SMRT® Link Software Installation (v9.0)

Introduction

This document describes the procedure for installing **SMRT Link v9.0**. This document is for Customer IT or SMRT Link Administrators.

SMRT Link is the web-based end-to-end workflow manager for the Sequel®/Sequel II System. It includes software applications for designing and monitoring sequencing runs, and analyzing and managing sequence data. SMRT Link provides a web interface that can control **multiple** Sequel/Sequel II Systems.

SMRT Link is the primary access point for applications used by researchers, laboratory technicians, instrument operators, and bioinformaticians for various interactions with applications related to the Sequel platform. The applications include:

- **Sample Setup**: Calculate binding and annealing reactions for preparing DNA samples for use on the Sequel/Sequel II System.
- **Run Design**: Design runs and create and/or import sample sheets which become available on the Sequel/Sequel II System.
- **Run QC**: Monitor run progress, status and quality metrics.
- **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, and barcode files.
- **SMRT Analysis**: Perform multiple types of secondary analysis, including sequence alignment, variant detection, *de novo* assembly, structural variant calling, and RNA analysis.

Note: SMRT Link and the Sequel/Sequel II System are for **research use only** (RUO).

Overview

1. Install or upgrade the SMRT Link software. (See “Installation Summary” on page 5 and “Configuring LDAP” on page 12 for details.)
2. (**Optional**) Configure SMRT Link to use an SSL Certificate. (See “Step 1: Obtain a domain-specific certificate from the appropriate Certification Authority.” on page 15 for details.)
3. (**Optional**) Add SMRT Link Users and Assign User Roles. (See “Adding SMRT Link Users and Assigning User Roles” on page 14 for details.)
4. (**Optional**) Change the admin and pbicsuser passwords. (See “Changing admin and pbicsuser Passwords” on page 11 for details.)
5. (**Optional**) Configure LDAP. (See “LDAP Integration” on page 12 for details.)

PacBio Compute Infrastructure Partners (https://www.pacb.com/products-and-services/smrt-compatible-products/analysis-products/) provide HPC solutions designed to support the Sequel II System.

Sequel II System Compute Requirements

Head Node	
Cores	**32**
RAM	**64 GB**
tmp_dir (Local Storage)	**1 TB recommended**, **500 GB minimum**
db_datadir (Local Storage)	**250 GB**
Compute Nodes	
Cores (Total)	**384**[a]
Minimum RAM per Slot (1 slot = 1 core)	**4 GB/8 GB *de novo* assembly large complex genomes**
tmp_dir (Local Storage)	**100 GB**
Shared Data Storage[b]	
Sequence Data	**40 TB**
(jobs_root) Analysis Data	**70 TB**
Network	
10 GBE recommended, 1 GBE required	

a. For a standard CCS sequencing collection (415 GB sequencing data, 25 GB Unique Molecular Yield, 15 kb insert size, 30-hours movie), CCS Analysis takes 6.5 hours on this configuration. SMRT Link will work on less powerful compute configurations, however analysis time will be significantly longer.

b. Storage is calculated for one Sequel II System, assuming 100 human genomes per year at 50-fold coverage, *de novo* assembly.

Data Examples

Human Assembly

- Genome size: 3.3 GB; Sequence data 400 GB; Analysis data 700 GB; Analysis time: 72 hours wall. This is 50-fold coverage human genome analyzed on the compute configuration listed above.

Rice Assembly

- Genome size: 0.43 GB; Sequence data 55 GB; Analysis data 90 GB; Analysis time: 20 hours wall. This is 50-fold coverage rice genome analyzed on the compute configuration listed above.

For Sequel Instrument requirements, see “Appendix C: Sequel System Compute Requirements” on page 22 for details.

Data storage

- The SMRT Link software **root** directory **must** be readable and writable by the SMRT Link install user and **must** have the same path across all compute nodes via NFS. PacBio recommends `/opt/pacbio/smrtlink` for the SMRT Link software root directory (referred to as `$SMRT_ROOT`), and `smrtanalysis` for the SMRT Link install user (referred to as `$SMRT_USER`).

- The SMRT Analysis **output** directory is used to store output from SMRT Analysis jobs. The software accesses this directory from a symbolic link at `$SMRT_ROOT/userdata/jobs_root`, which can be modified manually or by using the installation script. The symbolic link destination should be on a shared file system (NFS); it **must** be writable by the `$SMRT_USER`, and it **must** be accessible along the same path on **all** compute nodes. This is usually symbolically linked to a large storage volume.
- The SMRT Analysis **database** directory is used to store database files and backups. The software accesses this directory from a symbolic link at `$SMRT_ROOT/userdata/db_datadir`, and it can be modified manually or by using the installation script. This symbolic link destination should be a **local** directory (**not** NFS) and be writable by `$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 from a symbolic link at `$SMRT_ROOT/userdata/tmp_dir`, and it can be modified manually or using the installation script. This symbolic link destination should be a **local** directory (**not** NFS), it must be writable by `$SMRT_USER`, and it must exist (or be creatable) as an independent directory on **all** compute nodes. The temporary directory exists on **both** the head node, and the compute nodes.

