



SMRT<sup>®</sup> Link  
software installation  
guide (v25.1)



Research use only. Not for use in diagnostic procedures.

P/N 103-566-000 Version 01 (December 2024)

© 2024 Pacific Biosciences of California, Inc. ("PacBio")

Information in this document is subject to change without notice. PacBio assumes no responsibility for any errors or omissions in this document.

Certain notices, terms, conditions and/or use restrictions may pertain to your use of PacBio products and/or third party products. Refer to the applicable PacBio terms and conditions of sale and to the applicable license terms at <https://www.pacb.com/legal-and-trademarks/terms-and-conditions-of-sale/>.

Trademarks:

Pacific Biosciences, the PacBio logo, PacBio, Circulomics, Omniome, SMRT, SMRTbell, Iso-Seq, Sequel, Nanobind, SBB, Revio, Onso, Apton, Kinnex, PureTarget, Vega, and SPRQ are trademarks of PacBio.

See <https://github.com/broadinstitute/cromwell/blob/develop/LICENSE.txt> for Cromwell redistribution information. PacBio

1305 O'Brien Drive Menlo Park, CA 94025

---

<b>Introduction</b> .....	<b>4</b>
Definitions and variables .....	4
Overview.....	4
<b>System requirements and configurations</b> .....	<b>5</b>
Operating system requirements.....	5
Software dependency requirements.....	5
Hardware requirements and configuration .....	6
Server environment requirements.....	6
Network configuration .....	7
Keycloak Admin interface.....	7
SMRT Analysis configuration .....	7
<b>Installation/upgrade checklist</b> .....	<b>8</b>
<b>Installation instructions</b> .....	<b>8</b>
SMRT Link installation options .....	8
<b>Upgrade instructions</b> .....	<b>10</b>
Supported upgrade path .....	10
<b>Installing only SMRT Tools</b> .....	<b>11</b>
<b>Changing admin and pbinstrument passwords</b> .....	<b>11</b>
<b>Enabling the Keycloak admin console</b> .....	<b>12</b>
<b>LDAP integration</b> .....	<b>12</b>
Configuring LDAP in Keycloak.....	12
SMRT Link user roles .....	14
Adding SMRT Link users via LDAP integration and assigning user roles .....	15
Adding local users to SMRT Link using Keycloak.....	16
<b>SMRT Link and SSL certificate procedures</b> .....	<b>19</b>
Installing an SSL certificate for NGINX.....	19
Restoring the default self-signed SSL certificate .....	20
Using SMRT Link with a PacBio self-signed SSL certificate .....	20
<b>Appendix</b> .....	<b>21</b>
SMRT Link configuration terminology .....	21
Distributed computing setup.....	21
Revio system and SMRT Link, or SMRT Link Lite, network ports and protocols .....	22
SMRT Link Server Network diagram .....	23
Security .....	24
SMRT Link database backups.....	24
Sending log files to Technical Support.....	24
Changing usage tracking settings .....	25
Starting SMRT Link automatically on server boot .....	25
Migrating from WSO2 API Manager .....	25

## Introduction

This document describes the procedure for installing **SMRT Link v25.1** or **SMRT Link Lite v25.1**. This document is for Customer IT or SMRT Link administrators.

- **SMRT Link v25.1** and **SMRT Link Lite v25.1** support Vega™ and Revio® systems. Sequel® II systems, Sequel Ile systems, and Sequel 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:** Generate protocols for binding polymerase to SMRTbell libraries and diluting libraries for loading libraries on SMRT Cells.
- **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; access 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, and the Vega, Revio, Sequel II, and Sequel Ile systems are for research use only (RUO).

