSL/TLS Certificate* on page 333.
7. Restore files and configurations.
   - Copy any custom scripts into their folder locations.
   - For PostgreSQL database, copy/merge the database configuration file (eg, `pg_hba.conf` and `postgresql.conf`).
   - Restore crontab from file.
   - Copy / Merge any additional application configurations.

[Optional] Change the Clarity LIMS Hostname

This step is required only if the new instance hostname is different from the old instance hostname.

For details, refer to *Change the Clarity LIMS Hostname* on page 326

[Optional] Update Application Configuration

This step is required only if the passwords for glsftp and/or apiuser have changed.

To update the application configuration, complete the following steps:

1. Update glsftp password.
2. Update apiuser password.

3. Update database connection details.

For details, refer to *Update Server Passwords and Database Connection Details* on page 331.

Perform Application Migration

In this step, the clarity-migrator tool is used to perform the changes required to make the database compatible with the new Clarity LIMS version.

On the command-line interface, run the following commands as the glsjboss user:

```
cd /opt/gls/clarity/config/
./migrate_claritylims_database.sh
```

[Optional] Install NGS, IPP, and Sequencing RPMs

This step is required only if the RPMs have been installed on the existing Clarity LIMS instance.

- Install the latest NGS, IPP, and Sequencing RPMs compatible with the new Clarity LIMS version, as listed in `clarityrpms.txt`.

All existing workflows, protocols, steps, and master steps are restored during the restoration process. After installing the NGS and IPP RPMs, you do not need to install the workflows again.

- If the automation/External Program Plugin (EPP) scripts installed on the new instance are of a later version (eg, `/opt/gls/cla/opt/gls/clarity/extensions/ngs-common/v5/EPP)`) to your old instance (eg, `/opt/gls/clarity/extensions/ngs-common/v4/EPP`), you must manually update the script location in your automation / EPP command lines. You can do update the script location in the Clarity LIMS interface or the Operations interface.
- If you intend to install NovaSeq API-based integration, NextSeq integration, or MiSeq integration, use the latest package to ensure OS compatibility.

Delete ElasticSearch indexes and Restart Clarity LIMS on the New Instance

On the command-line interface, run the following commands as the root user:

- Make sure that ElasticSearch is running:

```
service elasticsearch start
```

- When ElasticSearch service is running, remove the ElasticSearch indexes:

```
for indexname in `curl -s 'http://localhost:9200/_cat/indices?h=index'`; do echo
"Delete index: $indexname"; curl -XDELETE "http://localhost:9200/$indexname";
echo ""; done
```

- Restart Clarity LIMS:

```
/opt/gls/clarity/bin/run_clarity.sh stop
/opt/gls/clarity/bin/run_clarity.sh start
```


For Research Use Only. Not for use in diagnostic procedures.

Verify the New Instance

The following verification steps are the minimum required to confirm that the various services are up and running properly.

To conduct a thorough verification, perform your verification steps or daily routine on the new Clarity LIMS instance.

1. ElasticSearch, Search Indexer, and RabbitMQ
   a. Log in to Clarity LIMS LIMS via `https://<FQDN>/clarity` and perform a basic search.
   b. Check that search results are returned.
   c. If no search results are returned, try again later as the search indexes are still building.
2. Tomcat, Apache, Automation Worker
   a. Run a sample through a QC protocol step. Create a temporary workflow if necessary.
   b. Make sure that the automation executes successfully and the log files are accessible.
   c. Open a browser window and access `https://<FQDN>/api/v2/projects`.
   d. Log in with api user credentials.
   e. Check that all projects are returned in the response.
3. LabLink
   a. Open a browser window and access `https://<FQDN>/lablink/`.
   b. Log in with administrator credentials.
   c. On the page, make sure that all data are properly displayed.
4. [Optional] Sequencing Service
   To make sure that the service is running properly, you must initiate an actual sequencing run on the instrument.

Upgrade Procedure for On Premise to On Premise Deployments

From Versions 4.2 / 5.0 / 5.1 (PostgreSQL) and 4.3 / 5.2 (Oracle) to 6.1

This section provides the steps required to upgrade an existing on-premise deployment of Clarity LIMS to a RedHat Enterprise Linux / CentOS compatible on-premise deployment of Clarity LIMS v6.1.

The installation procedure includes provisioning and configuring the new instance, and installing and then verifying the new Clarity LIMS version.

For installation requirements, refer to the *Technical Requirements* on page 5.

If you have questions about the upgrade procedure, contact the Clarity LIMS Support team.

Migration Paths

The following table shows the applicable migration paths.

From	To	Notes
PostgreSQL: v4.2 On-premise v5.0 On-premise v5.1 On-premise	v6.1 On-premise	Upgrading from CentOS6 to CentOS7.
Oracle: v4.3 On-premise v5.2 On-premise	v6.1 On-premise	Migrating from Oracle to PostgresQL. v6.1 supports PostgreSQL only.

Prerequisites

1. Provision the New Instance

We recommend you provision an instance with similar or higher specifications to the current Clarity LIMS instance.

Note the following:

- Your system must meet the requirements listed in the Clarity LIMS*Technical Requirements* on page 5.
- All standard operating system (OS) security updates must have been applied.
- Upgrades are only supported from Clarity LIMS versions 4.2, 5.0, and 5.1 and 4.3 and 5.2 (Oracle).
- The command `hostname -f` must resolve to the fully qualified domain name (FQDN) of the server. For details, refer to the Verify Hostname Resolution section of *Pre-Installation Requirements* on page 232.

> Before installing Clarity LIMS on the new instance, make sure that the instance has the same FQDN as the existing production instance. If your new instance cannot have the same FQDN as the production instance, contact the Illumina Support team.

2. Configure the New Instance

To configure the new instance, follow the instructions provided in the Clarity LIMS *Pre-Installation Requirements* on page 232 and refer to *Technical Overview* on page 2.

- Custom configurations: If you have made any additional configurations that are not part of the Clarity LIMS pre-installation requirements, apply these configurations to the new instance.
- Passwords: Configure all passwords to be same as the existing instance. After you have verified the new instance, you can change passwords as needed.

3. Verify the User Account Email Addresses

Make sure that all user accounts have email addresses associated with them. Users must reset their passwords after the upgrade is complete.

4. Install and Run the Pre-Validation Script on the Source Server

To assist with validating the system before an upgrade, install the UpgradePreValidation RPM on the source server.

- This RPM is installed temporarily, and provides tools to help check the system before an upgrade.
- If validation is successful, you can remove this RPM and proceed with the upgrade.

1. Install the UpgradePreValidation RPM (make sure you have the correct repo enabled).
   - On the source server, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-UpgradePreValidation
```

2. [Optional] Set up Secret Utility.
   - If ClarityLIMS-SecretUtil was installed previously, run the following command to set up Secret Utility as the glsjboss user:

```
/opt/gls/clarity/config/pending/05_configure_claritylims_secretutil.sh
```

   > Using a vault is the safer way of storing application secrets. If using a vault is not possible, the configuration script supports file-based storage.

   - For more information on the prompts, refer to the Configuration Script section of *Guide to Secret Management* on page 315.

3. Run the validation script.
   a. Make sure that the Clarity LIMS server is running.
   b. As the root user, run the following command:

```
bash /opt/gls/ClarityUpgradeValidation/bin/validate.sh
```

   c. Review the output of the script to determine if you can proceed with the upgrade. If the script outlines any issues with the potential upgrade, review the generated log files and contact the Clarity LIMS Support team for further assistance.

4. Remove the PreValidation RPM.
   Remove the PreValidation RPM only after you confirm that you can upgrade. If you are unsure, consult the Clarity LIMS LIMS Support team.
   - As the root user, run the following command:

```
yum remove ClarityLIMS-UpgradePreValidation
```

5. Back Up the Current Database and Clarity LIMS

Archive the backup in case a rollback is required.

Before performing the backup, stop Clarity LIMS.

1. Stop Clarity LIMS:
   - On the command-line interface, run the following command as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

   This command stops all Clarity LIMS components, including Automation Worker and integration services.

2. Back up PostgreSQL database:
   On the PostgreSQL server, best practice recommends backing up the database using the pg_dump utility.
   The following example assumes the following:
   - The database server and the application server are on the same server.
   - The pg_dump utility is accessible to the glsjboss user.

   Example:
   The Postgres DBA uses the following commands to create a database backup in the glsjboss home directory. Substitute the variables as appropriate for the specific environment.
   - As the glsjboss user:

```
cd ~glsjboss
mkdir -p backups/database
pg_dump -U <database_user> -b -O -Ft <database_name> -f
~glsjboss/backups/database/clarity-old_version-`date +%Y%m%d%H%M`.tar
```

3. Make sure that the following items, and any other files and configurations, are backed up safely:
   - crontab -l
   - Custom scripts
   - OS configuration files
   - Firewall rules
   - Network configuration

   If there are custom changes to any application configurations (to increase performance, security, etc.), restore/configure these items manually later by referencing the backup.
   We recommend that you back up the items into a single zip file and transfer them to the new instance.
   Directories:

```
/opt/gls/clarity/users/glsftp or /home/glsftp (Clarity LIMS file store location)
/opt/gls/clarity/customextensions
/opt/gls/clarity/glscontents
/etc/httpd/conf.d
/etc/httpd/sslcertificate
```

   Files:

For Research Use Only. Not for use in diagnostic procedures.

```
.pgpass
/opt/gls/pgsql/9.x/pg_hba.conf
/opt/gls/pgsql/9.x/postgresql.conf
```

Additional configurations:

```
rpm -qa | grep "BaseSpace\|Clarity" > clarityrpms.txt
```

Upgrade Steps

Install Latest Clarity LIMS on New Instance

1. Make sure that the repository file exists in the following location:

```
/etc/yum.repos.d/
```

2. As the root user, install the RPMs required on the new instance by referencing the content of `clarityrpms.txt`.
   - If you are upgrading from Clarity LIMS v4.x, some RPMs (eg, Server RPM) are now included under other RPMs.
   - Install any other required RPMs, eg, Python packages, which are not part of the Clarity LIMS setup.
   - Do not install NGS, Illumina Preset Protocols (IPP), and Sequencing RPMs during this step. You install these RPMs later in the installation process.
3. Configure and validate the new system, following the procedure outlined in the *Installation Procedure (Clarity LIMS v6.1)* on page 240.
   - When prompted for user passwords, enter the passwords used in the previous instance.
4. Stop Clarity LIMS. To do so, on the command-line interface, run the following command as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

> The following steps are only required if you are restoring from a previous instance. If you are installing in a test environment, proceed to *Verify the New Instance* on page 271 section.

Install and Configure LabLink v2.3

LabLink v2.3 is compatible with Clarity LIMS v6.1.

If upgrading from Clarity LIMS v4.x, Illumina migrates your LabLink-related data with the following exceptions:

- Sample submission templates
- Customized UI CSS
- LabLink property table configurations

Before completing the following steps, make sure that a database named lablink is created with the same database user as Clarity LIMS database.

1. Install the LabLink RPM. Make sure that you have the correct repo enabled.
   - On the new instance, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-LabLink
```

2. Run the pending initialization script.
   - As the glsjboss user, run the following command:

```
bash /opt/gls/clarity/config/pending/60_initialize_lablink.sh
```

3. The script prompts for a Google reCAPTCHA URL, site key, and secret key.
   - Google reCAPTCHA URL: https://www.google.com/recaptcha/
   - Google reCAPTCHA site key and secret key: View these keys from the Google reCAPTCHA Admin Console, under Settings.

   > If you prefer not to use reCAPTCHA, leave the site-key and secret-key fields blank when running the configuration script. LabLink does not display the reCAPTCHA when these fields are left blank. You can also use your own reCAPTCHA accounts when configuring LabLink.

   - To reconfigure LabLink (without initializing the database), run the following command as the glsjboss user:

```
bash /opt/gls/clarity/config/configure_lablink.sh
```

Restore Backup Onto the New Instance

1. Extract the backup zip file into a suitable location (eg, `/tmp/restore`).

   > If using Oracle database, skip the following steps 2 and 3. Contact the Clarity LIMS Support team for assistance in performing the migration from Oracle to PostgreSQL.

2. If using PostgreSQL database, the DBA imports the database dump into the new database instance. Dropping and recreating the database might be necessary. If you need to do this, use the following command:

```
dropdb -U postgres "CentOS7DB"
createdb -U postgres "CentOS7DB"
psql -U postgres -d "CentOS7DB" -c 'ALTER DATABASE "CentOS7DB" OWNER TO
"CentOS7User"'
```

3. Restore the database exported from the previous instance.
4. Extract and restore the following directories to the same directory on the new instance:
   - Clarity LIMS file store: `/opt/gls/clarity/users/glsftp` or `/home/glsftp`
   - `/opt/gls/clarity/custom/extensions`
   - `/opt/gls/clarity/glscontents`

For Research Use Only. Not for use in diagnostic procedures.

- `/etc/httpd/conf.d`

> As of RedHat Enterprise Linux / CentOS v7.9, Apache v2.4 is installed. There are several configuration changes in this version. You can use the new configuration, or merge your previous configuration file cautiously to the new configuration file. For details on the changes, refer to: httpd.apache.org.

5. Copy the SSL certificate files to the following location (create the directory if it does not exist):

```
/etc/httpd/sslcertificate
```

6. To configure the certificates, run the following command on the command-line interface, as the root user:

```
/opt/gls/clarity/config/installCertificates.sh
```

   For more information, refer to *Install a Purchased SSL/TLS Certificate* on page 333.

7. Restore files and configurations.
   - Copy any custom scripts into their folder locations.
   - For PostgreSQL database, copy/merge the database configuration file (eg, `pg_hba.conf` and `postgresql.conf`).
   - Restore crontab from file.
   - Copy / Merge any additional application configurations.

[Optional] Change the Clarity LIMS Hostname

This step is required only if the new instance hostname is different from the old instance hostname.

For details, refer to *Change the Clarity LIMS Hostname* on page 326

[Optional] Update Application Configuration

This step is required only if the passwords for glsftp and/or apiuser have changed.

To update the application configuration, complete the following steps:

1. Update glsftp password.
2. Update apiuser password.
3. Update database connection details.

For details, refer to *Update Server Passwords and Database Connection Details* on page 331.

Perform Application Migration

In this step, the clarity-migrator tool is used to perform the changes required to make the database compatible with the new Clarity LIMS version.

On the command-line interface, run the following commands as the glsjboss user:

```
cd /opt/gls/clarity/config/
```

```
./migrate_claritylims_database.sh
```

[Optional] Install NGS, IPP, and Sequencing RPMs

This step is required only if the RPMs have been installed on the existing Clarity LIMS instance.

- Install the latest NGS, IPP, and Sequencing RPMs compatible with the new Clarity LIMS version, as listed in `clarityrpms.txt`.

All existing workflows, protocols, steps, and master steps are restored during the restoration process. After installing the NGS and IPP RPMs, you do not need to install the workflows again.

- If the automation/External Program Plugin (EPP) scripts installed on the new instance are of a later version (eg, `/opt/gls/cla/opt/gls/clarity/extensions/ngs-common/v5/EPP)`) to your old instance (eg, `/opt/gls/clarity/extensions/ngs-common/v4/EPP`), you must manually update the script location in your automation / EPP command lines. You can do update the script location in the Clarity LIMS interface or the Operations interface.
- If you intend to install NovaSeq API-based integration, NextSeq integration, or MiSeq integration, use the latest package to ensure OS compatibility.

Delete ElasticSearch indexes and Restart Clarity LIMS on the New Instance

On the command-line interface, run the following commands as the root user:

- Make sure that ElasticSearch is running:

```
service elasticsearch start
```

- When ElasticSearch service is running, remove the ElasticSearch indexes:

```
curl _XDELETE 'http://localhost:9200/_all'
```

- Restart Clarity LIMS:

```
/opt/gls/clarity/bin/run_clarity.sh stop
/opt/gls/clarity/bin/run_clarity.sh start
```

Verify the New Instance

The following verification steps are the minimum required to confirm that the various services are up and running properly.

To conduct a thorough verification, perform your verification steps or daily routine on the new Clarity LIMS instance.

1. ElasticSearch, Search Indexer, and RabbitMQ
   a. Log in to Clarity LIMS LIMS via `https://<FQDN>/clarity` and perform a basic search.
   b. Check that search results are returned.
   c. If no search results are returned, try again later as the search indexes are still building.
2. Tomcat, Apache, Automation Worker

For Research Use Only. Not for use in diagnostic procedures.

a. Run a sample through a QC protocol step. Create a temporary workflow if necessary.
b. Make sure that the automation executes successfully and the log files are accessible.
c. Open a browser window and access `https://<FQDN>/api/v2/projects`.
d. Log in with api user credentials.
e. Check that all projects are returned in the response.

3. LabLink
   a. Open a browser window and access `https://<FQDN>/lablink/`.
   b. Log in with administrator credentials.
   c. On the page, make sure that all data are properly displayed.
4. [Optional] Sequencing Service
   To make sure that the service is running properly, you must initiate an actual sequencing run on the instrument.

