PacBio

SMRT® Link software installation guide (v13.1)

P/N 103-349-500 Version 01 (April 2024)

PacBio
1305 O’Brien Drive
Menlo Park, CA 94025
www.pacb.com

SMRT® Link software installation guide (v13.1)

Introduction

This document describes the procedure for installing **SMRT Link v13.1** or **SMRT Link Lite v13.1**. This document is for Customer IT or SMRT Link administrators.

- **SMRT Link v13.1** supports Revio™ systems, Sequel® II systems and Sequel IIe systems. Sequel systems are **not** supported.
- **SMRT Link Lite v13.1** supports Revio systems and Sequel IIe systems **only**. Sequel and Sequel II systems are **not** supported.

SMRT Link is the web-based end-to-end workflow manager for PacBio long-read systems. It includes software applications for designing and monitoring sequencing runs, and analyzing and managing sequence data.

SMRT Link is the primary access point for applications used by researchers, laboratory technicians, instrument operators, and bioinformaticians. The applications include:

- **Instruments:** View information about systems connected to SMRT Link.
- **Sample Setup**: Calculate binding and annealing reactions for preparing DNA libraries for use on **all** supported systems.
- **Runs**: View information about sequencing runs, monitor run progress, status and quality metrics, design sequencing runs and create and/or import run designs.
- **Data Management**: Create Projects and Data Sets; manage access permissions for Projects and users; generate QC reports for Data Sets; view, import, export, or delete sequence, reference, barcode and BED files.
- **SMRT® Analysis**: Perform secondary analysis on the basecalled data (such as sequence alignment, variant detection, structural variant calling, and RNA analysis) after a run has completed.
  Note: The SMRT Analysis module is **not** included when you install **SMRT Link Lite**.

Note: SMRT Link, SMRT Link Lite, the Revio system, Sequel II systems and Sequel IIe systems are for **research use only** (RUO).

Overview

1. Install or upgrade the SMRT Link software. (See “Installation summary” on page 7 and “Upgrading SMRT Link” on page 10 for details.)
2. (**Optional**) Configure SMRT Link or SMRT Link Lite to use an SSL certificate. (See “Installing an SSL certificate for NGINX” on page 21 for details.)
3. (**Optional**) Add SMRT Link Users and Assign User Roles. (See “Adding SMRT Link users via LDAP integration and assigning user roles” on page 18 for details.)
4. (**Optional**) Change the admin and pbicsuser passwords. (See “Changing admin and pbicsuser passwords” on page 13 for details.)
5. (**Optional**) Configure LDAP. (See “LDAP integration” on page 14 for details.)

Compute requirements for Revio systems and Sequel IIe systems

Network connection		
Connection	**1 GbE or 10 GbE copper**	
Shared data storage		
	Per Revio system	**Per Sequel IIe system**
Sequencing data[a]	**72 TB/year**	**20 TB/year**
SMRT Link server		
	SMRT Link	**SMRT Link Lite**
CPU cores	**16**	**4**
RAM	**64 GB**	**16 GB**
Local storage	**1 TB SSD**	**500 GB SSD**
HPC node (SMRT Link only)		
CPU cores	**64**	
RAM	**4 GB per core, 256 GB total**	
Local storage	**100 GB SSD or HDD (500 GB preferred as future workflows may use more local disk space.)**	
Recommended HPC nodes by application[b] (SMRT Link only)		
	Per Revio system	**Per Sequel IIe system**
Human genome	**2 nodes**	**1 node**
Single-cell transcriptome	**2 nodes**	**1 node**
Large gene panels	**1 node**	**1 node**

a. Per Revio system. Assumes standard `hifi_reads.bam` file **without** kinetics. Does **not** include data files produced in data analysis, which approximately doubles the storage requirement.
b. Per Revio system at utilization of 1,300 SMRT Cells per year. Compute is proportional to the number of SMRT Cells run. For example, half the number of nodes is needed at 650 SMRT Cells per year compared to 1,300 SMRT Cells per year. The number of nodes assumes that analysis is performed as data is generated throughout a year.

Note: Single-system compute configurations are available – contact your PacBio Bioinformatics Field Application Specialist (FAS) for details.

Data storage

- The SMRT Link software's installation **root** directory **must** be readable and writable by the SMRT Link install user (`$SMRT_USER`) and **must** be addressable along the same installation path (`$SMRT_ROOT`) on **all** relevant cluster nodes via NFS. PacBio recommends `/opt/pacbio/smrtlink` for the SMRT Link software's installation root directory (referred to as `$SMRT_ROOT`), and `smrtanalysis` for the SMRT Link install user (referred to as `$SMRT_USER`).

- The SMRT Analysis job **output** directory is used to store output from SMRT Analysis jobs. The software accesses this directory through a symbolic link (`$SMRT_ROOT/userdata/jobs_root`) that points to the desired job output directory location. The link can be modified by using the installation script. The symbolic link destination should be on a shared file system (NFS); it **must** be writable by the `$SMRT_USER`, and it **must** be addressable along the same path on **all** compute nodes. The default is to keep these output directories on the **same** NFS export as the SMRT Link installation, but optionally may be symbolically linked to a larger storage volume.
- The SMRT Analysis **database** directory is used to store database files and backups. The software accesses this directory through a symbolic link (`$SMRT_ROOT/userdata/db_datadir`) that points to the desired database directory location. The link can be modified by using the installation script. This symbolic link destination should be a **local** directory (**not** NFS) and be writable by `$SMRT_USER`. This directory should exist **only** on the SMRT Link install host.
- The SMRT Analysis **temporary** directory is used for fast I/O operations during run time. The software accesses this directory through a symbolic link (`$SMRT_ROOT/userdata/tmp_dir`) that points to the desired temporary directory location. The link can be modified manually or using the installation script. This symbolic link destination should be a **local** directory (**not** NFS), it must be writable by `$SMRT_USER`, and the link destination must exist (or be creatable) as an independent directory on **both** the head node and the compute nodes.

Software prerequisites: Server operating systems and pre-installed software

- SMRT Link server software is supported on English-language distributions of:
  - Rocky Linux 8.x and 9.x.
  - Ubuntu 20.04 Linux® (until end-of-life on 4/1/2025).
  - Ubuntu 22.04 Linux®.
  - These supported versions **also** apply to SMRT Link compute nodes.
- SMRT Link is **not** guaranteed to work on Linux versions that are no longer supported by the operating systems' vendors.
- SMRT Link server software **cannot** be installed on systems running other versions of UNIX, macOS® or Windows®.
- Singularity v3.10.5 or later is **required** for the **Variant Calling** and **HiFi Target Enrichment** analysis workflows.
  - We recommend installing Singularity as `root`, with the `setuid` bit enabled (`chmod u+s singularity`) in the `/bin` or `/usr/bin` directory.
  - If you run jobs with a scheduler (such as SLURM), we recommend installing the `singularity-ce` package on the SMRT Link server, as well as each of the nodes within the relevant partition that you are submitting jobs to.
  - Singularity should **not** be installed in an NFS area of the file system.
  - The singularity binary **cannot** be installed to any file system area mounted with the `nosuid` and/or `noexec` mount options.
  - To run **Variant Calling** or **HiFi Target Enrichment**, Singularity will need to download several Docker images (`docker://google/deepvariant:1.5.0`; `docker://google/deepvariant:1.5.0-gpu`; `docker://quay.io/biocontainers/whatshap:1.4--py39hc16433a_1`; `docker://ghcr.io/dnanexus-rnd/glnexus:v1.4.1` and `docker://broadinstitute/picard:2.27.5`). To save these images locally, we provide a script, `$SMRT_ROOT/admin/bin/fetch-singularity-cache`, which uses the `root` account to download the images, using `/tmp` as a temporary file space, before depositing the `.sif` files into `$SMRT_ROOT/userdata/singularity` and changing ownership to the requesting user. We recommend running this script **after** installing SMRT Link.
  - For further details on configuring Cromwell for Singularity, see here.

Software/hardware prerequisites: Client systems

To use SMRT Link on a client operating system:

- SMRT Link **requires** an up-to-date version of the Google® Chrome web browser.
- SMRT Link **requires** a minimum screen resolution of 1600 by 900 pixels.