## 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
```

## Overview

1. Install or upgrade the SMRT Link software. (See [“Installation instructions”](#) and [“Upgrading SMRT “Upgrade instructions”](#) for details.)
2. **(Optional)** Configure SMRT Link or SMRT Link Lite to use an SSL certificate. (See [“Installing an SSL certificate for NGINX”](#) for details.)
3. **(Optional)** Configure LDAP. (See [“LDAP integration”](#) for details.)
4. **(Optional)** Add SMRT Link Users and Assign User Roles. (See [“Adding SMRT Link users via LDAP and assigning user roles”](#) for details.)
5. **(Optional)** Change the admin password. (See [“Changing admin and pbicsuser passwords”](#) for details.)

# System requirements and configurations

## Operating system requirements

- SMRT Link server software is supported on the following English-language operating systems:
  - Rocky Linux 8 and 9.
  - Ubuntu 22.04 and 24.04
  - This also applies to SMRT Link compute nodes.
- SMRT Link is not guaranteed to work on operating system versions that are no longer supported by their vendors.
- SMRT Link server software cannot be installed on Mac OS or Windows systems.

## Software dependency requirements

- SMRT Link server should run on a dedicated 64-bit Linux host with `libc 2.17` or greater.
- SMRT Link requires the Google Chrome web browser.
- SMRT Link requires a minimum screen resolution of 1600 by 900 pixels.
- Configuring your SMRT Link server with Job Management System (JMS) is required if running SMRT Analysis workflows. SLURM is our supported JMS. For details on other JMS see the Appendix.
- 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. The `singularity` binary should then have `-rwsr-xr-x` permissions.
  - Because a SMRT Link server running SMRT Analysis should be configured to run with SLURM, we recommend installing the `singularity-ce` package on the SMRT Link server, as well as each of the nodes within the relevant partition where you are submitting jobs.
  - 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 requires the following Docker images
    - `docker://google/deepvariant:1.6.1;`
    - `docker://google/deepvariant:1.6.1-gpu;`
    - `docker://quay.io/biocontainers/whatshap:1.4--py39hc16433a_1;`
    - `docker://ghcr.io/dnanexus-rnd/ glnexus:v1.4.1`
    - `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](#).

## Hardware requirements and configuration

Component	SMRT Link multi-node configuration		SMRT Link single node configuration	SMRT Link Lite
	Head node	HPC node		
CPUs	8 cores	64 cores	16 cores/32 threads	4 cores
RAM	32 GB	4 GB per core	64 GB	16 GB
Local storage	500 GB SSD	100 GB SSD or HDD	1 TB SSD	50 GB SSD

**Note:** SMRT Link servers configured with HPC node(s) are required to support running Variant Calling analysis (standalone or within HiFi Target Enrichment) and larger Iso-Seq® Analysis jobs (>20M reads).

**SMRT Link Lite** is a modified configuration that uses the same installer and software as SMRT Link, but with the most compute-intensive components (SMRT Analysis) disabled to support running on non-server hardware.

Recommended analysis input size limits for a single node SMRT Link server configuration

Workflow	Limit with recommended single node server
HiFi Mapping	150 Gb
HiFi Target Enrichment	Disable variant calling
Iso-Seq Analysis	20 million reads
Microbial Genome Analysis	No limit
PureTarget repeat expansion	No limit
Read Segmentation	No limit
Single-Cell Iso-Seq	60 million reads
Variant calling	Not supported

## Server environment requirements

- 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 or Vega instrument you should ensure that the configured hostname is and will remain accessible across the network.

## Network configuration

For network connectivity considerations, see the network diagram in Appendix.

## 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 and Vega systems as well.

- If your network configuration already allows access to port 8243, no additional changes are required to use SMRT Link v25.1 or SMRT Link Lite v25.1.
- 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 and Vega instruments and SMRT Link is bidirectional, so SMRT Link **must** have access to TCP port 9243 on any associated Revio and Vega instruments.

## Keycloak Admin interface

In SMRT Link v25.1, 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 v25.1/SMRT Link Lite v25.1** table.

## SMRT Analysis configuration

- 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.
- SMRT Analysis job output directory storage will approximately double the per SMRT Cell storage requirement. The amount of job storage required will depend on your utilization and analyses used.
  - For the **Revio** system, the sequencing data storage required is up to 78TB/year, assuming approximately 60GB of HiFi data per SMRT Cell and utilization at 1,300 SMRT Cells per year.
  - For the **Vega** system, the sequencing data storage required is up to 6TB/year, assuming approximately 30GB of HiFi data per SMRT Cell and utilization at 200 SMRT Cells per year.
- 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.

## Installation/upgrade checklist

### Installation instructions

Following are the steps for installing SMRT Link v25.1 or SMRT Link Lite v25.1 on a new system. (See Appendix for details.)

- To upgrade SMRT Link to v25.1 from a previous version, see “Upgrading SMRT Link” on page 10.

SMRT Link v25.1 and SMRT Link Lite v25.1 can be used with the following supported version of ICS:

- v13.3 for Revio systems.
- v1.0 for Vega 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 <sup>a</sup>	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 (v25.1)** for more information.



Step	Installation summary - SMRT Link v25.1/SMRT Link Lite v25.1
1	<p><b>Download SMRT Link software:</b></p> <p>Download and extract the SMRT Link software installer from <a href="#">here</a>. (The same installer can install <b>both</b> SMRT Link and SMRT Link Lite.)</p>
2	<p>Log onto the SMRT Link Install Host (such as the hostname or IP address) as the SMRT Link Install User (such as <code>\$SMRT_USER</code>.)</p>