Software Prerequisites: Server Operating Systems

- SMRT Link server software is supported on English-language CentOS 6.x; 7.x and Ubuntu 16.04; 18.04 64-bit Linux® distributions. (This also applies to SMRT Link compute nodes.)
- **Note**: SMRT Link v9.0 is the **last** version that will be supported on CentOS 6.x.
- 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®.

Software/Hardware Prerequisites: Client Systems

To use SMRT Link on a client operating system:

- SMRT Link **requires** the Google® Chrome web browser, version 74 or later.
- SMRT Link **requires** a minimum screen resolution of 1600 by 900 pixels.

Network Configuration

- Please refer to the **IT Site Prep Guide** provided with your instrument purchase for more details.
- For network connectivity considerations, see the network diagram in the **Computer Requirements** section of the **IT Site Prep Guide**.

SMRT Link Server Environment Assumptions

- The SMRT Link server should run on a dedicated 64-bit Linux host with `libc 2.12.1` or greater.
- The installation is performed by the **same** non-root user (`$SMRT_USER`) that will be used to run the system.
- The `$SMRT_USER` has full permissions in the file system in the `$SMRT_ROOT` directory and in all linked directories for `jobs_root`, `db_datadir` and `tmp_dir`. (Common problems include NFS setup problems, ACLs, and so on.)
- When running in distributed mode, all other nodes have the **same path** for `$SMRT_ROOT` and for all linked directories. (The NFS exports should have identical mount points on **all** cluster nodes.)
- During the installation, 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 public NTP time server.
- The `$SMRT_USER` service account **must** have both the `nofile` and `nproc` 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.

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 v9.0 Security Notes

SMRT Link v9.0 restricts access to the web services API to clients running on `localhost` (such as the WSO2 server that handles authentication and permissions) or remotely using SSL encryption and password-based authentication.

Ports and firewalls: The instrument **must** be able to access the SMRT Link server on port `8243`. This port is also used by the Sequel Instrument Control Software (ICS), so it needs to be available to **any** Sequel Systems as well.

- If your network is already configured to leave this port open, **no additional changes** are required to use v9.0.
- The instrument must have access to port `8243` of the SMRT Link server.
- End users must also have access to port `8243` of the SMRT Link server for access to the browser UI.

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 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” on page 12 for details.
- **(Optional)** SSL Certificate for WS02. See “SMRT® Link and SSL Certificate Procedures” on page 15 for details.

Installation Summary

Following are the steps for installing SMRT Link v9.0 on a **new** system. (See "Appendix A: SMRT Link Workflow Terminology" on page 20 for details.) To upgrade SMRT Link to v9.0 from a **previous version**, follow the upgrade steps on Page 7. SMRT Link v9.0 can be used with three versions of ICS:

- v8.0.0.78867 (Sequel II System)
- v8.0.0.84541 (Sequel System)
- v9.0.0.92233 (Sequel II 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 & Reference Files	SAT (Site Acceptance Test)	SMRT Link Services	Cromwell	Cromwell w/Call Caching
Full SMRT Link	Y	Y	Y	Y	Y	Y	Y	Y	Y
SMRT Tools only	N	Y	N[a]	N	N	N	N	Y	N

a. JMS with a SMRT Tools-only installation may be setup using `pbcromwell`. See **SMRT Tools Reference Guide** for more information.

Step	Installation Summary - SMRT Link v9.0
1	**Download SMRT Link software:** Download and extract the SMRT Link software installer from http://www.pacb.com/support/software-downloads.
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 `$SMRT_ROOT`, define a convenience variable in the shell so the commands below may be run verbatim. To do so, use something like: `SMRT_ROOT=/opt/pacbio/smrtlink` The fully qualified version of the SMRT Link Install Host may always be used in place of the short host name. But in some cases, particularly when working with WSO2, the fully qualified domain name is required.
3	Log onto the SMRT Link Install Host (such as the hostname or IP address) as the SMRT Link Install User (such as `$SMRT_USER`.)

4	**Install SMRT Link by invoking the SMRT Link Installer:**
	`smrtlink_9.0.0.92188.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_9.0.0.92188.run --rootdir $SMRT_ROOT --no-extract`
	See "Appendix A: SMRT Link Workflow Terminology" on page 20 for additional information.