Network configuration

- Refer to the **Site prep guide** provided with your instrument purchase for more details.
- For network connectivity considerations, see the network diagram in the **Network requirements** section of the **Site prep guide**.

SMRT Link server environment assumptions

- The SMRT Link server should run on a dedicated 64-bit Linux host with `libc 2.17` or greater.
- The installation is performed by the **same** non-root user (`$SMRT_USER`) that will be used to run the SMRT Link web services.
- The `$SMRT_USER` has full permissions recursively throughout the install directory, and in all linked directories for `jobs_root`, `db_datadir` and `tmp_dir`. (Common problems include NFS setup problems, ACLs, and so on.)
- When running in distributed mode, all other nodes have the **same path** for `$SMRT_ROOT` and for all linked directories. (The NFS exports should have identical mount points on **all** cluster nodes.)
- No other daemons/services processes are bound to the same ports as the SMRT Link services.
- PacBio **highly recommends** that the system clock be synchronized to a domain or public NTP time server.
- The `$SMRT_USER` service account **must** have both the `nofile` and `nproc` soft user limits set to a minimum of 8192. (See the `ulimit(1)` and `limits.conf(5)` Linux man pages for more information.)
- The host operating system **must** provide the `en_US.UTF-8` locale/character set.
- **SMRT Link** and **SMRT Link Lite** are **not** designed to handle changes in the hostname. If you are using them to connect to a Revio instrument you should ensure that the configured hostname is and will remain accessible across the network.

SMRT Link database note

- SMRT Link v13.1 no longer includes weekly automatic database backups. A database backup is still automatically performed once, during installation or upgrade. Failure to back up the SMRT Link database on a regular schedule risks losing all records in SMRT Link (including users, Data Sets, analyses, barcodes, and references) if a file system or reconfiguration error occurs. The underlying sequencing or analysis files, such as BAM files, are **not** affected.
- We **strongly** recommend asking your local Linux system administrator to schedule regular weekly backups of the SMRT Link database using standard Linux utilities. A utility script to generate an appropriate `cron` server command was added at `$SMRT_ROOT/admin/bin/generate-cron-backup`. For additional details, please contact PacBio Technical Support.

General security notes

- PacBio **recommends** that you install the SMRT Link server on networks that are only accessible to **trusted** users, and discourages installing SMRT Link on public networks.
- Do **not** install SMRT Link or run SMRT Link services as the `root` user.

SMRT Link v13.1 security notes

SMRT Link v13.1 restricts access to the web services API to clients running on `localhost` (such as the API gateway that handles authentication and permissions) or remotely using SSL encryption and password-based authentication.

Support for the WSO2 API Manager was **deprecated** in v12.0, and this API is **no longer** supported. New installations will **automatically** start the replacement API gateway. **Customers who are upgrading existing SMRT Link installations will need to migrate to the new API gateway**.

Ports and firewalls: SMRT Link end users **must** be able to access the SMRT Link server on port `8243`. This port is also used by the Instrument Control Software (ICS), so it must be accessible to **any** Revio systems, Sequel II systems or Sequel IIe systems as well.

- If your network configuration already allows access to port `8243`, **no additional changes** are required to use SMRT Link v13.1 or SMRT Link Lite v13.1.
- The instrument must have access to TCP port `8243` of the SMRT Link server.
- End users must also have access to TCP port `8243` of the SMRT Link server for access to the browser UI.
- Communication between Revio instruments and SMRT Link is bidirectional, so SMRT Link **must** have access to TCP port `9243` on any associated Revio instruments.

Keycloak Admin interface

In SMRT Link v13.1, the Keycloak Admin interface on port `https:9443` is **no longer enabled by default** due to security concerns. Instructions for starting SMRT Link with the Keycloak Admin interface exposed are included in the **Installation summary - SMRT Link v13.1/SMRT Link Lite v13.1** table.

SMRT Link Lite v13.1

SMRT Link Lite v13.1 is a modified configuration that uses the **same** installer and software as SMRT Link v13.1, but with the most compute-intensive components (SMRT Analysis) disabled to support running on non-server hardware. Without these components, SMRT Link Lite can comfortably run on laptops with at least 16 GB RAM available, and supports configuring and displaying run results for a **single** Revio instrument.

Installation/upgrade checklist

Following is a list of items you should have ready **before** starting a new installation or upgrading an existing installation. **Note**: Paths that include spaces are **not** supported.

- Full path to the `$SMRT_ROOT` directory.
- A service account (called the `$SMRT_USER` in this document) to install and run the web services.
- Full path to the installation root directory, used for the main installation root.
- Job Management System settings.
- Full path to a directory on the shared file system - the `jobs_root` directory.
- Full path to a directory on the local file system on each node - the `tmp_dir` directory.
- Full path to a directory on the local file system on the install node - the `db_datadir` directory.
- **(Optional)** LDAP settings. See “Configuring LDAP in Keycloak” on page 15 for details.
- **(Optional)** SSL certificate for NGINX. See “SMRT Link and SSL certificate procedures” on page 21 for details.

Installation summary

Following are the steps for installing SMRT Link v13.1 or SMRT Link Lite v13.1 on a **new** system. (See “Appendix A: SMRT Link workflow terminology” on page 24 for details.)

- To upgrade SMRT Link to v13.1 from a **previous version**, see “Upgrading SMRT Link” on page 10.

SMRT Link v13.1 and SMRT Link Lite v13.1 can be used with the following supported version of ICS:

- v13.1 for Revio systems. **Note**: SMRT Link Lite v13.1 works **only** with ICS v13.0 or later.
- v11.0.1+ for Sequel II systems and Sequel IIe systems.

SMRT Link installation options

The following table lists the types of SMRT Link installations and what they include:

Installation type	GUI	Command-line tools	JMS integration	Sample data	Barcode and reference files	SMRT Link services	Cromwell	Cromwell with call caching
Full SMRT Link	Y	Y	Y	Y	Y	Y	Y	Y
SMRT® Tools only	N	Y	Y[a]	N	N	N	Y	N
SMRT Link Lite	Y	Y	N	Y	Barcode **only**	Y	N	N

a. JMS integration on a SMRT Tools-only installation may be setup using `pbcromwell`. See **SMRT Tools reference guide (v13.1)** for more information.

Step	Installation summary - SMRT Link v13.1/SMRT Link Lite v13.1
1	**Download SMRT Link software:** Download and extract the SMRT Link software installer from here. (The same installer can install **both** SMRT Link and SMRT Link Lite.)
2	**Definitions and variables:** For clarity, this document uses these conventions to refer to site-specific information: • `$SMRT_ROOT`: The SMRT Link Install Root Directory, such as `/opt/pacbio/smrtlink`. • `$SMRT_USER`: The SMRT Link Install User, such as `smrtanalysis`. • `smrtlinkhost.mydomain.com`: The fully-qualified domain name of the SMRT Link Install Host. • `smrtlinkhost`: The short host name of the SMRT Link Install Host. For `$SMRT_ROOT`, defining the variable in the shell allows the commands below to be run verbatim. To do so, use something like: `SMRT_ROOT=/opt/pacbio/smrtlink` The fully-qualified domain name of the SMRT Link Install Host may always be used in place of the short host name. But in some cases, particularly when working with WSO2, the fully-qualified domain name is required.
3	Log onto the SMRT Link Install Host (such as the hostname or IP address) as the SMRT Link Install User (such as `$SMRT_USER`.)

4	**Install SMRT Link by invoking the SMRT Link Installer:**
	`./smrtlink_<version number>.run --rootdir $SMRT_ROOT`
	Note: The `$SMRT_ROOT` directory must **not** exist when the installer is invoked, as the installer will try to create it, and will abort the installation if an existing `$SMRT_ROOT` location is found.
	If a previous installation was canceled or otherwise failed, the installer can be invoked **without** extraction. Rerun using the `--no-extract` option:
	`./smrtlink_<version number>.run --rootdir $SMRT_ROOT --no-extract`
	Alternatively, install **SMRT Link Lite** by using the following command instead:
	`./smrtlink_<version number>.run --lite true --jmstype NONE --rootdir $SMRT_ROOT --nworkers 4`
	See “Appendix A: SMRT Link workflow terminology” on page 24 for additional information.