3	<p><b>Install SMRT Link by invoking the SMRT Link Installer:</b></p> <pre>./smrtlink_&lt;version number&gt;.run --rootdir \$SMRT_ROOT</pre> <p><b>Note:</b> The <code>\$SMRT_ROOT</code> directory must <b>not</b> exist when the installer is invoked, as the installer will try to create it, and will abort the installation if an existing <code>\$SMRT_ROOT</code> location is found. If a previous installation was canceled or otherwise failed, the installer can be invoked <b>without</b> extraction. Rerun using the <code>--no-extract</code> option:</p> <pre>./smrtlink_&lt;version number&gt;.run --rootdir \$SMRT_ROOT --no-extract</pre> <p>Alternatively, install <b>SMRT Link Lite</b> by using the following command instead:</p> <pre>./smrtlink_&lt;version number&gt;.run --lite true --jmstype NONE --rootdir \$SMRT_ROOT --nworkers 4</pre> <p><b>Note:</b> For the single node configuration, the following settings are recommended: <code>nproc=12</code>, <code>nchunks=1</code>, <code>nworkers=4</code></p> <p>See Appendix for additional information.</p>
4	<p>On the instrument, click <b>Install</b> when prompted to install the Chemistry Update.</p>
5	<p><b>Start SMRT Link services:</b></p> <pre>\$SMRT_ROOT/admin/bin/services-start</pre> <p>If you need the Keycloak Admin interface enabled on external port 9443, use this command:</p> <pre>\$SMRT_ROOT/admin/bin/services-start --enable-keycloak-console</pre>
6	<p><b>(SMRT Link only) Run the Site Acceptance Test from the command line:</b></p> <pre>\$SMRT_ROOT/admin/bin/run-sat-services</pre> <p>Successful completion of <code>run-sat-services</code> 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.</p>
7	<p><b>(Optional) Clear the browser cache:</b></p> <p>This is a good troubleshooting step if needed.</p> <p>I. Open the Chrome Browser and choose <b>More Tools &gt; Clear browsing data</b>, choose <b>All Time</b> from the <b>Time Range</b> control, then check <b>Cached images and files</b>. Click <b>Clear data</b>. Restart the browser.</p>
8	<p><b>(Optional) Configure LDAP and/or add local users:</b></p> <p>See <a href="#">“Configuring LDAP in Keycloak”</a>, <a href="#">“Adding local users to SMRT Link using Keycloak”</a> for details.</p>
9	<p><b>(Optional) Configure SMRT Link/SMRT Link Lite to use a signed SSL certificate:</b></p> <p>See <a href="#">“Installing an SSL certificate for NGINX”</a> for details.</p>
10	<p><b>(Optional) Change the admin and pbicsuser passwords:</b></p> <p>We recommend that you change the <code>admin</code> and <code>pbicsuser</code> account passwords from the default values. See <a href="#">“Changing admin and pbicsuser passwords”</a> for details.</p>

# Upgrade instructions

## Supported upgrade path

- SMRT Link upgrades to v25.1 are supported from any v8.x, v9.x, v10.x, v11.x, v12.x or v13.x releases.
- SMRT Link Lite upgrades to v25.1 from v13.0 are supported.
- **Note:** You can upgrade from SMRT Link v12.0 to SMRT Link Lite v25.1 - see Step 5 in the **Upgrading SMRT Link/SMRT Link Lite** table.
- SMRT Link v25.1/SMRT Link Lite v25.1 can be used with the following supported version of ICS:
  - v13.3 for Revio systems
  - v1.0 for Vega systems

Step	Upgrading SMRT Link/SMRT Link Lite
1	Download and extract the SMRT Link software installer from <a href="#">here</a> . (The same installer can install <b>both</b> SMRT Link and SMRT Link Lite.)
2	Log onto the SMRT Link Install Host (such as the hostname or IP address) as the SMRT Link Install User (such as <code>\$SMRT_USER</code> .)
3	<b>Stop the SMRT Link services:</b> <code>\$SMRT_ROOT/admin/bin/services-stop</code> <b>Note:</b> Ensure that no active SMRT Link analysis jobs are running before stopping services.
4	<b>Upgrade SMRT Link by invoking the SMRT Link installer:</b> <code>./smrtlink_&lt;version number&gt;.run --rootdir \$SMRT_ROOT --upgrade</code> <b>Note:</b> The <code>\$SMRT_ROOT</code> directory must be an existing SMRT Link installation. Several validation steps will occur to ensure that a valid <code>\$SMRT_ROOT</code> is being updated. <b>Upgrade SMRT Link Lite:</b> <code>./smrtlink_&lt;version number&gt;.run --rootdir \$SMRT_ROOT --upgrade --lite true</code> If a previous upgrade was canceled or otherwise failed, the installer can be invoked without extraction. Rerun using the <code>--no-extract</code> option: <code>./smrtlink_&lt;version number&gt;.run --rootdir \$SMRT_ROOT --upgrade --no-extract</code>  See Appendix for additional information.
5	<b>Start the SMRT Link services:</b> <code>\$SMRT_ROOT/admin/bin/services-start</code>  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: <code>\$SMRT_ROOT/admin/bin/services-start --migrate</code>  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.
6	<b>(SMRT Link only) Run the Site Acceptance Test from the command line:</b> <code>\$SMRT_ROOT/admin/bin/run-sat-services</code> Successful completion of <code>run-sat-services</code> 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.
7	<b>(Optional) Clear the browser cache:</b> This is a good troubleshooting step if needed. <ol style="list-style-type: none"><li>1. Open the Chrome Browser and choose <b>More Tools &gt; Clear browsing data</b>, choose <b>All Time</b> from the <b>Time Range</b> control, then check <b>Cached images and files</b>. Click <b>Clear data</b>.</li><li>2. Restart the browser.</li></ol>
8	<b>(Optional) Change the admin and instrument user passwords:</b> We recommend that you change the <code>admin</code> and <code>pbicsuser</code> account passwords from the default values. See <a href="#">“Changing admin and pbicsuser passwords”</a> for details.

## 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-25.1.0.xxxxx.run --rootdir smrtlink --smrttools-only
./smrtlink-25.1.0.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 (v25.1)** on how to setup JMS integration using `pbcromwell`.

**Warning:** Revio and Vega systems cannot communicate with a `--smrttools-only` installation.

## Changing admin and pbinstrument 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 (`pbinstrument`) which is used by the Revio and Vega systems to communicate with SMRT Link web services over a secure, encrypted connection. The `pbinstrument` account is required for instruments to communicate with SMRT Link (**Note:** the `pbinstrument` 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 `pbinstrument` 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/smrtcmds/developer/bin/pbservice-instrument set-smrtlink-password --user admin
--ask-pass
```

