Oxford Nanopore Technologies

PROTOCOL

Q-Line sequencing software installation and maintenance guide

V Q_SSI_revB_25Feb2025

FOR RESEARCH USE ONLY

Contents

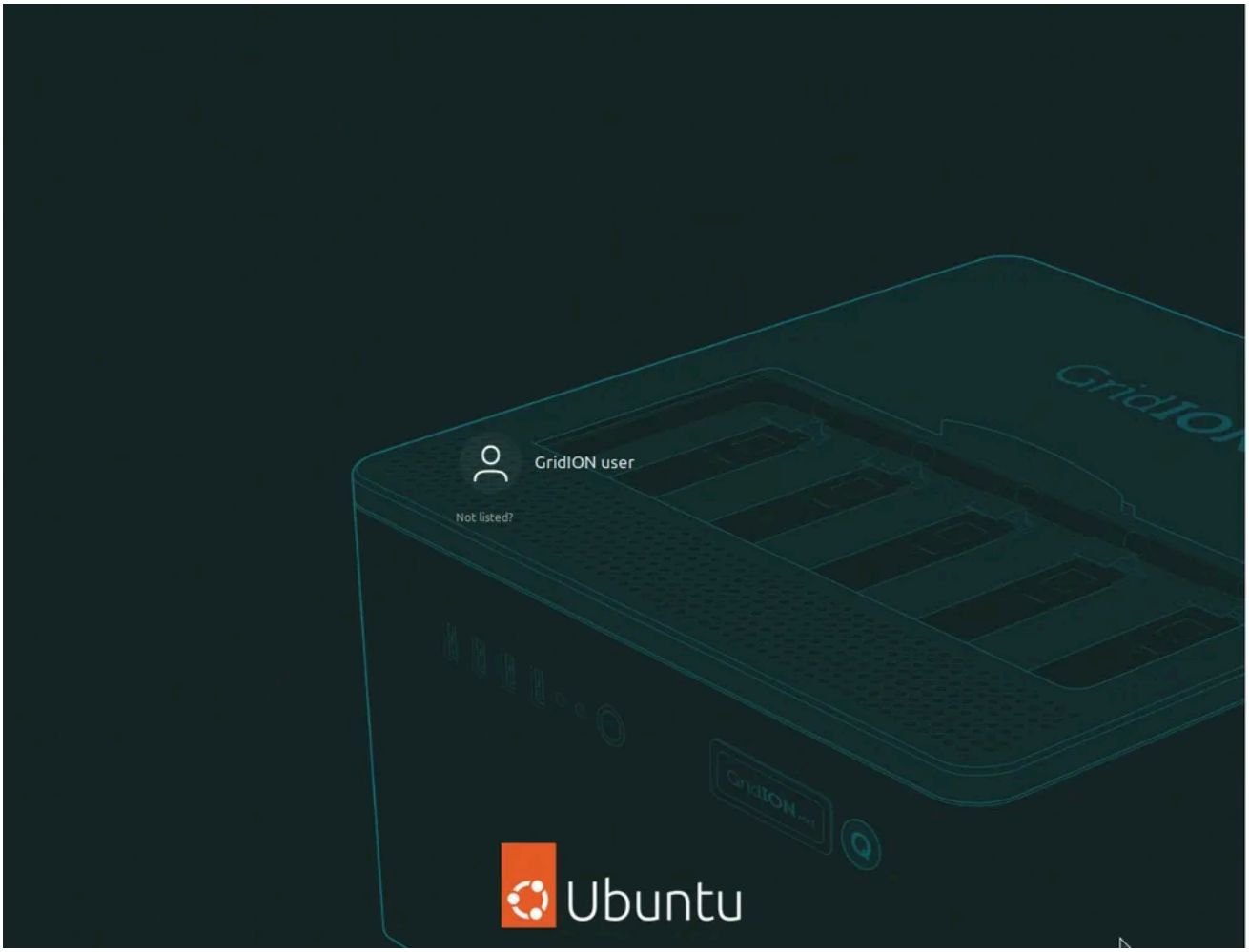
1. Starting your device

Every time you boot up your Q GridION, you will need to decrypt the device's hard drive and log into the user account. The Q GridION is shipped with a default encryption passphrase and account credentials; you must change the username after your first login. It is also highly recommended to change the passphrase.

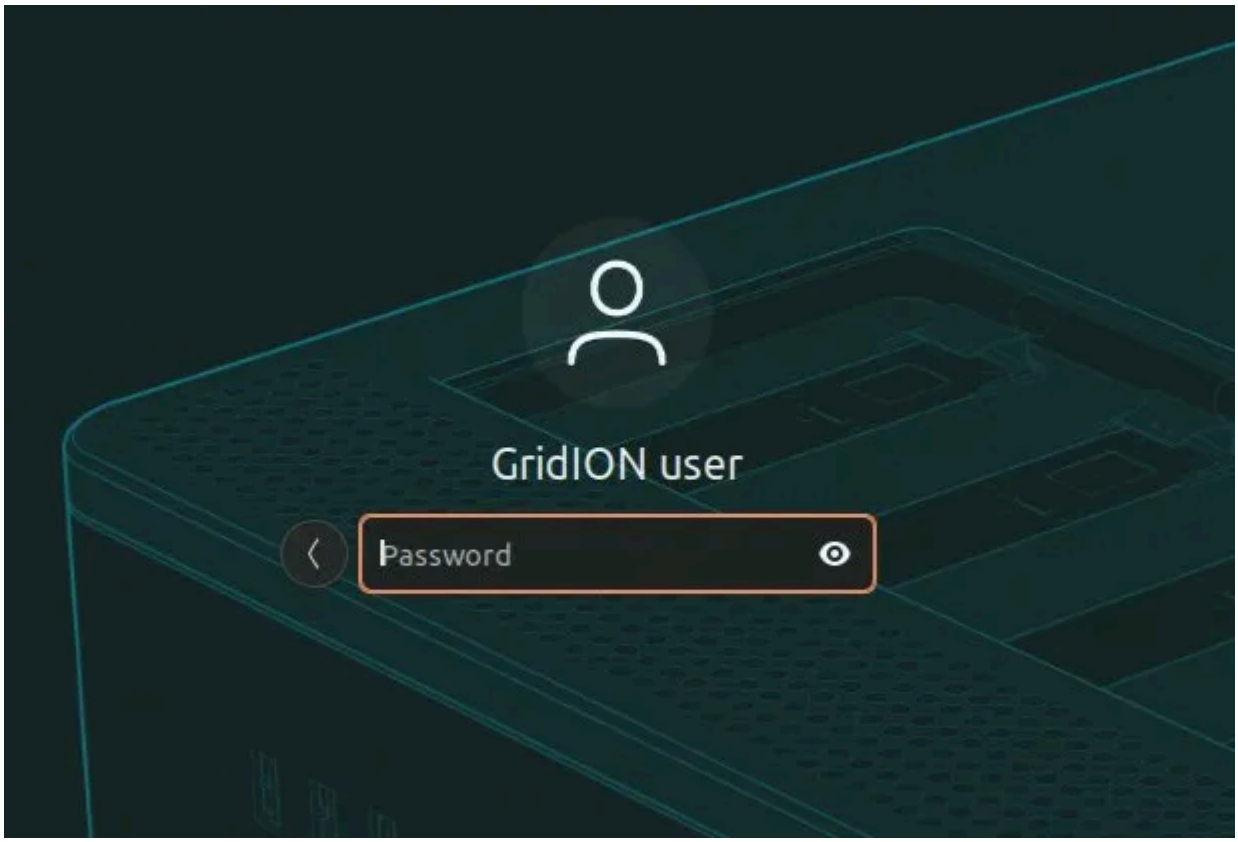
1 **Power on your Q GridION.**

2 **When prompted, enter the encryption passphrase (note: this is not the same as the user password). When booting your device for the first time, the passphrase for every Q GridION is nanopore.**

3 **Click on the user account. You will be asked for your password.**



4 **Enter the password. The first time you log in to the user account, the password will be grid.**



5 **If you are logging in for the first time, you will be asked to change the Q GridION user password. Keep your new password secure. For more information about password requirements, see the "Changing your password" section of the Q-Line sequencing software user guide.**

IMPORTANT

Only use the GridION User account for backup; do not use it to run your assays. The GridION User account retains the highest level of security clearance. For day-to-day use of the Q GridION, we recommend user accounts capable of simply running assays. Managers will have accounts capable of managing assays, while IT admins have accounts with full access to the system. GridION User remains as a last-resort recovery method, as it would be capable of all the above plus creating and managing the account levels.

2. Changing the encryption passphrase

We recommend changing the encryption passphrase when you log into your Q GridION and using a different passphrase per device if you have multiple GridIONs.

1. **Open a Terminal window from an account within the IT Administrators group and enter the following command:**

```
sudo /ont/platform/bin/encrypted_drive_change_passphrase --check-quality yes
```

Note: If this is the first time setting up, use the default GridION User account.

2. **Enter your Admin account password.**

3. **Enter your current encryption passphrase. By default, the passphrase is nanopore.**

4. **Enter your new encryption passphrase.**

5. **Confirm the new encryption passphrase.**

Note: If you do not want the device to have encryption, contact Oxford Nanopore Technologies Technical Support.

Every time you boot the GridION after this, you will need to enter the new encryption passphrase and log into your user account with your new credentials.

3. User management: local user

Management and configuration of users

The Q GridION device supports both local user accounts that can only be used on a specific GridION, and Windows Active Directory integrations (accounts that can be used on multiple devices and services). Local and Active Directory accounts can coexist if needed. If available, we recommend using an active directory integration to aid compliance and simplify user management across your organisation.

The Q GridION supports three user groups with different levels of authorisation: IT administrator, Laboratory manager, and Laboratory user.

- Members of the **IT administrator** group have full access to the system using the `sudo` command.
- Members of the the **Laboratory manager** group have view and edit access to `/data` and other Lab user account directories. Lab managers have limited access to create and manage both Lab user and Lab manager accounts.
- Members of the **Laboratory user** group can access the sequencing software application and run assays on the Q GridION. They can also view results. By default, they have neither access to data created by others, nor access to system administrative functions.