5	On the instrument, click **Install** when prompted to install the Chemistry Update.

6	**Start SMRT Link services:**
	`$SMRT_ROOT/admin/bin/services-start`
	If you need the Keycloak Admin interface enabled on external port `9443`, use this command:
	`$SMRT_ROOT/admin/bin/services-start --enable-keycloak-console`

Step	Installation summary - SMRT Link v13.1/SMRT Link Lite v13.1
7	**(SMRT Link only) Run the Site Acceptance Test from the command line:** `$SMRT_ROOT/admin/bin/run-sat-services` Successful completion of `run-sat-services` indicates that the HPC configuration is functioning correctly. This creates a "PacBio Example SAT Job" analysis entry in the SMRT Analysis section of the SMRT Link GUI.
8	**(Optional) Clear the browser cache:** This is a good troubleshooting step if needed. 1. Open the Chrome Browser and choose **More Tools > Clear browsing data**, choose **All Time** from the **Time Range** control, then check **Cached images and files**. Click **Clear data**. 2. Restart the browser.
9	**(Optional) Configure LDAP and/or add local users:** See "Configuring LDAP in Keycloak" on page 15, "Adding local users to SMRT Link using Keycloak" on page 18 for details.
10	**(Optional) Configure SMRT Link/SMRT Link Lite to use a signed SSL certificate:** See "Installing an SSL certificate for NGINX" on page 21 for details.
11	**(Optional) Change the admin and pbicsuser passwords:** We recommend that you change the `admin` and `pbicsuser` account passwords from the default values. See "Changing admin and pbicsuser passwords" on page 13 for details.

Upgrading SMRT Link

Supported upgrade path

- SMRT Link upgrades to v13.1 are supported from any v8.x, v9.x, v10.x, v11.x or v12.x releases.
- **SMRT Link Lite** upgrades to v13.1 from v13.0 are supported. (**Note**: You can upgrade from SMRT Link v12.0 to SMRT Link Lite v13.1 - see Step 5 in the **Upgrading SMRT Link/SMRT Link Lite** table.)
- SMRT Link v13.1/SMRT Link Lite v13.1 can be used with the following supported version of ICS:
  - v13.1 for Revio systems
  - v11.0.1+ for Sequel II systems and Sequel IIe systems

Step	Upgrading SMRT Link/SMRT Link Lite
1	Download and extract the SMRT Link software installer from here. (The same installer can install **both** SMRT Link and SMRT Link Lite.)
2	**Definitions and variables:** For clarity, this document uses these conventions to refer to site-specific information: • `$SMRT_ROOT`: The SMRT Link Install Root Directory, such as `/opt/pacbio/smrtlink`. • `$SMRT_USER`: The SMRT Link Install User, such as `smrtanalysis`. • `smrtlinkhost.mydomain.com`: The fully-qualified domain name of the SMRT Link Install Host. • `smrtlinkhost`: The short host name of the SMRT Link Install Host. For `$SMRT_ROOT`, defining the variable in the shell allows the commands below to be run verbatim. To do so, use something like: `SMRT_ROOT=/opt/pacbio/smrtlink` The fully-qualified domain name of the SMRT Link Install Host may always be used in place of the short host name. But in some cases, particularly when working with WSO2, the fully-qualified domain name is required.
3	Log onto the SMRT Link Install Host (such as the hostname or IP address) as the SMRT Link Install User (such as `$SMRT_USER`.)
4	**Stop the SMRT Link services:** `$SMRT_ROOT/admin/bin/services-stop` **Note**: Ensure that no active SMRT Link analysis jobs are running before stopping services.

5	**Upgrade SMRT Link by invoking the SMRT Link installer:**
	`./smrtlink_<version number>.run --rootdir $SMRT_ROOT --upgrade`
	Note: The `$SMRT_ROOT` directory must be an existing SMRT Link installation. Several validation steps will occur to ensure that a valid `$SMRT_ROOT` is being updated.
	If a previous upgrade was canceled or otherwise failed, the installer can be invoked **without** extraction. Rerun using the `--no-extract` option:
	`./smrtlink_<version number>.run --rootdir $SMRT_ROOT --upgrade --no-extract`
	
	Alternatively, upgrade **SMRT Link Lite** by using the following command instead:
	`./smrtlink/admin/bin/smrtupdater --batch tarball.run`
	
	To upgrade SMRT Link v12.0 to SMRT Link Lite v13.1, use the following commands:
	`./smrtlink_<version number>.run --rootdir $SMRT_ROOT --upgrade`
	`$SMRT_ROOT/admin/bin/smrt_reconfig --batch --lite true`
	
	See “Appendix A: SMRT Link workflow terminology” on page 24 for additional information.

6	On the instrument, click **Install** when prompted to install the Chemistry Update.

Step	Upgrading SMRT Link/SMRT Link Lite

7	**Start the SMRT Link services:**
	`$SMRT_ROOT/admin/bin/services-start`
	If you are upgrading from an installation that used WSO2 API Manager, you **must** migrate to the new API gateway in order to connect to Revio systems:
	`$SMRT_ROOT/admin/bin/services-start --migrate`
	The migration launches an interactive CLI tool after the server starts; as this is a new installation very few steps are required. Once migration is finished, SMRT Link automatically starts with the new API gateway in the future.

8	**Run the Site Acceptance Test from the command line:** `$SMRT_ROOT/admin/bin/run-sat-services` Successful completion of `run-sat-services` indicates that the HPC configuration is functioning correctly. This creates a "PacBio Example SAT Job" analysis entry in the SMRT Analysis section of the SMRT Link GUI.
9	**(Optional) Clear the browser cache:** This is a good troubleshooting step if needed. 1. Open the Chrome Browser and choose **More Tools > Clear browsing data**, choose **All Time** from the **Time Range** control, then check **Cached images and files**. Click **Clear data**. 2. Restart the browser.
10	**(Optional) Change the admin and instrument user passwords:** We recommend that you change the `admin` and `pbicsuser` account passwords from the default values. See "Changing admin and pbicsuser passwords" on page 13 for details.

Updating the SMRT Link Chemistry and UI Bundles

SMRT Link Bundle updates allow updating of SMRT Link features **without** having to reinstall the SMRT Link software. As of SMRT Link v13.1, there are two Bundle types for which an update indicator may appear:

SMRT Link Chemistry Bundle

- This includes kit and DNA Control Complex names used in the Sample Setup and Runs modules. The update also updates Instrument Control Software (ICS).

SMRT Link UI Bundle

- This includes changes and fixes to the SMRT Link graphical user interface (GUI).

Updating the SMRT Link Bundles from SMRT Link

Note: Only SMRT Link users with the **Admin** role can perform these updates. In addition, SMRT Link **must** have a route to the internet and update services **must** be enabled.

1. In SMRT Link, choose **Settings > Updates**. (A red circle indicates that one or more Bundle Update(s) are available.)
2. Click the **Update Chemistry Bundle** button.
3. Click the **Update UI Bundle and Restart UI Server** button, if applicable.
4. If there are any problems, clear the browser cache: Choose **More Tools > Clear browsing data**, choose **All Time** from the **Time Range** control, then check **Cached images and files**. Click **Clear data.** Refreshing the browser tab or clearing the browser cache may be necessary for the Bundle update(s) to take effect.

Updating the SMRT Link Chemistry Bundle on the instrument

The SMRT Link Chemistry Bundle will also need to be upgraded with the same Chemistry Bundle files used by the SMRT Link web services. Once SMRT Link's Chemistry Bundle is updated, the updates are passed along to

any PacBio instruments configured to use that same instance of SMRT Link. Once available, follow the instructions below to update the Chemistry Bundle on the instrument side.

1. On the instrument, choose **Admin** from the Main menu. (A red circle indicates that a Chemistry Bundle Update is available.)
2. Click the **Updates** tab, then click **Install**. The instrument software then restarts, which will take around 10 minutes.
3. Click the **question mark** to check the version number to validate the Chemistry Bundle update.