To verify the `admin` and `pbinstrument` 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 pbinstrument --
ask-pass
```

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

**Note:** If the Keycloak Admin interface on HTTPS port `9443` is enabled, you can use it to change the `admin` password. (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.)

## Enabling the Keycloak admin console

If you need a graphical interface to administer user authorization functions, the Keycloak software that is included in SMRT Link is optionally available. In SMRT Link 25.1 the port on which this GUI runs is closed by default for maximum security, but it can be enabled at start by adding an argument:

```
$SMRT_ROOT/admin/bin/services-start --enable-keycloak-console
```

Alternately, you can toggle the admin interface while the server is running:

```
$SMRT_ROOT/admin/bin/restart-gui --enable-keycloak-console
```

```
$SMRT_ROOT/admin/bin/restart-gui --disable-keycloak-console
```

Since this only requires restarting a single component, it will only interrupt external connections for a few seconds at most. We recommend leaving the console disabled when you are not actively managing server access.

## 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.

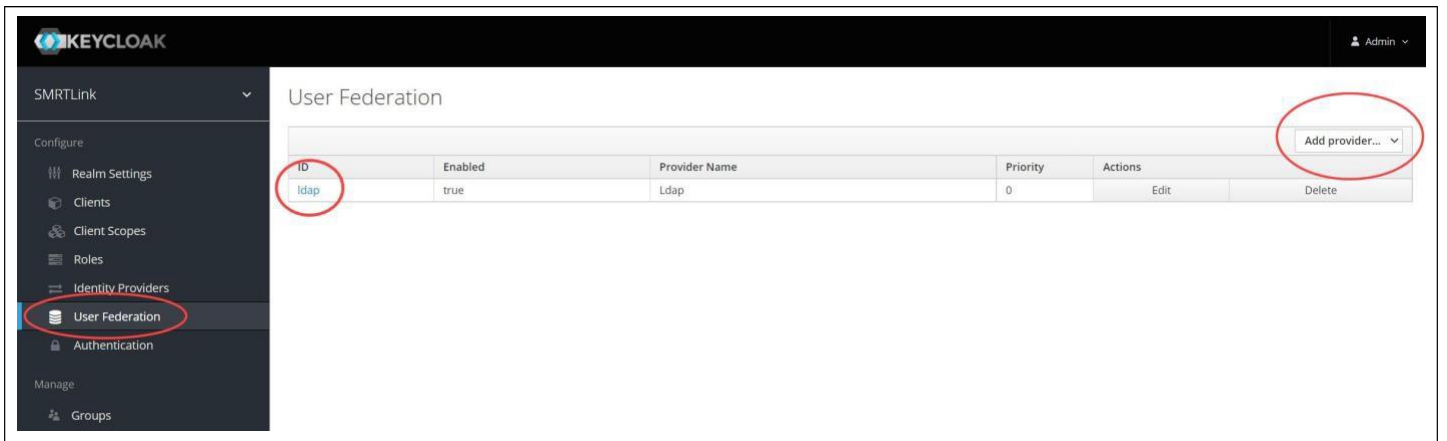
If you are interested in configuring SMRT Link integration with your organization's LDAP, PacBio recommends that you consult your LDAP administrator to help determine the correct LDAP settings. Note: Existing LDAP configurations are automatically migrated during upgrade.

## Configuring LDAP in Keycloak

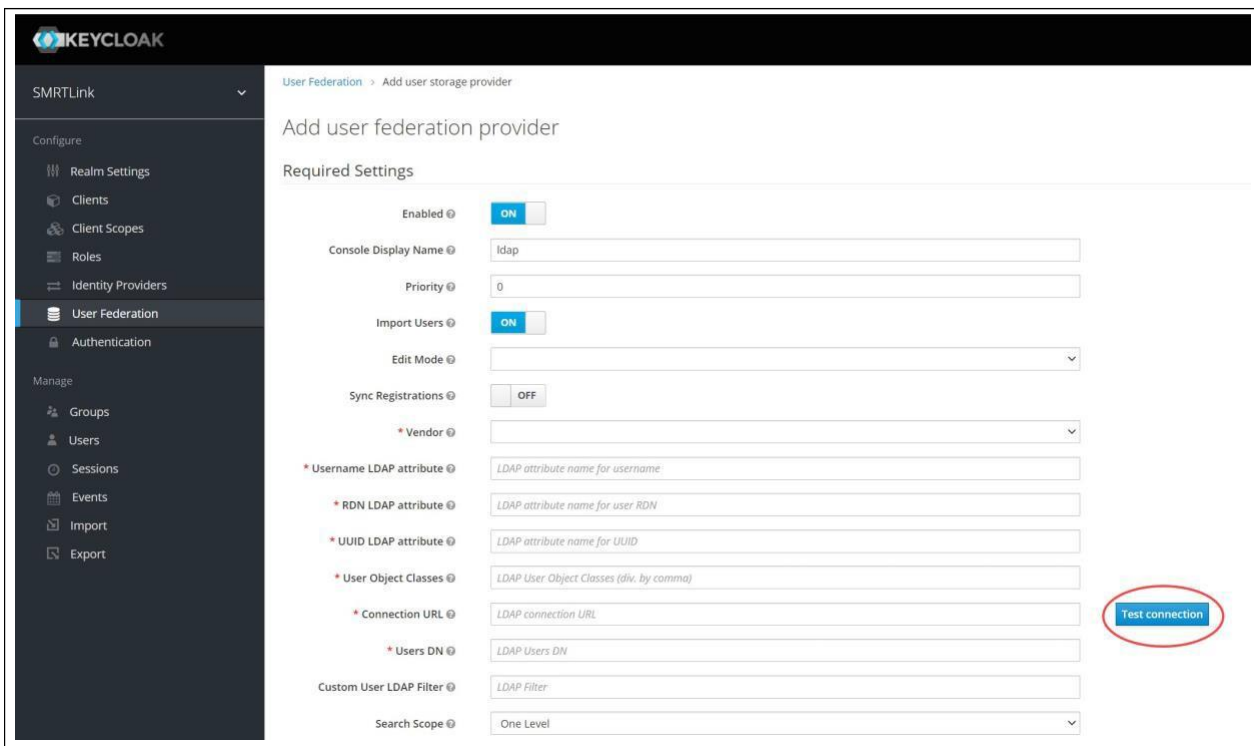
- LDAP is configured after SMRT Link v25.1 is installed, using the **Keycloak** authentication server software, as shown below.
  - SMRT Link must first synchronize with your organization's LDAP objects before any directory accounts can be enabled and given a role to facilitate SMRT Link access.
1. Enter the following in your browser: `https://<hostname>:9443/auth/admin/` where `<hostname>` is the host where SMRT Link is installed. (The Keycloak console must be enabled, as shown above.)