Setting up the device

When you first set up the device, we recommend that you create one or more IT Administrator accounts using the default GridION User account and then switch to managing the device using one of those accounts and treating the GridION User account as a backup with a secure password.

Management of local users

User accounts are managed via the command-line tool `ont-platform-security-users`.

If you have already set up local user accounts, ensure that the internal representation of the username does not clash with the domain username system.

The `ont_lab_user` and `ont_lab_manager` group have defined roles within the Q-Line sequencing software. Membership of the `ont_lab_user` group allows the user account to access the application and run assays.

The `ont_lab_manager` group allows users access to some administrative functions of the software such as:

- Disabling/enabling an assay
- Creating and deactivating API keys
- Starting the UI and seeing the assay configuration and API key management options available
- Adding a user to the `ont_lab_user` group
- Adding a user to the `ont_lab_manager` group

Both local and domain accounts may join these groups. Any new usernames created must be unique and cannot match any existing user groups.

The new user is automatically added to the `ont_lab_user` group. Laboratory managers are able to view and edit access to all files and directories created by the new user.

Local user set-up

Important: The local user set-up can only be done through the command line. You must not perform this through the Ubuntu graphical user interface or key features will not function correctly.

To create a new user, open the Terminal and enter the following command:

```
sudo /opt/ont/platform/bin/ont-platform-security-users --create-user <unique> "
<display>"
```

where `<unique>` is a unique username and `<display>` is the display name for the user, for example:

```
sudo /opt/ont/platform/bin/ont-platform-security-users --create-user john "John Smith"
```

To add a local user to the Laboratory manager group, use the following command:

```
sudo /opt/ont/platform/bin/ont-platform-security-users --add-labmgr <unique>
```

where `<unique>` is the user's unique username (not their display name).

To add a local user to the IT Administrator group, use the following command:

```
sudo /opt/ont/platform/bin/ont-platform-security-users --add-itadmin <unique>
```

where `<unique>` is the user's unique username (not their display name).

To deactivate a local user account, enter the following command:

```
sudo /opt/ont/platform/bin/ont-platform-security-users --deactivate-user john
```

Note: Deactivating an account will stop the user from logging in. However, the account and its data will be retained. Fully deleting accounts is not recommended.

Enabling and configuring auto-lockout

The tool `ont-platform-security-auto-lockout` enables, configures, and disables automatic account lockout on failed logins. It may also be used to reset user accounts that have been locked due to too many failed login attempts.

Configurable options include setting the number of failed attempts after which an account will be locked and a time period after which a locked account will be automatically unlocked.

By default, any accounts locked by auto-lockout will be re-enabled at system boot time. This behaviour can be changed using the configuration option `--reset-on-boot NO`

Usage examples

Enable auto-lockout after three failed attempts:

```
sudo /opt/ont/platform/bin/ont-platform-security-auto-lockout --enable --deny-count 3
```

Enable auto-lockout after five attempts and prevent re-enabling at reboot time:

```
sudo /opt/ont/platform/bin/ont-platform-security-auto-lockout --enable --deny-count 5 –
reset-on-boot NO
```

Reset failure counters for the user ID ‘john’. This will permit John to log in again if his account had been locked as a result of too many login failures:

```
sudo /opt/ont/platform/bin/ont-platform-security-auto-lockout --reset john
```

Disable auto-lockout:

```
sudo /opt/ont/platform/bin/ont-platform-security-auto-lockout --disable
```

Display the status of auto-lockout:

```
sudo /opt/ont/platform/bin/ont-platform-security-auto-lockout --status
```

4. User management: Active Directory

Management and configuration of users

Important: You will need your IT department to add your GridION to an AD or LDAP domain.

The Q GridION device supports both local user accounts and remote directory services. Local accounts can only be used on a specific GridION while remote directory services and be shared amongst many systems. The Q GridION supports remote directories using the Windows Active Directory (AD) and Lightweight Directory Access protocols (LDAP) . Local and remote accounts may coexist if needed. If available, we recommend using remote directory services to aid compliance and simplify user management across your organisation.

The Q GridION supports three user groups with different levels of authorisation: IT administrator, Laboratory manager, and Laboratory user. For domain accounts, you will need to add the individual to the Lab Manager group on every device.

- Members of the **IT administrator** group have full access to the system using the `sudo` command.
- Members of the **Laboratory manager** group have view and edit access to `/data` and other Lab user account directories. Lab managers have limited access to create and manage both Lab user and Lab

manager accounts.
- Members of the **Laboratory user** group can access the sequencing software application, run assays on GridION, and view results. By default, they have neither access to data created by others nor access to system administrative functions.

All the above groups are local to the platform and while AD users may be added to local groups the management of local groups must be done on the platform itself. The tool `ont-platform-security-users` performs the configuration of local user accounts and groups on the sequencing device. The local users and groups will remain necessary. It also allows the management of login permit/deny functions for domain accounts.

For more information on local user and group management see the section "User management: local user".

Joining an LDAP or Active Directory domain

You may only join one domain at any given time; the GridION does not support multiple domains.

The tool `/opt/ont/platform/bin/ont-platform-security-ad` is used to connect (join) the system to an Active Directory or LDAP domain. After the join is complete, domain accounts will be recognised by the platform, although logins using domain accounts are not enabled by default.

To join a system to a domain, you need to know the domain name, a domain administrator account and password. Optionally, depending on site requirements, you should know what type of user ID mapping will be used, if and how Windows SIDs from the domain are translated into Unix uid/gids) and whether or not all domain logins are allowed.

By default, no domain users will be able to log in until explicitly allowed. If you want to permit login access for all domain accounts, this must be specified when joining the domain. If you do not permit access for all domain users, you can allow individual domain accounts later.

Verifying the platform configuration

Connecting to an LDAP or AD domain can lead to errors due to configuration errors. The main items to check are:

1. Time synchronisation is configured and active.
2. DNS (Domain Name System) is configured and using an AD/LDAP domain server.
3. The username and password used for the connection has domain admin rights.

These configurations account for most of the problems encountered when joining a domain.

To ease the process, `ont-platform-security-ad --join` will perform configuration checks automatically upon a join attempt. If the join fails, execute these checks manually.

1 Check the time synchronisation

The system clock must be synchronised with the same source as is used by the domain controllers. If the system clock deviates by more than five minutes from that of the domain controllers, all domain authentications will fail, domain accounts will no longer be usable, and all domain users will be locked out of the system.

To check that time synchronisation is working, open a Terminal and enter the following command:

```
timedatectl
```

If the time synchronisation works properly, the 'System clock synchronized' status in the output should read 'yes'.

Example output:

```
Local time: Wed 2023-06-21 08:46:54 UTC
Universal time: Wed 2023-06-21 08:46:54 UTC
RTC time: Wed 2023-06-21 08:46:54
Time zone: Etc/UTC (UTC, +0000)
System clock synchronized: yes
NTP service: active
RTC in local TZ: no
```

2 Check the DNS

The system must be configured as a DNS client and using DNS servers that are also AD/LDAP domain controllers. If you have chosen to separate AD and DNS functions for security and performance reasons, the DNS domain must contain standardised entries for AD/LDAP servers.

The tests below are valid for either configuration as they represent a manual implementation of the method used by the system for the domain join.

1. Establish your AD domain name. Many organisations use the same name for DNS and AD. If this is the case, the AD domain name can be found in `/etc/resolv.conf` . Open a Terminal and enter the following command:

```
egrep '^(domain|search)' /etc/resolv.conf
```

Example output (in this example, the local domain name is `example.local`):

```
search example.local^^^^^^^^^^^^
```

2. After establishing the domain name, test the DNS configuration by running the following command:

```
resolvectl -t SRV query _ldap._tcp.example.local
```

If the test is successful, a list of AD servers will be returned for this domain:

```
_ldap._tcp.example.local IN SRV 0 100 389 ghjnycad01.example.local -- link: eno1
_ldap._tcp.example.local IN SRV 0 100 389 ondddsad01.example.local -- link: eno1
_ldap._tcp.example.local IN SRV 0 100 389 avytenad01.example.local -- link: eno1
_ldap._tcp.example.local IN SRV 0 100 389 krnfglad00.example.local -- link: eno1
_ldap._tcp.example.local IN SRV 0 100 389 FJWOXFAD12.example.local -- link: eno1
_ldap._tcp.example.local IN SRV 0 100 389 okdhdlad01.example.local -- link: eno1
_ldap._tcp.example.local IN SRV 0 100 389 ondnsywd10.example.local -- link: eno1
_ldap._tcp.example.local IN SRV 0 100 389 ntsjsywn01.example.local -- link: eno1
_ldap._tcp.example.local IN SRV 0 100 389 mdunxfad13.example.local -- link: eno1
_ldap._tcp.example.local IN SRV 0 100 389 KLGSHAAD00.example.local -- link: eno1
_ldap._tcp.example.local IN SRV 0 100 389 uivcinad01.example.local -- link: eno1
_ldap._tcp.example.local IN SRV 0 100 389 KOJWINAD00.example.local -- link: eno1
_ldap._tcp.example.local IN SRV 0 100 389 pwnsfoad01.example.local -- link: eno1
```

The failed test below indicates that the current DNS configuration is not correct for AD/LDAP. Joining the domain will not be possible until this is resolved:

```
_ldap._tcp.oxfordnan0labs.local: resolve call failed: '_ldap._tcp.example.local' not found
```

3 Check that the user has domain admin rights

Connecting any system to an AD or LDAP domain requires privileged access. Within AD, such a user must be a member of the group 'Domain Admins'.

Checking group membership must be done on a system that is already connected to the domain. This can be achieved via three methods:

- Using a Windows AD controller (GUI)
- Using a Windows AD client using PowerShell
- Using a Linux AD client using `ldapsearch`

The examples below were taken from a functioning domain and the username 'john' (John.Smith@example.local) is used throughout.

Using a Windows AD controller (GUI)

This process requires domain admin rights and login access to a domain controller.

1. Log into an AD controller.
2. From the Start menu, navigate to **Windows Administrative Tools** and select **Active Directory Users and Computers (ADUC)**.
3. Within ADUC, find the user account to be checked and right-click **Properties** to display the account properties. In the properties windows, select the **Member Of** tab.

The user account should be a member of the group ‘Domain Admins’.

Using a Windows AD client using PowerShell

Using this method requires a domain login to a Windows client.