Rolling back a SMRT Link UI Bundle update

SMRT Link UI Bundle updates allow updating of SMRT Link UI features **without** having to reinstall the SMRT Link software. This includes changes and bug fixes to the SMRT Link graphical user interface. When you upgrade the SMRT Link UI by clicking **Setting > Updates > Update UI Bundle and Restart UI Server**, the previous version of the UI is saved to a time-stamped folder. For example:

```
$ ls -l $SMRT_ROOT/current//bundles/smrtlink-analysisservices-gui/current/private/pacbio/smrtlink-
analysisservices-gui/tomcat_current/webapps/ROOT/
-rw------- 1 fas Domain Users   158 Jan 22 12:11 index.jsp
-rw-r--r-- 1 fas Domain Users 36780 Oct  4 15:16 pacbio-manifest.json
-rw-r--r-- 1 fas Domain Users 10357 Oct  4 15:16 pacbio-manifest.txt
drwx------ 7 fas Domain Users  4096 Oct 10 08:30 sl
drwx------ 7 fas Domain Users  4096 Oct 10 08:30 sl_20200103_135348
lrwxrwxrwx 1 fas Domain Users    20 Oct  4 15:16 version.json -> pacbio-manifest.json
lrwxrwxrwx 1 fas Domain Users    19 Oct  4 15:16 version.txt -> pacbio-manifest.txt
```

In this example, `sl` is the `tomcat_current/webapps/ROOT` root directory installed by the bundle update, and `sl_20200103_135348` is the backup of the original UI code.

To **downgrade** to the previous UI version, follow these steps:

1. Stop the server: `$SMRT_ROOT/admin/bin/services-stop.`
2. Rename the `sl` directory to any unique, recognizable name.
3. Rename the backup directory to `sl`.
4. Start the server: `$SMRT_ROOT/admin/bin/services-start.`

Skipping a SMRT Link UI Bundle update

To skip a specific SMRT Link UI Bundle update, use the `pbservice skip-update` command:

```
$ pbservice skip-update smrtlink-ui --user admin --password admin --host smrtlink-uri –port 8243
Marked bundle update smrtlink-ui/9.0.0.99999 as ignored.  Note that you will need to re-login to the
SMRT Link UI for this to take effect.

$ pbservice skip-update smrtlink-ui --user admin --password admin --host smrtlink-uri –port 8243
No upgrades found for bundle smrtlink-ui
```

To **undo** skipping the bundle, run an identical command using `unskip-update`. Note that the UI will still show the pending update unless you log out and log in again (the bundle's update status is cached upon initial login.)

Installing only SMRT Tools

To install **only** command-line SMRT Tools, use the `--smrttools-only` switch when calling the installer, whether for a new installation or an upgrade. (This installs the **same** command-line tools as a full installation.) Examples:

```
./smrtlink-13.1.0.xxxxx.run --rootdir smrtlink --smrttools-only
./smrtlink-13.1.0.xxxxx.run --rootdir smrtlink --smrttools-only --upgrade
```

Note: Using `--smrttools-only` will **only** unpack the command-line applications, and will **not** run through the configuration prompts or provide the web services of a full SMRT Link installation. If command-line only use with JMS integration is desired, see the **SMRT Tools reference guide (v13.1)** on how to setup JMS integration using `pbcromwell`.

Warning: Revio systems, Sequel II systems and Sequel IIe systems **cannot** communicate with a `--smrttools-only` installation.

Updating the SMRT Link Chemistry Bundle on smrttools-only installations

Use this procedure **only** if you have installed the SMRT Link package using the `--smrttools-only` switch.

Download the Chemistry Bundle from the PacBio website, then unpack the files and place them in a user-defined directory. The value of the `$SMRT_CHEMISTRY_BUNDLE_DIR` environment variable then defines where the software finds the updated files. Following are the suggested best practices for installing the Chemistry Bundle:

1. Download the Chemistry Bundle from the PacBio web site's **Software Downloads** page.
2. (**Optional**) Define `$SMRT_ROOT` for convenience:
   `SMRT_ROOT=/opt/pacbio/smrtlink`
3. Make directories, unpack, and link:

```
mkdir -p $SMRT_ROOT/userdata/chemistry/chemistry-pb-13.1.0.xxxxx
tar -C $ SMRT_ROOT/userdata/chemistry/chemistry-pb-13.1.0.xxxxx -xf /path/to/chemistry-pb-
13.1.0.xxxxx.tar.gz
ln -s ./chemistry-pb-13.1.0.xxxxx $SMRT_ROOT/userdata/chemistry/chemistry-pb-active
```

4. Define and export the `$SMRT_CHEMISTRY_BUNDLE_DIR` environmental variable and validate:

```
export SMRT_CHEMISTRY_BUNDLE_DIR=$SMRT_ROOT/userdata/chemistry/chemistry-pb-active
```

5. Define the `$SMRT_CHEMISTRY_BUNDLE_DIR` environment variable in the appropriate startup script for your shell to make it permanent. **Example**: Use `~/.bashrc`.

Changing admin and pbicsuser passwords

The SMRT Link `admin` account has full access to SMRT Link, and is used to create users and grant users access.

SMRT Link comes with a default Instrument Control Software (ICS) user account (`pbicsuser`) which is used by the Revio system, Sequel II system, and Sequel IIe system to communicate with SMRT Link web services over a secure, encrypted connection. The `pbicsuser` account is **required** for instruments to communicate with SMRT Link. (Note that the `pbicsuser` credentials can **only** be used to access SMRT Link resources – it is **not** an LDAP account or a local account on the Linux system.)

The passwords for the `admin` and `pbicsuser` accounts are set to default values that are the same for **all** SMRT Link installations. Because the passwords can be used to access SMRT Link accounts and information, the passwords should be changed and only given to **trusted** users who require access.

To change the built-in account passwords for the new API gateway, use the following procedure while the server is running:

```
$SMRT_ROOT/admin/bin/set-keycloak-creds --user admin --password 'NEW-PASSWORD' --admin-password
'CURRENT-PASSWORD'
$SMRT_ROOT/admin/bin/set-keycloak-creds --user pbicsuser --password 'NEW-PASSWORD'
```

To verify the `admin` and `pbicsuser` passwords, use the following procedure:

```
$SMRT_ROOT/smrtcmds/bin/pbservice status --host localhost --user admin --ask-pass
$SMRT_ROOT/smrtcmds/bin/pbservice status --host localhost --user pbicsuser --ask-pass
```

The `pbservice` status information should display, before exiting with an exit status of `0` indicating success.

Sequel II/Sequel IIe users must **also** change the `pbicsuser` account password in the Instrument Control Software (ICS) to match the new password. To do so: Select **Menu > Admin > SMRT Link** on the instrument touch screen to change the password.

Note: You can also use the Keycloak Admin interface on HTTPS port 9443 to change these passwords. (Unlike in previous versions of SMRT Link, changing the `admin` account password or even the user name with the user management interface now works correctly.)

Changing usage tracking settings

When first logging in to the SMRT Link GUI after a successful installation or upgrade, users are prompted to notify PacBio of the upgrade/installation success and whether they wish to share SMRT Link analysis usage information with PacBio. Once set, these settings may **only** be viewed and modified from the command line using the `accept-user-agreement` tool.

WARNING: To use the `accept-user-agreement` tool, services must be running:

```
$SMRT_ROOT/admin/bin/services-start
```

To set new settings, use the following command, specifying `true` or `false` for the options accordingly. For example:

```
$SMRT_ROOT/admin/bin/accept-user-agreement --install-metrics true --job-metrics true
```

PacBio is notified of a successful installation or upgrade **immediately** if the install metrics setting is `true`.

To view the current settings, run the command without any arguments:

```
$SMRT_ROOT/admin/bin/accept-user-agreement
```

Note: If `accept-user-agreement` is run **without** arguments and the settings have not been previously set (either in the GUI or on the command line), **both** the install and job metrics settings will automatically be set to `true` and PacBio will be immediately notified of the installation or upgrade.

Starting SMRT Link automatically on server boot

To start SMRT Link automatically when the server boots using `systemd`, refer to the template service file located here:

```
$SMRT_ROOT/admin/template/smrtlink.service.tmpl
```

Follow the instructions in the template comments to make site-specific modifications and install as a `systemd` service unit.

LDAP integration

SMRT Link supports integration with LDAP for user login authentication, as well as using local Keycloak users that exist **only** within SMRT Link.

