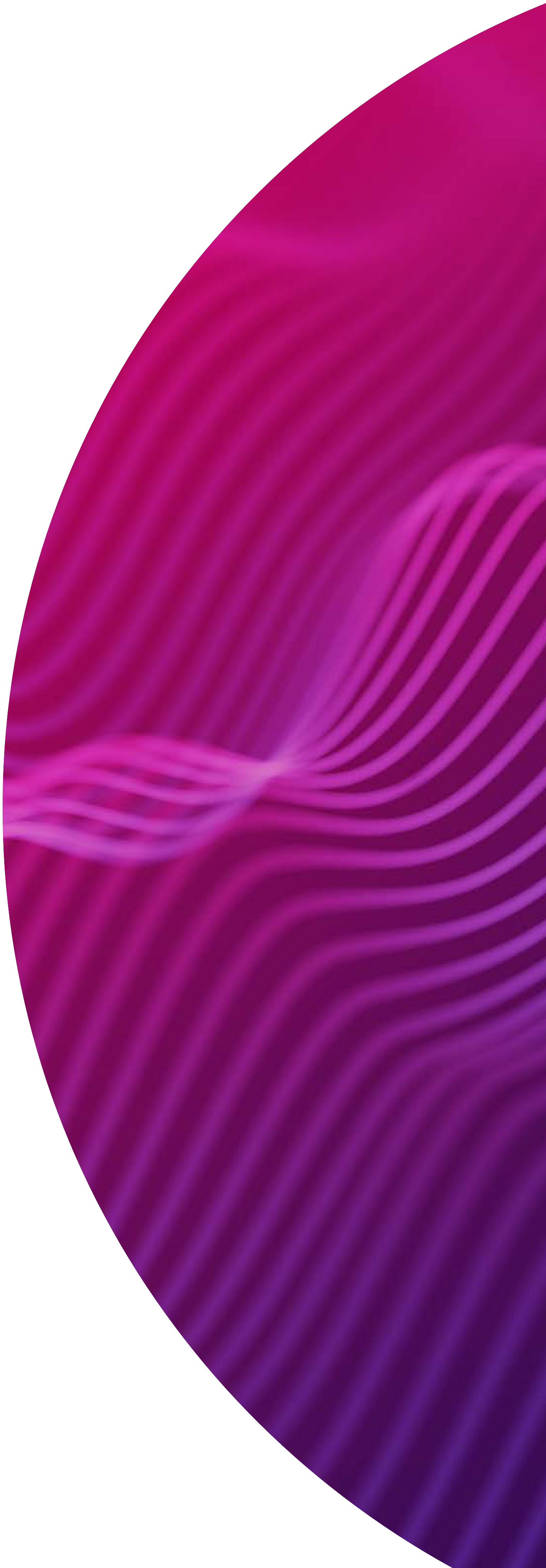
PacBio

SMRT® Link software installation guide (v11.0)



Research use only. Not for use in diagnostic procedures.

P/N 102-278-600 Version 01 (April 2022)

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

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

SMRT® Link software installation guide (v11.0)

Introduction

This document describes the procedure for installing **SMRT Link v11.0**. This document is for Customer IT or SMRT Link administrators.

Note: SMRT Link v11.0 is for use with Sequel® II systems and Sequel IIe systems **only**.

SMRT Link is the web-based end-to-end workflow manager for the Sequel II systems. 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 II and Sequel IIe 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 II platform. The applications include:

- **Sample Setup**: Calculate binding and annealing reactions for preparing DNA samples for use on the Sequel II and Sequel IIe systems.
- **Run Design**: Design runs and create and/or import sample sheets which become available on the Sequel II and Sequel IIe systems.
- **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 II systems are for **research use only** (RUO).

Overview

1. Install or upgrade the SMRT Link software. (See “Installation summary” on page 5 and “Configuring LDAP in WSO2” on page 12 for details.)
2. (**Optional**) Configure SMRT Link to use an SSL certificate. (See “Step 1: Obtain a domain-specific signed certificate from the appropriate Certification Authority.” on page 19 for details.)
3. (**Optional**) Add SMRT Link Users and Assign User Roles. (See “Adding SMRT Link users via LDAP integration and assigning user roles” on page 15 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 systems.

Note: SMRT Link v10.0 and later offer a SMRT Link Cloud deployment option using AWS as an alternative to installing SMRT Link on a local network. For SMRT Link Cloud compute requirements, see the document **SMRT Link Cloud reference guide (v11.0)**.

Sequel IIe system compute requirements

Head node	
Cores	**32**
RAM	**64 GB**
Local Storage	**1 TB SSD/Flash storage**
db_datadir (Local Storage)	**250 GB**
Compute nodes	
Cores (Total)	**64**
Minimum RAM per Slot (1 slot = 1 core)	**> 4 GB**
Local Storage	**100 GB**
Shared data storage	
Sequence Data	**20 TB**[a]
Analysis Data	**40 TB**[a]
Network	
10 GBE recommended, 1 GBE required[b]	

[a] Storage is calculated for one Sequel IIe system, assuming 100 human genomes per year at 30-fold coverage, *de novo* assembly.

[b] This information is specific to the network connection between the SMRT Link head node and the Sequel IIe system.

Notes:

- Single-system compute configurations are available – contact your Pacbio Bioinformatics Field Application Specialist (FAS) for details.
- For **Sequel II** system compute requirements, see "Appendix C: Sequel II system compute requirements" on page 26 for details.

Data storage

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

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

Software prerequisites: Server operating systems

- SMRT Link server software is supported on:
  - English-language CentOS 7.x, supported until end-of-life 6/30/2024.
  - English-language Rocky Linux 8.x supported until end-of-life 5/31/2029.
  - Ubuntu 18.04 and 20.04 64-bit Linux® distributions.
  - These supported versions **also** apply to SMRT Link compute nodes.
- **Note**: PacBio advises **against** new installations of CentOS for use with SMRT Link.
- 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 90 or later.
- SMRT Link **requires** a minimum screen resolution of 1600 by 900 pixels.