1. Obtain a PowerShell prompt and issue the command `net user john /domain` . Look for 'Domain Users' within 'Global Group memberships'.

```
PS C:\Users\andrew> net user john /domain
User name john
Full Name John Smith
...
Local Group Memberships *Administrators
Global Group memberships *Group Policy Creator *Domain Users
*Enterprise Admins *Domain Admins
*Schema Admins
```

2. Obtain a list of members of the 'Domain Admins' group via the PowerShell CmdLet 'Get-ADGroup' to check that the expected users have been added as members:

```
PS C:\Users\john> Get-ADGroup -Identity "Domain Admins" -Properties Members
DistinguishedName : CN=Domain Admins,CN=Users,DC=example,DC=local
GroupCategory : Security
GroupScope : Global
Members : {CN=Jane Doe,OU=IT,OU=Example Users,DC=example,DC=local, CN=John
Smith,OU=IT,OU=Example Users,DC=example,DC=local,
CN=Administrator,CN=Users,DC=example,DC=local}
Name : Domain Admins
ObjectClass : group
ObjectGUID : 7aca97e1-3d76-4267-b63d-039098178fe9
SamAccountName : Domain Admins
SID : S-1-5-21-3271649479-1020880420-2291191405-512
```

Using a Linux AD client using ldapsearch

After logging into a Linux system already joined to the domain and using a domain authenticated account, it is possible to view the membership of the "Domain Admins" group using `ldapsearch`. This is a two-step process.

1. Find the name of a domain controller. There are various methods you can use for this. The example below illustrates a generic method which should work on any Unix/Linux platform, and uses the AD domain name `example.local`.

```
resolvectl -t SRV query _ldap._tcp.example.local
_ldap._tcp.example.local IN SRV 0 100 389 arthur.example.local -- link: enp1s0
```

2. Use ldapsearch. From the output above, one AD server is called `arthur.example.local`. Use this name in the LDAP URI (`-H` option):

```
/usr/bin/ldapsearch -o ldif-wrap=no -Y GSSAPI -H ldap://arthur.example.local -b
"dc=EXAMPLE,dc=LOCAL" "(sAMAccountName=Domain Admins)"

...
# Domain Admins, Users, example.local
dn: CN=Domain Admins,CN=Users,DC=example,DC=local
objectClass: top
objectClass: group
cn: Domain Admins
description: Designated administrators of the domain
member: CN=John Smith,OU=IT,OU=Example Users,DC=example,DC=local
member: CN=Jane Doe,OU=IT,OU=Example Users,DC=example,DC=local
member: CN=Administrator,CN=Users,DC=example,DC=local
...
```

4 Join the domain (simple use case)

To join the platform to an AD or LDAP domain without any advanced options, run the tool with just the domain name and, optionally, the name of the user account with domain administrator privileges. You will be prompted to enter the account password. The username is provided.

To join the domain `example.local` using the domain account john.smith, use this command:

```
sudo /opt/ont/platform/bin/ont-platform-security-ad --join example.local --username
john.smith
```

Domain user accounts will be recognised by the system, but login access is not permitted.

Login access may be granted via the tool `opt-platform-security-users` .

You will see an output similar to the one below. Enter your password when prompted:

```
Attempting to join domain example.local with username john.smith
Password for john.smith:
SUCCESS! This system is now a member of the domain example.local
```

For more details about the domain connection, use the `–test` option.

To enable additional diagnostic messages, use `--debug {1...9}` .

To verify other accounts, modify this command accordingly, e.g.,

```
getent passwd <domain user>\\<domain>
```

You will see an output similar to the one below:

```
jane.doe:*:2823263:165863:Jane Doe:/home/jane.doe:/usr/bin/bash
```

Join the domain (advanced use case)

The following advanced use cases are considered here:

- User ID mapping strategy differs from the default.
- The platform joins the domain within an OU inside the domain and not at the top level.
- All domain logins are permitted after joining the domain.
- User account password is not prompted for (scripted usage).

Using POSIX/RFC2307 user IDs

To use POSIX user attributes from the domain, use the option `--id-mapping-strategy POSIX`

```
sudo /opt/ont/platform/bin/ont-platform-security-ad --join example.local --username
john.smith --id-mapping-strategy POSIX
```

You will see an output similar to the one below. Enter your password when prompted:

```
Attempting to join domain example.local with username john. smith
Password for john.smith:
SUCCESS! This system is now a member of the domain example.local
```

5 Permit a specific user to log in

Enter the following command:

```
sudo /opt/ont/platform/bin/ont-platform-security-users --permit-ad-user john.smith
```

6 Permit all members of a domain group login access

Enter the following command:

```
sudo /opt/ont/platform/bin/ont-platform-security-users --permit-ad-group ‘UnixUsers’
```

7 Add a user (local or domain) to the Lab Manager or IT administrator group

Enter the following command to add to the Lab Manager group:

```
sudo /opt/ont/platform/bin/ont-platform-security-users --add-labmgr john.smith
```

Enter the following command to add to the IT administrator group:

```
sudo /opt/ont/platform/bin/ont-platform-security-users --add-itadmin john.smith
```

To join the platform to a specific organisational unit (OU):

To join the platform to a specific OU within the domain, use the `--ou` option. Note that the order in which OU hierarchy is specified is bottom-to-top, i.e. specify the OU with the lowest level first, highest last.

For example, if the system should be added to the 'Research' OU within ‘Computer’ and the OU hierarchy is DOMAIN -> Computers -> Research, the OU argument should look like this:

```
--ou "OU=Research,OU=Computers"
```

Quote marks are essential if any of the OU names contain spaces.

Example command:

```
sudo /opt/ont/platform/bin/ont-platform-security-ad --join example.local ---username
john.smith --ou "OU=Research,OU=Computers"
```

You will see an output similar to the one below. Enter your password when prompted:

```
Attempting to join domain example.local with username 'john.smith'
Password for john.smith:
SUCCESS! This system is now a member of the domain example.local
```

Providing the password by a different method

By using the option `--passwd-stdin`, the password prompt can be eliminated. The password will instead be obtained by the tool by way of the STDIN file channel. Note that this is intended for scripting usage. Do not store any password in plain text.

```
echo "PASSWORD" | sudo /opt/ont/platform/bin/ont-platform-security-ad --join example.local
--username john.smith --permit-all
```

You will see an output similar to the one below.

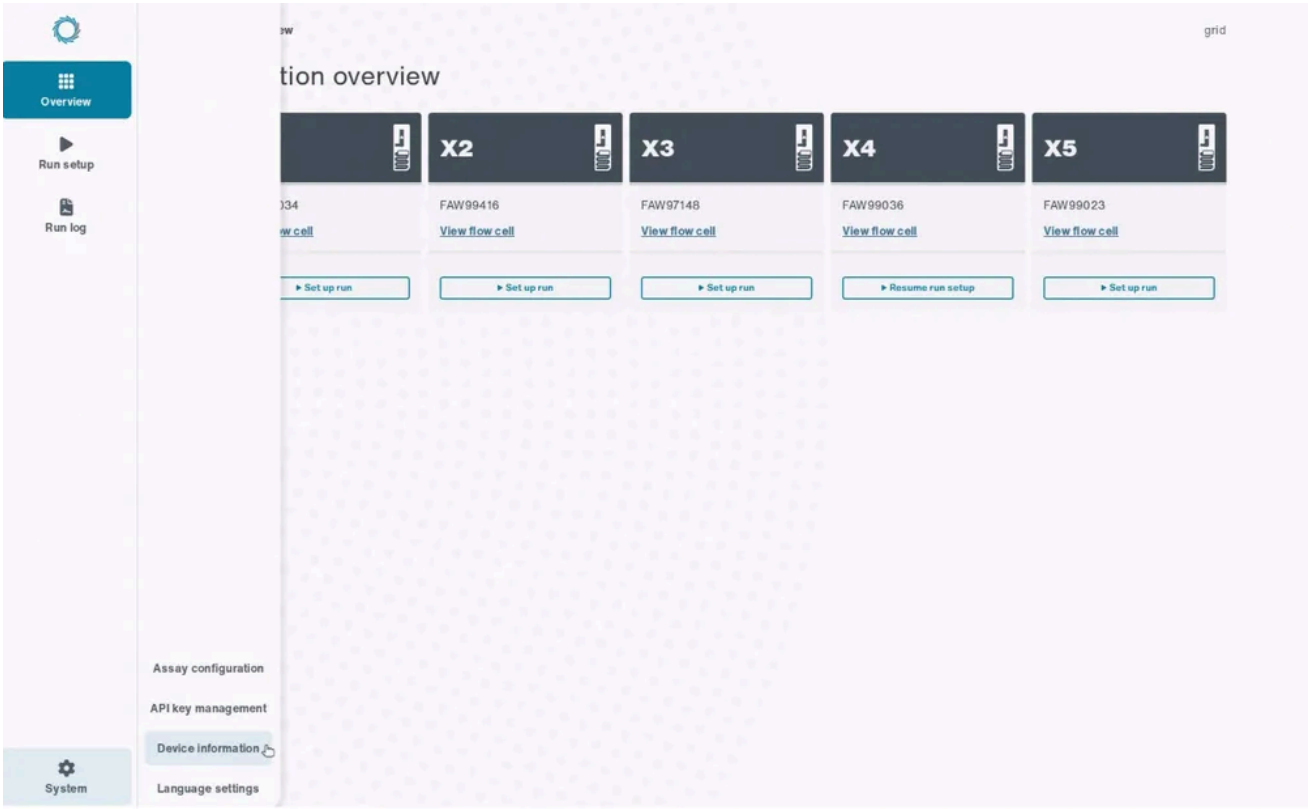
```
Attempting to join domain example.local with username 'john.smith'
SUCCESS! This system is now a member of the domain example.local
```