Upgrade Procedure for On Premise to On Premise Deployments

From Versions 4.2 / 5.0 / 5.1 (PostgreSQL) and 4.3 / 5.2 (Oracle) to 6.0

This section provides the steps required to upgrade an existing on-premise deployment of Clarity LIMS to a RedHat Enterprise Linux / CentOS compatible on-premise deployment of Clarity LIMS v6.0.

The installation procedure includes provisioning and configuring the new instance, and installing and then verifying the new Clarity LIMS version.

For installation requirements, refer to the *Technical Requirements* on page 5.

If you have questions about the upgrade procedure, contact the Clarity LIMS Support team.

Migration Paths

The following table shows the applicable migration paths.

From	To	Notes
PostgreSQL: v4.2 On-premise v5.0 On-premise v5.1 On-premise	v6.0 On-premise	Upgrading from CentOS6 to CentOS7.
Oracle: v4.3 On-premise v5.2 On-premise	v6.0 On-premise	Migrating from Oracle to PostgresQL. v6.0 supports PostgreSQL only.

Prerequisites

1. Provision the New Instance

We recommend you provision an instance with similar or higher specifications to the current Clarity LIMS instance.

Note the following:

- Your system must meet the requirements listed in the Clarity LIMS *Technical Requirements* on page 5
- All standard operating system (OS) security updates must have been applied.
- Upgrades are only supported from Clarity LIMS versions 4.2, 5.0, and 5.1 and 4.3 and 5.2 (Oracle).
- The command `hostname -f` must resolve to the fully qualified domain name (FQDN) of the server. For details, refer to the Verify Hostname Resolution section of *Pre-Installation Requirements* on page 232.

> Before installing Clarity LIMS on the new instance, make sure that the instance has the same FQDN as the existing production instance. If your new instance cannot have the same FQDN as the production instance, contact the Illumina Support team.

2. Configure the New Instance

To configure the new instance, follow the instructions provided in the Clarity LIMS *Pre-Installation Requirements* on page 232 and refer to *Technical Overview* on page 2.

- Custom configurations: If you have made any additional configurations that are not part of the Clarity LIMS pre-installation requirements, apply these configurations to the new instance.
- Passwords: Configure all passwords to be same as the existing instance. After you have verified the new instance, you can change passwords as needed.

3. Verify the User Account Email Addresses

Make sure that all user accounts have email addresses associated with them. Users must reset their passwords after the upgrade is complete.

4. Install and Run the Pre-Validation Script on the Source Server

To assist with validating the system before an upgrade, install the UpgradePreValidation RPM on the source server.

- This RPM is installed temporarily, and provides tools to help check the system before an upgrade.
- If validation is successful, you can remove this RPM and proceed with the upgrade.

1. Install the UpgradePreValidation RPM (make sure you have the correct repo enabled).
    - On the source server, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-UpgradePreValidation
```

2. [Optional] Set up Secret Utility.

For Research Use Only. Not for use in diagnostic procedures.

- If ClarityLIMS-SecretUtil was installed previously, run the following command to set up Secret Utility as the glsjboss user:

```
/opt/gls/clarity/config/pending/05_configure_claritylims_secretutil.sh
```

> Using a vault is the safer way of storing application secrets. If using a vault is not possible, the configuration script supports file-based storage.

- For more information on the prompts, refer to the Configuration Script section of *Guide to Secret Management* on page 315.

3. Run the validation script.
   a. Make sure that your Clarity LIMS server is running.
   b. As the root user, run the following command:

```
bash /opt/gls/ClarityUpgradeValidation/bin/validate.sh
```

   c. Review the output of the script to determine if you can proceed with the upgrade. If the script outlines any issues with the potential upgrade, review the generated log files and contact the Clarity LIMS Support team for further assistance.
4. Remove the PreValidation RPM.
   Remove the PreValidation RPM only after you confirm that you can upgrade. If you are unsure, consult the Clarity LIMS LIMS Support team.
   - As the root user, run the following command:

```
yum remove ClarityLIMS-UpgradePreValidation
```

5. Back Up the Current Database and Clarity LIMS

Archive the backup in case a rollback is required.

Before performing the backup, stop Clarity LIMS.

1. Stop Clarity LIMS:
   - On the command-line interface, run the following command as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

   This command stops all Clarity LIMS components, including Automation Worker and integration services.
2. Back up PostgreSQL database:
   On the PostgreSQL server, best practice recommends backing up the database using the pg_dump utility.
   The following example assumes the following:
   - The database server and the application server are on the same server.
   - The pg_dump utility is accessible to the glsjboss user.

   Example:

For Research Use Only. Not for use in diagnostic procedures.

The Postgres DBA uses the following commands to create a database backup in the glsjboss home directory. Substitute the variables as appropriate for the specific environment.

- As the glsjboss user:

```
cd ~glsjboss
mkdir -p backups/database
pg_dump -U <database_user> -b -O -Ft <database_name> -f
~glsjboss/backups/database/clarity-old_version-`date +%Y%m%d%H%M`.tar
```

3. Make sure that the following items, and any other files and configurations, are backed up safely:
   - crontab -l
   - custom scripts
   - OS configuration files
   - firewall rules
   - network configuration

   If there are custom changes to any application configurations (to increase performance, security, etc.), restore/configure these items manually later by referencing the backup.
   We recommend that you back up the items into a single zip file and transfer them to the new instance.
   Directories:

```
/opt/gls/clarity/users/glsftp or /home/glsftp (Clarity LIMS file store location)
/opt/gls/clarity/customextensions
/opt/gls/clarity/glscontents
/etc/httpd/conf.d
/etc/httpd/sslcertificate
```

   Files:

```
.pgpass
/opt/gls/pgsql/9.x/pg_hba.conf
/opt/gls/pgsql/9.x/postgresql.conf
```

   Additional configurations:

```
rpm -qa | grep "BaseSpace\|Clarity" > clarityrpms.txt
```

Upgrade Steps

Install Latest Clarity LIMS on New Instance

1. Make sure that the repository file exists in the following location:

```
/etc/yum.repos.d/
```

2. As the root user, install the RPMs required on the new instance by referencing the content of `clarityrpms.txt`.

For Research Use Only. Not for use in diagnostic procedures.

- If you are upgrading from Clarity LIMS v4.x, some RPMs (eg, Server RPM) are now included under other RPMs.
- Install any other required RPMs, eg, Python packages, which are not part of the Clarity LIMS setup.
- Do not install NGS, Illumina Preset Protocols (IPP), and Sequencing RPMs during this step. You install these RPMs later in the installation process.

3. Configure and validate the new system, following the procedure outlined in the *Installation Procedure (Clarity LIMS v6.0)* on page 243
   - When prompted for user passwords, enter the passwords used in the previous instance.
4. Stop Clarity LIMS. To do so, on the command-line interface, run the following command as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

> The following steps are only required if you are restoring from a previous instance. If you are installing in a test environment, proceed to *Verify the New Instance* on page 279 section.

Install and Configure LabLink v2.2

LabLink v2.2 is compatible with Clarity LIMS v6.0.

If upgrading from Clarity LIMS v4.x, Illumina migrates your LabLink-related data with the following exceptions:

- Sample submission templates
- Customized UI CSS
- LabLink property table configurations

Before completing the following steps, make sure that a database named lablink is created with the same database user as Clarity LIMS database.

1. Install the LabLink RPM (make sure that you have the correct repo enabled).
   - On the new instance, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-LabLink
```

2. Run the pending initialization script.
   - As the glsjboss user, run the following command:

```
bash /opt/gls/clarity/config/pending/60_initialize_lablink.sh
```

3. The script prompts for a Google reCAPTCHA URL, site key, and secret key.
   - Google reCAPTCHA URL: https://www.google.com/recaptcha/
   - Google reCAPTCHA site key and secret key: View these keys from the Google reCAPTCHA Admin Console, under Settings.

If you prefer not to use reCAPTCHA, leave the site-key and secret-key fields blank when running the configuration script and LabLink does not display the reCAPTCHA. You can also use your own reCAPTCHA accounts when configuring LabLink.

- To reconfigure LabLink (without initializing the database), run the following command as the glsjboss user:

```
bash /opt/gls/clarity/config/configure_lablink.sh
```

Restore Backup Onto the New Instance

1. Extract the backup zip file into a suitable location (eg, `/tmp/restore`).

   If using Oracle database, skip the following steps 2 and 3. Contact the Clarity LIMS Support team for assistance in performing the migration from Oracle to PostgreSQL.

2. If using PostgreSQL database, the DBA imports the database dump into the new database instance. Dropping and recreating the database can be necessary. If needed, use the following command to do so:

```
dropdb -U postgres "CentOS7DB"
createdb -U postgres "CentOS7DB"
psql -U postgres -d "CentOS7DB" -c 'ALTER DATABASE "CentOS7DB" OWNER TO
"CentOS7User"'
```

3. Restore the database exported from the previous instance.
4. Extract and restore the following directories to the same directory on the new instance:
   - Clarity LIMS file store: `/opt/gls/clarity/users/glsftp` or `/home/glsftp`
   - `/opt/gls/clarity/custom/extensions`
   - `/opt/gls/clarity/glscontents`
   - `/etc/httpd/conf.d`

   As of RedHat Enterprise Linux / CentOS v7.9, Apache v2.4 is installed. There are several configuration changes in this version. You can use the new configuration, or merge your previous configuration file cautiously to the new configuration file. For details on the changes, refer to: httpd.apache.org.

5. Copy the SSL certificate files to the following location (create the directory if it does not exist):

```
/etc/httpd/sslcertificate
```

6. To configure the certificates, run the following command on the command-line interface, as the root user:

```
/opt/gls/clarity/config/installCertificates.sh
```

   For more information, refer to *Install a Purchased SSL/TLS Certificate* on page 333.

7. Restore files and configurations.

For Research Use Only. Not for use in diagnostic procedures.

- Copy any custom scripts into their folder locations.
- For PostgreSQL database, copy/merge the database configuration file (eg, `pg_hba.conf` and `postgresql.conf`).
- Restore crontab from file.
- Copy / Merge any additional application configurations.

[Optional] Change the Clarity LIMS Hostname

This step is required only if the new instance hostname is different from the old instance hostname.

For details, refer to *Change the Clarity LIMS Hostname* on page 326

[Optional] Update Application Configuration

This step is required only if the passwords for glsftp and/or apiuser have changed.

To update the application configuration, complete the following steps:

1. Update glsftp password.
2. Update apiuser password.
3. Update database connection details.

For details, refer to *Update Server Passwords and Database Connection Details* on page 331.

Perform Application Migration

In this step, the clarity-migrator tool is used to perform the changes required to make the database compatible with the new Clarity LIMS version.

On the command-line interface, run the following commands as the glsjboss user:

```
cd /opt/gls/clarity/config/
./migrate_claritylims_database.sh
```

[Optional] Install NGS, IPP, and Sequencing RPMs

This step is required only if the RPMs have been installed on the existing Clarity LIMS instance.

- Install the latest NGS, IPP, and Sequencing RPMs compatible with the new Clarity LIMS version, as listed in `clarityrpms.txt`.

All existing workflows, protocols, steps, and master steps are restored during the restoration process. After installing the NGS and IPP RPMs, you do not need to install the workflows again.

- If the automation/External Program Plugin (EPP) scripts installed on the new instance are of a later version (eg, `/opt/gls/cla/opt/gls/clarity/extensions/ngs-common/v5/EPP)` d to your old

For Research Use Only. Not for use in diagnostic procedures.

instance (eg, `/opt/gls/clarity/extensions/ngs-common/v4/EPP`), you must manually update the script location in your automation / EPP command lines. You can do update the script location in the Clarity LIMS interface or the Operations interface.

- If you intend to install NovaSeq API-based integration, NextSeq integration, or MiSeq integration, use the latest package to ensure OS compatibility.

Delete ElasticSearch indexes and Restart Clarity LIMS on the New Instance

On the command-line interface, run the following commands as the root user:

- Make sure that ElasticSearch is running:

```
service elasticsearch start
```

- When ElasticSearch service is running, remove the ElasticSearch indexes:

```
curl _XDELETE 'http://localhost:9200/_all'
```

- Restart Clarity LIMS:

```
/opt/gls/clarity/bin/run_clarity.sh stop
/opt/gls/clarity/bin/run_clarity.sh start
```

Verify the New Instance

The following verification steps are the minimum required to confirm that the various services are up and running properly.

To conduct a thorough verification, perform your verification steps or daily routine on the new Clarity LIMS instance.

1. ElasticSearch, Search Indexer, and RabbitMQ
   a. Log in to Clarity LIMS LIMS via `https://<FQDN>/clarity` and perform a basic search.
   b. Check that search results are returned.
   c. If no search results are returned, try again later as the search indexes are still building.
2. Tomcat, Apache, Automation Worker
   a. Run a sample through a QC protocol step. (Create a temporary workflow if necessary.)
   b. Make sure that the automation executes successfully and the log files are accessible.
   c. Open a browser window and access `https://<FQDN>/api/v2/projects`.
   d. Log in with api user credentials.
   e. Check that all projects are returned in the response.
3. LabLink
   a. Open a browser window and access `https://<FQDN>/lablink/`.
   b. Log in with administrator credentials.
   c. On the page, make sure that all data are properly displayed.

For Research Use Only. Not for use in diagnostic procedures.

4. [Optional] Sequencing Service
   To make sure that the service is running properly, you must initiate an actual sequencing run on the instrument.

Upgrade Procedure for On Premise to On Premise Deployments

From Versions 4.3/5.2/6.0 to 6.1

This document provides the steps required to upgrade from Clarity LIMS v4.3, v5.2, or v6.0 to Clarity LIMS v.6.1.

If you have questions about the upgrade procedure, contact the Clarity LIMS Support team.

Migration Paths

The following table shows the applicable migration paths.

From	To
PostgreSQL: v4.3 On-premise v5.2 On-premise v6.0 On-premise	v6.1 On-premise

Prerequisites

- The system meets the requirements listed in the Clarity LIMS *Technical Requirements* on page 5.
- All standard operating system (OS) security updates have been applied.
- The command `hostname -f` resolves to the fully qualified domain name (FQDN) of the server. For details, refer to the Verify Hostname Resolution section of *Pre-Installation Requirements* on page 232.
- All user accounts have email addresses associated with them. Users must reset their passwords after the upgrade is done.

Upgrade Pre-Validation

To assist with validating the system before an upgrade, install the UpgradePreValidation RPM on the source server.

- This RPM is installed temporarily, and provides tools to help check the system before an upgrade.
- If validation is successful, you can remove this RPM and proceed with the upgrade.

1. Install the UpgradePreValidation RPM. Make sure you have the correct repo enabled.
   - On the source server, as the root user, run the following command:

For Research Use Only. Not for use in diagnostic procedures.

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-UpgradePreValidation
```

2. [Optional] Set up Secret Utility.
   - If ClarityLIMS-SecretUtil was installed previously, run the following command to set up Secret Utility as the glsjboss user:

```
./opt/gls/clarity/config/pending/05_configure_claritylims_secretutil.sh
```

   > Using a vault is the safer way of storing application secrets. If using a vault is not possible, the configuration script supports file-based storage.

   - For more information on the prompts, refer to *Guide to Secret Management* on page 315 and refer to the Configuration Script section.
3. Run the validation script.
   a. Make sure that your Clarity LIMS server is running.
   b. As the root user, run the following command:

```
bash /opt/gls/ClarityUpgradeValidation/bin/validate.sh
```

   c. Review the output of the script to determine if you can proceed with the upgrade. If the script outlines any issues with the potential upgrade, review the generated log files and contact the Clarity LIMS Support team for further assistance.
4. Remove the PreValidation RPM.
   Remove the PreValidation RPM only after you confirm that you can upgrade. If you are unsure, consult the Clarity LIMS LIMS Support team.
   - As the root user, run the following command:

```
yum remove ClarityLIMS-UpgradePreValidation
```

Upgrading the Clarity LIMS Server

The following steps are required to update the Clarity LIMS server.

> All instances of Clarity LIMS must have a purchased SSL Certificate installed before installation or upgrade. For instructions on creating the necessary Certificate Signing Request to send to your SSL Certificate vendor, and installing the certificate files received from your vendor into Clarity LIMS, refer to *Install a Purchased SSL/TLS Certificate* on page 333.

Shut Down Clarity LIMS Components

> As of Clarity LIMS v5, the term *AI node* has been replaced with *automation worker*.

1. Determine if Remote Automation Workers Are Running

1. As the glsjboss user, run the following command. Substitute the variables as appropriate for your specific environment.

For Research Use Only. Not for use in diagnostic procedures.