5	**Start SMRT Link services:** `$SMRT_ROOT/admin/bin/services-start`

Step	Installation Summary - SMRT Link v9.0
6	**Run the Site Acceptance Test from the command line:** `$SMRT_ROOT/admin/bin/run-sat-services` Successful completion of `run-sat-services`, which produces a Site Acceptance Test (SAT) analysis job in the SMRT Analysis module of the SMRT Link GUI, indicates that the HPC configuration is functioning correctly.
7	**(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** droplist, then check **Cached images and files**. Click **Clear data**. 2. Restart the browser.
8	**Run the Site Acceptance Test from the browser:** 1. Using the Chrome browser, open SMRT Link at `http://smrtlinkhost:9090`. – The port number should match the `GUI port` defined during installation; the default is `9090`. The URL will redirect to a secure URL at hard-coded port `8243`. If port `9090` is blocked, go directly to the redirect URL at `https://smrtlinkhost.mydomain.com:8243/sl/home`. – Check with your IT group if port `8243` is blocked; access to port `8243` on the SMRT Link Install Host is **required** to access the browser UI and for communication with the instrument. 2. Bypass the Chrome browser's privacy error check: Without an SSL certificate installed, Chrome will issue a "Privacy Error" and state that "Your connection is not private". Bypass by clicking on the **Advanced** link on the bottom left of the page. Then click on the **Proceed to smrtlinkhost.mydomain.com (unsafe)** link. To avoid the "Privacy Error" in the future, follow the instructions for installing the SSL Certificate in Step 10 below. 3. Log in to SMRT Link by entering the default Administrator credentials: `admin/admin`. 4. Submit SMRT Link notification selections: Select options for notifying PacBio of successful installations and for sending ongoing SMRT Link analysis usage information. Click **Save**. 5. Go to the SMRT Analysis page: On the SMRT Link home page (`https://smrtlinkhost.mydomain.com:8243/sl/`), click **SMRT Analysis**. 6. Create a new analysis: Click **+ Create New Analysis**. 7. Select analysis settings and start the analysis: a) Enter `SMRT Link 9.0.0 SAT Test` (or any descriptive name) in the **Analysis Name** field. b) Select **Sequel Data** as the Data Type. c) In the **Data Sets** table, check the box next to `PacBio Tiny SAT Dataset Example`. d) Click **Next**. e) Select **Site Acceptance Test (SAT)** from the Analysis Application drop down list, at the top left. The Reference field is auto-populated with `lambdaNEB`. f) Click **Start** in the top right corner to start the analysis. 8. Wait for the analysis to complete successfully. On the **Analysis Results - SMRT Link 9.0 SAT Test** page (Example: `https://smrtlinkhost.mydomain.com:8243/sl/analysis/job/15`): – The Analysis Overview page is updated periodically, and will clearly indicate success or failure. Successful completion of the **Site Acceptance Test (SAT)** indicates that SMRT Link analysis is working correctly. It shows that the analysis was configured and started via the browser GUI, through the SMRT Link Services, and dispatched jobs to the HPC cluster (if distributed mode was configured during installation).
9	**(Optional) Configure LDAP:** See "Configuring LDAP" on page 12 for details.
10	**(Optional) Configure SMRT Link to use a Signed SSL Certificate:** See "SMRT® Link and SSL Certificate Procedures" on page 15 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 11 for details.

Upgrading SMRT® Link

Supported Upgrade Path

- SMRT Link upgrades to v9.0 are supported from any v8.xx release.
- You **cannot** upgrade to SMRT Link from SMRT Analysis v2.3.0 or earlier. Additionally, analysis job directories and run history from SMRT Analysis v2.3.0 or earlier are **not** compatible with SMRT Link and **cannot** be imported.

SMRT Link v9.0 can be used with three versions of ICS:

- v8.0.0.78867 (Sequel II System)
- v8.0.0.84541 (Sequel System)
- v9.0.0.92233 (Sequel II Systems)

Step	Upgrading SMRT Link
1	**Download SMRT Link software:** Download and extract the SMRT Link software installer from http://www.pacb.com/support/software-downloads.
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 `$SMRT_ROOT`, define a convenience variable in the shell so the commands below may be run verbatim. To do so, use something like: `SMRT_ROOT=/opt/pacbio/smrtlink` The fully qualified version of the SMRT Link Install Host may always be used in place of the short host name. But in some cases, particularly when working with WSO2, the fully qualified domain name is required.
3	Log onto the SMRT Link Install Host (such as the hostname or IP address) as the SMRT Link Install User (such as `$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_9.0.0.92188.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_9.0.0.92188.run --rootdir $SMRT_ROOT --upgrade --no-extract`
	See “Appendix A: SMRT Link Workflow Terminology” on page 20 for additional information.

6	**Start the SMRT Link services:** `$SMRT_ROOT/admin/bin/services-start`
7	**Run the Site Acceptance Test from the command line:** `$SMRT_ROOT/admin/bin/run-sat-services` Successful completion of `run-sat-services`, which produces a Site Acceptance Test (SAT) analysis job in the SMRT Analysis module of the SMRT Link GUI, indicates that the HPC configuration is functioning correctly.