5. Position check

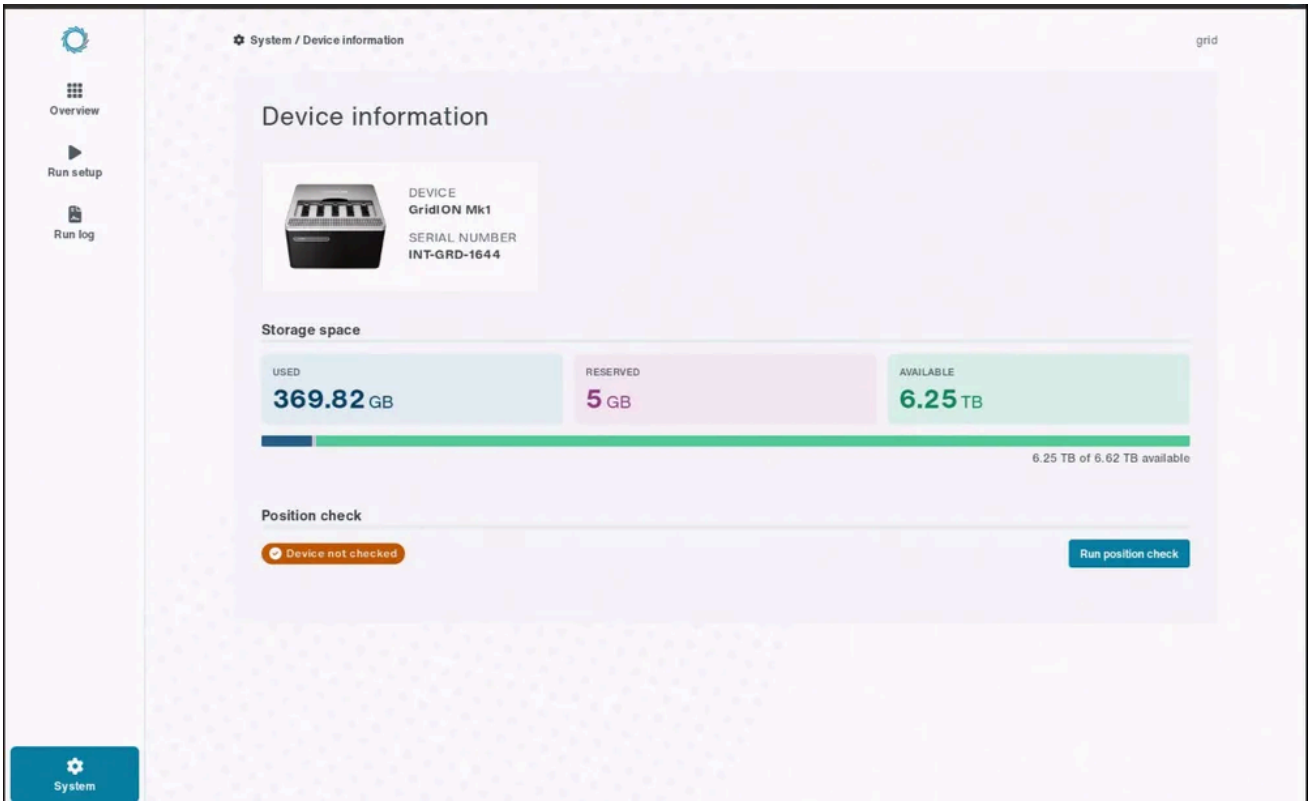
We advise you to run a position check to ensure your GridION works properly. This step can be completed at the same time as the Instrument qualification.

1 Open the sequencing software.

2 Click System, then click Device information.



You will see the following screen:



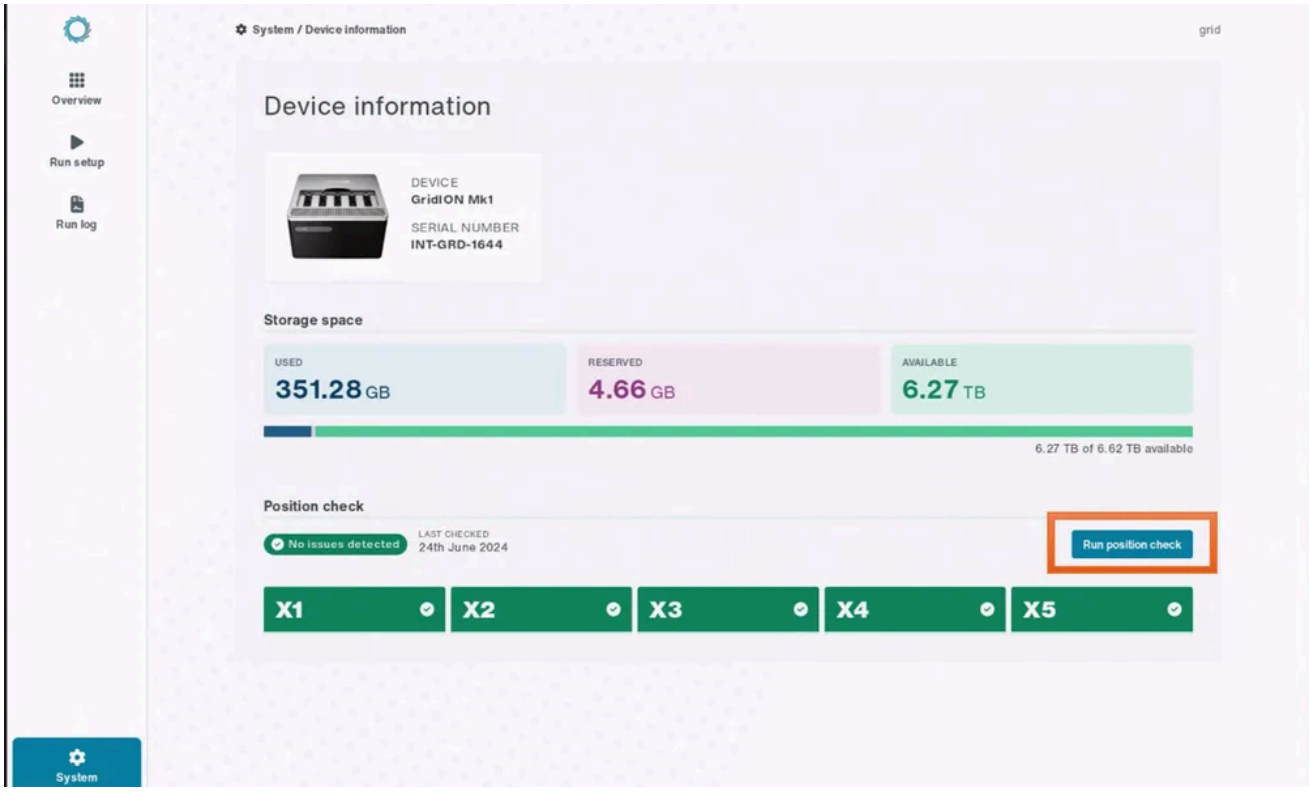
The Storage space section features a summary of the storage available for your assay outputs, where space can be classified as one of:

- Used (blue) is all the data used on the GridION.
- Reserved (magenta) is the space currently reserved by any runs being set up.
- Available (green) is the space left available for usage.

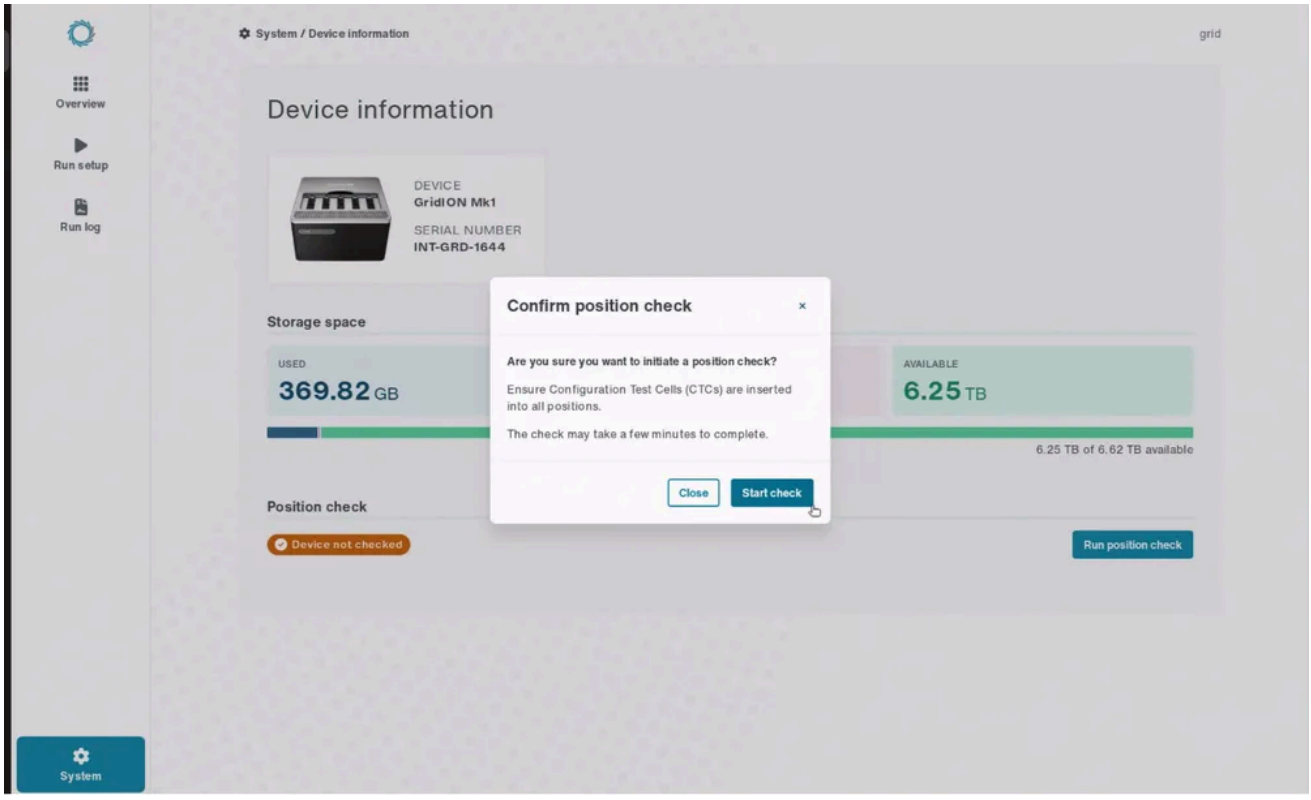
You can free up space by moving the data off the device or deleting the data entirely. We recommend automated offload; instructions can be found in the "Managing data" section of this guide.