```
java -jar /opt/gls/clarity/tools/ai-monitor/ai-monitor.jar -u <apiuser> -p
<password> -i https://<apihost>/api/ -n
```

2. Make a note of any remote automation workers. Let these automation workers complete their current commands.

2. Stop All Integration Services

Find and stop all integration services, as described in the integration documentation.

3. Shut Down Clarity LIMS Services

On the command-line interface, run the following command as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

- If a service is already stopped, it is ignored.
- If a service fails to stop, the script exits. No further services are stopped.

In rare circumstances, the previous commands might fail to stop JBoss and/or Tomcat. In this scenario, use the following `kill` commands to stop these components.

JBoss

1. Check if you must kill the JBoss application:

```
pgrep jboss
```

2. As the glsjboss user, kill the JBoss application:

```
/etc/init.d/jboss kill
```

Tomcat

1. Check if you must kill the Tomcat application:

```
pgrep jsvc
```

2. As the root user, kill the Tomcat processes:

```
pkill jsvc
```

Back Up Database and Clarity LIMS

1. PostgreSQL Database Backup

On the PostgreSQL server, Clarity LIMS best practice recommends backing up the database using the pg_dump utility.

Assumptions of the following example:

- The database server and the application server are on the same server.
- The pg_dump utility is accessible to the glsjboss user.

Example:

The Postgres DBA can use the following commands to create a database backup in the glsjboss home directory. Substitute the variables as appropriate for your specific environment:

- As the glsjboss user:

```
cd ~glsjboss
mkdir -p backups/database
pg_dump -U <database_user> -b -Ft <database_name> -f
~glsjboss/backups/database/clarity-old_version-`date +%Y%m%d%H%M`.tar
```

2. Clarity LIMS Backup

On the Clarity LIMS server, back up the contents of the folder /opt/gls/clarity/glscontents/ as follows.

- As the glsjboss or root user, run the following commands:

```
cd ~glsjboss
mkdir -p backups/clarity
tar czf ~glsjboss/backups/clarity/glscontents-old_version-`date
+%Y%m%d$H$M`.tar.gz /opt/gls/clarity/glscontents/
```

Upgrade the Clarity LIMS Components

1. As the root user, run the following script:

```
yum --enablerepo=GLS_Clarity6 update "ClarityLIMS-App"
```

2. As the glsjboss user, run the following script:

```
/opt/gls/clarity/config/configuration_test.sh
```

   This script analyzes the system and lists any required configuration steps.

3. Carefully apply the instructions provided in the output of the scripts. For example, as root, run the following sequence:

```
su - glsjboss -c /opt/gls/clarity/config/pending/27_update_claritylims_
platform.sh
su - glsjboss -c /opt/gls/clarity/config/pending/28_update_claritylims_
tenant.sh
/opt/gls/clarity/config/pending/32_root_configure_rabbitmq.sh
/opt/gls/clarity/config/pending/33_root_configure_elasticsearch.sh
/opt/gls/clarity/config/pending/40_root_install_proxy.sh
```

4. If your database server is standalone or remote, update the `/opt/gls/clarity/tomcat/current/lib/activity-management-ui-config.groovy` file with the following code snippet. Substitute the `Remote DB IP` and `Remote DB Port` placeholders with the information for your server.

```
hibernate {
    isis {
```


For Research Use Only. Not for use in diagnostic procedures.

```
        template {
            url="jdbc:postgresql://<Remote DB IP>:<Remote DB Port>/{0}"
        }
    }
}
```

If you do not update the script, log and database connection errors can occur.

5. Check that all scripts have been run. As the glsjboss user, run any remaining scripts as follows.

```
su - glsjboss -c /opt/gls/clarity/config/configuration_test.sh
```

Install / Upgrade LabLink

LabLink v2.3 is compatible with Clarity LIMS v6.1. If you are running an older version of LabLink, you must upgrade to the latest version.

If upgrading from Clarity LIMS v4.3, Illumina migrates your LabLink-related data with the following exceptions:

- Sample submission templates
- Customized UI CSS
- LabLink property table configurations

Install LabLink

Before installing LabLink v2.3, make sure that a database named LabLink is created with the same database user as Clarity LIMS database.

1. Install the LabLink RPM. Make sure that you have the correct repo enabled.
    - On the instance, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-LabLink
```

2. Run the pending initialization script.
    - As the glsjboss user, run the following command:

```
bash /opt/gls/clarity/config/pending/60_initialize_lablink.sh
```

3. The script prompts for a Google reCAPTCHA URL, site key, and secret key.
    - Google reCAPTCHA URL: https://www.google.com/recaptcha/
    - Google reCAPTCHA site key and secret key: View these keys from the Google reCAPTCHA Admin Console, under Settings.

If you prefer not to use reCAPTCHA, leave the site-key and secret-key fields blank when running the configuration script. LabLink does not display the reCAPTCHA when these fields are blank. You can also use your own reCAPTCHA accounts when configuring LabLink.

- To reconfigure LabLink (without initializing the database), as the glsjboss user, run the following command:

```
bash /opt/gls/clarity/config/configure_lablink.sh
```

Upgrade LabLink

If you are running an older version of LabLink, upgrade to the latest version as follows.

1. Upgrade the LabLink RPM. Make sure that you have the correct repo enabled.
2. On the instance, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity6 update ClarityLIMS-LabLink
```

Upgrade the PostgreSQL Database Server

Upgrade your PostgreSQL database server to v12.7. Consult a DBA to perform the upgrade.

Start the Clarity LIMS Services

Use the `run_clarity.sh` script to start all services (Elasticsearch, RabbitMQ, Search Indexing, Tomcat, httpd/Apache proxy, AI) in the required order, with one command.

- As the root user:

```
/opt/gls/clarity/bin/run_clarity.sh start
```

After the script has completed, all Clarity LIMS services will be ready for use.

Upgrade Clarity LIMS Integrations

Start the Sequencing services (if applicable).

- Find all the integration services and start them as described in the integration documentation.

Check Clarity LIMS Components

1. Determine which components are running as follows.
   As glsjboss or root user, run the following commands:

   Tomcat:

   ```
   ps -ef | grep jsvc
   ```

   Automation Workers:

   ```
   ps -ef | grep automat
   ```

   Sequencing services:

   ```
   ps -ef | grep seq
   ```

2. Note which components are running.
3. If applicable, restart Remote Automation Workers.

- If remote automation workers were reported as running, manually restart each one from its local machine.

Validate the Installation

1. Log in to Clarity LIMS.
2. Using your own acceptance criteria, make sure that Clarity LIMS is operating as you would expect.

Upgrade Procedure for On Premise to On Premise Deployments

From Versions 4.3 and 5.2 (PostgreSQL) to 6.0

This document provides details on the steps required to upgrade from Clarity LIMS v4.3 or v5.2 to Clarity LIMS v6.0.

If you have questions about the upgrade procedure, contact the Clarity LIMS Support team.

Migration Paths

The following table shows the applicable migration paths.

From	To
PostgreSQL: v4.3 On-premise v5.2 On-premise	v6.0 On-premise

Prerequisites

- The system meets the requirements listed in the Clarity LIMS *Technical Requirements* on page 5.
- All standard operating system (OS) security updates have been applied.
- The command `hostname -f` resolves to the fully qualified domain name (FQDN) of the server. For details, refer to the Verify Hostname Resolution section of *Pre-Installation Requirements* on page 232.
- All user accounts have email addresses associated with them. Users must reset their passwords after the upgrade is done.

Upgrade Pre-Validation

To assist with validating the system before an upgrade, install the UpgradePreValidation RPM on the source server.

- This RPM is installed temporarily, and provides tools to help check the system before an upgrade.
- If validation is successful, you can remove this RPM and proceed with the upgrade.

1. Install the UpgradePreValidation RPM (make sure you have the correct repo enabled).
    - On the source server, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-UpgradePreValidation
```

2. [Optional] Set up Secret Utility.
    - If ClarityLIMS-SecretUtil was installed previously, run the following command to set up Secret Utility as the glsjboss user:

```
./opt/gls/clarity/config/pending/05_configure_claritylims_secretutil.sh
```

    Using a vault is the safer way of storing application secrets. If using a vault is not possible, the configuration script supports file-based storage.

    - For more information on the prompts, refer to *Guide to Secret Management* on page 315 and refer to the Configuration Script section.

3. Run the validation script.
    a. Make sure that your Clarity LIMS server is running.
    b. As the root user, run the following command:

```
bash /opt/gls/ClarityUpgradeValidation/bin/validate.sh
```

    c. Review the output of the script to determine if you can proceed with the upgrade. If the script outlines any issues with the potential upgrade, review the generated log files and contact the Clarity LIMS Support team for further assistance.

4. Remove the PreValidation RPM.
   Remove the PreValidation RPM only after you confirm that you can upgrade. If you are unsure, consult the Clarity LIMS LIMS Support team.
    - As the root user, run the following command:

```
yum remove ClarityLIMS-UpgradePreValidation
```

Upgrading the Clarity LIMS Server

The following steps are required to update the Clarity LIMS server.

All instances of Clarity LIMS must have a purchased SSL Certificate installed before installation or upgrade. For instructions on creating the necessary Certificate Signing Request to send to your SSL Certificate vendor, and installing the certificate files received from your vendor into Clarity LIMS, refer to *Install a Purchased SSL/TLS Certificate* on page 333.

Shut Down Clarity LIMS Components

As of Clarity LIMS v5, the term *AI node* has been replaced with *automation worker*.

1. Determine if Remote Automation Workers Are Running

1. As the glsjboss user, run the following command. Substitute the variables as appropriate for your specific environment.

```
java -jar /opt/gls/clarity/tools/ai-monitor/ai-monitor.jar -u <apiuser> -p
<password> -i https://<apihost>/api/ -n
```

2. Make a note of any remote automation workers. Let these automation workers complete their current commands.

2. Stop All Integration Services

Find and stop all integration services, as described in the integration documentation.

3. Shut Down Clarity LIMS Services

On the command-line interface, run the following command as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

- If a service is already stopped, it is ignored.
- If a service fails to stop, the script exits. No further services are stopped.

In rare circumstances, the previous commands might fail to stop JBoss and/or Tomcat. In this scenario, use the following `kill` commands to stop these components.

JBoss

1. Check if you must kill the JBoss application:

```
pgrep jboss
```

2. As the glsjboss user, kill the JBoss application:

```
/etc/init.d/jboss kill
```

Tomcat

1. Check if you must kill the Tomcat application:

```
pgrep jsvc
```

2. As the root user, kill the Tomcat processes:

```
pkill jsvc
```

Back Up Database and Clarity LIMS

1. PostgreSQL Database Backup

On the PostgreSQL server, Clarity LIMS best practice recommends backing up the database using the pg_dump utility.

Assumptions of the following example:

- The database server and the application server are on the same server.

- The pg_dump utility is accessible to the glsjboss user.

Example:

Your Postgres DBA can use the following commands to create a database backup in the glsjboss home directory. Substitute the variables as appropriate for your specific environment:

- As the glsjboss user:

```
cd ~glsjboss
mkdir -p backups/database
pg_dump -U <database_user> -b -Ft <database_name> -f
~glsjboss/backups/database/clarity-old_version-`date +%Y%m%d%H%M`.tar
```

2. Clarity LIMS Backup

On the Clarity LIMS server, back up the contents of the folder /opt/gls/clarity/glscontents/

- As the glsjboss or root user, run the following commands:

```
cd ~glsjboss
mkdir -p backups/clarity
tar czf ~glsjboss/backups/clarity/glscontents-old_version-`date
+%Y%m%d$H$M`.tar.gz /opt/gls/clarity/glscontents/
```

Upgrade the Clarity LIMS Components

1. As the root user, run the following script:

```
yum --enablerepo=GLS_Clarity6 update "ClarityLIMS-App"
```

2. As the glsjboss user, run the following script:

```
/opt/gls/clarity/config/configuration_test.sh
```

   This script analyzes the system and lists any required configuration steps.

3. Carefully apply the instructions provided in the output of the scripts. For example, as root, run the following sequence:

```
su - glsjboss -c /opt/gls/clarity/config/pending/27_update_claritylims_
platform.sh
su - glsjboss -c /opt/gls/clarity/config/pending/28_update_claritylims_
tenant.sh
/opt/gls/clarity/config/pending/32_root_configure_rabbitmq.sh
/opt/gls/clarity/config/pending/33_root_configure_elasticsearch.sh
/opt/gls/clarity/config/pending/40_root_install_proxy.sh
```

4. If your database server is standalone or remote, update the `/opt/gls/clarity/tomcat/current/lib/activity-management-ui-config.groovy` file with the following code snippet. Substitute the `Remote DB IP` and `Remote DB Port` placeholders with the information for your server.

For Research Use Only. Not for use in diagnostic procedures.

```
hibernate {
    isis {
        template {
            url="jdbc:postgresql://<Remote DB IP>:<Remote DB Port>/{0}"
        }
    }
}
```

If you do not update the script, log and database connection errors can occur.

5. Check that all scripts have been run. As the glsjboss user, run any remaining scripts:

```
su - glsjboss -c /opt/gls/clarity/config/configuration_test.sh
```

Install / Upgrade LabLink

LabLink v2.2 is compatible with Clarity LIMS v6.0. If you are running an older version of LabLink, you must upgrade to the latest version.

Install LabLink

If upgrading from Clarity LIMS v4.3, Illumina migrates your LabLink-related data with the following exceptions:

- Sample submission templates
- Customized UI CSS
- LabLink property table configurations

Before installing LabLink v2.2, make sure that a database named LabLink is created with the same database user as Clarity LIMS database.

1. Install the LabLink RPM (make sure that you have the correct repo enabled).
   - On the instance, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-LabLink
```

2. Run the pending initialization script.
   - As the glsjboss user, run the following command:

```
bash /opt/gls/clarity/config/pending/60_initialize_lablink.sh
```

3. The script prompts for a Google reCAPTCHA URL, site key, and secret key.
   - Google reCAPTCHA URL: https://www.google.com/recaptcha/
   - Google reCAPTCHA site key and secret key: View these keys from the Google reCAPTCHA Admin Console, under Settings.

If you prefer not to use reCAPTCHA, leave the site-key and secret-key fields blank when running the configuration script and LabLink does not display the reCAPTCHA. You can also use your own reCAPTCHA accounts when configuring LabLink.

- To reconfigure LabLink (without initializing the database), as the glsjboss user, run the following command:

```
bash /opt/gls/clarity/config/configure_lablink.sh
```

Upgrade LabLink

If you are running an older version of LabLink, upgrade to the latest version as follows.

1. Upgrade the LabLink RPM (make sure that you have the correct repo enabled).
2. On the instance, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity6 update ClarityLIMS-LabLink
```

Upgrade the PostgreSQL Database Server

Upgrade your PostgreSQL database server to v12.7. Consult a DBA to perform the upgrade.

Start the Clarity LIMS Services

Use the `run_clarity.sh` script to start all services (Elasticsearch, RabbitMQ, Search Indexing, Tomcat, httpd/Apache proxy, AI) in the required order, with one command.

- As the root user:

```
/opt/gls/clarity/bin/run_clarity.sh start
```

After the script has completed, all Clarity LIMS services will be ready for use.

Upgrade Clarity LIMS Integrations

Start the Sequencing services (if applicable).

- Find all the integration services and start them as described in the integration documentation.

Check Clarity LIMS Components

Determine which components are running.

1. As glsjboss, or root user, run the following commands.

   Tomcat:

   ```
   ps -ef | grep jsvc
   ```

   Automation Workers:

   ```
   ps -ef | grep automat
   ```


For Research Use Only. Not for use in diagnostic procedures.

Sequencing services:

```
ps -ef | grep seq
```

2. Note which components are running.
3. If applicable, restart Remote Automation Workers.

- If remote automation workers were reported as running, manually restart each one from its local machine.

Validate the Installation

1. Log in to Clarity LIMS.
2. Using your own acceptance criteria, make sure that Clarity LIMS is operating as you would expect.

Cloud to On Premise Upgrade Procedures

This section provides instructions for upgrading existing cloud hosted Clarity LIMS deployments to on premise deployments. For assistance with upgrade steps, contact the Clarity LIMS Support team.

Upgrade Procedure for Cloud to On Premise Deployments

From Versions 4.2 / 4.3 / 5.0 / 5.1/ 5.2 / 5.3 / 5.4 / 6.0 / 6.1 to 6.2

This document provides details on the steps required to upgrade an existing Clarity LIMS to RedHat Enterprise Linux/Oracle Linux compatible Clarity LIMS v6.2.

For installation requirements and Oracle Linux compatibility, refer to *Technical Requirements* on page 5.

Migration Paths

The following table shows the applicable migration paths.

From	To	Notes
v4.2 Cloud v4.3 Cloud v5.0 Cloud v5.1 Cloud v5.2 Cloud v5.3 Cloud v5.4 Cloud v6.0 Cloud v6.1 Cloud	v.6.2 On-premise	Changing environment from Illumina Cloud hosted to On-premise.

Prerequisites

Before Illumina can proceed with the upgrade, complete the following prerequisite steps.

Provision the New Instance

- The system must meet the requirements listed in the *Technical Overview* on page 2.
- All standard OS security updates must have been applied.
- Upgrades are only supported from Clarity LIMS v4.2/4.3/5.0/5.1/5.2/5.3/5.4/6.0/6.1.
- The command hostname -f must resolve to the fully-qualified domain name of the server. For details, refer to the *Confirm Hostname Resolution* section of *Pre-Installation Requirements* on page 232.

Before installing Clarity LIMS on the new instance, make sure that the instance has the same fully-qualified domain name as the existing Production instance. If it is not possible to have the same fully-qualified domain name, contact the Clarity LIMS Support team.

Configure the New Instance

To configure the new instance, follow the instructions provided in the Clarity LIMS *Pre-Installation Requirements* on page 232. Refer to the *Technical Overview* on page 2.

- Custom configurations: If you have made any additional configurations that are not part of the Clarity LIMS pre-installation requirements, apply these configurations to the new instance.
- Passwords: Configure all passwords to be same as the existing instance. After you have verified the new instance, you can change passwords as needed.