Step	Upgrading SMRT Link
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** droplist, then check **Cached images and files**. Click **Clear data**. 2. Restart the browser.
9	**Run the Site Acceptance Test from the browser:** 1. Using the Chrome browser, open SMRT Link at `http://smrtlinkhost:9090`. – The port number should match the `GUI port` defined during installation; the default is `9090`. The URL will redirect to a secure URL at hard-coded port `8243`. If port `9090` is blocked, go directly to the redirect URL at `https://smrtlinkhost.mydomain.com:8243/sl/home`. – Check with your IT group if port `8243` is blocked; access to port `8243` on the SMRT Link Install Host is **required** to access the browser UI and for communication with the instrument. 2. Bypass the Chrome browser's privacy error check: Without an SSL certificate installed, Chrome will issue a "Privacy Error" and state that "Your connection is not private". Bypass by clicking on the **Advanced** link on the bottom left of the page. Then click on the **Proceed to smrtlinkhost.mydomain.com (unsafe)** link. 3. Log in to SMRT Link by entering the Administrator credentials: `admin/admin`. (`admin` is the built-in password, which may have been changed previously.) 4. Submit SMRT Link notification selections: Select options for notifying PacBio of successful installations and for sending ongoing SMRT Link analysis usage information. Click **Save**. 5. Go to the SMRT Analysis page: On the SMRT Link home page (`https://smrtlinkhost.mydomain.com:8243/sl/`), click **SMRT Analysis**. 6. Create a new analysis: Click **+ Create New Analysis**. 7. Select analysis settings and start the analysis: a) Enter `SMRT Link 9.0.0 SAT Test` (or any descriptive name) in the **Analysis Name** field. b) Select **Sequel Data** as the Data Type. c) In the **Data Sets** table, check the box next to `PacBio Tiny SAT Dataset Example`. d) Click **Next**. e) Select **Site Acceptance Test (SAT)** from the Analysis Application drop down list, at the top left. The Reference field is auto-populated with `lambdaNEB`. f) Click **Start** in the top right corner to start the analysis. 8. Wait for the analysis to complete successfully. On the **Analysis Results - SMRT Link 9.0.0 SAT Test** page (Example: `https://smrtlinkhost.mydomain.com:8243/sl/analysis/job/15`): – The Analysis Overview page is updated periodically, and will clearly indicate success or failure. Successful completion of the **Site Acceptance Test (SAT)** indicates that SMRT Link analysis is working correctly. It shows that the analysis was configured and started via the browser GUI, through the SMRT Link Services, and dispatched jobs to the HPC cluster (if distributed mode was configured during installation).
10	**(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 11 for details.

Updating the SMRT Link Bundles Using the SMRT Link GUI

SMRT Link Bundle updates allow updating of SMRT Link features **without** having to reinstall the SMRT Link software. As of SMRT Link v9.0, 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 Run Design modules. The update also updates Sequel® Instrument Control Software (ICS).

SMRT Link UI Bundle

- This includes changes and fixes to the SMRT Link Graphical User Interface.

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

1. In SMRT Link, choose **About SMRT Link** from the Gear menu. (A red circle indicates that one or two 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** droplist, 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 bundle file 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 **Gear > About SMRT Link > 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.  Please 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 (since the bundle information is cached from the initial login).

Installing only SMRT Tools

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

```
smrtlink-*.run --rootdir smrtlink --smrttools-only
smrtlink-*.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** on how to setup JMS integration using `pbcromwell`.

Warning: Sequel/Sequel II instruments **cannot** communicate with a `--smrttools-only` installation.

Updating the SMRT Link Chemistry Bundle for 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 http://www.pacb.com/support/software-downloads.
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-6.0.0.xxxxx
tar -C $ SMRT_ROOT/userdata/chemistry/chemistry-pb-6.0.0.xxxxx -xf /path/to/chemistry-pb-
6.0.0.xxxxx.tar.gz
ln -s ./chemistry-pb-6.0.0.xxxxx $SMRT_ROOT/userdata/chemistry/chemistry-pb-active
```

4. Set/export `$SMRT_CHEMISTRY_BUNDLE_DIR` and validate:

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

5. Export the `$SMRT_CHEMISTRY_BUNDLE_DIR` environment variable in the startup script 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 Sequel/Sequel II Systems 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 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 `admin` and `pbicsuser` passwords, use the following procedure:

```
$SMRT_ROOT/admin/bin/services-stop
$SMRT_ROOT/admin/bin/set-wso2-creds -u admin -p 'NEW-PASSWORD'
$SMRT_ROOT/admin/bin/set-wso2-creds -u pbicsuser -p 'NEW-PASSWORD'
```

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

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

Printing `pbservice` status information and exiting with an exit status of `0` indicates success.

You 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.

Warning: Do **not** change either the `admin` or `pbicsuser` passwords using the WSO2 API Manager (the 'carbon' page), as this is only part of the `set-wso2-creds` script.