3 Insert your Configuration Test Cells (CTCs) into all five flow cell positions by sliding the CTCs under the clip. The LEDs on all positions will turn green when the CTCs are recognised.

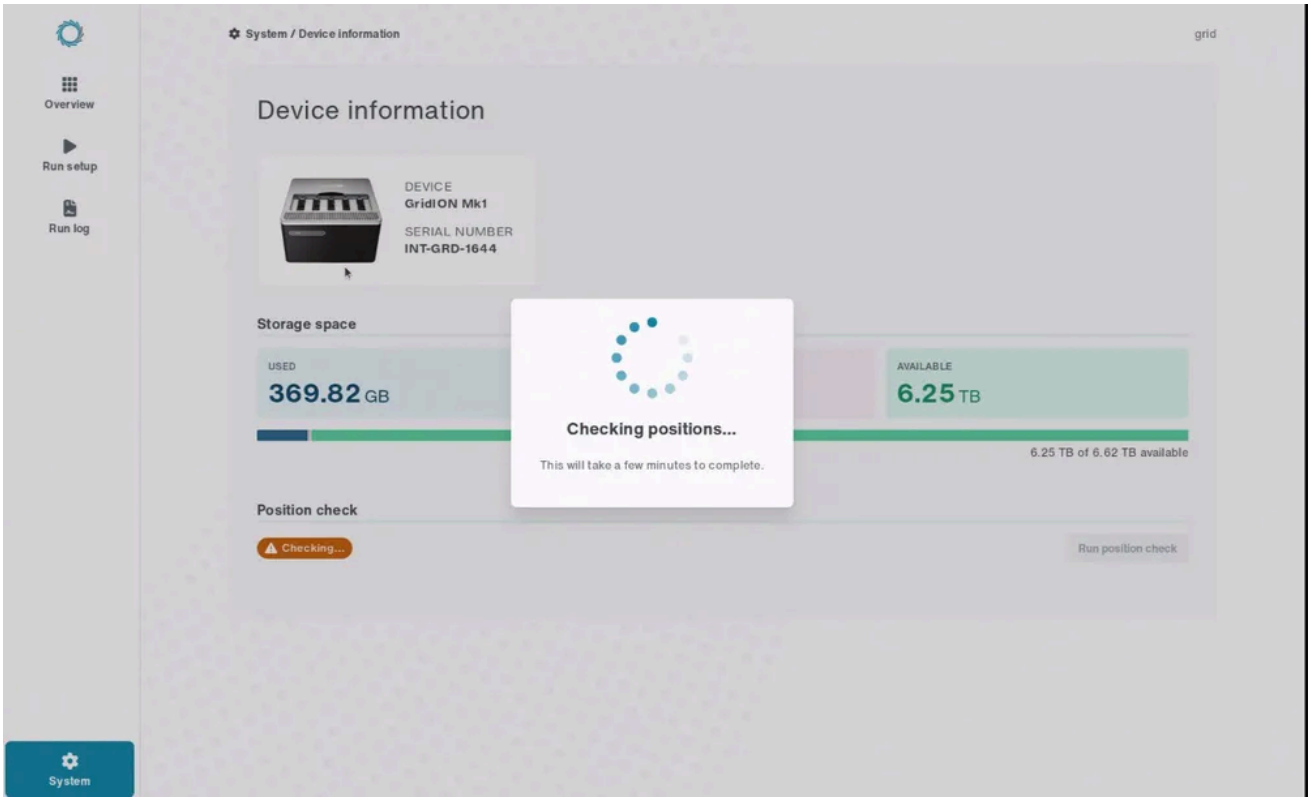
4 Click Run Position check.



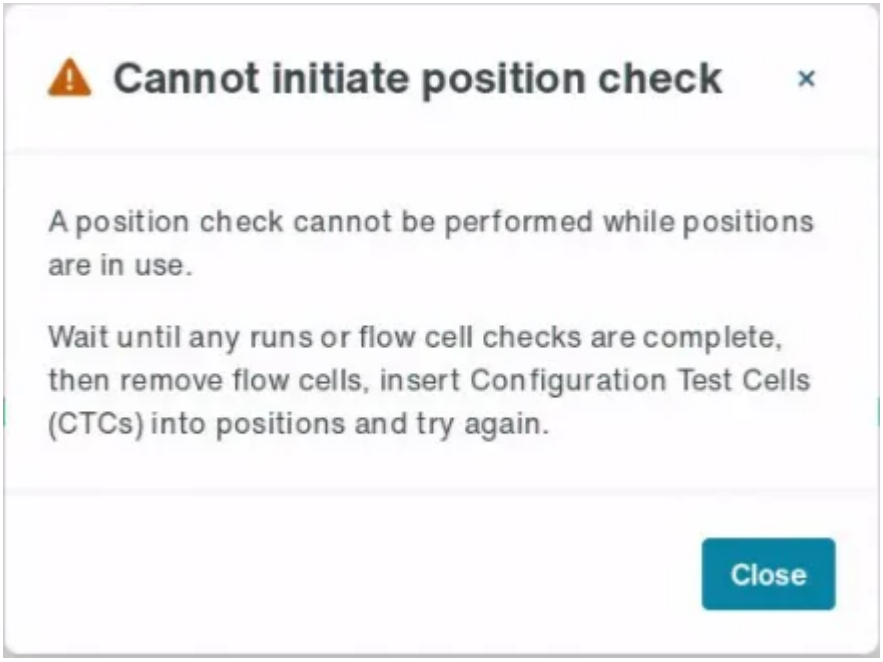
Then click **Start check**.



You will see the following screen:



It is important that you do not have any assays running when you perform a position check since this will prevent the position check from starting.



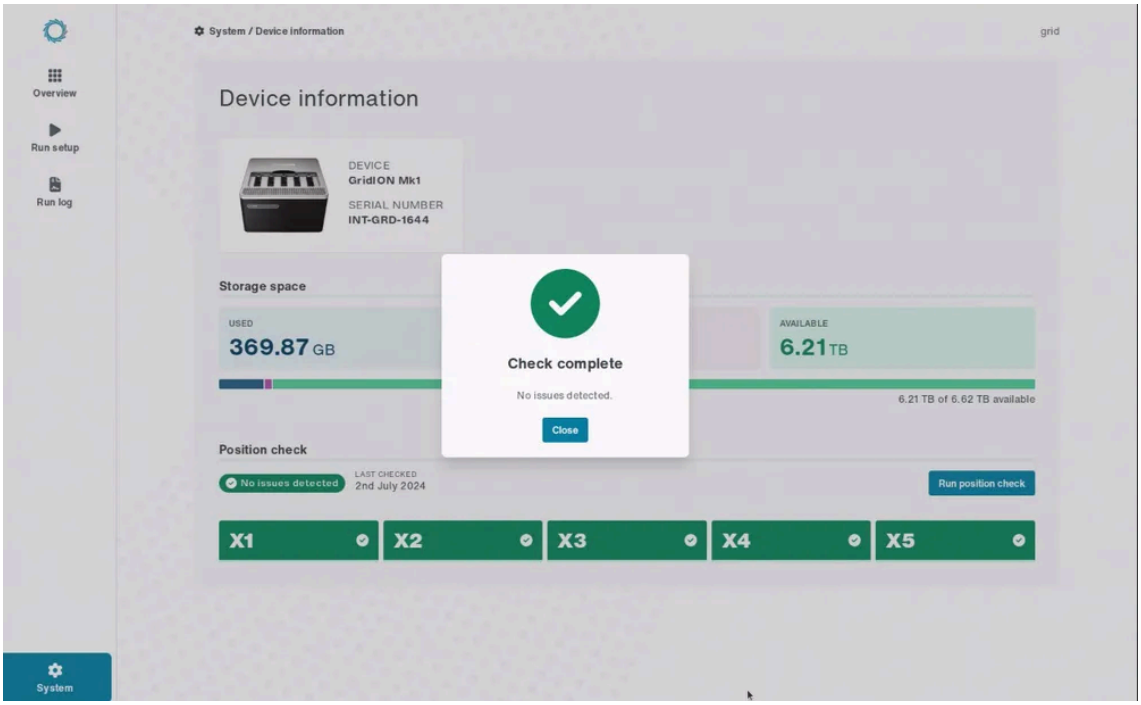
OPTIONAL ACTION

If the position check fails, swap the failed position's CTC with a CTC that has passed the position check. Then repeat the Position check by clicking Run position check.

Note: if the position check fails again, contact a member of Technical Support via Live Support within the Nanopore Community or support@nanoporetech.com.

END OF STEP

Once the check has been completed and passed, you will see the screen below stating that the check is complete and no issues have been detected.



6. Networking

The network parameters for your GridION must be suited to your local network.

Note: Your IT department should complete these instructions.

Networking requirements

GridION uses a 1x1 Gbps copper interface to connect to your local infrastructure. This interface has a single port. By default, the IP address is configured to DHCP. However, static IPs are configurable. This connection will be used for:

- Sending telemetry* information to Oxford Nanopore Technologies.
- Receiving critical software updates to the device (optional).
- Streaming biological sequence data to your local storage infrastructure.

You will need 1 Gbps Ethernet cable on your device to connect to your Ethernet port, your device and your Local Access Network (LAN).

* The sequencing software collects telemetry information during sequencing runs per the Terms and Conditions to allow monitoring of device performance and enable remote troubleshooting. Telemetry contains metadata about the settings and conditions of a sequencing run. Nothing specific about the genomic content of individual reads is included—only generic information, such as sequence length and q-score, is logged. Some of this information comes from free-form text entry fields, therefore no personally-identifiable information should be included.

1 Configure your network

If you want to connect your GridION to a network, use the search function from the desktop and search for “network”.

2 Validate the IP address

You can check connectivity by running:

```
sudo ont-check-connectivity
```

If this fails, look at your internet/firewall rules. As a minimum, you will need outbound access to:

Telemetry feedback

- HTTPS/port 443 to 52.17.110.146, 52.31.111.95, 79.125.100.3 (outbound-only access) or DNS rule for ping.oxfordnanoportal.com

In addition, we advise that you allow access to the following.