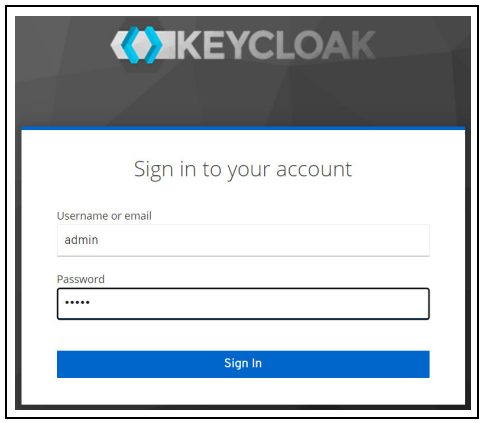
If you are interested in configuring SMRT Link integration with your organization's LDAP, PacBio recommends that you consult your LDAP administrator to help determine the correct LDAP settings.

Note: Existing LDAP configurations are **automatically** migrated during upgrade.

Configuring LDAP in Keycloak

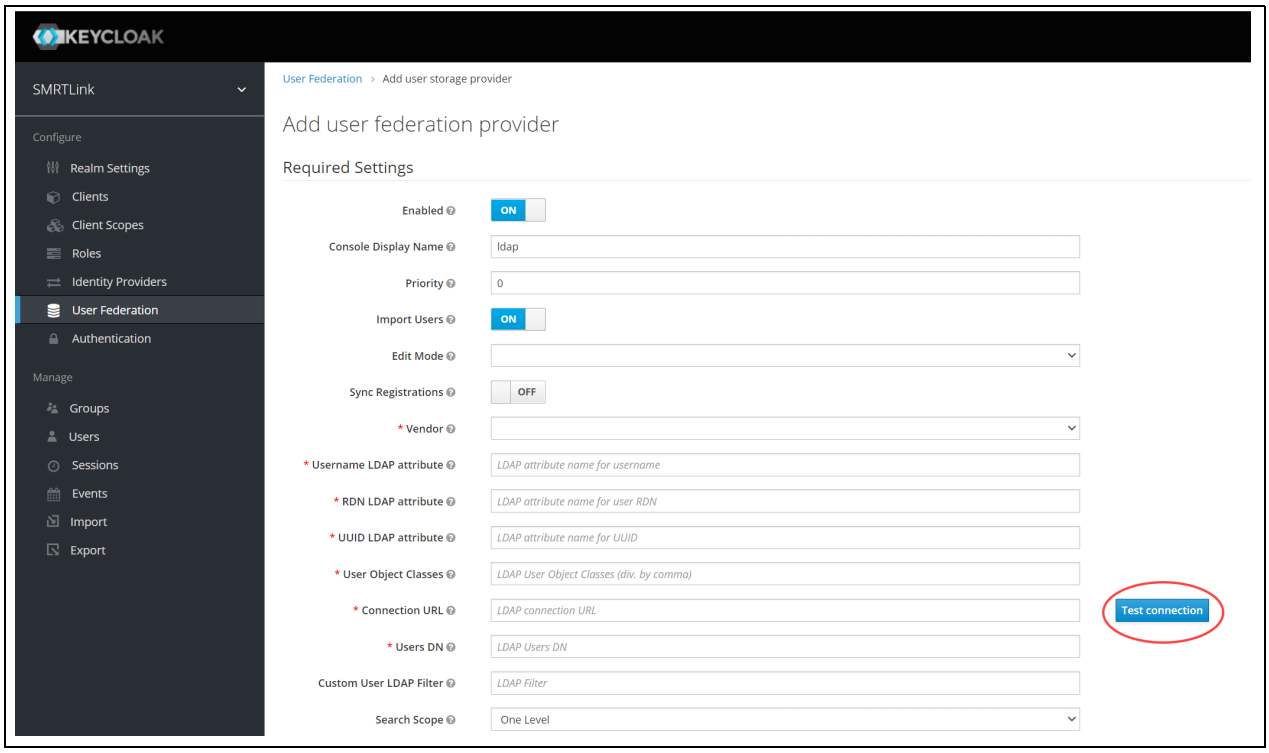
- LDAP is configured **after** SMRT Link v13.1 is installed, using the **Keycloak** authentication server software, as shown below.
- SMRT Link must **first** synchronize with your organization's LDAP objects before any directory accounts can be enabled and given a role to facilitate SMRT Link access.

1. Enter the following in your browser: `https://<hostname>:9443/auth/admin/` where `<hostname>` is the host where SMRT Link is installed.
2. Login using `admin/admin` (unless you have changed the password).



3. Under **Configure** on the left hand side of the window, click **User Federation**.

4. On the right hand side of the window, click **Add provider…** and select the **ldap** option.
5. Enter the required fields (and any others necessary for your LDAP server) and verify that you can connect to the server using the **Test connection** and **Test authentication** buttons.



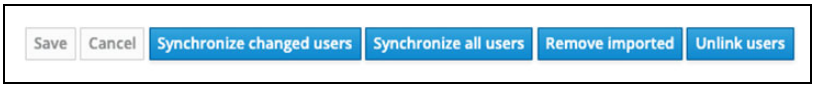
The following fields are **required**. (**Note**: Values provided in the example above are listed below for clarity. Actual values should be provided by your LDAP administrator):

- Username LDAP attribute: `uid` (if you are using Active Directory, the most likely value is `sAMAccountName`)
- RDN LDAP attribute: `uid` (usually the same as the Username LDAP Attribute)
- UUID LDAP attribute: `entryUUID`
- User Object Classes: `person, organizationalPerson, user`
- Connection URL: `ldap://ldap.university:389`
- Users DN: `CN=users,DC=university,DC=edu`
- (**Optional**) Custom User LDAP Filter: `(objectClass=person)`

If `Bind Type` is `simple`, you **also** need to enter credentials for accessing the directory:

- Bind DN: `CN=ldapadmin,CN=users,DC=university,DC=edu` (This is the user account that is used to authenticate to the LDAP environment.)
- Bind Credential: <`password`>

6. When you are finished click **Save**.
7. After you save the LDAP configuration, additional buttons display at the bottom of the window. Clicking **Synchronize all users** imports **all** users to the Keycloak database **without** assigning them SMRT Link roles.



8. Enable SMRT Link users individually as described in the next section.

For more information on LDAP, consult the following web pages:

https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
https://en.wikipedia.org/wiki/LDAP_Data_Interchange_Format
https://msdn.microsoft.com/en-us/library/ms677605%28v=vs.85%29.aspx

Problems with the LDAP server may be debugged by looking at the log file located here:

```
$SMRT_ROOT/userdata/log/smrtlink-analysisservices-gui/keycloak.stdout
```

Note: If LDAPS needs to be used, the appropriate SSL certificate needs to be installed in a format understood by Keycloak. Use `keytool` to add the LDAPS X.509-formatted public certificate to a JKS file named `keycloak-truststore.jks`, set the passphrase to `password1`, and enter `yes` to force trust when prompted. To install the keystore, simply copy it to this location:

```
$SMRT_ROOT/userdata/config/security/keycloak-truststore.jks
```

Start the SMRT Link services, and in step 5 of the LDAP Integration instructions above, change the Connection URL to use an `ldaps:// URI` format, and, if necessary, adjust the port number. (**Note**: By default, LDAP uses TCP port `389` and LDAPS uses TCP port `636`).

SMRT Link user roles

SMRT Link supports three user roles: **Admin**, **Lab Tech**, and **Bioinformatician**. Roles define which SMRT Link modules a user can access. The following table lists the privileges associated with the three user roles: PacBio recommends the following role assignments:

Tasks/privileges	Admin	Lab Tech	Bioinformatician
Add/delete SMRT Link users	Y	N	N
Assign roles to SMRT Link users	Y	N	N
Update SMRT Link software	Y	N	N
Add/update instruments	Y	N	N
Access **Instruments** module	Y	Y	Y
Access **Sample Setup** module	Y	Y	N
Access **Runs** module	Y	Y	N
Access **Data Management** module	Y	Y	Y
Access **SMRT Analysis** module	Y	Y	Y

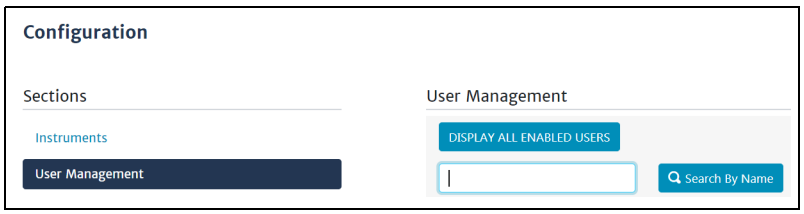
- Assign **at least** one user per site to the **Admin** role. That individual is responsible for enabling and disabling SMRT Link users, as well as specifying their roles and adding/removing associated Revio instruments. The **Admin** can also access all SMRT Link modules, as well as every file in the system. (**Note**: SMRT Link supports **multiple** users with the **Admin** role per site.)
- Assign users who work in the lab preparing samples and performing runs the **Lab Tech** role. **Lab Tech** can also access all SMRT Link modules.
- Assign users who work **only** on data analysis the **Bioinformatician** role. **Bioinformatician** can **only** access the Instruments, Data Management and SMRT Analysis modules; this is the lowest access level.