Changing Your 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, and asked to enable the sending of SMRT Link analysis usage information to 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 will be 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.

LDAP Integration

SMRT Link supports integration with LDAP for user login authentication. **Without** LDAP integration with SMRT Link, only **one** user (with the login `admin/admin`) is enabled.

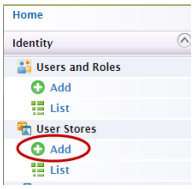
If you are interested in configuring SMRT Link integration with your organization's LDAP, PacBio recommends that you consult your LDAP administrator to help determine the correct LDAP settings.

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

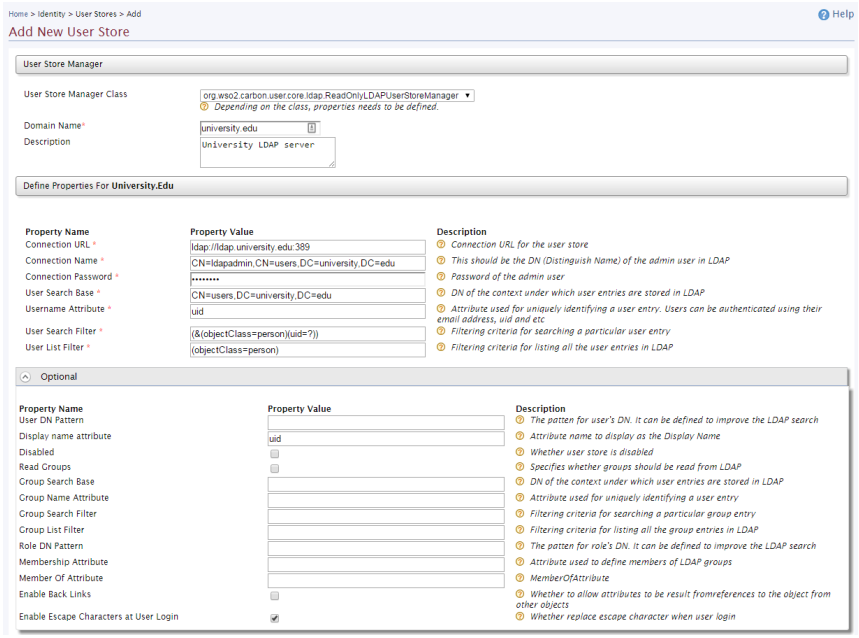
Configuring LDAP

- LDAP is configured **after** SMRT Link v9.0 is installed, using the **WSO2 API Manager** 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/carbon/` where <`hostname`> is the host where SMRT Link is installed.
2. Login using `admin/admin`.
3. Click **User Stores > Add**.



4. Edit the fields as necessary for your site.



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):

- User Store Manager Class: `org.wso2.carbon.user.core.ldap.ReadOnlyLDAPUserStoreManager`
- Domain Name: `university.edu`
- Connection URL: `ldap://ldap.university:389` (The port is **required** in the URI.)
- Connection Name: `CN=ldapadmin,CN=users,DC=university,DC=edu` (This is the bind DN, which is used to authenticate to the LDAP environment.)
- Connection Password: `<password>`
- User Search Base: `CN=users,DC=university,DC=edu`
- Username Attribute: `uid`
- User Search Filter: `(&(objectClass=person)(uid=?))`
- User List Filter: `(objectClass=person)`
- Display name attribute: `uid`

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/wso2/wso2-apigw-errors.log`

Note: If LDAPS needs to be used, simply change the Connection URL to use `ldaps` and adjust the port (LDAPS uses `636` by default). Then, use `keytool` to add the LDAPS public certificate to the `client-truststore.jks` file and force trust if necessary. The `client-truststore.jks` file can be found in the following location:

`$SMRT_ROOT/current/bundles/smrtlink-analysisservices-gui/current/private/pacbio/smrtlink-analysisservices-gui/wso2am-2.0.0/repository/resources/security/client-truststore.jks`

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:

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
Access Sample Setup Module	Y	Y	N
Access Run Design Module	Y	Y	N
Access Run QC Module	Y	Y	Y
Access Data Management Module	Y	Y	Y
Access SMRT Analysis Module	Y	Y	Y

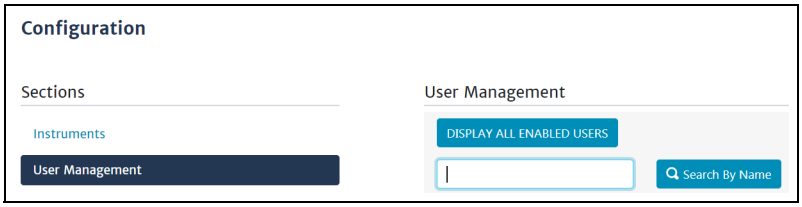
PacBio recommends the following role assignments:

- 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. 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 Run QC, Data Management and SMRT Analysis modules; this is the lowest access level.