Verify User Account Email Addresses

Make sure that all user accounts have email addresses associated with them. Users must reset their passwords after the upgrade is complete.

Install and Run the Pre-Validation Script on the Source Server

To assist with validating the system before an upgrade, install the `UpgradePreValidation` RPM on the source server.

- This RPM is installed temporarily, and provides tools to help check the system before an upgrade.
- If validation is successful, remove this RPM and proceed with the upgrade.

1. Install the `UpgradePreValidation` RPM (make sure that the correct repo is enabled).
   - On the source server, as the root user, run the following command:
     ```
     yum --enablerepo=GLS_Clarity6 install ClarityLIMS-UpgradePreValidation
     ```
2. [Optional] Set up Secret Utility.
   - If ClarityLIMS-SecretUtil was installed previously, run the following command to set up Secret Utility as the glsjboss user:

```
/opt/gls/clarity/config/pending/05_configure_claritylims_secretutil.sh
```

Using a vault is the safer way of storing application secrets. If using a vault is not possible, the configuration script supports file-based storage.

- For more information on the prompts, refer to the *Configuration Script* section of *Guide to Secret Management* on page 315.

3. Run the validation script.
   a. Make sure that the Clarity LIMS server is running.
   b. As the root user, run the following command:

```
bash /opt/gls/ClarityUpgradeValidation/bin/validate.sh
```

   c. Review the output of the script to determine if you can proceed with the upgrade. If the script outlines any issues with the potential upgrade, review the generated log files and contact the Clarity LIMS Support team for further assistance.
4. Remove the `Pre-Validation` RPM.
   Remove the `Pre-Validation` RPM only after you confirm that you can upgrade. If you are unsure, consult the Clarity LIMS Support team.
   - As the root user, run the following command:

```
yum remove ClarityLIMS-UpgradePreValidation
```

Back Up the Current Database and Clarity LIMS

Archive the backup in case a rollback is required. Before performing the backup, stop Clarity LIMS.

1. Stop Clarity LIMS:
   - On the command-line interface, run the following command as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

   This command stops all Clarity LIMS components, including Automation Worker and integration services.
2. Back up PostgreSQL database:
   On the PostgreSQL server, best practice recommends backing up the database using the pg_dump utility.
   The example provided makes the following assumptions:
   - The database server and the application server are on the same server.
   - The pg_dump utility is accessible to the glsjboss user.

   Example:
   The Postgres DBA uses the following commands to create a database backup in the glsjboss home directory. Substitute the variables as appropriate for the specific environment.
   - As the glsjboss user:

```
cd ~glsjboss
```


For Research Use Only. Not for use in diagnostic procedures.

```
mkdir -p backups/database
pg_dump -U <database_user> -b -O -Ft <database_name> -f
~glsjboss/backups/database/clarity-old_version-`date +%Y%m%d%H%M`.tar
```

3. Make sure that the following items, and any other files and configurations, are backed up safely:
   - crontab -l
   - Custom scripts
   - OS configuration files
   - Firewall rules
   - Network configuration

   If there are custom changes to any application configurations (to increase performance, security, and so on), restore/configure these items manually later by referencing the backup.
   We recommend that you back up the items into a single zip file and transfer them to the new instance.

   Directories:

```
/opt/gls/clarity/users/glsftp or /home/glsftp (Clarity LIMS file store location)
/opt/gls/clarity/customextensions
/opt/gls/clarity/glscontents
/etc/httpd/conf.d
/etc/httpd/sslcertificate
```

   Files:

```
.pgpass
/opt/gls/pgsql/9.x/pg_hba.conf
/opt/gls/pgsql/9.x/postgresql.conf
```

   Additional configurations:

```
rpm -qa | grep "BaseSpace\|Clarity" > clarityrpms.txt
```

Upgrade Steps

Install Latest Clarity LIMS on New Instance

1. Make sure that the repository file exists in the following location:

```
/etc/yum.repos.d/
```

2. As the root user, install the RPMs required on the new instance by referencing the content of `clarityrpms.txt`.
   - If you are upgrading from Clarity LIMS v4.x, some RPMs (eg, Server RPM) are now included under other RPMs.
   - Install any other required RPMs (eg, Python packages) that are not part of the Clarity LIMS setup.

For Research Use Only. Not for use in diagnostic procedures.

- Do not install NGS, Illumina Preset Protocols (IPP), and Sequencing RPMs during this step. You install these RPMs later in the installation process.

3. Configure and validate the new system, following the procedure outlined in the *Installation Procedure (Clarity LIMS v6.2)* on page 237.
   - When prompted for user passwords, enter the passwords used in the previous instance.
4. Stop Clarity LIMS. To do so, on the command-line interface, run the following command as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

The following steps are only required if you are restoring from a previous instance. If you are installing in a test environment, proceed to the *Verify the New Instance* on page 299 section.

Install and Configure LabLink v2.4

LabLink v2.4 is compatible with Clarity LIMS v6.2.

If upgrading from Clarity LIMS v4.x, Illumina migrates your LabLink-related data with the following exceptions:

- Sample submission templates
- Customized UI CSS
- LabLink property table configurations

Before completing the following steps, make sure that a database with the name of lablink is created with the same database user as Clarity LIMS database.

1. Install the LabLink RPM. Make sure that you have the correct repo enabled.
   - On the new instance, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity62 install ClarityLIMS-LabLink
```

2. Run the pending initialization script.
   - As the glsjboss user, run the following command:

```
bash /opt/gls/clarity/config/pending/60_initialize_lablink.sh
```

3. The script prompts for a Google reCAPTCHA URL, site key, and secret key.
   - Google reCAPTCHA URL: https://www.google.com/recaptcha/
   - Google reCAPTCHA site key and secret key: View these keys from the Google reCAPTCHA Admin Console, under Settings.

   If you prefer not to use reCAPTCHA, leave the site-key and secret-key fields blank when running the configuration script. LabLink does not display the reCAPTCHA when these fields are blank. You can also use your own reCAPTCHA accounts when configuring LabLink.

For Research Use Only. Not for use in diagnostic procedures.

- To reconfigure LabLink (without initializing the database), run the following command as the glsjboss user:

```
bash /opt/gls/clarity/config/configure_lablink.sh
```

Restore Backup Onto the New Instance

1. Extract the backup zip file into a suitable location (eg, `/tmp/restore`).

   If using Oracle database, skip the following steps 2 and 3. Contact the Clarity LIMS Support team for assistance in performing the migration from Oracle to PostgreSQL.

2. If using PostgreSQL database, the DBA imports the database dump into the new database instance. Dropping and recreating the database might be necessary. If this is needed, use the following command:

```
dropdb -U postgres <OLOS8DB>
createdb -U postgres <OLOS8DB>
psql -U postgres -d <OLOS8DB> -c 'ALTER DATABASE "<OLOS8DB>" OWNER TO
"<OLOS8User>"'
```

3. Restore the database exported from the previous instance.
4. Extract and restore the following directories to the same directory on the new instance:
   - Clarity LIMS file store: `/opt/gls/clarity/users/glsftp` or `/home/glsftp`
   - `/opt/gls/clarity/custom/extensions`
   - `/opt/gls/clarity/glscontents`
   - `/etc/httpd/conf.d`

   As of RedHat Enterprise Linux/Oracle Linux 8.7, Apache v2.4 is installed. There are several configuration changes in this version. You can use the new configuration, or merge your previous configuration file cautiously to the new configuration file. For details on the changes, refer to `httpd.apache.org`.

5. Copy the SSL certificate files to the following location (create the directory if it does not exist):

```
/etc/httpd/sslcertificate
```

6. To configure the certificates, run the following command on the command-line interface, as the root user:

```
/opt/gls/clarity/config/installCertificates.sh
```

   For more information, refer to *Install a Purchased SSL/TLS Certificate* on page 333.

7. Restore files and configurations.
   - Copy any custom scripts into their folder locations.
   - For PostgreSQL database, copy/merge the database configuration file (ie, `pg_hba.conf` and `postgresql.conf`).

For Research Use Only. Not for use in diagnostic procedures.

- Restore crontab from file.
- Copy / Merge any additional application configurations.

[Optional] Change the Clarity LIMS Hostname

This step is required only if the new instance hostname is different from the old instance hostname.

For details, refer to *Change the Clarity LIMS Hostname* on page 326.

[Optional] Update Application Configuration

This step is required only if the passwords for glsftp and/or apiuser have changed.

To update the application configuration, complete the following steps:

1. Update glsftp password.
2. Update apiuser password.
3. Update database connection details.

For details, refer to *Update Server Passwords and Database Connection Details* on page 331.

Perform Application Migration

In this step, the clarity-migrator tool is used to perform the changes required to make the database compatible with the new Clarity LIMS version.

On the command-line interface, run the following commands as the glsjboss user:

```
cd /opt/gls/clarity/config/
./migrate_claritylims_database.sh
```

[Optional] Install NGS, IPP, and Sequencing RPMs

This step is required only if the RPMs have been installed on the existing Clarity LIMS instance.

- Install the latest NGS, IPP, and Sequencing RPMs compatible with the new Clarity LIMS version, as listed in `clarityrpms.txt`.

All existing workflows, protocols, steps, and master steps are restored during the restoration process. After installing the NGS and IPP RPMs, you do not need to install the workflows again.

- If the automation/External Program Plugin (EPP) scripts installed on the new instance are of a later version (eg, `/opt/gls/cla/opt/gls/clarity/extensions/ngs-common/v5/EPP) than` your old instance (eg, `/opt/gls/clarity/extensions/ngs-common/v4/EPP`), you must manually update the script location in your automation / EPP command lines. You can do update the script location in the Clarity LIMS interface or the Operations interface.
- If you intend to install NovaSeq API-based integration, NextSeq integration, or MiSeq integration, use the latest package to ensure OS compatibility.

Delete ElasticSearch indexes and Restart Clarity LIMS on the New Instance

On the command-line interface, run the following commands as the root user:

- Make sure that ElasticSearch is running:

```
service elasticsearch start
```

- When ElasticSearch service is running, remove the ElasticSearch indexes:

```
for indexname in `curl -s 'http://localhost:9200/_cat/indices?h=index'`; do echo
"Delete index: $indexname"; curl -XDELETE "http://localhost:9200/$indexname";
echo ""; done
```

- Restart Clarity LIMS:

```
/opt/gls/clarity/bin/run_clarity.sh stop
/opt/gls/clarity/bin/run_clarity.sh start
```

Verify the New Instance

The following verification steps are the minimum required to confirm that the various services are up and running properly.

To conduct a thorough verification, perform your verification steps or daily routine on the new Clarity LIMS instance.

1. ElasticSearch, Search Indexer, and RabbitMQ
   a. Log in to Clarity LIMS LIMS via `https://<FQDN>/clarity` and perform a basic search.
   b. Check that search results are returned.
   c. If no search results are returned, try again later as the search indexes are still building.
2. Tomcat, Apache, Automation Worker
   a. Run a sample through a QC protocol step. Create a temporary workflow if necessary.
   b. Make sure that the automation executes successfully and the log files are accessible.
   c. Open a browser window and access `https://<FQDN>/api/v2/projects`.
   d. Log in with api user credentials.
   e. Check that all projects are returned in the response.
3. LabLink
   a. Open a browser window and access `https://<FQDN>/lablink/`.
   b. Log in with administrator credentials.
   c. On the Projects page, make sure that all data are properly displayed.
4. [Optional] Sequencing Service
   To make sure that the service is running properly, you must initiate an actual sequencing run on the instrument.

For Research Use Only. Not for use in diagnostic procedures.

Upgrade Procedure for Cloud to On Premise Deployments

From Versions 4.2 / 4.3 / 5.0 / 5.1 / 5.2 / 5.3 / 5.4 / 6.0 to 6.1

This document provides details on the steps required to upgrade an existing Clarity LIMS to RedHat Enterprise Linux /CentOS 7.9 compatible Clarity LIMS v.6.1.

For installation requirements, refer to *Technical Requirements* on page 5.

Migration Paths

The following table shows the applicable migration paths.

From	To	Notes
v4.2 Cloud v4.3 Cloud v5.0 Cloud v5.1 Cloud v5.2 Cloud v5.3 Cloud v5.4 Cloud v6.0 Cloud	v.6.1 On-premise	Changing environment from Illumina cloud hosted to on-premise.

Prerequisites

Before Illumina can proceed with the upgrade, complete the following prerequisite steps.

1. Provision the New Instance

- The system must meet the requirements listed in the Clarity LIMS *Technical Overview* on page 2.
- All standard OS security updates must have been applied.
- Upgrades are only supported from Clarity LIMS v4.2/4.3/5.0/5.1/5.2/5.3/5.4/6.0.
- The command hostname -f must resolve to the fully-qualified domain name of the server. For details, refer to the Clarity LIMS *Pre-Installation Requirements* on page 232 document and refer to the Ensure Hostname resolution section.

> Before installing Clarity LIMS on the new instance, make sure that the instance has the same fully-qualified domain name as the existing Production instance. If it is not possible to have the same fully-qualified domain name, contact the Clarity LIMS Support team.

2. Configure the New Instance

To configure the new instance, follow the instructions provided in the Clarity LIMS *Pre-Installation Requirements* on page 232. Refer to the *Technical Overview* on page 2.

- Custom configurations: If you have made any additional configurations that are not part of the Clarity LIMS pre-installation requirements, apply these configurations to the new instance.
- Passwords: Configure all passwords to be same as the existing instance. After you have verified the new instance, you can change passwords as needed.

3. Verify User Account Email Addresses

Make sure that all user accounts have email addresses associated with them. Users must reset their passwords after the upgrade is complete.

4. Install and Run the Pre-Validation Script on the Source Server

To assist with validating the system before an upgrade, install the UpgradePreValidation RPM on the source server.

- This RPM is installed temporarily, and provides tools to help check the system before an upgrade.
- If validation is successful, remove this RPM and proceed with the upgrade.

1. Install the UpgradePreValidation RPM (make sure that the correct repo is enabled).
   - On the source server, as the root user, run the following command:
     ```
     yum --enablerepo=GLS_Clarity6 install ClarityLIMS-UpgradePreValidation
     ```
2. [Optional] Set up Secret Utility.
   - If ClarityLIMS-SecretUtil was installed previously, run the following command to set up Secret Utility as the glsjboss user:
     ```
     /opt/gls/clarity/config/pending/05_configure_claritylims_secretutil.sh
     ```
     Using a vault is the safer way of storing application secrets. If using a vault is not possible, the configuration script supports file-based storage.
   - For more information on the prompts, refer to the Configuration Script section of *Guide to Secret Management* on page 315.
3. Run the validation script.
   a. Make sure that the Clarity LIMS server is running.
   b. As the root user, run the following command:

```
bash /opt/gls/ClarityUpgradeValidation/bin/validate.sh
```

   c. Review the output of the script to determine if you can proceed with the upgrade. If the script outlines any issues with the potential upgrade, review the generated log files and contact the Clarity LIMS Support team for further assistance.

For Research Use Only. Not for use in diagnostic procedures.

4. Remove the Pre-Validation RPM.
   Remove the Pre-Validation RPM only after you confirm that you can upgrade. If you are unsure, consult the Clarity LIMS LIMS Support team.
   - As the root user, run the following command:

```
yum remove ClarityLIMS-UpgradePreValidation
```

5. Back Up the Current Database and Clarity LIMS

Archive the backup in case a rollback is required. Before performing the backup, stop Clarity LIMS.

1. Stop Clarity LIMS:
   - On the command-line interface, run the following command as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

   This command stops all Clarity LIMS components, including Automation Worker and integration services.
2. Back up PostgreSQL database:
   On the PostgreSQL server, best practice recommends backing up the database using the pg_dump utility.
   The example provided makes the following assumptions:
   - The database server and the application server are on the same server.
   - The pg_dump utility is accessible to the glsjboss user.

   Example:
   The Postgres DBA uses the following commands to create a database backup in the glsjboss home directory. Substitute the variables as appropriate for the specific environment.
   - As the glsjboss user:

```
cd ~glsjboss
mkdir -p backups/database
pg_dump -U <database_user> -b -O -Ft <database_name> -f
~glsjboss/backups/database/clarity-old_version-`date +%Y%m%d%H%M`.tar
```

3. Make sure that the following items, and any other files and configurations, are backed up safely:
   - crontab -l
   - Custom scripts
   - OS configuration files
   - Firewall rules
   - Network configuration

   If there are custom changes to any application configurations (to increase performance, security, and so on), restore/configure these items manually later by referencing the backup.

For Research Use Only. Not for use in diagnostic procedures.

We recommend that you back up the items into a single zip file and transfer them to the new instance.

Directories:

```
/opt/gls/clarity/users/glsftp or /home/glsftp (Clarity LIMS file store location)
/opt/gls/clarity/customextensions
/opt/gls/clarity/glscontents
/etc/httpd/conf.d
/etc/httpd/sslcertificate
```

Files:

```
.pgpass
/opt/gls/pgsql/9.x/pg_hba.conf
/opt/gls/pgsql/9.x/postgresql.conf
```

Additional configurations:

```
rpm -qa | grep "BaseSpace\|Clarity" > clarityrpms.txt
```

Upgrade Steps

Install Latest Clarity LIMS on New Instance

1. Make sure that the repository file exists in the following location:

```
/etc/yum.repos.d/
```

2. As the root user, install the RPMs required on the new instance by referencing the content of `clarityrpms.txt`.
   - If you are upgrading from Clarity LIMS v4.x, some RPMs (eg, Server RPM) are now included under other RPMs.
   - Install any other required RPMs, eg, Python packages, that are not part of the Clarity LIMS setup.
   - Do not install NGS, Illumina Preset Protocols (IPP), and Sequencing RPMs during this step. You install these RPMs later in the installation process.
3. Configure and validate the new system, following the procedure outlined in the *Installation Procedure (Clarity LIMS v6.1)* on page 240.
   - When prompted for user passwords, enter the passwords used in the previous instance.
4. Stop Clarity LIMS. To do so, on the command-line interface, run the following command as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

The following steps are only required if you are restoring from a previous instance. If you are installing in a test environment, proceed to the *Verify the New Instance* on page 307 section.

Install and Configure LabLink v2.3

LabLink v2.3 is compatible with Clarity LIMS v6.1.

If upgrading from Clarity LIMS v4.x, Illumina migrates your LabLink-related data with the following exceptions:

- Sample submission templates
- Customized UI CSS
- LabLink property table configurations

Before completing the following steps, make sure that a database with the name of lablink is created with the same database user as Clarity LIMS database.

1. Install the LabLink RPM. Make sure that you have the correct repo enabled.
   - On the new instance, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-LabLink
```

2. Run the pending initialization script.
   - As the glsjboss user, run the following command:

```
bash /opt/gls/clarity/config/pending/60_initialize_lablink.sh
```

3. The script prompts for a Google reCAPTCHA URL, site key, and secret key.
   - Google reCAPTCHA URL: https://www.google.com/recaptcha/
   - Google reCAPTCHA site key and secret key: View these keys from the Google reCAPTCHA Admin Console, under Settings.