Note: The Admin role only allows a user account to administer the configuration options available through the SMRT Link browser UI. It does **not** provide access to the Keycloak management interface, which is intentionally restricted to the built-in admin user **only**.

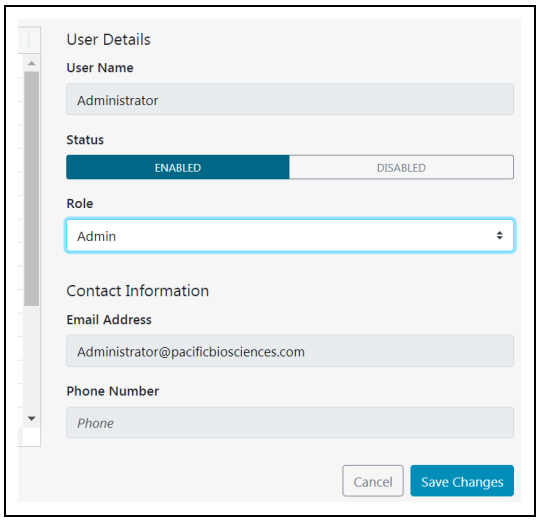
Adding SMRT Link users via LDAP integration and assigning user roles

- To enable users via LDAP integration, you must **first** configure LDAP **before** you can manage users and assign SMRT Link roles to users.
- After LDAP is configured, if you do **not** assign a SMRT Link role to a user, that user will **not** be able to login to SMRT Link.

1. Access **SMRT Link**: Enter `https://<hostname>:8243/sl/home`, where `<hostname>` is the host where SMRT Link is installed.
2. Choose **Settings > User Management** at the top of the page.
3. There are two ways to find users:
   - **To display all SMRT Link users**: Click **Display all Enabled Users**.
   - **To find a specific user**: Enter a user name, or partial name and click **Search By Name**.



4. Click the desired user. If the Status is **Enabled**, the user has access to SMRT Link; **Disabled** means the user **cannot** access SMRT Link.
   - To **add** a SMRT Link user: Click the **Enabled** button, then assign a role. (See Step 5.)
   - To **disable** a SMRT Link user: Click the **Disabled** button.
5. Click the **Role** field and select one of the three roles. (A **blank** role means that this user **cannot** access SMRT Link.)
6. Click **Save Changes**. The user now has access to SMRT Link, based on the role just assigned.



Adding local users to SMRT Link using Keycloak

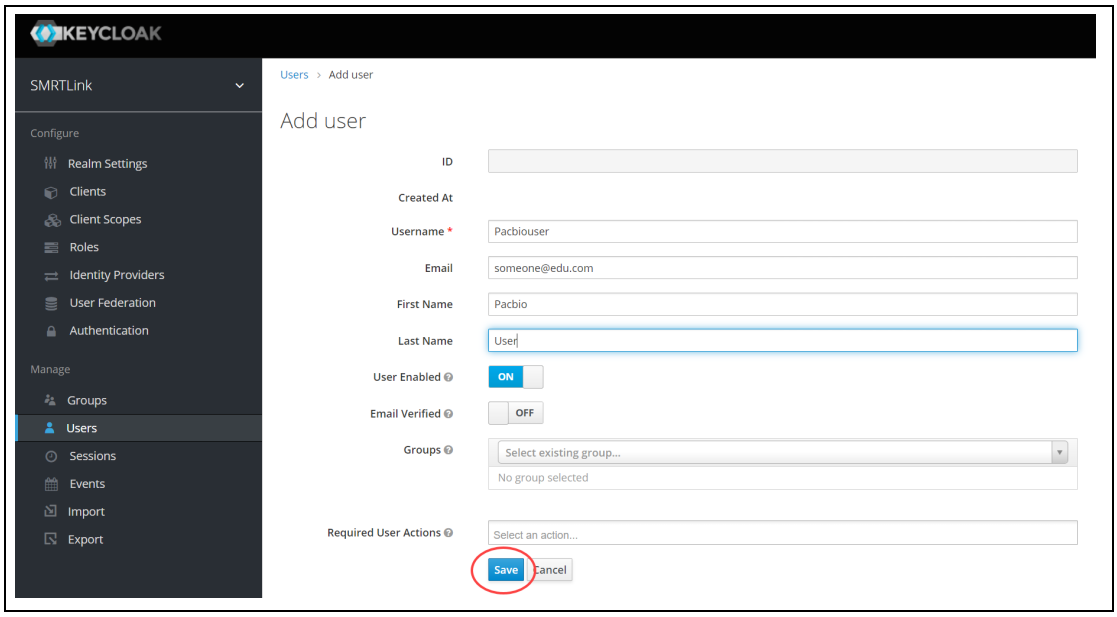
SMRT Link is designed to integrate with an LDAP server to provide user account information, but it is also possible to add **local** user accounts using the Keycloak server that handles authentication for the API gateway.

To add a local account:

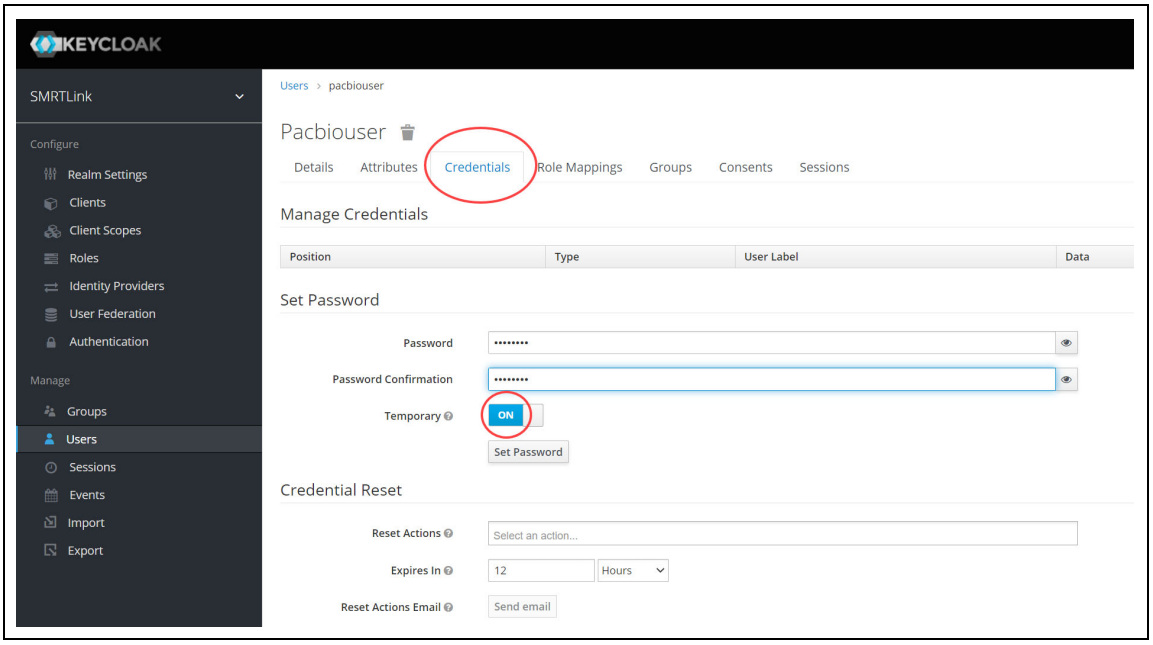
1. Access the Keycloak Admin interface at https://<servername>:9443/auth/admin and log in with the SMRT Link built-in admin account credentials (`admin/admin` by default.)
2. On the left-hand menu, under **Manage**, click **Users**.