Updates to the sequencing software and the Linux Operating System:

- cdn.oxfordnanoportal.com
- *.ubuntu.com
- *.nvidia.com

If you want to use EPI2ME:

*.github.com

You may also need access to Okta if you want to log into your Nanopore account:

- *.okta.com
- *.mtls.okta.com
- *.oktapreview.com
- *.mtls.oktapreview.com
- *.oktacdn.com
- *.okta-emea.com
- *.mtls.okta-emea.com
- *.kerberos.okta.com
- *.kerberos.okta-emea.com
- *.kerberos.oktapreview.com
- *.okta-gov.com
- *.mtls.okta-gov.com

3 To validate that the IP address has been set correctly using a static or DHCP address, use the command:

```
ip -c -br address
```

The returned information will contain the IP address for the Ethernet link, as below:

```
lo  UNKNOWN  127.0.0.1/8 ::1/128
eno1  UP  10.160.38.123/24 fe80::3eb4:1c73:20c:5530/64
docker0  DOWN  172.17.0.1/16
```

Note that `lo` and `docker0` are for internal, system use only.

Enabling and configuring the firewall

The tool `ont-platform-security-firewall` is used to start, stop, enable, disable, and configure the firewall.

Note that the firewall is enabled by default and SSH disabled. When SSH service is allowed, all other ports are disabled.

Individual services may be enabled and disabled by using their service name or port number. In addition to the service names defined in `/etc/services`, the tool recognises the name "samba" which, when used, will enable or disable all the ports required by Samba: 137/udp,138/udp,139/tcp,445/tcp All rules apply to both IPv4 and IPv6.

Usage examples

Enable the firewall with the currently defined set of services allowed:

```
sudo /opt/ont/platform/bin/ont-platform-security-firewall --enable
```

Disable the firewall with currently defined set of services allowed:

```
sudo /opt/ont/platform/bin/ont-platform-security-firewall --disable
```

Deny incoming SSH connections:

```
sudo /opt/ont/platform/bin/ont-platform-security-firewall --deny ssh
```

Allow incoming traffic on port #123, as if for an NTP server:

```
sudo /opt/ont/platform/bin/ont-platform-security-firewall --allow 123
```

Allow ports required by Samba, as if for a Samba server:

```
sudo /opt/ont/platform/bin/ont-platform-security-firewall --allow samba
```

Disable the firewall:

```
sudo /opt/ont/platform/bin/ont-platform-security-firewall --disableConfiguring syslog
```

Show the current status of the firewall, including configured and allowed services:

```
sudo /opt/ont/platform/bin/ont-platform-security-firewall --status
```

Output

```
--- Configuration options:
ENABLE: YES
DEFAULT_SERVICES: ssh
ALLOWED_SERVICES: ssh
--- Current firewall status:
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip
To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
Configuration is unchanged, no action taken.
```

7. Managing data

By default, sequencing data and analysis results are stored in the GridION. However, we recommend to offload data by mounting a drive to avoid running out of memory.

> **IMPORTANT**
>
> **Only your IT department with full access rights will be able to take the following steps. To do this, they will need to use the GridION User account.**

The instructions below are examples of methods for mounting an external NFS and transferring data. Consult your local IT department to ensure it is compatible with the local infrastructure and that the correct permissions are in place.

1 Open the terminal in the GridION.

2 Create a directory to mount sudo mkdir /data/network/nfs

Ensure this is in /data/network to avoid permission issues.

```
sudo mount -t nfs ontlonqlnfs01:/data/export /data/network/nfs
```

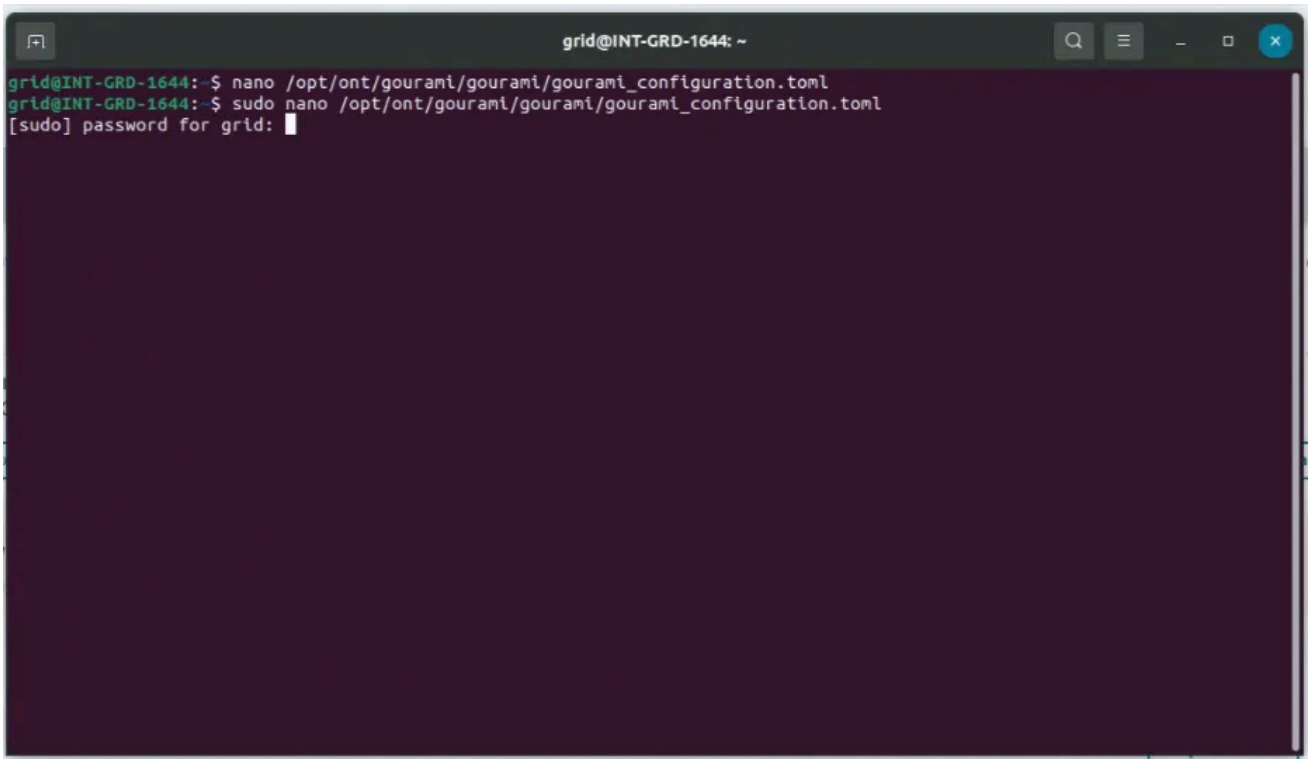
OPTIONAL ACTION

Check that the NFS-mounted drive (a remote drive created on the GridION accessible in the local network) is ready to be used by connecting to the GridION via RDP/KVM.

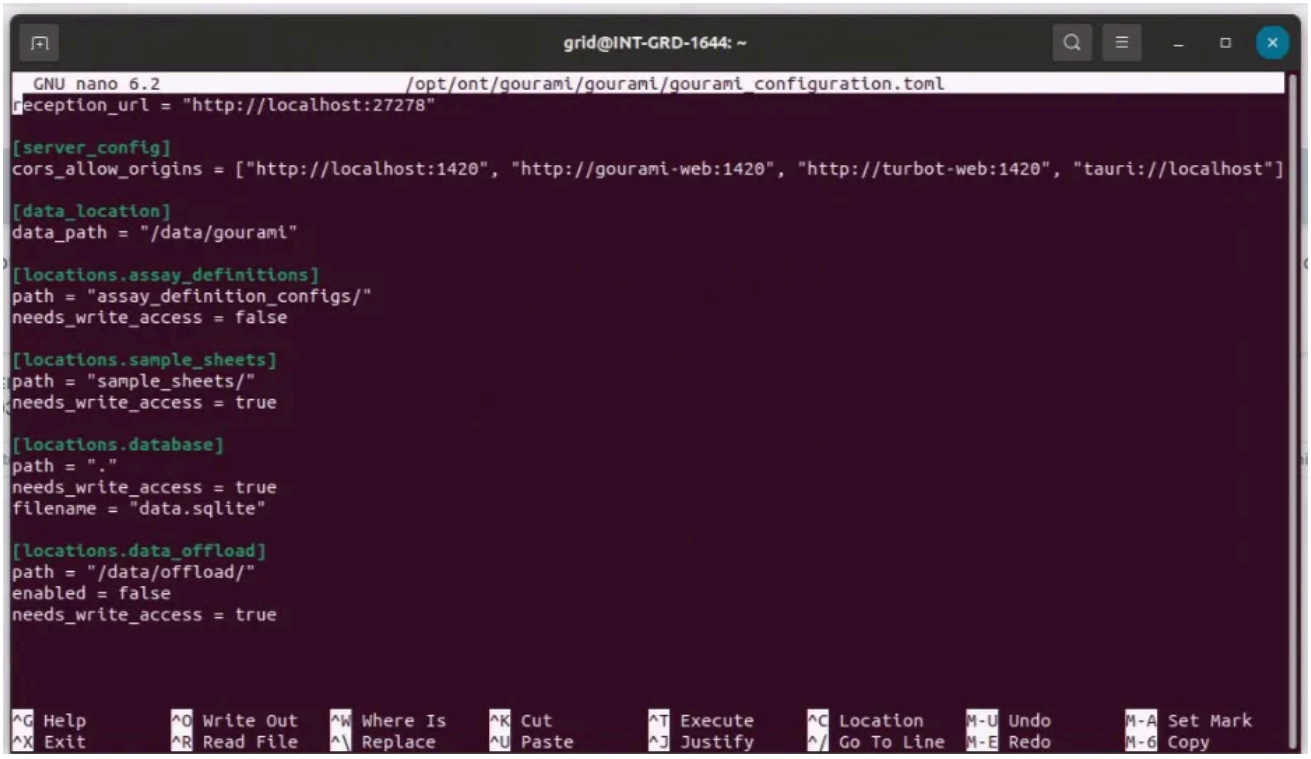
3 Enter the command:

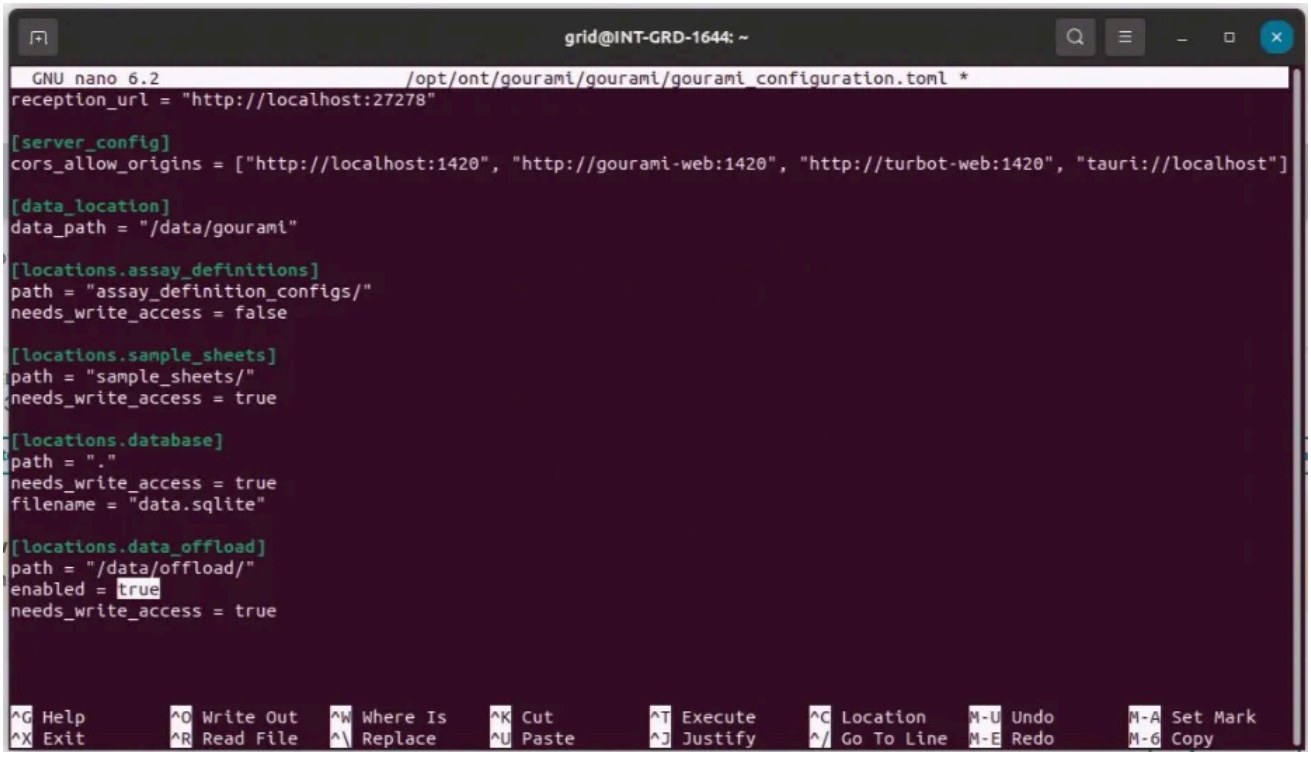
```
sudo nano /opt/ont/gourami/gourami/gourami_configuration.toml
```

4 You will be prompted for the GridION's passphrase. Enter the passphrase.

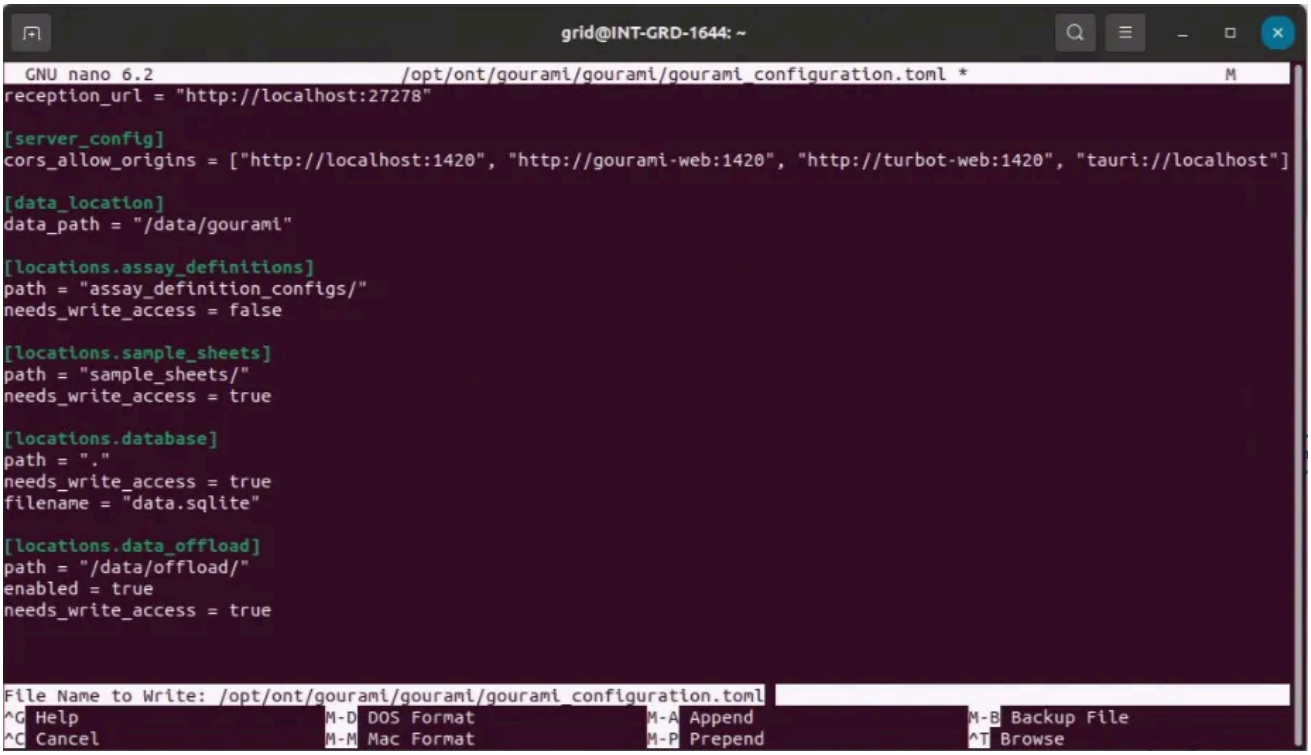


5 In the section under locations.data_offload, change the "enabled" setting from "false" to "true".



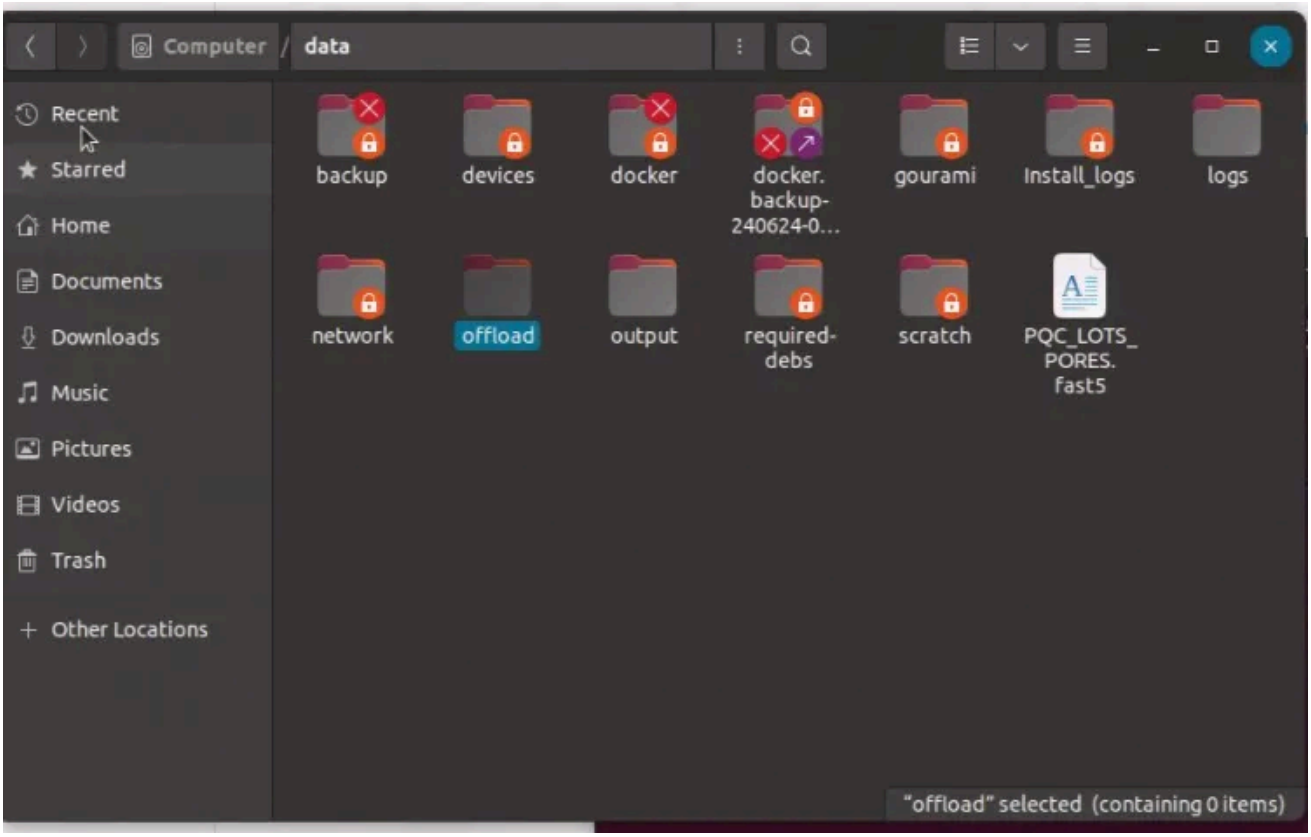


6 **Save the file after editing it by clicking Ctrl+O. When prompted to save the file, click Enter. Then click Ctrl+X to exit.**



7 Create the folder “offload” under /data if it does not already exist.

```
mkdir /data/offload
```



8 Restart the sequencing software with the command:

```
sudo systemctl restart gourami
```

9 As the GridION User, make a destination directory on the created network (this is an external network destination to the GridION) by entering the command:

```
mkdir /data/network/nfs/destination_dir
```

Important: Do **not** run `sudo` on this command.