   > If you prefer not to use reCAPTCHA, leave the site-key and secret-key fields blank when running the configuration script. LabLink does not display the reCAPTCHA when these fields are blank. You can also use your own reCAPTCHA accounts when configuring LabLink.

   - To reconfigure LabLink (without initializing the database), run the following command as the glsjboss user:

```
bash /opt/gls/clarity/config/configure_lablink.sh
```

Restore Backup Onto the New Instance

1. Extract the backup zip file into a suitable location (eg, `/tmp/restore`).

   > If using Oracle database, skip the following steps 2 and 3. Contact the Clarity LIMS Support team for assistance in performing the migration from Oracle to PostgreSQL.

2. If using PostgreSQL database, the DBA imports the database dump into the new database instance. Dropping and recreating the database might be necessary. If this is needed, use the following command:

```
dropdb -U postgres "CentOS7DB"
```

```
createdb -U postgres "CentOS7DB"
psql -U postgres -d "CentOS7DB" -c 'ALTER DATABASE "CentOS7DB" OWNER TO
"CentOS7User"'
```

3. Restore the database exported from the previous instance.
4. Extract and restore the following directories to the same directory on the new instance:
   - Clarity LIMS file store: `/opt/gls/clarity/users/glsftp` or `/home/glsftp`
   - `/opt/gls/clarity/custom/extensions`
   - `/opt/gls/clarity/glscontents`
   - `/etc/httpd/conf.d`

   As of RedHat Enterprise Linux / CentOS v7.9, Apache v2.4 is installed. There are several configuration changes in this version. You can use the new configuration, or merge your previous configuration file cautiously to the new configuration file. For details on the changes, refer to: httpd.apache.org.
5. Copy the SSL certificate files to the following location (create the directory if it does not exist):

```
/etc/httpd/sslcertificate
```

6. To configure the certificates, run the following command on the command-line interface, as the root user:

```
/opt/gls/clarity/config/installCertificates.sh
```

   For more information, refer to *Install a Purchased SSL/TLS Certificate* on page 333.
7. Restore files and configurations.
   - Copy any custom scripts into their folder locations.
   - For PostgreSQL database, copy/merge the database configuration file (ie, `pg_hba.conf` and `postgresql.conf`).
   - Restore crontab from file.
   - Copy / Merge any additional application configurations.

[Optional] Change the Clarity LIMS Hostname

This step is required only if the new instance hostname is different from the old instance hostname.

For details, refer to *Change the Clarity LIMS Hostname* on page 326.

[Optional] Update Application Configuration

This step is required only if the passwords for glsftp and/or apiuser have changed.

To update the application configuration, complete the following steps:

1. Update glsftp password.

2. Update apiuser password.
3. Update database connection details.

For details, refer to *Update Server Passwords and Database Connection Details* on page 331.

Perform Application Migration

In this step, the clarity-migrator tool is used to perform the changes required to make the database compatible with the new Clarity LIMS version.

On the command-line interface, run the following commands as the glsjboss user:

```
cd /opt/gls/clarity/config/
./migrate_claritylims_database.sh
```

[Optional] Install NGS, IPP, and Sequencing RPMs

This step is required only if the RPMs have been installed on the existing Clarity LIMS instance.

- Install the latest NGS, IPP, and Sequencing RPMs compatible with the new Clarity LIMS version, as listed in `clarityrpms.txt`.

All existing workflows, protocols, steps, and master steps are restored during the restoration process. After installing the NGS and IPP RPMs, you do not need to install the workflows again.

- If the automation/External Program Plugin (EPP) scripts installed on the new instance are of a later version (eg, `/opt/gls/cla/opt/gls/clarity/extensions/ngs-common/v5/EPP) than` your old instance (eg, `/opt/gls/clarity/extensions/ngs-common/v4/EPP`), you must manually update the script location in your automation / EPP command lines. You can do update the script location in the Clarity LIMS interface or the Operations interface.
- If you intend to install NovaSeq API-based integration, NextSeq integration, or MiSeq integration, use the latest package to ensure OS compatibility.

Delete ElasticSearch indexes and Restart Clarity LIMS on the New Instance

On the command-line interface, run the following commands as the root user:

- Make sure that ElasticSearch is running:

```
service elasticsearch start
```

- When ElasticSearch service is running, remove the ElasticSearch indexes:

```
curl _XDELETE 'http://localhost:9200/_all'
```

- Restart Clarity LIMS:

```
/opt/gls/clarity/bin/run_clarity.sh stop
/opt/gls/clarity/bin/run_clarity.sh start
```

Verify the New Instance

The following verification steps are the minimum required to confirm that the various services are up and running properly.

To conduct a thorough verification, perform your verification steps or daily routine on the new Clarity LIMS instance.

1. ElasticSearch, Search Indexer, and RabbitMQ
   a. Log in to Clarity LIMS LIMS via `https://<FQDN>/clarity` and perform a basic search.
   b. Check that search results are returned.
   c. If no search results are returned, try again later as the search indexes are still building.
2. Tomcat, Apache, Automation Worker
   a. Run a sample through a QC protocol step. Create a temporary workflow if necessary.
   b. Make sure that the automation executes successfully and the log files are accessible.
   c. Open a browser window and access `https://<FQDN>/api/v2/projects`.
   d. Log in with api user credentials.
   e. Check that all projects are returned in the response.
3. LabLink
   a. Open a browser window and access `https://<FQDN>/lablink/`.
   b. Log in with administrator credentials.
   c. On the Projects page, make sure that all data are properly displayed.
4. [Optional]Sequencing Service
   To make sure that the service is running properly, you must initiate an actual sequencing run on the instrument.

Upgrade Procedure for Cloud to On Premise Deployments

From Versions 4.2 / 4.3 / 5.0 / 5.1/ 5.2 / 5.3 / 5.4 to 6.0

This document provides details on the steps required to upgrade an existing Clarity LIMS to RedHat Enterprise Linux /CentOS 7.9 compatible Clarity LIMS v6.0.

For installation requirements, refer to *Technical Requirements* on page 5.

Migration Paths

The following table shows the applicable migration paths.

From	To	Notes
v4.2 Cloud v4.3 Cloud v5.0 Cloud v5.1 Cloud v5.2 Cloud v5.3 Cloud v5.4 Cloud	v6.0 On-premise	Changing environment from Illumina cloud hosted to on-premise.

Prerequisites

Before Illumina can proceed with the upgrade, complete the following prerequisite steps.

1. Provision the New Instance

- The system must meet the requirements listed in the Clarity LIMS *Technical Overview* on page 2.
- All standard OS security updates must have been applied.
- Upgrades are only supported from Clarity LIMS v4.2/4.3/5.0/5.1/5.2/5.3/5.4.
- The command hostname -f must resolve to the fully-qualified domain name of the server. For details, refer to the Clarity LIMS *Pre-Installation Requirements* on page 232 document and refer to the Ensure Hostname resolution section.

Before installing Clarity LIMS on the new instance, make sure that the instance has the same fully-qualified domain name as the existing Production instance. If it is not possible to have the same fully-qualified domain name, contact the Clarity LIMS Support team.

2. Configure the New Instance

To configure the new instance, follow the instructions provided in the Clarity LIMS *Pre-Installation Requirements* on page 232. Refer to the *Technical Overview* on page 2.

- Custom configurations: If you have made any additional configurations that are not part of the Clarity LIMS pre-installation requirements, apply these configurations to the new instance.
- Passwords: Configure all passwords to be same as the existing instance. After you have verified the new instance, you can change passwords as needed.

3. Verify User Account Email Addresses

Make sure that all user accounts have email addresses associated with them. Users must reset their passwords after the upgrade is complete.

4. Install and Run the Pre-Validation Script on the Source Server

To assist with validating the system before an upgrade, install the UpgradePreValidation RPM on the source server.

- This RPM is installed temporarily, and provides tools to help check the system before an upgrade.
- If validation is successful, remove this RPM and proceed with the upgrade.

1. Install the UpgradePreValidation RPM (make sure that the correct repo is enabled).
   - On the source server, as the root user, run the following command:
     ```
     yum --enablerepo=GLS_Clarity6 install ClarityLIMS-UpgradePreValidation
     ```
2. [Optional] Set up Secret Utility.
   - If ClarityLIMS-SecretUtil was installed previously, run the following command to set up Secret Utility as the glsjboss user:
     ```
     /opt/gls/clarity/config/pending/05_configure_claritylims_secretutil.sh
     ```
     Using a vault is the safer way of storing application secrets. If using a vault is not possible, the configuration script supports file-based storage.
   - For more information on the prompts, refer to the Configuration Script section of *Guide to Secret Management* on page 315.
3. Run the validation script.
   a. Make sure that the Clarity LIMS server is running.
   b. As the root user, run the following command:
   ```
   bash /opt/gls/ClarityUpgradeValidation/bin/validate.sh
   ```
   c. Review the output of the script to determine if you can proceed with the upgrade. If the script outlines any issues with the potential upgrade, review the generated log files and contact the Clarity LIMS Support team for further assistance.
4. Remove the Pre-Validation RPM.
   Remove the Pre-Validation RPM only after you confirm that you can upgrade. If you are unsure, consult the Clarity LIMS LIMS Support team.
   - As the root user, run the following command:
   ```
   yum remove ClarityLIMS-UpgradePreValidation
   ```

5. Back Up the Current Database and Clarity LIMS

Archive the backup in case a rollback is required. Before performing the backup, stop Clarity LIMS.

1. Stop Clarity LIMS:
   - On the command-line interface, run the following command as the root user:
   ```
   /opt/gls/clarity/bin/run_clarity.sh stop
   ```


For Research Use Only. Not for use in diagnostic procedures.

This command stops all Clarity LIMS components, including Automation Worker and integration services.

2. Back up PostgreSQL database:
   On the PostgreSQL server, best practice recommends backing up the database using the pg_dump utility.
   The example provided makes the following assumptions:
   - The database server and the application server are on the same server.
   - The pg_dump utility is accessible to the glsjboss user.

   Example:
   The Postgres DBA uses the following commands to create a database backup in the glsjboss home directory. Substitute the variables as appropriate for the specific environment.
   - As the glsjboss user:

```
cd ~glsjboss
mkdir -p backups/database
pg_dump -U <database_user> -b -O -Ft <database_name> -f
~glsjboss/backups/database/clarity-old_version-`date +%Y%m%d%H%M`.tar
```

3. Make sure that the following items, and any other files and configurations, are backed up safely:
   - crontab -l
   - Custom scripts
   - OS configuration files
   - Firewall rules
   - Network configuration

   If there are custom changes to any application configurations (to increase performance, security, and so on), restore/configure these items manually later by referencing the backup.
   We recommend that you back up the items into a single zip file and transfer them to the new instance.
   Directories:

```
/opt/gls/clarity/users/glsftp or /home/glsftp (Clarity LIMS file store location)
/opt/gls/clarity/customextensions
/opt/gls/clarity/glscontents
/etc/httpd/conf.d
/etc/httpd/sslcertificate
```

   Files:

```
.pgpass
/opt/gls/pgsql/9.x/pg_hba.conf
/opt/gls/pgsql/9.x/postgresql.conf
```

   Additional configurations:

```
rpm -qa | grep "BaseSpace\|Clarity" > clarityrpms.txt
```


For Research Use Only. Not for use in diagnostic procedures.

Upgrade Steps

Install Latest Clarity LIMS on New Instance

1. Make sure that the repository file exists in the following location:

```
/etc/yum.repos.d/
```

2. As the root user, install the RPMs required on the new instance by referencing the content of `clarityrpms.txt`.
   - If you are upgrading from Clarity LIMS v4.x, some RPMs (eg, Server RPM) are now included under other RPMs.
   - Install any other required RPMs, eg, Python packages, that are not part of the Clarity LIMS setup.
   - Do not install NGS, Illumina Preset Protocols (IPP), and Sequencing RPMs during this step. You install these RPMs later in the installation process.
3. Configure and validate the new system, following the procedure outlined in the *Installation Procedure (Clarity LIMS v6.0)* on page 243.
   - When prompted for user passwords, enter the passwords used in the previous instance.
4. Stop Clarity LIMS. To do so, on the command-line interface, run the following command as the root user:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

> The following steps are only required if you are restoring from a previous instance. If you are installing in a test environment, proceed to the *Verify the New Instance* on page 314 section.

Install and Configure LabLink v2.2

LabLink v2.2 is compatible with Clarity LIMS v6.0.

If upgrading from Clarity LIMS v4.x, Illumina migrates your LabLink-related data with the following exceptions:

- Sample submission templates
- Customized UI CSS
- LabLink property table configurations

Before completing the following steps, make sure that a database with the name of lablink is created with the same database user as Clarity LIMS database.

1. Install the LabLink RPM (make sure that you have the correct repo enabled).
   - On the new instance, as the root user, run the following command:

```
yum --enablerepo=GLS_Clarity6 install ClarityLIMS-LabLink
```

2. Run the pending initialization script.
   - As the glsjboss user, run the following command:

```
bash /opt/gls/clarity/config/pending/60_initialize_lablink.sh
```

3. The script prompts for a Google reCAPTCHA URL, site key, and secret key.
   - Google reCAPTCHA URL: https://www.google.com/recaptcha/
   - Google reCAPTCHA site key and secret key: View these keys from the Google reCAPTCHA Admin Console, under Settings.

   > If you prefer not to use reCAPTCHA, leave the site-key and secret-key fields blank when running the configuration script. This will prevent LabLink from displaying the reCAPTCHA. You can also use your own reCAPTCHA accounts when configuring LabLink.

   - To reconfigure LabLink (without initializing the database), run the following command as the glsjboss user:

```
bash /opt/gls/clarity/config/configure_lablink.sh
```

Restore Backup Onto the New Instance

1. Extract the backup zip file into a suitable location (eg, `/tmp/restore`).

   > If using Oracle database, skip the following steps 2 and 3. Contact the Clarity LIMS Support team for assistance in performing the migration from Oracle to PostgreSQL.

2. If using PostgreSQL database, the DBA imports the database dump into the new database instance. Dropping and recreating the database can sometimes be necessary. If needed, use the following command to do so:

```
dropdb -U postgres "CentOS7DB"
createdb -U postgres "CentOS7DB"
psql -U postgres -d "CentOS7DB" -c 'ALTER DATABASE "CentOS7DB" OWNER TO
"CentOS7User"'
```

3. Restore the database exported from the previous instance.
4. Extract and restore the following directories to the same directory on the new instance:
   - Clarity LIMS file store: `/opt/gls/clarity/users/glsftp` or `/home/glsftp`
   - `/opt/gls/clarity/custom/extensions`
   - `/opt/gls/clarity/glscontents`
   - `/etc/httpd/conf.d`

For Research Use Only. Not for use in diagnostic procedures.

> As of RedHat Enterprise Linux / CentOS v7.9, Apache v2.4 is installed. There are several configuration changes in this version. You can use the new configuration, or merge your previous configuration file cautiously to the new configuration file. For details on the changes, refer to: httpd.apache.org.

5. Copy the SSL certificate files to the following location (create the directory if it does not exist):

```
/etc/httpd/sslcertificate
```

6. To configure the certificates, run the following command on the command-line interface, as the root user:

```
/opt/gls/clarity/config/installCertificates.sh
```

   For more information, refer to *Install a Purchased SSL/TLS Certificate* on page 333.