3. Click the **Add user** button on the right-hand side of the screen.

4. Complete the form and click **Save**.



5. In the newly added user page, click **Credentials**, and enter a password for the user. If you are issuing a temporary password that the user needs to change on first login, make sure the **Temporary** toggle is **ON**. The section below covers password changes.

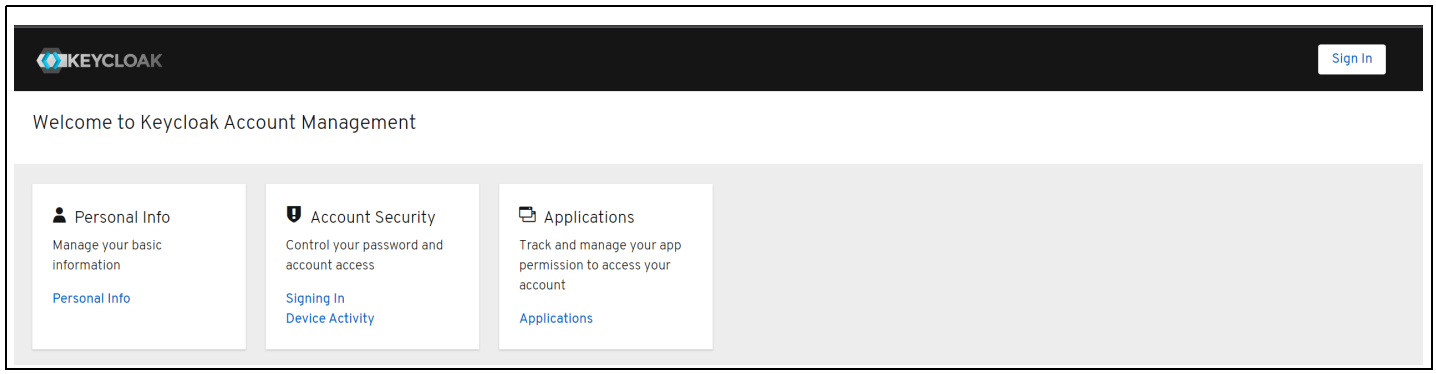


To change a temporary password:

1. When a new local user attempts to log in to SMRT Link with a temporary password, the login will fail with the message “Account is not fully set up”, and a button displays to open the Keycloak user console.

2. Log in to Keycloak with the same credentials. The Keycloak Admin interface will prompt the user to enter a new password.

3. Once the password has been changed, return to the SMRT Link login screen and enter the new password.
4. Local users may change their passwords again by navigating directly to the Keycloak user account page at https://<hostname>:9443/auth/realms/SMRTLink/account/#/.



SMRT Link and SSL certificate procedures

SMRT Link v13.1 uses SSL (Secure Sockets Layer) to enable access via HTTPS (HTTP over SSL), so that your SMRT Link logins and data are encrypted during transport to and from SMRT Link. SMRT Link includes an authentication server (Keycloak), which can be configured to integrate with your LDAP/AD servers and enable user authentication using your organizations' user name and password. To ensure a secure connection between the SMRT Link server and your browser, a domain-specific SSL certificate may be installed **after** completing SMRT Link installation.

It is important to note that PacBio will **not** provide a CA-signed SSL certificate. However, once your site has obtained a CA-signed SSL certificate, PacBio's tools can be used to install it for use with SMRT Link web services. (**Note**: PacBio recommends that you consult your IT administrator about obtaining an SSL certificate.) You will need a certificate issued by a certificate authority (CA). PacBio has tested SMRT Link with certificates from the following certificate vendors: VeriSign, Thawte and DigiCert.

If your site does **not** provide an SSL certificate, SMRT Link v13.1 will use a PacBio self-signed SSL certificate. If you use the self-signed SSL certificate, **each** user will need to accept the browser warnings related to access in insecure environment. You can also have your IT administrator configure desktops to **always trust** the provided self-signed certificate. Note that SMRT Link is installed within your organization's secure network, behind your organization's firewall.

See "Using SMRT Link with a PacBio self-signed SSL certificate" on page 22 for details on how to handle the security warnings when accessing SMRT Link.

Use the following procedures **only** if your site provides an SSL certificate. These procedures are **not** applicable if you are using PacBio's self-signed SSL certificate.

Note: If you have **already** setup an SSL certificate in SMRT Link v4.0.0 or later, those settings will **not** be carried over **automatically** when migrating from WSO2 API Manager to the new API gateway.

Installing an SSL certificate for NGINX

In the new API gateway, SSL transport is handled by the NGINX web server, which uses a simpler configuration consisting of a plain-text certificate and private key. By default SMRT Link will generate a self-signed certificate and key the first time you start the new API gateway:

```
$SMRT_ROOT/userdata/config/security/pb-smrtlink-default.crt
$SMRT_ROOT/userdata/config/security/pb-smrtlink-default.key
```

To install a custom certificate for NGINX

1. Stop SMRT Link services:
   `SMRT_ROOT/admin/bin/services-stop`

2. Copy the certificate and private key files to these paths:
   `$SMRT_ROOT/userdata/config/security/smrtlink-site.crt`
   `$SMRT_ROOT/userdata/config/security/smrtlink-site.key`
3. Start SMRT Link services:
   `${SMRT_ROOT}/admin/bin/services-start`

Restoring the default self-signed SSL certificate

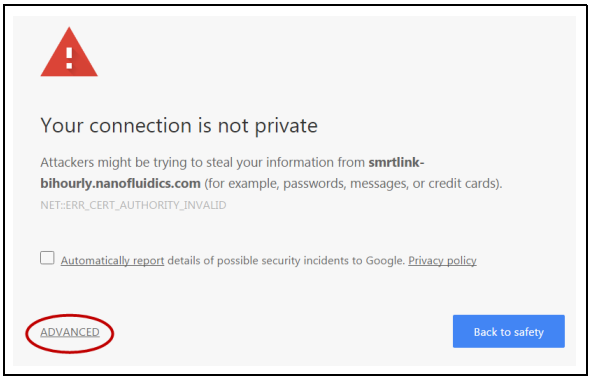
It may sometimes be necessary to uninstall the user-provided SSL certificate and restore the default certificate. All that is needed for this is to do the opposite of the install steps and remove or rename the site certificate.

Using SMRT Link with a PacBio self-signed SSL certificate

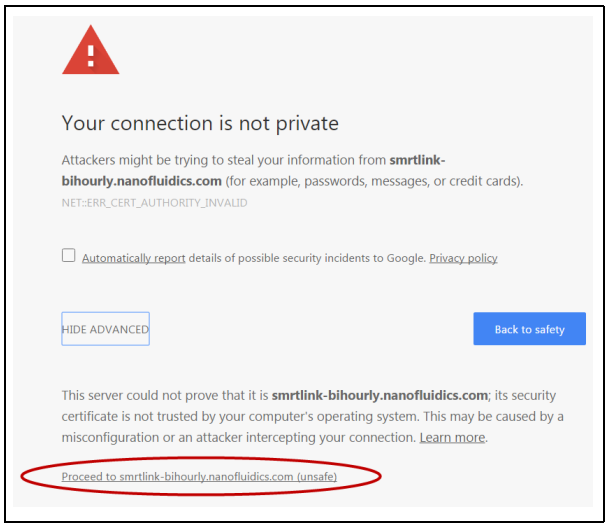
SMRT Link v13.1 uses self-signed SSL certificate generated by the installer. If your site does **not** have a signed SSL certificate **and** you use the self-signed SSL certificate, **each** user will need to accept the browser warnings related to access in insecure environment. You can also have your IT administrator configure desktops to **always trust** the provided self-signed certificate. Note that SMRT Link should be installed within your organization's secure network, **behind** your organization's firewall.

Security messages display when users try to login to SMRT Link for the **first time** using the Chrome browser. These messages may also display **other times** when accessing SMRT Link. **Each** SMRT Link user in your organization should address these browser warnings following the procedure below.