Network configuration

- 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 2.17` or greater.
- The installation is performed by the **same** non-root user (`$SMRT_USER`) that will be used to run the SMRT Link web services.
- The `$SMRT_USER` has full permissions recursively throughout the install directory, and in all linked directories for `jobs_root`, `db_datadir` and `tmp_dir`. (Common problems include NFS setup problems, ACLs, and so on.)
- When running in distributed mode, all other nodes have the **same path** for `$SMRT_ROOT` and for all linked directories. (The NFS exports should have identical mount points on **all** cluster nodes.)
- No other daemons/services processes are bound to the same ports as the SMRT Link services.

- PacBio **highly recommends** that the system clock be synchronized to a domain or public NTP time server.
- The `$SMRT_USER` service account **must** have both the `nofile` and `nproc` soft user limits set to a minimum of 8192. (See the `ulimit(1)` and `limits.conf(5)` Linux man pages for more information.)
- The host operating system **must** provide the `en_US.UTF-8` locale/character set.

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. You can also install SMRT Link Cloud on AWS - see **SMRT Link Cloud reference guide (v11.0)** for details.
- Do **not** install SMRT Link or run SMRT Link services as the `root` user.

SMRT Link v11.0 security notes

SMRT Link v11.0 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.

Starting in v11.0, the WSO2 API Manager can be replaced by a new API gateway that combines the KrakenD, Keycloak, and NGINX servers to provide a nearly identical API and user experience. Some additional setup is required after the installation to use this option. No changes to connected Sequel II systems/Sequel IIe systems are necessary. This new API Gateway will be the default in future SMRT Link releases.

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 Sequel Instrument Control Software (ICS), so it must be accessible to **any** Sequel II systems as well.

- If your network configuration already allows access to port `8243`, **no additional changes** are required to use SMRT Link v11.0.
- 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 `$SMRT_ROOT` directory.
- A service account (called the `$SMRT_USER` in this document) to install and run the web services.
- Full path to the installation root directory, used for the main installation root.
- Job Management System settings.
- Full path to a directory on the shared file system - the `jobs_root` directory.
- Full path to a directory on the local file system on each node - the `tmp_dir` directory.
- Full path to a directory on the local file system on the install node - the `db_datadir` directory.
- **(Optional)** LDAP settings. See "Configuring LDAP in WSO2" on page 12 for details.
- **(Optional)** SSL certificate for WS02 or NGINX. See "SMRT® Link and SSL certificate procedures" on page 18 for details.

Installation summary

Following are the steps for installing SMRT Link v11.0 on a **new** system. (See “Appendix A: SMRT Link workflow terminology” on page 24 for details.) To upgrade SMRT Link to v11.0 from a **previous version**, follow the upgrade steps on Page 7.

SMRT Link v11.0 can be used with the following supported version of ICS:

- v11.0 (Sequel II systems and Sequel IIe systems)

SMRT Link installation options

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

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

[a] JMS integration on a SMRT Tools-only installation may be setup using `pbcromwell`. See **SMRT Tools reference guide (v11.0)** for more information.

Step	Installation summary - SMRT Link v11.0
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 `$SMRT_ROOT`, defining the variable in the shell allows the commands below to be run verbatim. To do so, use something like: `SMRT_ROOT=/opt/pacbio/smrtlink` The fully-qualified domain name of the SMRT Link Install Host may always be used in place of the short host name. But in some cases, particularly when working with WSO2, the fully-qualified domain name is required.
3	Log onto the SMRT Link Install Host (such as the hostname or IP address) as the SMRT Link Install User (such as `$SMRT_USER`.)

4	**Install SMRT Link by invoking the SMRT Link Installer:**
	`./smrtlink_<version number>.run --rootdir $SMRT_ROOT`
	Note: The `$SMRT_ROOT` directory must **not** exist when the installer is invoked, as the installer will try to create it, and will abort the installation if an existing `$SMRT_ROOT` location is found.
	If a previous installation was canceled or otherwise failed, the installer can be invoked **without** extraction. Rerun using the `--no-extract` option:
	`./smrtlink_<version number>.run --rootdir $SMRT_ROOT --no-extract`
	See “Appendix A: SMRT Link workflow terminology” on page 24 for additional information.

Step	Installation summary - SMRT Link v11.0

5	**Start SMRT Link services:**
	`$SMRT_ROOT/admin/bin/services-start`
	Optionally, you can now migrate to the new API gateway:
	`$SMRT_ROOT/admin/bin/services-start --migrate`
	The migration launches an interactive CLI tool after the server starts; as this is a new installation very few steps are required. Once migration is finished, SMRT Link automatically starts with the new API gateway in the future.

6	**Run the Site Acceptance Test from the command line:** `$SMRT_ROOT/admin/bin/run-sat-services` Successful completion of `run-sat-services` indicates that the HPC configuration is functioning correctly. This creates a “PacBio Example SAT Job” analysis entry in the SMRT Analysis section of the SMRT Link GUI.
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** control, then check **Cached images and files**. Click **Clear data**. 2. Restart the browser.
8	**(Optional) Configure LDAP and/or add local users:** See “Configuring LDAP in WSO2” on page 12, “Adding local users to SMRT Link using WSO2” on page 16 for details.
9	**(Optional) Configure SMRT Link to use a signed SSL certificate:** See “Installing an existing certificate” on page 21 for details.
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.

Upgrading SMRT® Link

Supported upgrade path

- SMRT Link upgrades to v11.0 are supported from any v8.x, v9.x or v10.x releases.
- 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 v11.0 can be used with the following supported version of ICS:
  – v11.0 (Sequel II systems and Sequel IIe systems)

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

5	**Upgrade SMRT Link by invoking the SMRT Link installer:**
	`./smrtlink_<version number>.run --rootdir $SMRT_ROOT --upgrade`
	Note: The `$SMRT_ROOT` directory must be an existing SMRT Link installation. Several validation steps will occur to ensure that a valid `$SMRT_ROOT` is being updated.
	If a previous upgrade was canceled or otherwise failed, the installer can be invoked **without** extraction. Rerun using the `--no-extract` option:
	`./smrtlink_<version number>.run --rootdir $SMRT_ROOT --upgrade --no-extract`
	See “Appendix A: SMRT Link workflow terminology” on page 24 for additional information.