  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/Lightweight_Directory_Access_Protocol)
- [https://en.wikipedia.org/wiki/LDAP\\_Data\\_Interchange\\_Format](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 <b>Instruments</b> module	Y	Y	Y
Access <b>Sample Setup</b> module	Y	Y	N
Access <b>Runs</b> module	Y	Y	N
Access <b>Data Management</b> module	Y	Y	Y
Access <b>SMRT Analysis</b> 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 Revo 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.

User Details

User Name  
Administrator

Status  
ENABLED

Role  
Admin

Contact Information

Email Address  
Administrator@pacificbiosciences.com

Phone Number  
Phone

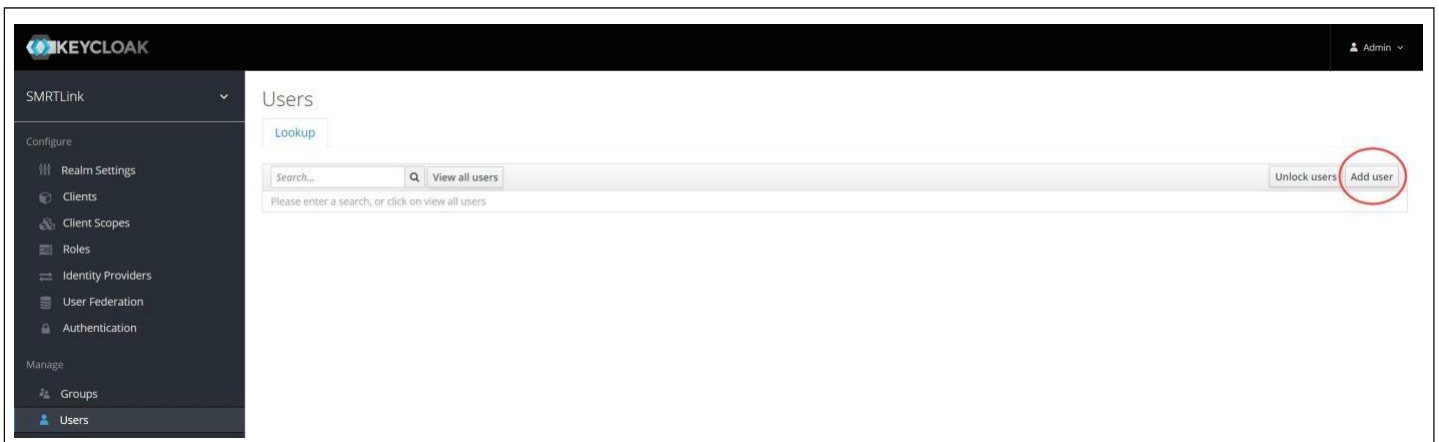
Cancel Save Changes

## 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**.

The screenshot shows the 'Add user' form in the Keycloak administration console. The left sidebar contains navigation options under 'Configure' (Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, Authentication) and 'Manage' (Groups, Users, Sessions, Events, Import, Export). The 'Users' option is selected. The main form area is titled 'Add user' and contains the following fields: ID (empty), Created At (empty), Username \* (Pacbiouser), Email (someone@edu.com), First Name (Pacbio), Last Name (User), User Enabled @ (ON), Email Verified @ (OFF), Groups @ (Select existing group... No group selected), and Required User Actions @ (Select an action...). The 'Save' button is circled in red.

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.

The screenshot shows the user page for 'Pacbiouser' in the Keycloak administration console. The left sidebar is the same as in the previous screenshot. The main area is titled 'Pacbiouser' and has tabs for Details, Attributes, Credentials (circled in red), Role Mappings, Groups, Consents, and Sessions. Below the tabs is the 'Manage Credentials' section, which includes a table with columns for Position, Type, User Label, and Data. The 'Set Password' section contains Password and Password Confirmation fields (both masked with dots), a Temporary @ toggle (ON, circled in red), and a Set Password button. The 'Credential Reset' section contains Reset Actions @ (Select an action...), Expires In @ (12 Hours), and Reset Actions Email @ (Send email).