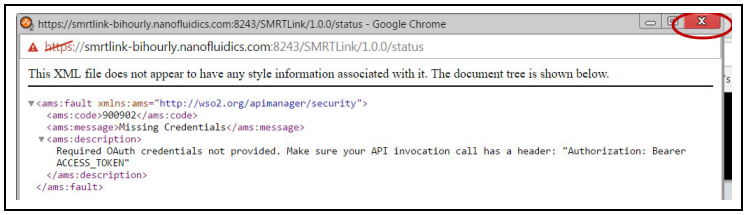
1. The first time you start SMRT Link after installation, you see the following text. Click the **Advanced** link.



2. Click the **Proceed...** link. (You may need to scroll down.)



3. Close the window by clicking the **Close** box in the corner.



4. The **Login** dialog displays, where you enter the User Name and Password. The next time you access SMRT Link, the Login dialog displays **directly**.

Migrating from WSO2 API Manager

If you are upgrading SMRT Link from an installation that used WSO2 API Manager for secure access and user accounts, you need to migrate your configuration to the replacement API gateway **before** you can use new features, such as support for Revio systems. Although some parts of this process are automated, re-entry of some account information (such as passwords) is usually required, and SSL certificates need to be manually imported as described in the previous section.

The migration can be initiated when you first start SMRT Link:

```
$SMRT_ROOT/admin/bin/services-start –migrate
```

When the server has fully started, an interactive script is launched to take you through the migration steps, including the configuration of LDAP server(s) if used, and migration of user account settings. The migration script will attempt to extract the essential fields from existing WSO2 LDAP configurations and register them with Keycloak; if this step is run you will be prompted to re-enter the connection password(s).

If any step in the automated migration fails, you can always complete the configuration manually using the Keycloak Admin interface as described previously.

Because the cleartext passwords for local user accounts are not available, these accounts will **not** be initially available after migration **until** you reset their passwords. See the previous section on creation of local users and setting temporary passwords for instructions on how to re-enable these accounts.

Importing data into SMRT Link

If you have a Revio system/Sequel II system/Sequel IIe system installed and it is linked to the SMRT Link software during the instrument installation, your data will be **automatically** imported into SMRT Link.

You can **manually** import the following types of files directly, using the Data Management module of the SMRT Link GUI:

- **Subreads**: XML file (`.subreadset.xml`) or ZIP file containing information about subreads from Sequel II and Sequel IIe systems, such as paths to the BAM files. Use **only** ZIP files created by SMRT Link.
- **HiFi reads**: XML file (`.consensusreadset.xml`) or ZIP file containing information about HiFi reads (reads generated with CCS analysis whose quality value is equal to or greater than 20.) Use **only** ZIP files created by SMRT Link.
- **Barcodes**: FASTA (`.fa` or `.fasta`), XML (`.barcodeset.xml`), or ZIP files containing barcodes.
- **References**: FASTA (`.fa` or `.fasta`), XML (`.referenceSet.xml`), or ZIP files containing a reference sequence for use in starting analyses.
- **Target regions**: BED (`.bed`) files that specify target genes or regions for analysis; used with the **PureTarget repeat expansion panel** application.

You can also import data in SMRT Link using the `pbservice` command-line utility, as shown below.

- The host and port for the analysis services are optional and default to `localhost:8070`. You can change these settings using the `--host` and `--port` arguments or by using the `$PB_SERVICE_HOST` and `$PB_SERVICE_PORT` environment variables.
- If using the authenticated port 8243, valid user credentials must also be supplied. Use the `--user` and `--password` switches (or `--ask-pass`), or set the `$PB_SERVICE_AUTH_USER` and `$PB_SERVICE_AUTH_PASSWORD` environment variables to specify the credential details.

Importing	Commands

BAM Data Sets generated by the Sequel II/IIe systems	**Import individual SubreadSet XML files:**
	`$> pbservice import-dataset --host $HOST --port $PORT --user $USER --ask-pass /path/to/subreads.subreadset.xml`
	Import a directory of SubreadSet XML files:
	`$> pbservice import-dataset --host $HOST --port $PORT --user $USER --ask-pass /path/to/tree/containing/subreadssets.xml/`

Sending log files to Technical Support

Troubleshooting information can be sent to PacBio Technical Support multiple ways. If there is a connection to the PacBio Event Server, do the following:

- From the SMRT Link menu: **About > Troubleshooting Information > Send**.
- From a SMRT Link "Failed" analysis Results page: Click **Send Log Files**.

If there is connectivity to the PacBio Event Server, run the following command to generate the information and automatically send it to PacBio Technical Support:

```
$SMRT_ROOT/admin/bin/tsreport-install --bundle --upload
```

If there is **no** connectivity to the PacBio Event Server, run the following command to generate a .tgz file and email the file to `support@pacb.com` to file a case:

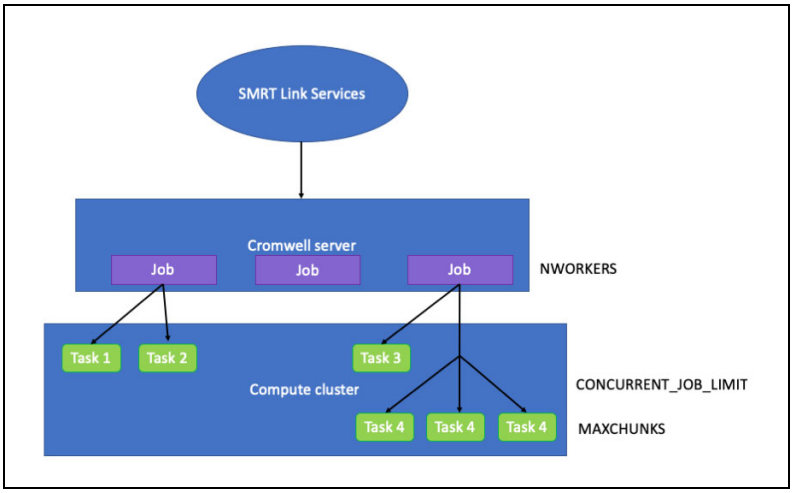
```
$SMRT_ROOT/admin/bin/tsreport-install --bundle
```

The generated file can be found here: `$SMRT_ROOT/userdata/tsreport/data/ts-install.tgz.`

Note: The SMRT Link logs archive bundle will be limited to logs from approximately the past 24 hours. Ensure the above `tsreport-install` options and SMRT Link menu's **Send** button are run within **one day** of experiencing the issue being addressed.

Appendix A: SMRT Link workflow terminology

Management of all SMRT Link activity is handled by the SMRT Link services. In SMRT Link v8.0 and later, the `pbsmrtpipe` workflow engine was replaced by `Cromwell`, an open-source engine developed by the Broad Institute (https://cromwell.readthedocs.io/en/stable/). A continually-running `Cromwell` server is launched at the same time as SMRT Link services, which executes all jobs directly without spawning new processes. Several user-configurable settings control the use of compute resources by `Cromwell`. A representation of the SMRT Link services hierarchy is shown below.



NWORKERS: A SMRT Link services setting that specifies the maximum number of simultaneous analysis jobs (or workflows, as `Cromwell` refers to them) that may be run.

CONCURRENT_JOB_LIMIT: A `Cromwell` configuration setting that limits the total number of job submissions to a specific backend, across all running workflows.

MAXCHUNKS: A `Cromwell` workflow that limits the maximum number of pieces a large Data Set may be broken into for parallelized analysis.

NPROC (Not shown in diagram): A `Cromwell` workflow setting that limits the maximum number of slots that any single JMS cluster submission may request.

Appendix B: Distributed computing setup

PacBio supports the following Job Management Systems (JMS): **Sun Grid Engine (SGE)**, **PBS**, **LSF**, and **SLURM**. You may attempt to manually configure for alternate job management systems, but these are **not** guaranteed to work.

A Job Management System may be used to dispatch jobs to a distributed compute environment. If **no** Job Management System is specified, the system will run in non-distributed mode, and **all** compute jobs will be run locally on the install host.

Available Job Management Systems are detected from the PATH environment variable, but may also be selected manually.

For more information on customizing all of the submissions to the Job Management Systems, see the comments in the file `$SMRT_ROOT/userdata/user_jmsenv/user.jmsenv.ish`. Note that changes to this file will apply to **every** job submitted to the cluster.