7. Restore files and configurations.
   - Copy any custom scripts into their folder locations.
   - For PostgreSQL database, copy/merge the database configuration file (eg, `pg_hba.conf` and `postgresql.conf`).
   - Restore crontab from file.
   - Copy / Merge any additional application configurations.

[Optional] Change the Clarity LIMS Hostname

This step is required only if the new instance hostname is different from the old instance hostname.

For details, refer to *Change the Clarity LIMS Hostname* on page 326

[Optional] Update Application Configuration

This step is required only if the passwords for glsftp and/or apiuser have changed.

To update the application configuration, complete the following steps:

1. Update glsftp password.
2. Update apiuser password.
3. Update database connection details.

For details, refer to *Update Server Passwords and Database Connection Details* on page 331.

Perform Application Migration

In this step, the clarity-migrator tool is used to perform the changes required to make the database compatible with the new Clarity LIMS version.

On the command-line interface, run the following commands as the glsjboss user:

```
cd /opt/gls/clarity/config/
./migrate_claritylims_database.sh
```

[Optional] Install NGS, IPP, and Sequencing RPMs

This step is required only if the RPMs have been installed on the existing Clarity LIMS instance.

- Install the latest NGS, IPP, and Sequencing RPMs compatible with the new Clarity LIMS version, as listed in `clarityrpms.txt`.

All existing workflows, protocols, steps, and master steps are restored during the restoration process. After installing the NGS and IPP RPMs, you do not need to install the workflows again.

- If the automation/External Program Plugin (EPP) scripts installed on the new instance are of a later version (eg, `/opt/gls/cla/opt/gls/clarity/extensions/ngs-common/v5/EPP) than` your old instance (eg, `/opt/gls/clarity/extensions/ngs-common/v4/EPP`), you must manually update the script location in your automation / EPP command lines. You can do update the script location in the Clarity LIMS interface or the Operations interface.
- If you intend to install NovaSeq API-based integration, NextSeq integration, or MiSeq integration, use the latest package to ensure OS compatibility.

Delete ElasticSearch indexes and Restart Clarity LIMS on the New Instance

On the command-line interface, run the following commands as the root user:

- Make sure that ElasticSearch is running:

```
service elasticsearch start
```

- When ElasticSearch service is running, remove the ElasticSearch indexes:

```
curl _XDELETE 'http://localhost:9200/_all'
```

- Restart Clarity LIMS:

```
/opt/gls/clarity/bin/run_clarity.sh stop
/opt/gls/clarity/bin/run_clarity.sh start
```

Verify the New Instance

The following verification steps are the minimum required to confirm that the various services are up and running properly.

To conduct a thorough verification, perform your verification steps or daily routine on the new Clarity LIMS instance.

1. ElasticSearch, Search Indexer, and RabbitMQ
   a. Log in to Clarity LIMS LIMS via `https://<FQDN>/clarity` and perform a basic search.
   b. Check that search results are returned.
   c. If no search results are returned, try again later as the search indexes are still building.
2. Tomcat, Apache, Automation Worker
   a. Run a sample through a QC protocol step. (Create a temporary workflow if necessary.)

For Research Use Only. Not for use in diagnostic procedures.

b. Make sure that the automation executes successfully and the log files are accessible.
c. Open a browser window and access `https://<FQDN>/api/v2/projects`.
d. Log in with api user credentials.
e. Check that all projects are returned in the response.

3. LabLink
   a. Open a browser window and access `https://<FQDN>/lablink/`.
   b. Log in with administrator credentials.
   c. On the Projects page, make sure that all data are properly displayed.
4. [Optional] Sequencing Service
   To make sure that the service is running properly, you must initiate an actual sequencing run on the instrument.

Guide to Secret Management

Secret Utility (secretutil) is a password management tool used to store, manage, and retrieve passwords. Secret Utility returns the passwords in plain text.

The following sections describe the configuration of Secret Utility, which is installed as part of the Clarity LIMS-SecretUtil RPM.

Installing Integration Packages on Clarity LIMS

Integration Package	Clarity LIMS Version	Secret Util Mode	Installation Steps
Packages that require Clarity LIMS-SecretUtil.	Illumina Cloud Hosted v5.4 and later	Vault	Secret Utility would have been configured during installation of Illumina cloud hosted deployments of Clarity LIMS v5.4 and later. For details on installing and configuring the integration package, see the related installation guide.
Packages that do not require Clarity LIMS-SecretUtil.	Illumina Cloud Hosted v5.4 and later	Vault	Clarity LIMS v5.4 and later do not support these integration packages.

Integration Package	Clarity LIMS Version	Secret Util Mode	Installation Steps
Packages that require Clarity LIMS-SecretUtil.	Illumina Cloud Hosted/On Premise v5.3 and earlier	File	Clarity LIMS-SecretUtil installs Secret Utility. Before continuing with the configuration of the integration package, complete the following steps: 1. In: `/opt/gls/clarity/config/pending` run the following script: `05_configure_claritylims_secretutil.sh` 2. Configure Secret Utility in File mode. 3. Refer to *Install/Upgrade Secret Management for Integration Modules* on page 321 for the passwords required to be configured in File mode.
Packages that do not require ClarityLIMS-SecretUtil.	Illumina Cloud Hosted/On Premise v5.3 and earlier	—	Refer to the integration package installation guide for more information on installing and configuring the integration package.

Configuration Script

If Secret Utility has not been configured, the `05_configure_claritylims_secretutil.sh` script is created in the `/opt/gls/clarity/config/pending` folder.

To reconfigure Secret Utility:

1. Remove the hidden file `/opt/gls/clarity/tools/secretutil/.configured`
2. Run the Secret Utility configuration script as follows:

```
/opt/gls/clarity/config/configure_claritylims_secretutil.sh
```

The following table describes the entries prompted by the `configure_claritylims_secretutil.sh` script.

Table 9 Configuration Script Entries

Prompts	Default	Description
Enter required value for Secret Utility Mode.	vault	Configure the mode for Secret Utility. Possible values: vault, file

For Research Use Only. Not for use in diagnostic procedures.

Prompts	Default	Description
Enter required value for Clarity Tenant Hostname.	localhost	Vault mode only Configure the Tenant hostname to be used as part of the vault path.
Enter required value for Vault Engine Path.	secret	Vault Mode only Configure the secret engine path.
Enter required value for Vault URI.		Vault Mode only Configure the Vault Server target.
Vault Enterprise (Y/N)	N	Vault Mode only Configure whether the Vault Server is an enterprise version.
Enter required value for Vault Namespace.		Vault Enterprise only Configure the Vault namespace.
Enter required value for Vault Authentication Mode.		Vault Mode only Configure the authentication method. Possible values: token, approle
Enter required value for Vault Token.		Token Authentication only
Enter required value for Vault AppRole Role-Id.		AppRole Authentication only Configure the AppRole role-id to use. Refer to Role ID noted during HashiCorp Vault configuration. (See *Configure Your HashiCorp Vault* on page 328)
Enter required value for Vault AppRole Secret-Id.		AppRole Authentication only Configure the AppRole secret-id to use. Refer to Secret ID noted during HashiCorp Vault configuration. (See *Configure Your HashiCorp Vault* on page 328)
Enter the required value for the following password prompts: • app.ftp.password • app.ldap.managerPass • app.rabbitmq.password • db.tenant.password • db.clarity.password • db.lablink.password • db.reporting.password		File Mode only Sets the secrets (encrypted with `CLARITYSECRET_ENCRYPTION_KEY env variable`) into `conf/secret.properties`.

For Research Use Only. Not for use in diagnostic procedures.

Prompts	Default	Description
Enter required value for Username for API user.	apiuser	File Mode only Sets the secrets (encrypted with `CLARITYSECRET_ENCRYPTION_KEY env variable`) into conf/secret.properties.
Enter required password for API user.		File Mode only Sets the password for the API user configuration.

Managing the Passwords (Vault Mode)

If Secret Utility is configured as Vault Mode, the passwords are stored and retrieved from Vault Enterprise.

- To use Secret Utility and perform the following steps, you must first remote into the instance before performing any of the following steps.
- To use the Vault user interface (UI) and perform the following steps, you must have the appropriate role and access control list (ACL) policies.

Vault ACL Paths

The Vault ACLs control three main paths: Clarity, Integration, and Ops. If there is an attempt to write into a read-only path, `secretutil.jar` returns an error.

Clarity (read only)

- Stores all passwords related to Clarity LIMS. The secrets/passwords are encrypted with `CLARITYSECRET_ENCRYPTION_KEY env variable`. Refer to *Configuration Script Entries* on page 316.

Integration (read write)

- Stores all integration-related passwords and allows read and write access.
- apiusers
  - Stores passwords that are used by packages and applications for API authentication (eg, the apiuser password).
  - Username is case sensitive.
  - For example, retrieve apiuser password from `integration/apiusers/apiuser`.
- external.file.stores
  - Stores password of external file stores used by Clarity LIMS.
  - External file store is optional to the Clarity LIMS system.

For Research Use Only. Not for use in diagnostic procedures.

- For example, retrieve file store password from `integration/external.file.stores/.password`.

Ops

- Stores secrets related to operations.
  - For Illumina cloud hosted deployments, Illumina manages this path.
  - This path is optional for on-premise customers.

Create a New Password

Using Secret Utility

The following command creates a new password:

```
java -jar /opt/gls/clarity/tools/secretutil/secretutil.jar [-h] [-n="namespace"]
[-u="newValue"] "key"
```

- When creating a new password for integration, specify the `-n=` integration option.
- Make sure that the key uses a forward slash for nested secrets. For example, `apiusers/apiuser`
- The same command is used for updating an existing password and creating a new password. Read the key you are planning to create to check whether it is an existing password.

Using Vault UI

1. Log in to the Vault UI.
2. Select the Key Value (KV) secret engine with the path `instances`.
3. Look for the FQDN instance that you want to create the password for.
4. Select the path where you want to create the new password, ie, `clarity/integration/ops`.
5. Select Create Secret +.
6. Under Path for this secret, enter the path for the new password, eg, `app.ldap.managerPass`.
7. Under Version data:
   a. Enter 'value' into the key field.
   b. Enter the new password into the value field.
8. Select Save.

Read an Existing Password

Using Secret Utility

Run the following command to create a new password:

```
java -jar /opt/gls/clarity/tools/secretutil/secretutil.jar "key"
```


For Research Use Only. Not for use in diagnostic procedures.

Using Vault UI

1. Log in to the Vault UI.
2. Select the KV secret engine with the path 'instances'.
3. Look for the FQDN instance that you want to create the password for.
4. Select the path where the existing password is located, ie, `clarity/integration/ops`.
5. Click into the secret and view the password by selecting the peek icon.

Update an Existing Password

Using Secret Utility

Run the following command to update an existing password:

```
java -jar /opt/gls/clarity/tools/secretutil/secretutil.jar [-h] [-n="namespace"]
[-u="newValue"] "key"
```

Using Vault UI

1. Log in to the Vault UI.
2. Select the KV secret engine with the path `instances`.
3. Look for the FQDN instance for which you want to create the password.
4. Select the path where the existing password is located, ie, `clarity/integration/ops`.
5. Select into the secret.
6. Select Create new version +.
7. Under Version Data, enter the new password.
8. Select Save.

Delete an Existing Password

Secret Utility does not support permanent deletion of a key by design.

Using Vault UI

1. Log in to the Vault UI.
2. Select the KV secret engine with the path 'instances'.
3. Look for the FQDN instance that you want to create the password for.
4. Select the path, ie, `clarity/integration/ops`, to the location of the existing password.
5. Select into the secret.
6. Select Delete secret.

Managing the Passwords (File Mode)

If Secret Utility is configured as File mode, the passwords are encrypted and stored in `/opt/gls/clarity/tools/secretutil/conf/secrets.properties`. Encryption is based on the `CLARITYSECRET_ENCRYPTION_KEY` environment variable.

To manage the passwords and perform the following steps, you must first remote into the instance.

Create a New Password

Run the following command to create a new password:

```
java -jar /opt/gls/clarity/tools/secretutil/secretutil.jar [-h] [-n="namespace"]
[-u="newValue"] "key"
```

- If you are creating a new password for integration, specify the -n=integration option.
- The same command is used for updating an existing password and creating a new password. Read the key you are planning to create to check whether it is an existing password.

Read an Existing Password

Run the following command to read an existing password:

```
java -jar /opt/gls/clarity/tools/secretutil/secretutil.jar "key"
```

Update an Existing Password

Run the following command to update an existing password:

```
java -jar /opt/gls/clarity/tools/secretutil/secretutil.jar [-h] [-n="namespace"]
[-u="newValue"] "key"
```

Delete an Existing Password

Confirm with the Illumina Support team before deleting passwords and secrets.

By design, Secret Utility does not support permanent deletion of a key. As an alternative, you can run the following steps.

1. Open the `secrets.properties` file with an editor, eg, vim.
2. Remove the key from the file and save the file.

Install/Upgrade Secret Management for Integration Modules

As of Clarity LIMS v5.4, the method used for managing passwords (secrets) for Clarity LIMS integration modules has changed.

Newer integration packages are not backward compatible with previous deployments that use file-based password storage.

Compatibility Overview

Table 10 Compatibility of Versions for Integration Modules

Module	Prior Release	Released with Clarity LIMS v5.4 and later	Released with Clarity LIMS v6.2 and later	Integration
BaseSpaceLIMS-Pre-configured-Workflows-Package	1.2.1.5 and 2.0 1.2.2 (released with NovaSeq v3.2.2, not supporting Vault / Secret Utility)	2.1	Not applicable	Not applicable
BaseSpaceLIMS-Illumina-Preset-Protocols	1.0.2	2.0	2.6.0	IPP
Clarity LIMS-NGS-Package	5.19	5.20	Not applicable	NGS
Clarity LIMS-NGS-Package-v5	Not applicable	Not applicable	5.23	NGS
BaseSpaceLIMS-sequencer-api	2.2.1.9	2.3	2.6.0	NovaSeq 6000/6000Dx API-based integration
BaseSpaceLIMS-novaseq-sequencing-service	2.2.2	2.3	2.5.0	NovaSeq 6000 file-based integration
BaseSpaceLIMS-novaseq-extensions	2.2.2	2.3	2.5.0	NovaSeq 6000 file-based integration
HiSeq	5.6.1	5.7	Not applicable	HiSeq
HiSeq 3k4k	1.2.0.6	1.3	Not applicable	HiSeq 3000/4000
HiSeq X	1.5.0.5	1.6	Not applicable	HiSeq X
NextSeq 550	2.0.3	2.1	Not applicable	NextSeq 550

Module	Prior Release	Released with Clarity LIMS v5.4 and later	Released with Clarity LIMS v6.2 and later	Integration
ClarityLIMS-Illumina-NextSeq-Package-v2	Not applicable	Not applicable	2.3.0	NextSeq 550
MiSeq	7.0	7.1	Not applicable	MiSeq
ClarityLIMS-Illumina-MiSeq-Package-v8	Not applicable	Not applicable	8.2.0	MiSeq
MiSeq Dx	1.7.0.5	1.8	Not applicable	MiSeqDx
BaseSpaceLIMS-miseqdx-sequencing-service	Not applicable	Not applicable	1.10.0	MiSeqDx
BaseSpaceLIMS-miseqdx-extensions	Not applicable	Not applicable	1.10.0	MiSeqDx
BaseSpaceLIMS-SIS-Core-Package	Not applicable	Not applicable	2.4.0	NextSeq 1000/2000, iScan, NovaSeq X Series
BaseSpaceLIMS-SIS-Nextseq1k2k-Package	Not applicable	Not applicable	2.4.0	NextSeq 1000/2000
BaseSpaceLIMS-SIS-NovaSeqXSeries-Package	Not applicable	Not applicable	1.1.0	NovaSeq X Series
BaseSpaceLIMS-SIS-iScan-Package	Not applicable	Not applicable	1.1.0	iScan
BaseSpaceLIMS-unified-product-analytics	Not applicable	Not applicable	1.2.0	Clarity LIMS Product Analytics

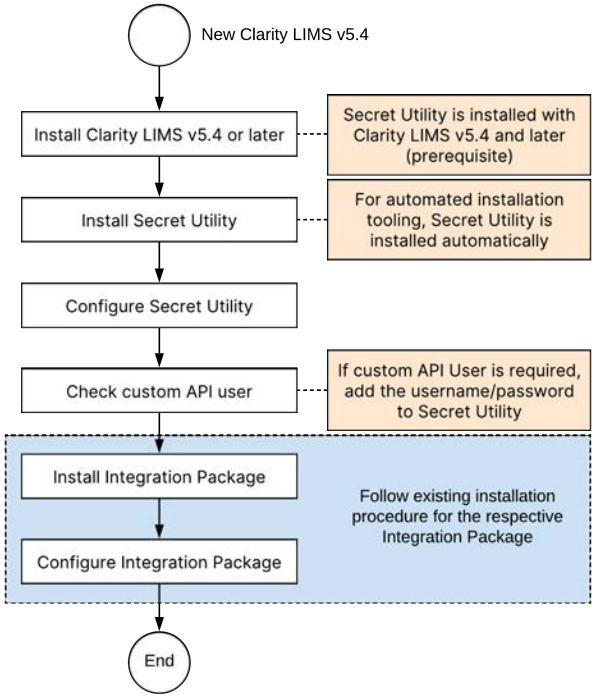
Module	Prior Release	Released with Clarity LIMS v5.4 and later	Released with Clarity LIMS v6.2 and later	Integration
BaseSpaceLIMS-unified-product-analytics-scripts	Not applicable	Not applicable	1.2.0	Clarity LIMS Product Analytics

Compatibility of Releases

- When installing Clarity LIMS v6.2 and later, only integration packages released with or after Clarity LIMS v6.2 are supported.
- HiSeq, HiSeq 3k4k and HiSeq X are no longer supported from Clarity LIMS v6.0 and later.
- When installing Clarity LIMS v5.4 and later, only integration packages released with or after Clarity LIMS v5.4 are supported.
- A newer integration package can be installed on older Clarity LIMS releases (* existing individual package requirements still apply). In this scenario, there will be two password management processes in the system:
  - Existing file-based password storage: used by Clarity LIMS and any older integration packages.
  - New secret management (Secret Util RPM): used by the newer integration package.
- Existing limitations or version compatibility of individual Integration packages with the Clarity LIMS version still apply.