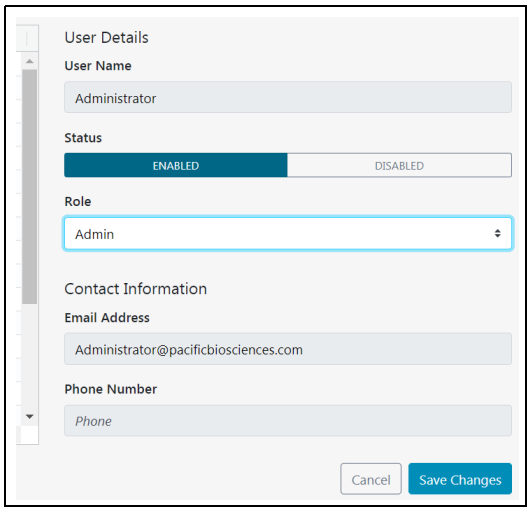
Adding SMRT Link Users and Assigning User Roles

- 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 `http://<hostname>:9090`, where <`hostname`> is the host where SMRT Link is installed.
2. Choose **Configure** from the **Gear** menu and click **User Management**.
3. There are 2 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**. The user now has access to SMRT Link, based on the role just assigned.



SMRT® Link and SSL Certificate Procedures

SMRT Link v9.0 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 Identity Server, 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, sometimes referred to as a "certification authority"). 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 v9.0 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 18 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 be carried over **automatically** when upgrading to SMRT Link v9.0.

Prerequisites

The `keytool` program is supplied with the SMRT Link installation.

Step 1: Obtain a domain-specific certificate from the appropriate Certification Authority.

Step 2: Download the new certificate in `.p12` or `.p7b` format from the DigiCert website `hostname_domain_com.p12`.

Step 3: Combine the certificate and the keystore files:

```
$ keytool -import -trustcacerts -alias server -file ${KEYNAME}.p7b -keystore ${KEYNAME}.jks
Enter keystore password:
Certificate reply was installed in keystore
```

Step 4: Generate an intermediate file in `.pem` format:

```
$ keytool -export -alias server -keystore ${KEYNAME}.jks -file ${KEYNAME}.pem
Enter keystore password:
Certificate stored in file <hostname_nanofluidics_com.pem>
```

Step 5: Generate the WSO2 truststore `client-truststore.jks` file using the `.pem` file:

```
$ keytool -import -alias server -file ${KEYNAME}.pem -keystore client-truststore.jks -storepass
$KEYPW

<Miscellaneous keytool output>

Trust this certificate? [no]:  y
Certificate was added to keystore
```

Step 6: Stop the services by entering `${SMRT_ROOT}/admin/bin/services-stop`.

Step 7: Install the new `.jks` files and update the configuration files:

```
${SMRT_ROOT}/admin/bin/install_ssl_cert.sh ${FQDN} ${KEYSTORE} ${TRUSTSTORE} ${KEYPW}
```

This script will install a signed SSL certificate to SMRT Link, removing the browser warnings that occur when using the default certificate. To run this script, you will need two files in Java Key Store (`.jks`) format:

- One containing the SSL keys and certificate.
- A separate `client-truststore.jks` required by the authentication manager.

Usage: `install_ssl_cert.sh $FQDN $KEYSTORE $TRUSTSTORE $KEYPW` where:

- `$FQDN` is the fully-qualified domain name appropriate to the signed SSL Certificate, such as `smrtlink.university.edu`.
- `$KEYSTORE` is the path to the keystore file generated from the SSL Certificate (`.jks` extension); this will be copied to the SMRT Link installation.
- `$TRUSTSTORE` is the path to `client-truststore.jks`.
- `$KEYPW` is the password used for generating keys.

The FQDN must match the `dnsname` specified in the installer configuration prompts. The shorthand unqualified subdomain name or alias (such as "`smrtlinkhost`") will **not** work because the certificate is for a domain name, **not** an unqualified host name. When running the SMRT Link installer, do this by selecting or specifying the FQDN during the configuration prompts or by passing the arguments `--dnsname $FQDN` to the installer.

Note: If you are using LDAP authentication, the `BIND distinguishedName` account password is stored encrypted with the SSL certificate key, which has now changed. The `BIND distinguishedName service account` password for the LDAP integration **must** be reentered and saved in the WSO2 API Management interface following services startup, for example: `https://smrtlink.pacb.com:9443/carbon`.

Step 8: Start SMRT Link services by entering `$SMRT_ROOT/admin/bin/services-start`.

Step 9: Final Check:

Go to `http://hostname:9090` and login as `admin/admin` (if LDAP is not enabled). Note that SSL is **not** used on the UI port (i.e. `9090`) because this only serves static content; the actual validation of the login credentials occurs over port `8243`, which only uses SSL.