## 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.



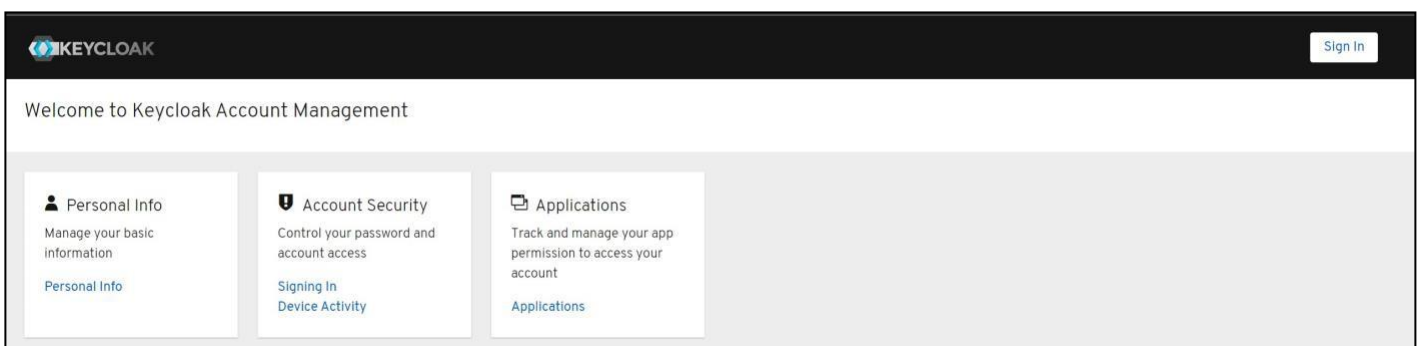
The image shows a login form titled "Please Sign In". It has two input fields: "Username" with the value "pacbiouser" and "Password" with masked characters. Below the password field is a blue "Log In" button. A red error message "Account is not fully set up" is displayed below the "Log In" button. At the bottom of the form is a grey "Update Password" button.

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



The image shows the "Update password" screen in the Keycloak Admin interface. At the top, it says "SMRTLINK". Below that, it says "Update password". There is a yellow warning box with a triangle icon and the text "You need to change your password to activate your account." Below the warning box are two input fields: "New Password" and "Confirm password". At the bottom is a blue "Submit" button.

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/#/>.



The image shows the Keycloak Account Management dashboard. At the top left is the Keycloak logo and "KEYCLOAK". At the top right is a "Sign In" button. Below the header is the text "Welcome to Keycloak Account Management". The main content area has three cards: "Personal Info" (Manage your basic information, link: Personal Info), "Account Security" (Control your password and account access, links: Signing In, Device Activity), and "Applications" (Track and manage your app permission to access your account, link: Applications).

## SMRT Link and SSL certificate procedures

SMRT Link v25.1 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 v25.1 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 an 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](#)" 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.