6	**Start the SMRT Link services:**
	`$SMRT_ROOT/admin/bin/services-start`
	Optionally, you can now migrate to the new API gateway:
	`$SMRT_ROOT/admin/bin/services-start --migrate`
	The migration launches an interactive CLI tool after the server starts; as this is a new installation very few steps are required. Once migration is finished, SMRT Link automatically starts with the new API gateway in the future.

Step	Upgrading SMRT Link
7	**Run the Site Acceptance Test from the command line:** `$SMRT_ROOT/admin/bin/run-sat-services` Successful completion of `run-sat-services` indicates that the HPC configuration is functioning correctly. This creates a “PacBio Example SAT Job” analysis entry in the SMRT Analysis section of the SMRT Link GUI.
8	**(Optional) Clear the browser cache:** This is a good troubleshooting step if needed. 1. Open the Chrome Browser and choose **More Tools > Clear browsing data**, choose **All Time** from the **Time Range** control, then check **Cached images and files**. Click **Clear data**. 2. Restart the browser.
9	**(Optional) 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 Chemistry and UI Bundles

SMRT Link Bundle updates allow updating of SMRT Link features **without** having to reinstall the SMRT Link software. As of SMRT Link v11.0, 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 (GUI).

Updating the SMRT Link Bundles from SMRT Link

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

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

Updating the SMRT Link Chemistry Bundle on the instrument

The SMRT Link Chemistry Bundle will also need to be upgraded with the same Chemistry Bundle files used by the SMRT Link web services. Once SMRT Link's Chemistry Bundle is updated, the updates are passed along to any PacBio instruments configured to use that same instance of SMRT Link. Once available, follow the instructions below to update the Chemistry Bundle on the instrument side.

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

Rolling back a SMRT Link UI Bundle update

SMRT Link UI Bundle updates allow updating of SMRT Link UI features **without** having to reinstall the SMRT Link software. This includes changes and bug fixes to the SMRT Link graphical user interface. When you upgrade the SMRT Link UI by clicking **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.  Note that you will need to re-login to the
SMRT Link UI for this to take effect.

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

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

Installing only SMRT Tools

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

```
    ./smrtlink-11.0.0.xxxxx.run --rootdir smrtlink --smrttools-only
    ./smrtlink-11.0.0.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 (v11.0)** on how to setup JMS integration using `pbcromwell`.

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

Updating the SMRT Link Chemistry Bundle on smrttools-only installations

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

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

1. Download the Chemistry Bundle from 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-10.0.0.xxxxx
tar -C $ SMRT_ROOT/userdata/chemistry/chemistry-pb-10.0.0.xxxxx -xf /path/to/chemistry-pb-
11.0.0.xxxxx.tar.gz
ln -s ./chemistry-pb-11.0.0.xxxxx $SMRT_ROOT/userdata/chemistry/chemistry-pb-active
```

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

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

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

Changing admin and pbicsuser passwords

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

SMRT Link comes with a default Instrument Control Software (ICS) user account (`pbicsuser`) which is used by the 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 LDAP account or a local account on the Linux system.)

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

To change the `admin` and `pbicsuser` passwords for WSO2 API Manager, 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’
```

If you are using the new API gateway, use the following procedure:

```
$SMRT_ROOT/admin/bin/services-stop
$SMRT_ROOT/admin/bin/set-keycloak-creds -u admin -p ‘NEW-PASSWORD’
$SMRT_ROOT/admin/bin/set-keycloak-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
```

The `pbservice` status information should display, before exiting with an exit status of `0` indicating 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: When using WSO2, **only** use the `set-wso2-creds` script to change the password for those accounts.

Note: If you are using the new API gateway, you can use the Keycloak administration interface to change both passwords.

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 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.

Starting SMRT Link automatically on server boot

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

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

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

LDAP integration

SMRT Link supports integration with LDAP for user login authentication, as well as using local WSO2 users that exist **only** within SMRT Link.

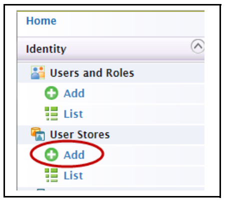
If you are interested in configuring SMRT Link integration with your organization’s LDAP, PacBio recommends that you consult your LDAP administrator to help determine the correct LDAP settings.

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

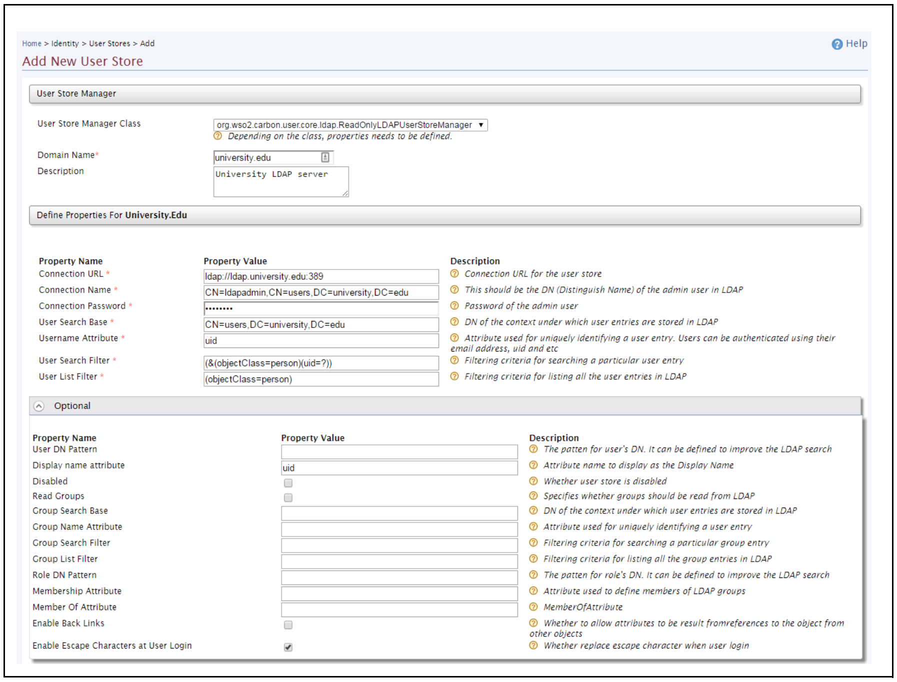
Configuring LDAP in WSO2

- LDAP is configured **after** SMRT Link v11.0 is installed, using the **WSO2 API Manager** software, as shown below. If you have migrated to the new API gateway, see instructions below for configuring the Keycloak server.
- 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.



Add New User Store

User Store Manager

User Store Manager Class	org.wso2.carbon.user.core.ldap.ReadOnlyLDAPUserStoreManager ▾ *Depending on the class, properties needs to be defined.*
Domain Name*	university.edu
Description	University LDAP server

Define Properties For **University.Edu**

Property Name	Property Value	Description
Connection URL *	ldap://ldap.university.edu:389	*Connection URL for the user store*
Connection Name *	CN=ldapadmin,CN=users,DC=university,DC=edu	*This should be the DN (Distinguish Name) of the admin user in LDAP*
Connection Password *	••••••••	*Password of the admin user*
User Search Base *	CN=users,DC=university,DC=edu	*DN of the context under which user entries are stored in LDAP*
Username Attribute *	uid	*Attribute used for uniquely identifying a user entry. Users can be authenticated using their email address, uid and etc*
User Search Filter *	(&(objectClass=person)(uid=?))	*Filtering criteria for searching a particular user entry*
User List Filter *	(objectClass=person)	*Filtering criteria for listing all the user entries in LDAP*

Optional

Property Name	Property Value	Description
User DN Pattern		*The patten for user's DN. It can be defined to improve the LDAP search*
Display name attribute	uid	*Attribute name to display as the Display Name*
Disabled	☐	*Whether user store is disabled*
Read Groups	☐	*Specifies whether groups should be read from LDAP*
Group Search Base		*DN of the context under which user entries are stored in LDAP*
Group Name Attribute		*Attribute used for uniquely identifying a user entry*
Group Search Filter		*Filtering criteria for searching a particular group entry*
Group List Filter		*Filtering criteria for listing all the group entries in LDAP*
Role DN Pattern		*The patten for role's DN. It can be defined to improve the LDAP search*
Membership Attribute		*Attribute used to define members of LDAP groups*
Member Of Attribute		*MemberOfAttribute*
Enable Back Links	☐	*Whether to allow attributes to be result fromreferences to the object from other objects*
Enable Escape Characters at User Login	☑	*Whether replace escape character when user login*