You will be redirected to `https://hostname.domain.com:8243/sl/home`, and should see a padlock sign in front of the URL, indicating that the site is secure.

Viewing a Java Keystore File

The keystore files for SSL certificates are binary files. Use the following command to verify if the same password was used in the SSL certificate generation and install process. If the same password was **not** used in the certificate installation process, this command will give an error. To list the contents of a Java keystore file, use the `keytool -list` command, as shown below:

Usage: `keytool -list -v -keystore keystore.jks`

Example: `keytool -list -v -keystore smrtlink-test_nanofluidics_com.jks`

```
Enter keystore password:
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 1 entry
Alias name: server
Creation date: Feb 13, 2017
Entry type: PrivateKeyEntry
Certificate chain length: 3
Certificate[1]:
Owner: CN=smrtlink-release-test.nanofluidics.com, O="Pacific Biosciences of California, Inc.",
L=Menlo Park,   ST=CA, C=US
Issuer: CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US
```

Errors/logs related to certificate installation can be found here:

```
$SMRT_ROOT/current/bundles/smrtlink-analysisservices-gui/current/private/pacbio/smrtlink-
analysisservices-gui/
```

Installing an Existing Certificate

If you **already** have a complete `.jks` file (suitable for Apache Tomcat, for example), including the signed certificate, you just need to change the alias of the keystore/certificate to `server` using the `keytool` command (`-keyclone` or `-changealias` subcommands).

Set the password to whatever you will supply to the install script in SMRT Link. Then, follow the instructions in "Adding the public key to client-truststore.jks" in https://docs.wso2.com/display/IS500/Creating+New+Keystores again with the same changes.

If you already have the SSL key in a `.jks` file and have obtained a certificate for this key in either PKCS #7 (`.p7b`) or PKCS #12 (`.p12`) Certificate format, the command below is an example of how combine them:

```
$ keytool -import -trustcacerts -alias server -file star.university.edu.p7b -keystore
star.university.edu.jks
```

Then follow the instructions above to generate the `client-truststore.jks` keystore, and finally run the `install _ssl_cert.sh` script as shown in the normal certificate installation process above.

Restoring the Default Self-Signed SSL Certificate

It may sometimes be necessary to uninstall the user-provided SSL certificate and restore the default certificate. The following steps will revert changes made by `$SMRT_ROOT/admin/bin/install_ssl_cert.sh`:

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

2. Check that all SMRT Link processes have terminated by running `ps -ef | grep smrtlink`. Remaining processes should be terminated with `kill <PID>` or `kill -9 <PID>`.

3. Restore backup settings:
   ```
   cd ${SMRT_ROOT}/current/bundles/smrtlink-analysisservices-gui/current/private/pacbio/smrtlink-analysisservices-gui/wso2am-2.0.0/repository
   mv conf conf.new
   mv conf.orig conf
   mv resources/security/client-truststore.jks.orig resources/security/client-truststore.jks
   ```

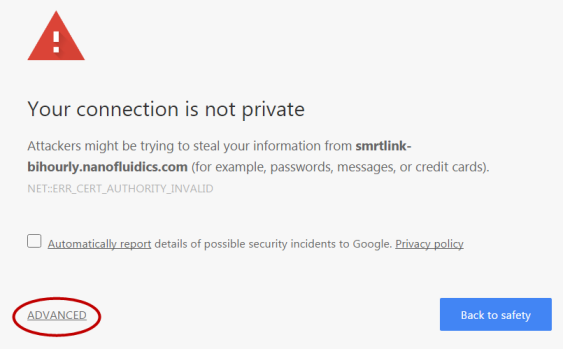
4. Start SMRT Link services:
   ```
   ${SMRT_ROOT}/admin/bin/services-start
   ```

Using SMRT Link with a PacBio Self-Signed SSL Certificate

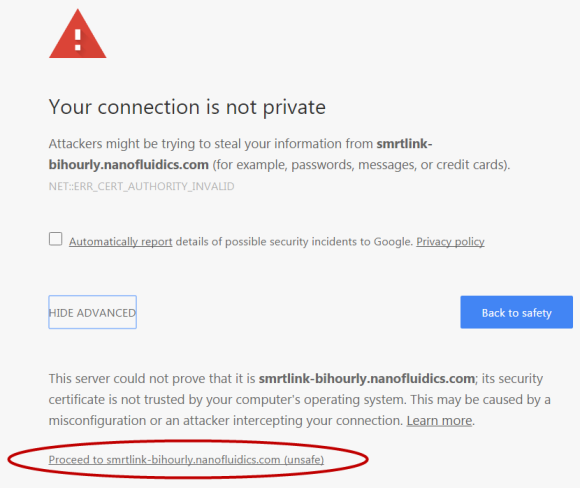
SMRT Link v9.0 ships with a PacBio self-signed SSL Certificate. If your site does **not** have a Signed SSL Certificate **and** you use the self-signed SSL Certificate, **each** user will need to accept the browser warnings related to access in insecure environment. You can also have your IT administrator 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.