### 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. This requires the following steps.

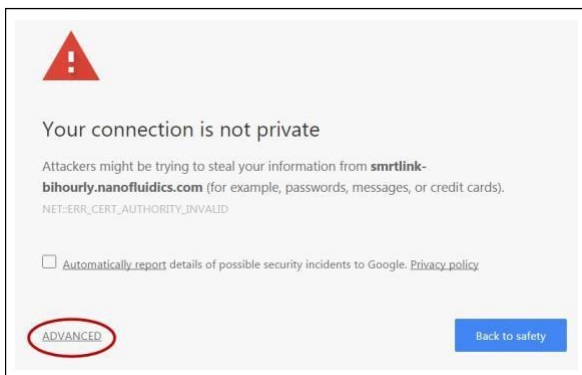
```
$SMRT_ROOT/admin/bin/services-stop
#remove or rename site certificates
$SMRT_ROOT/admin/bin/services-start
```

## Using SMRT Link with a PacBio self-signed SSL certificate

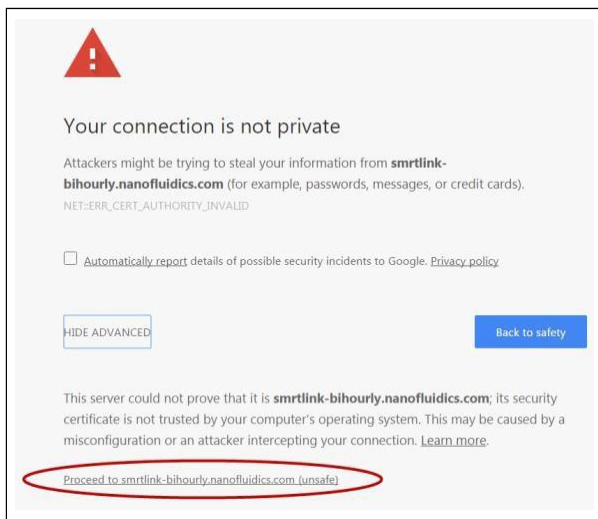
SMRT Link v25.1 uses self-signed SSL certificate generated by the installer. If your site does **not** have a signed SSL certificate **and** you use the self-signed SSL certificate, **each** user will need to accept the browser warnings related to access in an insecure environment. You can also have 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.

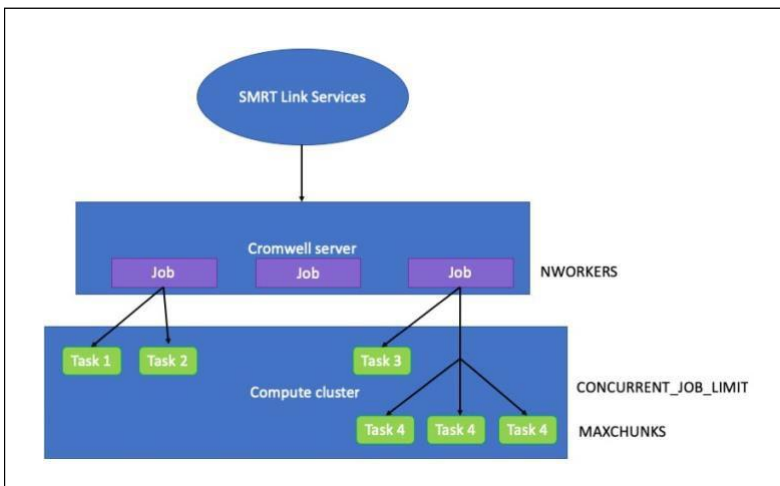


4. The **Login** dialog displays, where you enter the User Name and Password. The next time you access SMRT Link, the Login dialog displays **directly**.

## Appendix

### SMRT Link configuration terminology

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.

### Distributed computing setup

Running SMRT Link with SMRT Analysis requires the Slurm Job Management System (JMS). PBS and LSF can be used, but are not officially supported and will require additional configuration.

Because Slurm is required for SMRT Analysis it may be used to dispatch jobs to a distributed compute environment. If no JMS 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 JMS, 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.

### Revio and Vega system and SMRT Link, or SMRT Link Lite, network ports and protocols

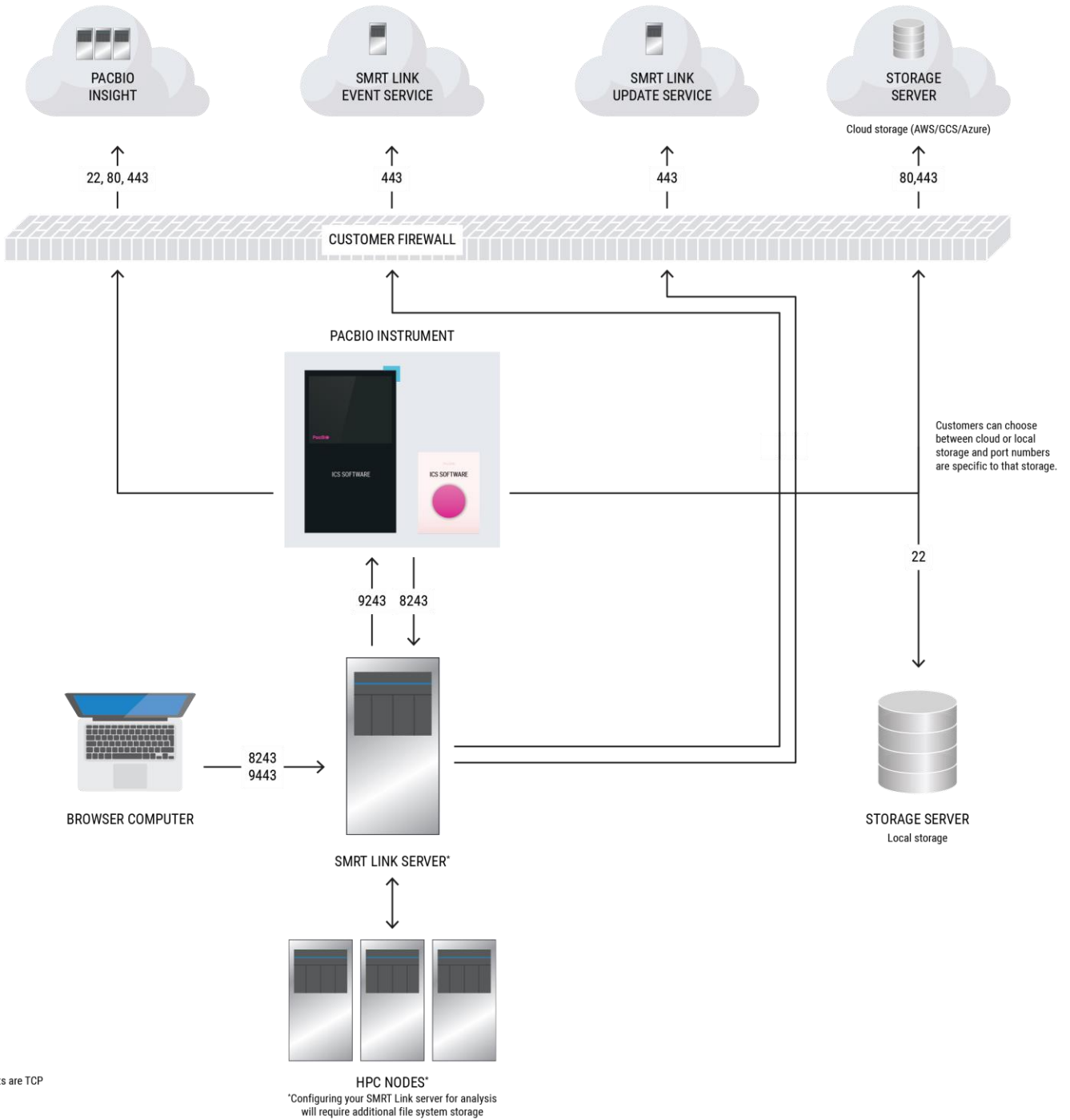
Source	Destination	Port/Protocol	Description
Revio and Vega system	SecureLink Servers	22/tcp, 80/tcp, or 443/tcp	Communication for remote support (PacBio Insight)
Revio and Vega system	Storage (Cloud or local)	RSYNC over SSH: 22/tcp, or Cloud: 80/tcp or 443/tcp depending on protocol	Data transfer from instrument to customer storage
Revio and Vega system	Customer or external NTP servers	123/udp	Used for updating machine time. Defaults to pool.ntp.org
Revio and Vega system	Customer server	53/udp or 53/tcp	Nameservers