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 URL.)
- 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`

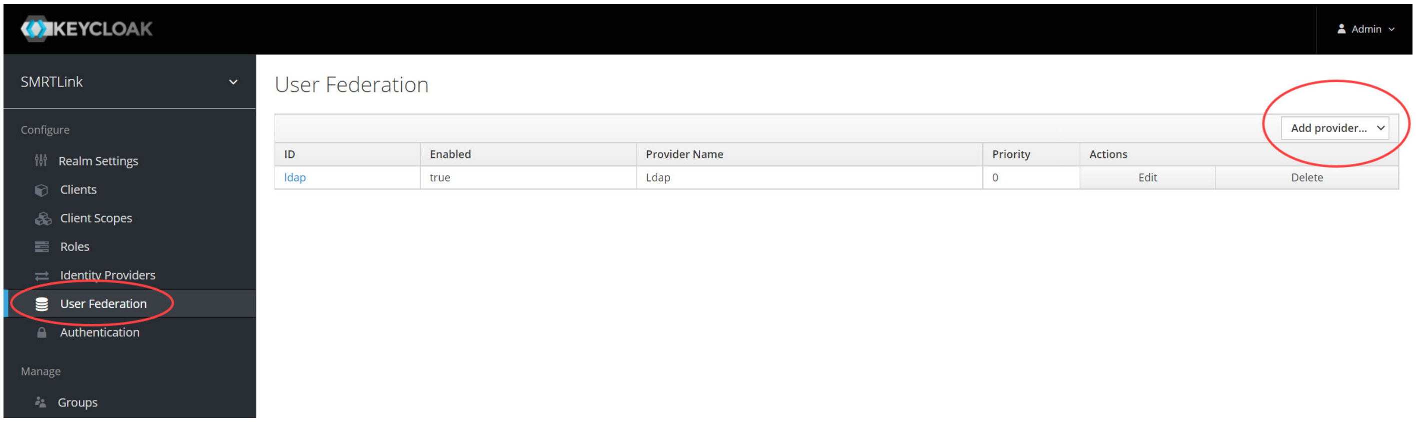
The `client-truststore.jks` file can be found in the following location:

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

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 X.509-formatted public certificate to the `client-truststore.jks` file and enter `yes` to force trust when prompted.

Configuring LDAP in Keycloak

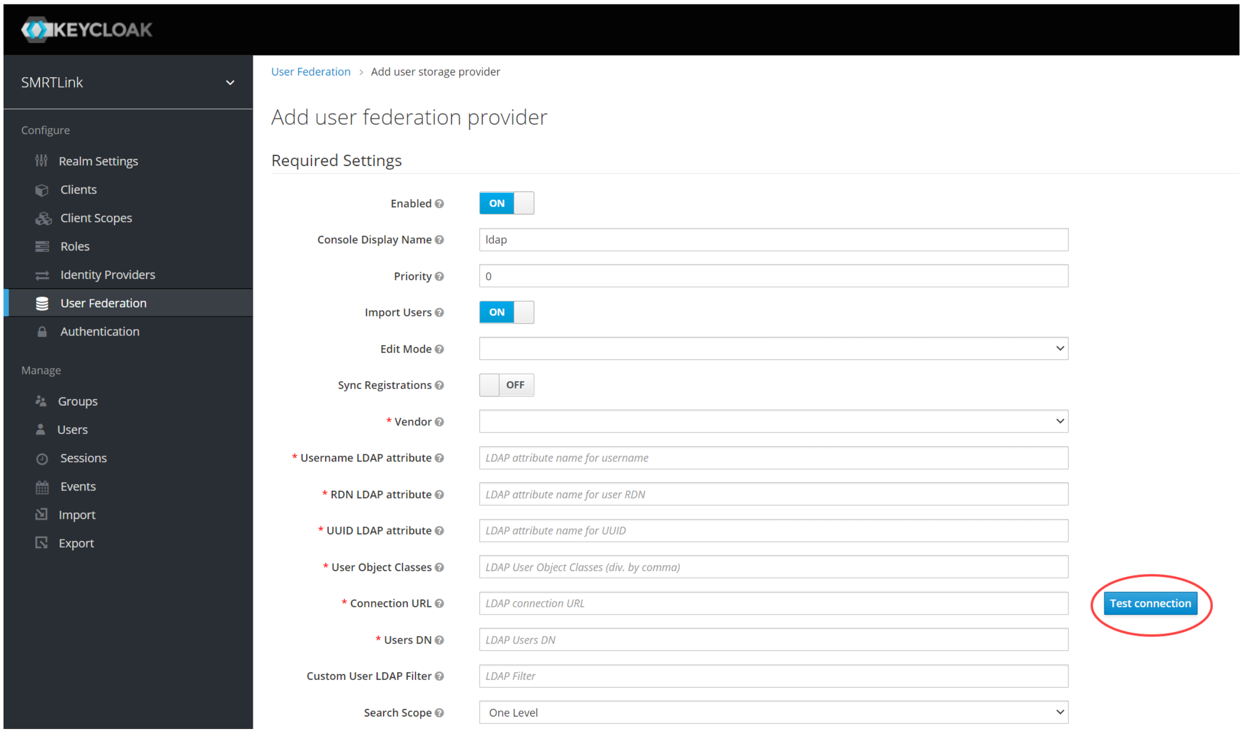
1. Enter the following in your browser: `https://<hostname>:9443/auth/admin/` where `<hostname>` is the host where SMRT Link is installed.
2. Login using `admin/admin` (unless you have changed the password).
3. Under **Configure** on the left hand side of the window, click **User Federation**.



User Federation

ID	Enabled	Provider Name	Priority	Actions	
ldap	true	Ldap	0	Edit	Delete

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.

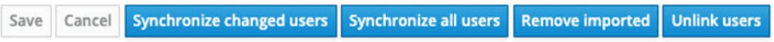


Add user federation provider

Required Settings

Enabled: ON
Console Display Name: ldap
Priority: 0
Import Users: ON
Edit Mode:
Sync Registrations: OFF
* Vendor:
* Username LDAP attribute: LDAP attribute name for username
* RDN LDAP attribute: LDAP attribute name for user RDN
* UUID LDAP attribute: LDAP attribute name for UUID
* User Object Classes: LDAP User Object Classes (div. by comma)
* Connection URL: LDAP connection URL
* Users DN: LDAP Users DN
Custom User LDAP Filter: LDAP Filter
Search Scope: One Level

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.

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.

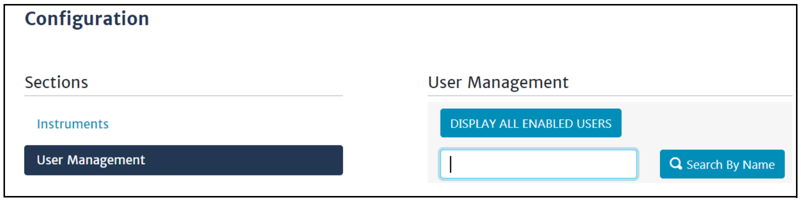
Note: The Admin role only allows a user account to administer the configuration options available through the SMRT Link browser UI. It does **not** provide access to the WSO2 API Management interface, which is intentionally restricted to the built-in admin user **only**.

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 **Configure** from the **Gear** menu and click **User Management**.
3. There are 2 ways to find users:

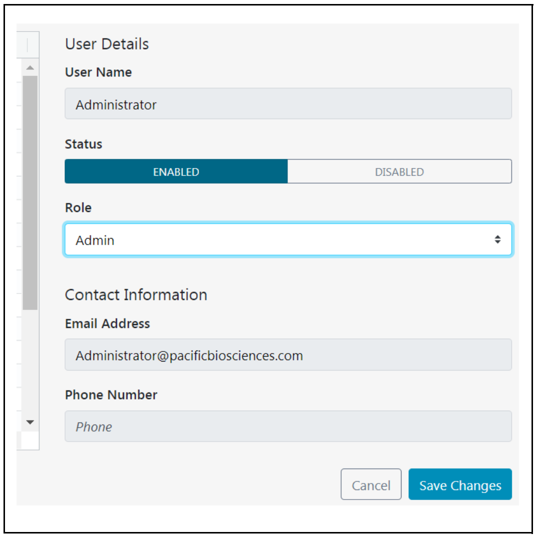
- **To display all SMRT Link users**: Click **Display all Enabled Users**.
- **To find a specific user**: Enter a user name, or partial name and click **Search By Name**.



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.



User Details

User Name: Administrator

Status: ENABLED | DISABLED

Role: Admin

Contact Information

Email Address: Administrator@pacificbiosciences.com

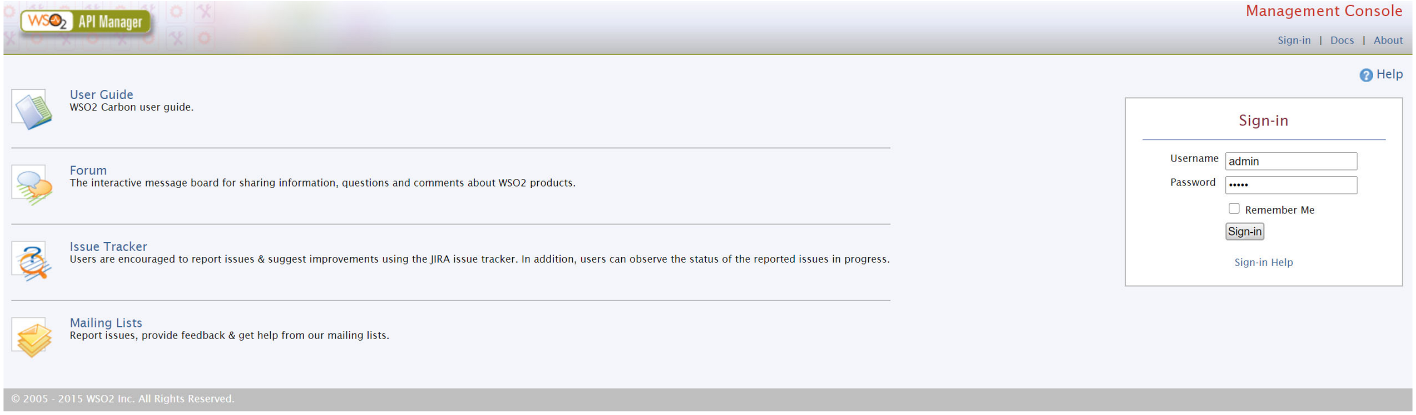
Phone Number: Phone

Adding local users to SMRT Link using WSO2

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 WSO2 API Manager that handles authentication and API access.

To add a local account:

1. Access the WSO2 management console at https://<servername>:9443/carbon and log in with SMRT Link's built-in admin account credentials (`admin/admin` by default.)



User Guide
WSO2 Carbon user guide.

Forum
The interactive message board for sharing information, questions and comments about WSO2 products.

Issue Tracker
Users are encouraged to report issues & suggest improvements using the JIRA issue tracker. In addition, users can observe the status of the reported issues in progress.

Mailing Lists
Report issues, provide feedback & get help from our mailing lists.

Sign-in

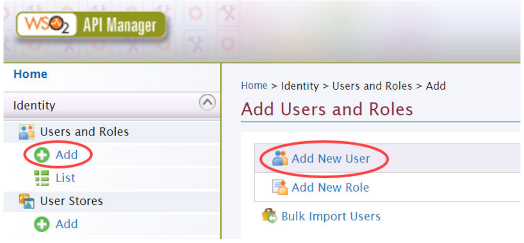
Username: admin

Password: •••••

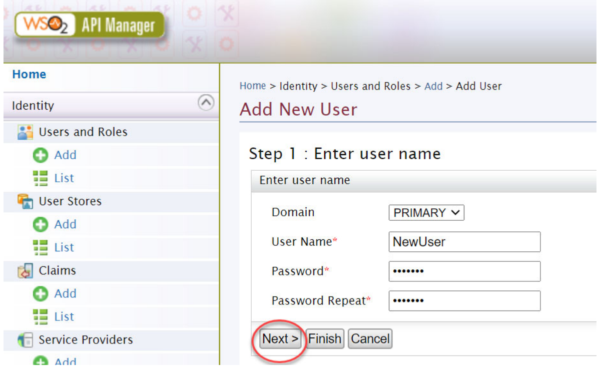
□ Remember Me

© 2005 - 2015 WSO2 Inc. All Rights Reserved.

2. On the left-hand menu, under **Claims,** click **List.**
3. Click the item labeled **http://wso2.org/claims**.
4. Scroll to the bottom, find **Username**, then click **Edit**.
5. Check the box **Supported by Default**, then click **Update**.The **Username** field will display as part of the local user profile.