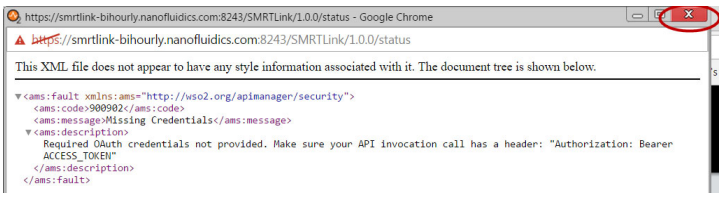
1. The first time you start SMRT Link after installation, you see the following text. Click the **Advanced** link.



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**.

Importing Data into SMRT® Link

If you have a Sequel/Sequel II 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 SMRT Link GUI:

- **Sequel Data**: XML file (`.subreadset.xml`) or ZIP file containing information about Sequel sequence data, such as paths to the BAM files.
- **CCS Data**: XML file (`.consensusreadset.xml`) or ZIP file containing information about CCS sequence data.
- **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.

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.

Importing	Commands

BAM Data Sets Generated by the Sequel/Sequel II System	**Import individual SubreadSet XML files:**
	`$> pbservice import-dataset --host $HOST --port $PORT /path/to/subreads.subreadset.xml`
	Import a directory of SubreadSet XML files:
	`$> pbservice import-dataset --host $HOST --port $PORT /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 a connection 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
```

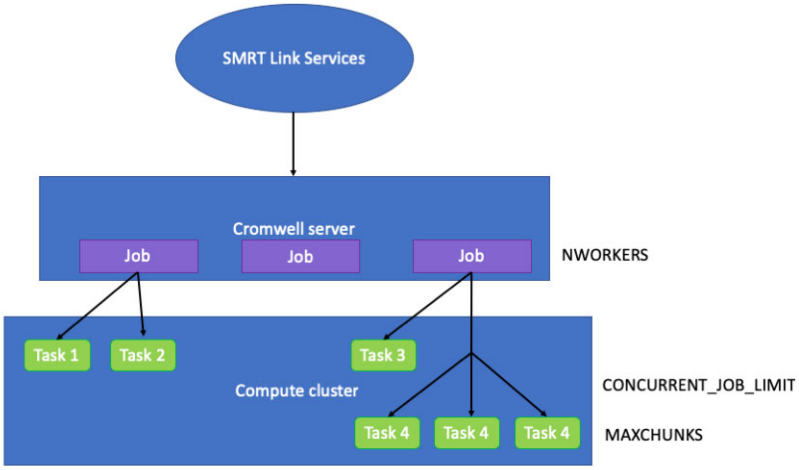
If there is **no** connection to the PacBio Event Server, run the following command to generate a .tgz file and email the file to `support@pacb.com` to file a case:

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

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

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 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.

Appendix C: Sequel System Compute Requirements

Head Node	
Cores	32
RAM	64 GB
tmp_dir (Local Storage)	1 TB recommended, 500 GB minimum
db_datadir (Local Storage)	250 GB
Shared Data Storage	
Sequence Data	40 TB
(Jobs_root) Analysis Data	70 TB
Network	
10 GBE recommended, 1 GBE required	

Compute Nodes			
	Targeted Applications HPC[a]	Targeted Applications PLUS HPC[b]	Whole Genome Applications HPC[c]
Cores (Total)	18	96	384
Minimum RAM per Slot (1 slot = 1 core)	4 GB	4 GB	4 GB/8 GB *de novo* assembly large complex genomes
tmp_dir (Local Storage)	100 GB		

a. Targeted Sequencing applications (LAA, Resequencing), assembly of bacterial genomes, targeted Iso-Seq application. Storage is calculated based on moderate usage of the Sequel® System per year.
b. Targeted Sequencing applications as noted above, plus occasional large-genome *de novo* assemblies, whole- transcriptome Iso-Seq. Storage is calculated based on moderate usage of the Sequel System per year.
c. For a standard CCS sequencing collection (300 GB sequencing data, 11 kb insert size, 30-hours movie), CCS Analysis takes 27 hours on this configuration. SMRT Link will work on less powerful compute configurations, however analysis time will be significantly longer.

Data Examples

Human Assembly CLR Data

- Genome size: 3.3 GB; Sequence data 400 GB; Analysis data 700 GB; Analysis time: 72 hours wall. This is 50-fold coverage human genome analyzed on the compute configuration listed above.

Rice Assembly CLR Data

- Genome size: 0.43 GB; Sequence data 55 GB; Analysis data 90 GB; Analysis time: 20 hours wall. This is 50-fold coverage rice genome analyzed on the compute configuration listed above.

P/N 101-910-100 Version 02 (June 2020)