Revio and Vega system	SMRT Link server	8243/tcp	Communication from instrument to SMRT Link
SMRT Link server	Revio and Vega system	9243/tcp	Communication from SMRT Link to instrument
Customer laptop/desktop PC	SMRT Link server	8243/tcp	SMRT Link web services and GUI https
Customer laptop/desktop PC	SMRT Link server	9443/tcp	Optional SMRT Link Administration https (API Management Interface)
SMRT Link server	Shared Network File System (NFS) <sup>a</sup>	NFS ports (may vary depending on configuration)	Shared file system (NFS) storage for analysis data
SMRT Link server	PacBio Event server ( <a href="https://smrtlink-eve.pacbcloud.com:443">https://smrtlink-eve.pacbcloud.com:443</a> )	443/tcp	Optional reporting of server metrics to PacBio Tech Support
SMRT Link server	PacBio Update server ( <a href="https://smrtlink-update.pacbcloud.com:8084">https://smrtlink-update.pacbcloud.com:8084</a> )	443/tcp	Downloading Chemistry Updates
HPC nodes	Shared Network File System (NFS) storage <sup>a</sup>	NFS ports (may vary depending on configuration)	Shared file system (NFS) storage for analysis data

a. Network file system requirements: If used, NFS mounts to the input and output locations; HPC compute nodes must be able to write back to the NFS; Additional file system storage may be required if using SMRT Link for analysis. This approximately doubles the storage requirement.

# SMRT Link Server Network diagram

## Vega and SMRT Link, including SMRT Link Lite, network diagram

INTERNET



## Security

### General security

- 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 v25.1 security

SMRT Link v25.1 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 WS02 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.**

### SMRT Link database backups

- SMRT Link v25.1 does not perform periodic 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.

### 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.



## 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.tpl
```

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

## 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.