Installation Steps for Clarity LIMS v5.4 and Later

The following diagram shows the installation steps required for installing Secret Utility and integration packages with Clarity LIMS v5.4 and later.



1. Install Clarity LIMS v6.0.
   - Install Clarity LIMS-App 6.0 and complete pending script.
   - Secret Utility (secretutil) is installed as part of Clarity LIMS-App 6.0 dependency, and the Secret Utility configuration is part of Clarity LIMS pending scripts.
2. Install Secret Utility.
   - In the automated installation tooling for Clarity LIMS v6.0, the installation and configuration of Secret Utility is included. No further action is necessary.
   - For manual installation:
     a. Install Clarity LIMS-SecretUtil.
     b. Configure Secret Utility by running the following script: `/opt/gls/clarity/config/pending/05_configure_claritylims_secretutil.sh`.

     Refer to *Guide to Secret Management* on page 315 for details on configuring Secret Utility.
3. Check usage of custom API username.
   - Check for any needs for custom API username, if any (eg `novaseq_user`). The documentation for the integration package provides the requirements for API username.

   > In a typical installation, a default API username (`apiuser`) is used. It is not necessary to add the default `apiuser` username, because it is configured as part of Clarity LIMS v6.0 installation. If no custom API username is required, skip step 4 and proceed to step 5.

For Research Use Only. Not for use in diagnostic procedures.

4. Configure custom API username.
   - If a custom API username is not required, proceed to step 5.
   - If a custom API username is required, configure the user/password with Secret Utility as follows. Substitute the values enclosed in double quotes with your own values, keeping the double quotes.

```
java -jar /opt/gls/clarity/tools/secretutil/secretutil.jar -n=INTEGRATION -
u="password" "key"
```

   Example:

```
java -jar /opt/gls/clarity/tools/secretutil/secretutil.jar -n=INTEGRATION -
u="mypassword" "apiusers/novaseq_user"
```

   - For a custom api username, set the key to `apiusers/{custom api username}`
5. Install integration package.
   There is no change to the installation of the integration package. Follow existing installation instructions.

   The new configuration script in the new integration package retrieves passwords directly from Secret Utility.

   For IAP access token and BSSH access token, follow the existing setup guide. There is no change in the configuration step.

Change the Clarity LIMS Hostname

The core Clarity LIMS product includes the `rename_claritylims_hostname.sh` script, which allows you to change the hostname to which Clarity LIMS responds.

Prerequisites and Considerations

Prerequisites

- Clarity LIMS must be fully installed and configured. If it is not, the script instructs you to complete the installation.
- The script stops all Clarity LIMS services. Make sure that all automation jobs are complete.
- If you are not using a wild card SSL Certificate, purchase a certificate for the new hostname.
- Update the hostname returned by the operating system to match the new name. Refer to *Pre-script Steps* on page 327 for more information.
- Running the renaming script requires root access.

Considerations

- The script does not update the Automation Worker installation. After you have completed the renaming steps, you must reconfigure all local and remote Automation Workers.

- You might need to reconfigure additional services, such as the Reporting and Sequencing services.

We recommend that you back up the database before performing the following renaming steps.

Settings Changed

The following table lists the settings changed by the `rename_claritylims_hostname.sh` script.

Property	Global	Description	Location
namingProviderHost	Yes	Configures appropriate endpoint for the Automation Worker	`/opt/gls/clarity/tomcat/current/lib/activity-management-ui-config.groovy`
api.uri	Per tenant setting	Base URI used by integrations for API calls	Property Table
ftp.host	Per tenant setting	Location of FTP host for this tenant*	Property Table
ServerName	Per tenant setting	Server name reference in lookup database	Lookup Database

* The ftp.host is only updated if it matches the previous IP address/hostname. This intended behavior accounts for the scenario in which the ftp host is on a different server.

Pre-script Steps

1. Change the internal hostname:
   Before running the `rename_claritylims_hostname.sh` script, change the internal hostname for the instance—that is, /etc/hosts and related areas. There is no need to change any other Clarity LIMS-related components.
   The new internal hostname is used in the renaming process.

For Research Use Only. Not for use in diagnostic procedures.

- To verify the internal hostname, use the following command:

```
hostname -f
```

If the hostname command does not return the correct new name, consult with your IT department to correct the name.

> Illumina does not edit the DNS or the local machine host file.

2. Verify SSL Certificate path:
   The script might prompt you for the SSL Certificate path. Be sure to have that ready.

Run the Script

1. Use the following command to change to the root user:

```
sudo su -
```

2. Navigate to the `/opt/gls/clarity/config` directory.
3. Run the script using the following command:
   `bash rename_claritylims_hostname.sh`
4. If prompted for your SSL Certificate path, enter this information.
5. The script prompts you to confirm that you have changed the internal hostname.
   - If you enter `no`, the script prompts you to change the hostname manually:

```
[root@qalocal config]# bash rename_claritylims_hostname.sh
Does your internal hostname match the new Clarity server hostname?: n
Please change your internal hostname to match the hostname you are passing to
this script to ensure Clarity can connect to it.
Do not change any Clarity related components.
```

   - If you enter `yes`, the script proceeds to modify Clarity LIMS-related components to use the new hostname.
6. When the renaming is complete, the script prompts you to restart Clarity LIMS by running the `run_clarity.sh` script:

```
/opt/gls/clarity/bin/run_clarity.sh start
```

7. When all Clarity LIMS services have restarted, make sure that the hostname has been changed successfully. Complete the following steps:
   a. Connect to all system components.
   b. Log in and test the Clarity LIMS user interface in your web browser.

Configure Your HashiCorp Vault

The following steps use the HashiCorp Vault user interface (UI) to guide you through the configuration of your HashiCorp Vault instance.

These configurations are mandatory for on premise Clarity LIMS deployments. For Illumina cloud hosted deployments, this configuration is completed by Illumina.

Detailed information and instructions for HashiCorp Vault are available on the HashiCorp website: www.hashicorp.com.

Prerequisites

- You are planning to install Clarity LIMS v6.0 or later.
- You have installed the latest version of either HashiCorp Vault Open Source or Enterprise.
- You have read the Getting Started tutorials for Vault on the HashiCorp website and/or possess a basic knowledge of HashiCorp Vault.
- You have system administrator permissions to perform the necessary operations to your HashiCorp Vault instance.
- You have allowed the necessary port 443 from the Clarity LIMS instance to your HashiCorp Vault instance.
- You have access to all the passwords required to be configured in your HashiCorp Vault instance.

Enable a New Key Value (KV) Secret Engine

To enable a new KV Secret Engine, refer to the Versioned Key/Value Secrets Engine tutorial provided on the HashiCorp Vault website.

Configure Secret Engine

The following table lists the secrets required for Clarity LIMS. To use the paths shown in the table, replace `$host` with your fully qualified domain name (FQDN).

When configuration is complete, these secrets are listed in the Vault user interface.

Path	Purpose
`$host/clarity/app.ftp.password`	Password for GLSFTP user on the Clarity LIMS instance.
`$host/clarity/app.rabbitmq.password`	Password for RabbitMQ admin on the Clarity LIMS instance.
`$host/clarity/db.clarity.password`	Password for the configured Clarity LIMS database user
`$host/clarity/db.lablink.password`	Password for the configured LabLink DB database user.
`$host/clarity/db.tenant.password`	Password for the configured Tenant Lookup DB database user.

Path	Purpose
`$host/clarity/app.ldap.managerPass`	[Optional] Password for the User DN configured for Clarity LIMS LDAP integration
`$host/integration/apiusers/apiuser`	Password for the apiuser user account that is used by Automation Worker to authenticate with Clarity LIMS API. If you have configured a different user account, create it under `$host/integration/apiusers/$username`

Authentication Methods

AppRole

AppRole is the recommended authentication method to use with the Clarity LIMS Secret Utility tool.

1. To enable the AppRole authentication method, refer to the AppRole Pull Authentication tutorial provided on the HashiCorp Vault website.
2. When AppRole is enabled, create an AppRole with the appropriate Access Control List (ACL) policy (see the following section).
3. Make a note of the Role ID and Secret ID. You need these IDs when configuring Secret Utility.

Secret Utility does not manage your Role ID and Secret ID for you (eg, renewing, revoking, and so on). It accepts the Role ID and Secret ID as-is, and attempts to authenticate with Vault.

Token

Alternatively, the Clarity LIMS Secret Utility tool also works with the token authentication method.

To learn more about tokens, see the Tokens documentation on the HashiCorp Vault website.

Secret Utility does not manage your tokens for you (eg, renewing, revoking, and so on). It accepts the token as-is, and attempts to authenticate with Vault.

Authentication ACL Policies

After enabling the AppRole authentication method, create ACL policies to access the Secret Engine.

In the following example, replace 'claritylims' with your Secret Engine path.

```
# For clarity instance to read from hashicorp vault
path "claritylims/data/+/clarity/*"
{
capabilities = ["read"]
}
```


For Research Use Only. Not for use in diagnostic procedures.

```
# For integration to write to hashicorp vault
path "claritylims/data/+/integration/*"
{
capabilities = ["read","create","update"]
}
```

You might need to update or create additional ACL policies for your System Administrator to rotate the credentials, when required.

To create the ACL policy, refer to the Vault Policies tutorial provided on the HashiCorp Vault website.

Verification

1. SSH into the Clarity LIMS instance.
2. After installing Clarity LIMS and configuring Secret Utility using the instructions provided in *Guide to Secret Management* on page 315, run the command to read an existing password/secret from HashiCorp Vault.

Update Server Passwords and Database Connection Details

Two levels of user passwords are created in the Clarity LIMS system: one at the operating system level and one at the Clarity LIMS level.

Following are details on the user passwords, instructions for changing them, and instructions for updating Clarity LIMS with the new database connection details.

The following steps are only required if the passwords for glsftp and/or apiuser have been changed.

Update Operating System User Passwords

The user passwords created at the operating system level are for the glsai, glsjboss, and glsftp users.

- glsai and glsjboss users—Have no associated configuration. You can change their passwords at any time.
- glsftp user—After installation of Clarity LIMS, you can change this password. However, you must also update it in the file/vault secret store, using the Secret Management Util tool.

To change the glsftp password after installing Clarity LIMS:

1. Change the glsftp password on the server.
2. Log in to the server as the glsjboss user.

3. Stop Clarity LIMS using the following command:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

4. Go to `/opt/gls/clarity/tools/secretutil`.
5. Update the password in the secret store.
   - For vault-based secret storage, use either the Vault command line interface (CLI) or Vault user interface (UI) to update the password.
   - For file-based secret storage, use Secret Management Util to update the password as follows:

```
$ java -jar /opt/gls/clarity/tools/secretutil/secretutil.jar -u="new-password"
app.ftp.password
```

6. Start Clarity LIMS using the following command:

```
/opt/gls/clarity/bin/run_clarity.sh restart
```

Update Clarity LIMS User Passwords

The user passwords created at the Clarity LIMS level are for the admin, facility, and apiuser users.

- admin and facility users—Have no associated configuration. You can change their passwords at any time.
- apiuser user—After installation of Clarity LIMS, you can change this password. However, you must also update it in the file/vault secret store, using the Secret Management Util.

To change the apiuser password after installing Clarity LIMS:

1. Check for any remote Automation Workers, and take note of their locations in your network. You will need to restart these after changing the password.
2. Log in to the server as the root user.
3. Stop Clarity LIMS using the following command:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

4. Go to `/opt/gls/clarity/tools/secretutil`.
5. Update the password in the secret store.
   - For vault-based secret storage, use either the Vault command line interface (CLI) or Vault user interface (UI) to update the password.
   - For file-based secret storage, use Secret Management Util to update the password as follows:

```
$ java -jar /opt/gls/clarity/tools/secretutil/secretutil.jar -n=integration -
u="new-password" "apiusers/apiuser"
```

6. Start Clarity LIMS using the following command:

```
/opt/gls/clarity/bin/run_clarity.sh restart
```

Update Database Connection Details

In some circumstances (such as security breaches/compromises), the database connection details (eg, database password) are updated, which prevents Clarity LIMS from connecting to the database. You can correct this issue by updating Clarity LIMS with the new database connection details as follows.

1. Check for any remote Automation Workers.
2. Update the existing tenant with the new details.
3. Restart any Automation Workers.

To update database connection details:

1. Check for any remote Automation Workers, and take note of their locations in your network.
2. Log in to the server as the root user.
3. Stop Clarity LIMS using the following command:

```
/opt/gls/clarity/bin/run_clarity.sh stop
```

4. Go to `/opt/gls/clarity/tools/secretutil`.
5. Update existing tenant with new details.
   - For vault-based secret storage, use either the Vault CLI or Vault UI to update the password.
   - For file-based secret storage, use the Secret Management Util to update the database password as the root user.

```
$ java -jar /opt/gls/clarity/tools/secretutil/secretutil.jar -u="db-password"
db.db-name.password
```

6. Start Clarity LIMS using the following command:

```
/opt/gls/clarity/bin/run_clarity.sh restart
```

Install a Purchased SSL/TLS Certificate

This section explains how to install purchased SSL/TLS certificates into Clarity LIMS v5 and later. Clarity LIMS can work with Named or WildCard certificates.

Typically, the process to install the certificates into Clarity LIMS is as follows:

1. Request a certificate from your IT organization, or purchase a certificate from a third-party SSL/TLS vendor.
2. Install the certificate using the script `installCertificates.sh` provided with Clarity LIMS. This script prompts for the required inputs and helps you to configure Clarity LIMS to use your SSL/TLS certificate.

> Some IT organizations have preexisting certificates issued by an internal organization, typically referred to as an 'internal CA.' These internal CA certificates are not fully compatible with Java, and prevent the automation worker—and all integrations—from properly communicating with the Clarity LIMS server. Internal CA certificates are therefore not supported in Clarity LIMS.

Obtain the Certificate

You will need your organization or the third-party SSL/TLS vendor to provide you with the following:

- An Apache 2.4-compatible SSL/TLS certificate
- The certificate private key
- The corresponding certificate chain, properly prepared for Apache 2.4. This component may not be required, depending on the organization that signs your certificate.

Your IT organization might provide you with a WildCard certificate. Clarity LIMS can use WildCard certificates, as long as the Apache 2.4-compatible certificate, private key, and certificate chain files are provided.

If purchasing from a third-party vendor, make sure that the vendor provides you with an Apache 2.4-compatible bundle that includes the components listed above. To purchase from a vendor, refer to their documentation.

Private Key Password Considerations

By default, a private key has a password associated with it. On startup, Apache requests a passphrase to access the private key. You can use either of the following methods to resolve this issue:

Method 1 — Place a passphrase file on the system and reference it in your clarity.conf file.

1. Create a passphrase file in a directory that has read, write, and execute permissions for only the root or apache user.

```
#! /bin/bash
echo "privatekeypassword"
```

2. Edit the clarity.conf file. The clarity.conf file is in the /etc/httpd/conf.d directory.

   Add the following line to your clarity.conf file, before the <VirtualHost> section:

```
SSLPassPhraseDialog exec:/path/to/passphrase-script
```

Method 2 — Remove the passphrase from the key.

⚠ Removing the passphrase from an OpenSSL key is a security risk. Only remove the passphrase if you know that this risk is acceptable.

Remove the password from an OpenSSL key using the following command:

```
% openssl rsa -in private.key -out private_nopassphrase.key
```

Install the SSL/TLS Certificates for Use with Clarity LIMS

Assumptions and Prerequisites

- You have installed Clarity LIMS and have run the `40_install_proxy.sh` script.
- You have OpenSSL (installed by default on the Clarity LIMS Linux server when you install Clarity LIMS). OpenSSL is used by the `installCertificates.sh` script.

- You have the files listed in the following table (obtained from the process described previously) available on the Clarity LIMS server. In the example shown below, these files are in the `/tmp/certs` directory.