6. Under **Users and Roles**, click **+ Add**, then click **Add New User**.



7. Enter the User ID and password of the new user, then click **Next**. (Make sure to use a unique password for the User ID that is **not** used elsewhere.)

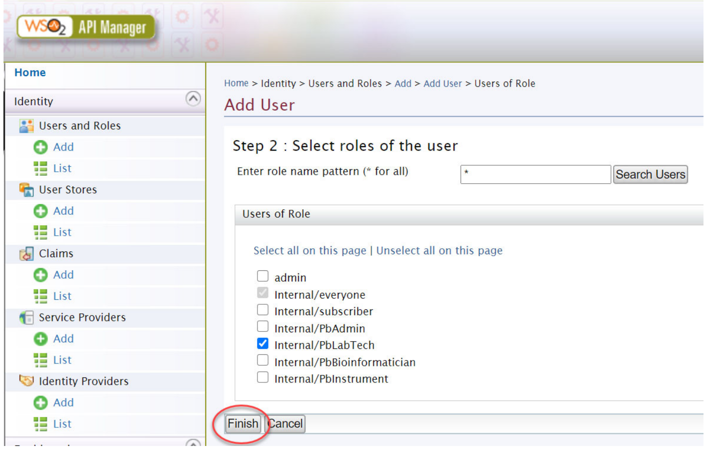


Step 1 : Enter user name

Enter user name

Domain	PRIMARY
User Name*	NewUser
Password*	•••••••
Password Repeat*	•••••••

8. Select the appropriate role for the new user. (See “Adding SMRT Link users via LDAP integration and assigning user roles” on page 15 for details.) Click **Finish** to register the new user.



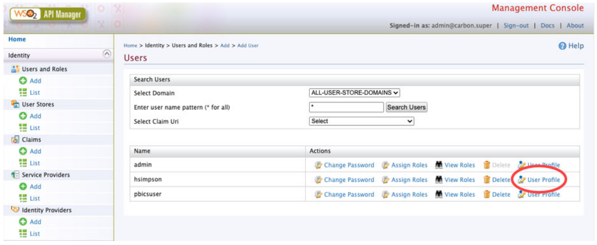
Step 2 : Select roles of the user

Enter role name pattern (* for all) *

Users of Role

- □ admin
- ☑ Internal/everyone
- □ Internal/subscriber
- □ Internal/PbAdmin
- ☑ Internal/PbLabTech
- □ Internal/PbBioinformatician
- □ Internal/PbInstrument

9. (**Recommended**) Click **User Profile** for the new user, then click **Add New Profile**.



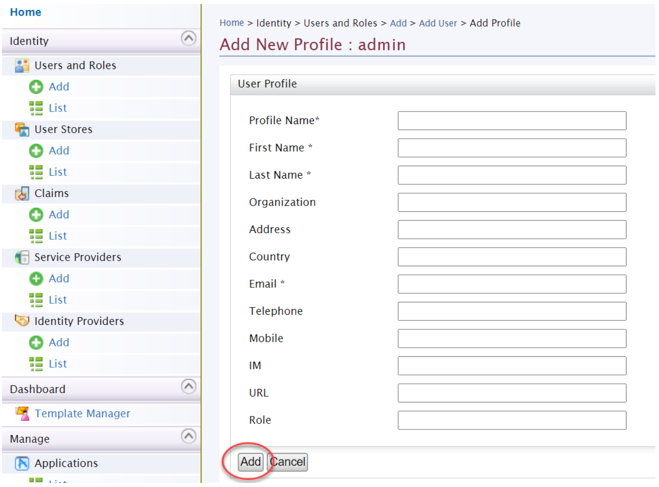
Signed-in as: admin@carbon.super

Search Users

Select Domain	ALL-USER-STORE-DOMAINS
Enter user name pattern (* for all)	*
Select Claim Uri	Select

Name	Actions
admin	Change Password Assign Roles View Roles Delete User Profile
hsimpson	Change Password Assign Roles View Roles Delete User Profile
pbicsuser	Change Password Assign Roles View Roles Delete User Profile

10. Enter user information such as name and email address. The starred fields are used by the SMRT Link UI user management features. **Note**: Filling in the **Username** field is **required** for the user search in the Configuration and Project pages to find local users.
11. Click **Add**.



Home > Identity > Users and Roles > Add > Add User > Add Profile

Add New Profile : admin

User Profile

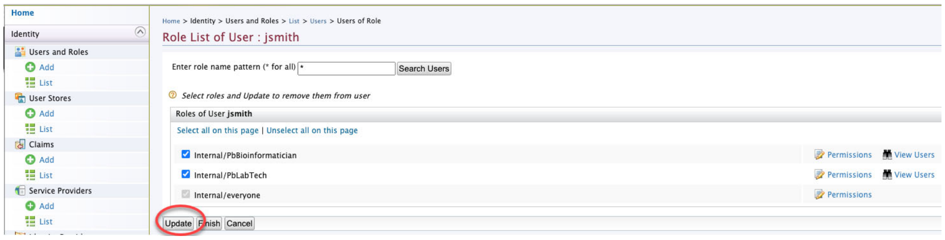
Profile Name*
First Name *
Last Name *
Organization
Address
Country
Email *
Telephone
Mobile
IM
URL
Role

12. Click **Sign-out**. The new user can then log into SMRT Link using the credentials just added.

Ensuring that SMRT Link users are assigned only one role

In some cases, changing a user's role in SMRT Link can cause that user to have **multiple** WSO2 roles. That can lead to accounts remaining enabled when an administrator tries to disable the user. Disabling a user with multiple roles may also still leave the user active. To ensure that users are only assigned **one** role:

1. Access the WSO2 management console at https://<servername>:9443/carbon and log in with your site administrator credentials.
2. Under **Users and Roles**, click **List** and find the user in question.
3. Click **View Roles**.
4. Uncheck one of the redundant roles and click **Update**.



Home > Identity > Users and Roles > List > Users > Users of Role

Role List of User : jsmith

Enter role name pattern (* for all) *

Select roles and Update to remove them from user

Roles of User **jsmith**

☑ Internal/PbBioinformatician
☑ Internal/PbLabTech
☑ Internal/everyone

SMRT® Link and SSL certificate procedures

SMRT Link v11.0 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 v11.0 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 22 for details on how to handle the security warnings when accessing SMRT Link.

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

Note: If you have **already** setup an SSL certificate in SMRT Link v4.0.0 or later, those settings will be carried over **automatically** when upgrading to SMRT Link v11.0.

Installing an SSL certificate for WSO2

Prerequisites: The `keytool` program is supplied with the SMRT Link installation, and can be found here: `$SMRT_ROOT/admin/bin/keytool`.

Step 1: Obtain a domain-specific signed 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 CA signed certificate and the keystore key that was generated alongside the CSR:

```
$ 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_domain_com.pem>
```

Step 5: Import the `.pem` file into the `client-truststore.jks`, which will be created if it does not exist:

```
$ 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 installs a CA-signed SSL certificate to SMRT Link, removing the browser warnings that occur when using the default certificate. To run this script, you will need the fully-qualified domain name of the SMRT Link server, the two private/public keystore files in Java Key Store (`.jks`) format, and the common passphrase used for the key and both keystores. The two keystores include:

- A domain-specific keystore, containing the encryption keys and private CA certificate.
- A separate `client-truststore.jks` required by the authentication manager.

Usage: `${SMRT_ROOT/admin/bin/install_ssl_cert.sh $FQDN $KEYSTORE $TRUSTSTORE $KEYPW` where the four required arguments include:

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

The FQDN **must** match the `dnsname` specified in the SMRT Link configuration. The shorthand unqualified subdomain name, hostname, or alias (such as "`smrtlinkhost`" and not the FQDN of "`smrtlink.university.edu`") will **not** work because the certificate is configured to match a specific fully-qualified domain name, and **not** an unqualified host name. When running the SMRT Link installer, the FQDN is set during the installer's 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 (`https://smrtlink.example.com:9443/carbon`.)

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

Step 9: Final check:

Go to `https://hostname.domain.com:8243/sl/home` and login as `admin/admin` (if LDAP is not enabled). You should see a padlock sign in front of the URL. This indicates that the CA certificate was validated and that the site is secure. This may require clearing the browser cache.