File Description	Example File Name (used in the examples that follow)
Apache private key	`private.key`
Signed SSL/TLS Certificate	`customer_domain.crt`
Intermediate chain file (optional)	`intermediate.crt`

Install the Signed SSL/TLS Certificates

On the Clarity LIMS server, as the root user, run the `installCertificates.sh` script:

```
[root@doclarity04 ~]# cd /opt/gls/clarity/config/
[root@doclarity04 config]# bash installCertificates.sh
Java KeyTool detected
   This script will prompt you to supply the required SSL Certificates for your
   ClarityLIMS server.
   These files include:
   - A private key file and signed Certificate file for use by apache.
   - Optionally, depending on the organization that signs your Certificate, you
   may receive a 'Chain' file.
Enter the full path to the SSL Private Key for your
server:/tmp/certs/private.key
Enter the full path to the Apache Certificate for your server - This is the
Certificate signed by the SSL Vendor or Certificate
Authority:/tmp/certs/customer_domain.crt
Enter the full path to the SSL Vendor Chain file:/tmp/certs/intermediate.crt
INFO: Testing Apache
Syntax OK
Apache Proxy is ready
```

Reference

Additional reference information for Clarity LIMS.

Clarity LIMS v6.2.1 Release Notes

These Release Notes describe the key changes made to software components for Clarity LIMS v6.2.1. The Clarity LIMS v6.2.1 patch release supersedes v6.2.0. It is intended for customers on or migrating to Clarity LIMS v6.2.0.

This release resolves customer-reported issues related to the following functions:

- Search-indexer performance
- Basic search failure when searching with multiple custom fields in the system
- Necessary handling of controls for a configured step

New Features

There are no new features added with this release.

Bug Fixes

- Fixed a bug where the search-indexer did not quickly consume messages from the queue. This issue caused data in the system to be non-searchable.
- Fixed a bug where the bulk indexing for a project, container, step, and file failed due to a limitation in memory space for search-indexer. This bug occurred when the indexing batch size was too large. Indexing bulk size can now be modified with an attribute in `/opt/gls/clarity/search-indexer/conf/search-index-config.properties`.
- Fixed a bug where the basic search failed when searching with large numbers of custom fields in the system.
- Fixed a bug where details about the step failed to show when selecting the LIMS ID link for steps in the Advanced Search results.
- Fixed a bug where controls and samples must be added in a certain order for the configured step. This issue caused an error that prevented the configured protocol step from starting.
- Fixed a bug where a step cannot be started when controls and samples are in the standard step and the Enable QC flag is set to Yes.

Known Issues

- If the client and server are in different time zones, there can be additional or missing search results when using Date Received of a sample as one of the search criteria in Advanced Search.
- Multiple accounts that share an email address only receive a reset password email for one of the accounts when a reset password request is made using Email information.
- Users with the Read-Only permission do not have access to Advanced Search.
- {ProjectName} in the {ProjectName} token appears as duplicated when there is more than one sample in a step.
- On the Place Samples screen, the sample well position in the source container takes precedence in the placement order of the destination plate when placing samples from the Sample View List table. This placement order change only happens when samples are transferred from more than one source container. If the Sample View List table is sorted by a specific column, the order of the listed samples is ignored when they are placed in a destination plate.

For Research Use Only. Not for use in diagnostic procedures.

Additional Notes

- Customers connecting remotely to PostgreSQL database must make sure that their JDBC driver is compatible with the PostgreSQL version used.
- For on-premise deployments, Clarity LIMS v6.2.1 is qualified to run with the following server OS versions:
  - Oracle Linux v8.8 and v8.9 (64-bit)
  - RedHat Enterprise Linux v8.8 and v8.9 (64-bit)
- Security vulnerabilities in PostgreSQL 15.x have been addressed. PostgreSQL 15.2–15.6 is at a low risk of security vulnerabilities for customers on Clarity LIMS v6.2.1.
- PostgreSQL 15.2 and 15.6 are now qualified to run in Clarity LIMS v6.2.1.

Clarity LIMS v6.2 Release Notes

These Release Notes describe the key changes made to software components for Clarity LIMS v6.2.

Clarity LIMS v6.2 is deployable in both cloud hosted and on-premise environments.

New Features

- The operating system (OS) changes from CentOS7 to Oracle Linux v8.8.
- Lab account management that allows you to create, update, and delete accounts in Clarity LIMS.
- You can now set and update account custom field values. These configured fields are available in the new Account management screen when you view, create, or update an account.
- A red dot alert that displays when a required field without a default value is added to Clarity LIMS. This alert shows up LabLink next to the Configuration menu, the drop-down list in the Custom Fields menu, and next to Custom Fields in the Configuration tab.
- Configure client custom fields in LabLink through the Custom Fields Configuration page after they have been created through the Custom Fields Configuration Page in Clarity LIMS. The Users page in LabLink shows the configured custom fields when creating, editing, viewing, and reviewing a user.

Defect Repairs

- The Queue View page performance has been optimized.
- Reviewed and addressed potential vulnerabilities for cross site scripting (XSS).

Bug Fixes

- Fixed a bug where the upload of the sample submission spreadsheet with leading or trailing spaces in any of the header tags (eg, </TABLE HEADER>) resulted in import errors.
- Fixed a bug where the LIMS ID (Process) in the Record Details step disappeared when you select No preset.
- Fixed a bug where the custom term for Projects did not propagate to LabLink.

For Research Use Only. Not for use in diagnostic procedures.

- Fixed a bug where samples were not placed correctly when you drag and drop from the plate GUI. This bug happened when a step was configured to have samples ordered by Column and placed by Row in the placement stage.
- Fixed a bug where false errors occured when the Config-slicer tool was used to import automation template files. In this update, the Config-slicer tool ignores any differences in the automation file XML tag, but logs a reminder in the `configslicer-issues.log` file. The file lists the different automation names that the users should check against so that the automation files for those names are uploaded properly. The file also shows warnings or errors logged.
- Fixed a bug where the Config-slicer command-line interface (CLI) tool showed false negative reports with control types and reagent kits when the values were empty during the import or validation of the slice.
- Fixed a bug that affected the UI for the File Attachment Method for the Demultiplexing step in Master Step and Step during the Configuration stage.
- Updated UI and API application logs so that they contain only useful log information.

Known Issues

- There is a bulk indexing error due to the memory space limitation for search-indexer when the indexing batch size is too large.
- There can be additional or missing search results when using Date Received of a sample as one of the search criteria in Advanced Search when the client and server are in different time zones.
- Multiple accounts that share the same email address only receive a reset password email for one of the accounts when a reset password request is made using Email information.

Additional Notes

Clarity LIMS v6.2 supports both Python2 and Python3 versions. However, there is no symbolic link created for `/usr/bin/python` to Python2 and there will not be a default link. Scripts have to be updated specifically to either Python2 or Python3.

Appendix

The following components and applications are updated in Clarity LIMS v6.2:

Component	Clarity LIMS v6.1	Clarity LIMS v6.2
Rabbitmq Server	3.8.16	3.11.9
Grails Web Framework	4.0.10	5.2.5
Elastic Search	7.16.3	8.6.2
Java JDK	8u292	8u362
Tomcat Application Server	9.0.54	9.0.71
PostgreSQL Database	12.7	15.2

Clarity LIMS v6.1 Release Notes

These Release Notes describe the key changes made to software components for Clarity LIMS v6.1.

When upgrading from a version before v6.0, review the release notes for v6.0 for a list of features and bug fixes introduced in that version.

Clarity LIMS v6.1 is deployable in both cloud hosted and on-premise environments.

For API related information, refer to the changes in the current revision of the API Portal. If you have created scripts using our pre-release API endpoints, contact the Illumina Support team for a complete change list to make sure that your scripts continue to function.

New Features

- Advanced Search can now be used to search by one or more user-customized conditions based on Sample, Project, Container, Step, or File. There are also options for saving and importing queries and exporting search results.
- Read-Only permission—Can be assigned to users that need to view system information, but cannot create, edit, or delete information.

Defect Repairs

- Includes a security improvement that updates jQuery from 3.2.1 to 3.5.1.

Bug Fixes

- The following issues applicable to Clarity Core v6.0.0 and v6.0.1 were resolved:
  - The association between the audit event log and the audit change log is missing in Clarity LIMS.
  - Adding a control to associated samples shows up in other unrelated workflows that contain the same samples.
  - Config slicer log file does not show the actual +/- difference of the conflict.
  - Log files fill up with error messages for the Clarity LIMS instance with the remote PostgreSQL database setup.
  - Downloaded version of the sample sheet cannot be uploaded when the modify samples function is used.
  - [v6.0.1] Samples cannot be assigned or routed into QC protocols when using the OpenAPI endpoint (/route/artifacts).
  - [v6.0.0 and v6.0.1] The derived pool name is not being updated properly based on the naming convention configured in the pooling step.
  - [v6.0.0 and v6.0.1] Pooled samples replicate using the same label, which does not allow users to continue the demultiplexing step.
- Fixes the following bug for LabLink v2.2.0: The association between the audit event log and the audit change log is missing in LabLink.

- Fixes the following bug in Clarity Core v4.3: A user with HTTP/HTTPS/FTP file stores is unable to upload or download files.

Known Issues

- There are no known issues.

Additional Notes

- Clarity LIMS no longer performs a full nightly indexing in v6.1 by default. Instead, Clarity LIMS performs rolling updates, which indexes entities for a configurable window of time.
- With the introduction of Advanced Search, basic search no longer finds samples using containers and project custom fields.
- For questions or assistance, contact the Illumina Support team.

Clarity LIMS v6.0 Release Notes

These Release Notes describe the key changes made to software components for Clarity LIMS since version 5.4.

When upgrading from a version prior to v5.4, review the release notes for v5.4 for a list of features and bug fixes introduced in that version.

Clarity LIMS v6 is deployable in both cloud hosted and on-premise environments.

New Features

- Technology updates—An up-to-date technical stack ensures continued reliability, improved speed and capacity, and optimized system performance. For a complete list of updates, refer to the Appendix.
- Project level automation—Users can now write custom scripts and perform custom actions on submitted samples. These custom actions can be triggered manually from the Projects & Samples screen.
- Performance improvements—Improvements to the overall performance of Clarity LIMS v6 and to the existing API endpoints. A complete list of enhancements is provided in the Appendix.
- Support for on-premise customers—Clarity LIMS v6 supports on-premise deployment renewals at launch. Contact your local sales specialist for more information.
- ICA integration—Wet lab data can now be made available to data analysis pipelines via step level scripts.

Defect Repairs

- An Elasticsearch error is no longer generated when date-formatted text is entered in a non-date field type.
- Resolved an issue where controls were added to more workflows than samples processed in a step.
- An API call to the reagent lot endpoint no longer fails when the lot status is expired automatically by the Clarity LIMS system.

For Research Use Only. Not for use in diagnostic procedures.

- Resolved inconsistent behavior on archived controls and deleted instrument types in Manifest and XML configuration slice files.
- The root artifact name no longer reverts to default when updates to submitted sample details are submitted via automation.
- Executing the Processes API endpoint on projects with over 500 samples and with a project name filter no longer returns an incomplete set of data.
- A completed workflow stage is no longer missing from the Artifacts API endpoint if the previous step was not an output step.
- Queue screen page load performance has been optimized.
- Users no longer experience decreased performance associated with the Queue API making too many calls.
- Users no longer experience decreased performance when loading Previous Step queue grouping.
- Users no longer experience decreased performance when grouping types on Ice Bucket screen.
- Dropdown fields that do not allow custom entries and have first option set as default are no longer silently applied to various API endpoints and sample sheet upload.
- The changeWorkflow script no longer fails when processing 1152 derived samples.
- Naming syntax LIST option now permits a combination of letters and numbers.
- Master step configuration can now be updated when there is a comma in the naming convention.

Known Issues

- There are no known issues at this time.

Additional Notes

- Clarity LIMS v4.x is no longer supported by Illumina.
- Clarity LIMS v6 does not support Oracle database. Illumina will continue to support v5.2 for on-premise customers requiring Oracle.
- Clarity LIMS v6 does not support the Reporting module.
- Clarity LIMS v6 has been reviewed for log4j vulnerabilities. All potential vulnerabilities have been addressed.

For questions or assistance, contact the Illumina Support team.

Appendix

Technical Update Details

Component	Clarity LIMS v5.4.0	Clarity LIMS v6.0.0
Elasticsearch	6.2.4	7.16.3

Component	Clarity LIMS v5.4.0	Clarity LIMS v6.0.0
Java	Oracle JDK 8u202	AdoptOpenJDK 8u292
RabbitMQ Server	3.6	3.8.16
Tomcat Application Server	8.5.54	9.0.54
Grails Web Framework	2.4.5	4.0.10
PostgreSQL Database	12.4	12.7

Performance Details

- The overall performance of the Clarity LIMS system has been optimized on the following screens/actions:
  - Sample accessioning
  - Assigning samples to workflow
  - Removing samples from workflow
  - Queue screen page load
  - Ice Bucket screen load and loading of all grouping types
  - Adding labels to samples
  - Record Details screen
  - Next Steps screen
  - Search indexing
- List of API endpoints with enhanced performance is as follows.
  - POST /api/{version}/samples/batch/retrieve
  - POST /api/{version}/samples/batch/create
  - POST /api/{version}/route/artifacts
  - POST /api/{version}/artifacts/batch/update
  - POST /api/{version}/artifacts/batch/retrieve
  - PUT /api/{version}/steps/{limsid}/actions
  - GET /api/{version}/steps/{limsid}/actions
  - POST /api/{version}/steps
  - GET /api/{version}/steps/{limsid}/details
  - GET /api/{version}/queues/{protocolStepId}
  - POST /api/{version}/steps/{limsid}/advance

For Research Use Only. Not for use in diagnostic procedures.

Revision History

Document	Date	Description of Change
Document # 200016943 v06	April 2024	Updated release notes to add qualified operating systems. Updated OS references to Oracle Linux v8.8 and v8.9.
Document # 200016943 v05	October 2023	Updated OS references to Oracle Linux v8.8. Added *Clarity LIMS v6.2.1 Release Notes*. Added link to release notes to *What's New*. Updated *Advanced Search* with steps for giving Advanced Search access to Read-Only users. Updated *Search* to include information on Advanced Search.

For Research Use Only. Not for use in diagnostic procedures.

Document	Date	Description of Change
Document # 200016943 v04	August 2023	Updated *What's New* to include Clarity LIMS v6.2. Added the following new procedures for v6.2: • *Installation Procedure (Clarity LIMS v6.2)* • *Upgrade Procedure for On Premise to Cloud Deployments - From Versions 4.2 / 4.3 / 5.0 / 5.1 / 5.2 / 6.0 / 6.1 (PostgreSQL) and 4.3 / 5.2 (Oracle) to 6.2* • *Upgrade Procedure for On Premise to On Premise Deployments - From Versions 4.2 / 4.3 / 5.0 / 5.1 / 5.2 / 6.0 / 6.1 (PostgreSQL) and 4.3 / 5.2 (Oracle) to 6.2* • *Upgrade Procedure for Cloud to On Premise Deployments - From Versions 4.2 / 4.3 / 5.0 / 5.1 / 5.2 / 5.3 / 5.4 / 6.0 / 6.1 to 6.2* Added the following procedures to *Add and Manage Accounts*: • *Add a New Account* • *Modify Account Details* • *Delete an Account* Added the red dot configuration error feature to the *Configuration* section under *About LabLink*. Updated the following sections of *Technical Requirements* with new operating system requirements and database versions: • *Server Operating System Requirements* • *Database Requirements* • *Web Client Requirements* • *Automation Worker Requirements* Added *Automation Worker Node on Windows Server* section to *Automation Worker Nodes*. Added *Performance Test Setup* section to *Queue Performance and Usability*. Added *Clarity LIMS v6.2 Release Notes*.

For Research Use Only. Not for use in diagnostic procedures.

Document	Date	Description of Change
Document # 200016943 v03	April 2023	Updated *Clarity LIMS v6.1 Release Notes* with additional bug fixes and correct RPM versions for ClarityLIMS-App and BaseSpaceLIMS-AutomationWorker.
Document # 200016943 v02	April 2023	Added the following new procedures for Clarity LIMS v6.1: • *Upgrade Procedure for On Premise to Cloud Deployments - From Versions 4.2 / 4.3 / 5.0 / 5.1 / 5.2 / 6.0 (PostgreSQL) and 4.3 / 5.2 (Oracle) to 6.1* • *Upgrade Procedure for On Premise to On Premise Deployments - From Versions 4.2 / 5.0 / 5.1 (PostgreSQL) and 4.3 / 5.2 (Oracle) to 6.1* • *Upgrade Procedure for On Premise to On Premise Deployments - From Versions 4.3/5.2/6.0 to 6.1* • *Upgrade Procedure for Cloud to On Premise Deployments - From Versions 4.2 / 4.3 / 5.0 / 5.1 / 5.2 / 5.3 / 5.4 / 6.0 to 6.1* • *Advanced Search (Clarity LIMS v6.1)* Updated *What's New* to include v6.1. Updated *Configuring Role-Based Permissions* to include information on the read-only permission. Added *Clarity LIMS v6.1 Release Notes*.
Document # 200016943 v01	July 2022	Updated installation and upgrade procedures to include `activity-management-ui-config.groovy` file updates for remote or standalone servers.
Document # 200016943 v00	March 2022	Initial release to support Clarity LIMS v6.

For Research Use Only. Not for use in diagnostic procedures.