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_example_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.example.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/userdata/log/smrtlink-analysisservices-gui/wso2/
```

Installing an existing certificate

If you **already** have a complete `.jks` file (suitable for Apache Tomcat in a Java Key Store format), 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 above certificate installation steps.

Restoring the default WSO2 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 ./cert-config.backup/orig/conf./conf
   mv ./resources/security/client-truststore.jks ./resources/security/client-truststore.jks.save
   mv ./cert-config.backup/orig/resources/security/client-truststore.jks./resources/security/
   client-truststore.jks
   ```

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

Installing an SSL certificate for NGINX

In the new API gateway, SSL transport is handled by the NGINX web server, which uses a much 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
   ```

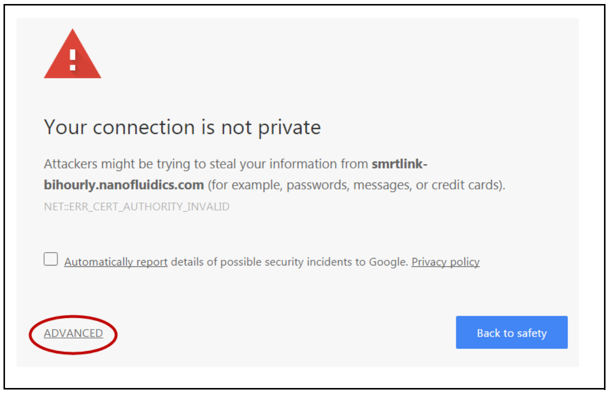
2. Copy the certificate and private key files to these paths:
```
$SMRT_ROOT/userdata/config/security/smrtlink-site.crt
$SMRT_ROOT/userdata/config/security/smrtlink-site.key
```
3. Start SMRT Link services:
```
${SMRT_ROOT}/admin/bin/services-start
```

Using SMRT Link with a PacBio self-signed SSL certificate

SMRT Link v11.0 uses self-signed SSL certificate provided by PacBio. 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.



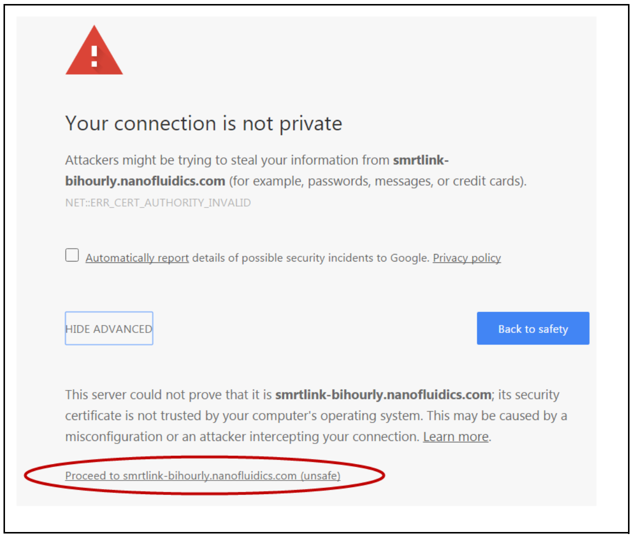
Your connection is not private

Attackers might be trying to steal your information from **smrtlink-bihourly.nanofluidics.com** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically report details of possible security incidents to Google. Privacy policy

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



Your connection is not private

Attackers might be trying to steal your information from **smrtlink-bihourly.nanofluidics.com** (for example, passwords, messages, or credit cards).

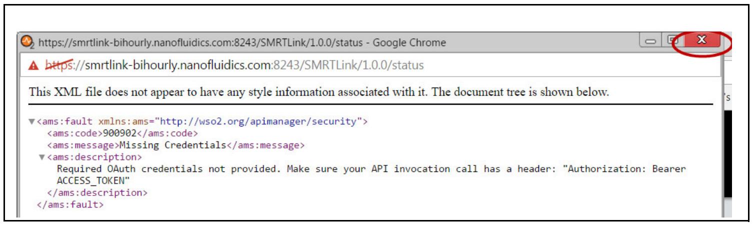
NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically report details of possible security incidents to Google. Privacy policy

This server could not prove that it is **smrtlink-bihourly.nanofluidics.com**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.

Proceed to smrtlink-bihourly.nanofluidics.com (unsafe)

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



https://smrtlink-bihourly.nanofluidics.com:8243/SMRTLink/1.0.0/status - Google Chrome
https://smrtlink-bihourly.nanofluidics.com:8243/SMRTLink/1.0.0/status

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<ams:fault xmlns:ams="http://wso2.org/apimanager/security">
   <ams:code>900902</ams:code>
   <ams:message>Missing Credentials</ams:message>
  ▼<ams:description>
     Required OAuth credentials not provided. Make sure your API invocation call has a header: "Authorization: Bearer
     ACCESS_TOKEN"
   </ams:description>
 </ams:fault>
```

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

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

- **Continuous Long Reads**: XML file (`.subreadset.xml`) or ZIP file containing information about subreads from Sequel II systems, such as paths to the BAM files.
- **HiFi reads**: XML file (`.consensusreadset.xml`) or ZIP file containing information about HiFi reads (reads generated with CCS analysis whose quality value is equal to or greater than 20.)
- **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 or by using the `$PB_SERVICE_HOST` and `$PB_SERVICE_PORT` environment variables.
- If using the authenticated port 8243, valid user credentials must also be supplied. Use the `--user` and `--password` switches (or `--ask-pass`), or set the `$PB_SERVICE_AUTH_USER` and `$PB_SERVICE_AUTH_PASSWORD` environment variables to specify the credential details.

Importing	Commands

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

Sending log files to Technical Support

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

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

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

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

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

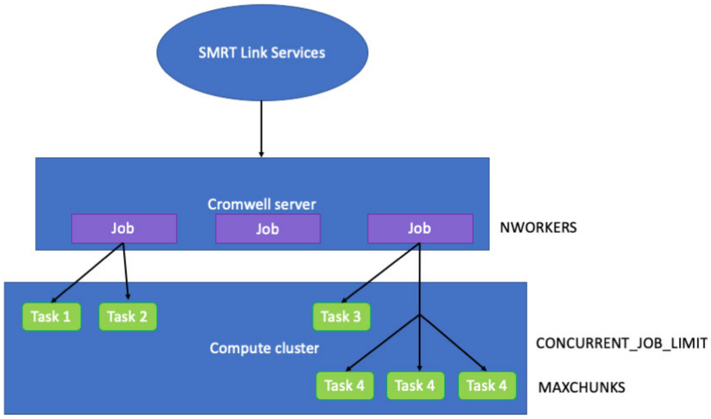
```
$SMRT_ROOT/admin/bin/tsreport-install --bundle
```

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

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

Appendix A: SMRT Link workflow terminology

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



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

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

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

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

Appendix B: Distributed computing setup

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

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

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

For more information on customizing all of the 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 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.