10 Edit the /etc/systemd/ont-platform-data-offload.conf file to add the source directory and the destination directory, and set the maximum file transfer to 5:

```
sudo nano /etc/systemd/ont-platform-data-offload.conf
```

11 Stop the data offload service by running the command:

```
sudo systemctl stop ont-platform-data-offload
```

12 Start the data offload service by running the command:

```
sudo systemctl start ont-platform-data-offload
```

Note: This service, once manually started, will automatically resume every time the device is rebooted.

To check that the service has started as expected, run the below command to check its status and verify that it is active:

```
sudo systemctl status ont-platform-data-offload
```

13 Set up an assay using the following steps described in the "Configuring an assay definition file for your own assay" section of this guide and start running the assay as described in the "Set up and run an assay" section of the Q-Line sequencing software user guide.

14 Once the run is completed, navigate to /data/network/nfs/destination_dir (this is the destination folder set up in step 9 above) where you will find the contents of the Sequencing folder.

15 Navigate to /data/network/destination_dir (the destination folder set in step 3 above) where you will find the contents of the Analysis folder.

16 Complete an IQ/OQ/PQ once the data offload service has been established.

Managing USB mounting

Removable USB storage devices can be used to move data onto and off the Q-line GridION. To use a removable USB storage device with the Q-line GridION, complete the following steps:

1. Insert the USB device into one of the USB ports on the rear of the GridION.
2. Open the file browser through either the favourites menu on the left of your desktop or via the list of applications installed on the GridION.
3. In the sidebar of the file browser, select the USB device.
4. When prompted, provide your password to authorise mounting of the USB device. You will now be able to access your removable storage device.

When removing a USB storage device, it is important to first unmount the device. You can do this by clicking the eject icon next to the device in the side bar of the file browser.

Encryption protocols for mounted drives

When transferring data from the device to another system on the network using drive mounting, in-transit data shall be encrypted with an encryption method appropriate to the mounting protocol. Supported methods are:

Mounting method	Encryption method
NFS	None
SMB v3.0+	AES-128-GCM
SMB v3.1.1	AES-128-CCM

Notes: Whether encryption is used and which protocol is used is determined by the drive that is being mounted.

SMB only supports data encryption in transit from SMB v3.0+ onwards.

8. Configuring the device for LIMS integration

> **IMPORTANT**
>
> **Only your IT department with full access rights will be able to take the following steps. To do this, they will need to use the GridION User account.**

The sequencing software REST API

You can integrate your LIMS with your GridION-Q through the Sequencing Software's REST API. The API serves as a secure communication channel (middleware) between the device and the LIMS. It provides the following features:

- Passing sample details from the LIMS to the Sequencing Software
- Monitoring runs from the LIMS
- Transfer of results to the LIMS

Before you can connect your LIMS to your device, follow the instructions below to enable the device's LIMS interface so that the device can communicate with the LIMS. This is disabled by default for security. It is important to note that this process ensures the device is visible to the LIMS but does not represent a complete LIMS integration, which should be handled separately by the IT department of your institution.

Enabling the device to integrate the LIMS requires you to:

- Generate API key in the sequencing software.
- Edit a configuration file to include the sequencing software API key and any client API keys needed for the LIMS to connect to the sequencing software.
- Start the REST API service.

From there, the LIMS can be configured to the REST API for device integration in the LIMS. Once your LIMS and GridION are integrated, you can streamline your workflow further by printing the Library ID as an optical barcode and using this to select your sample sheet during run setup.

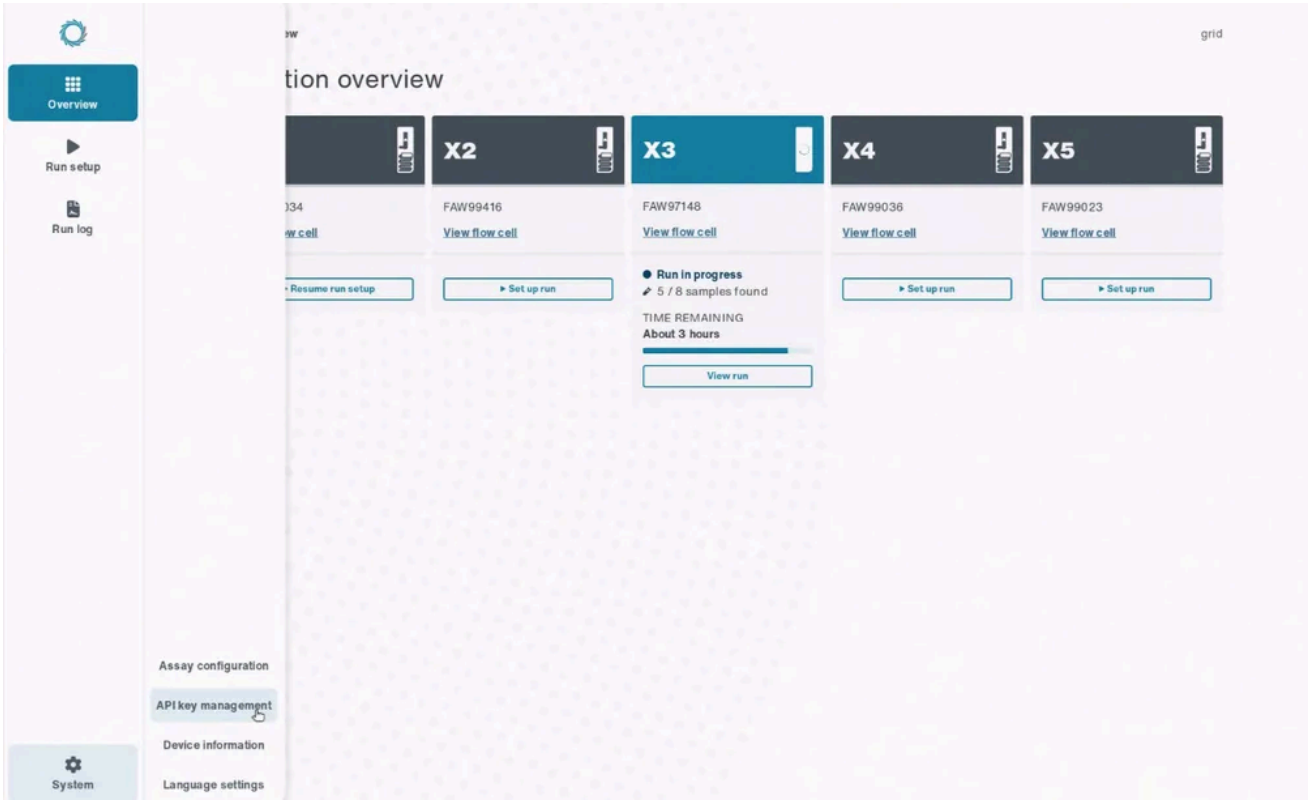
Configuring the device for LIMS integration

To enable your LIMS interface for a given device, complete the following steps.

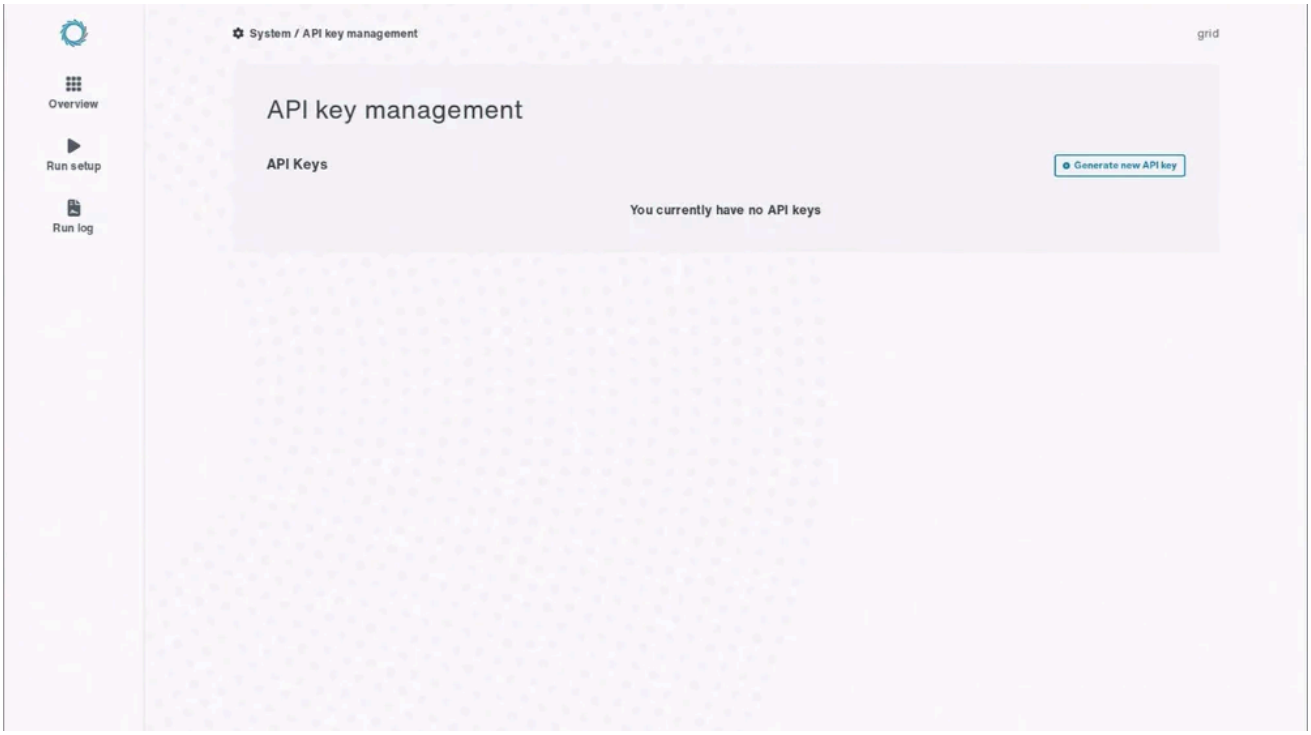
1 Open the terminal and run the command:

```
sudo systemctl enable nanoxint
```

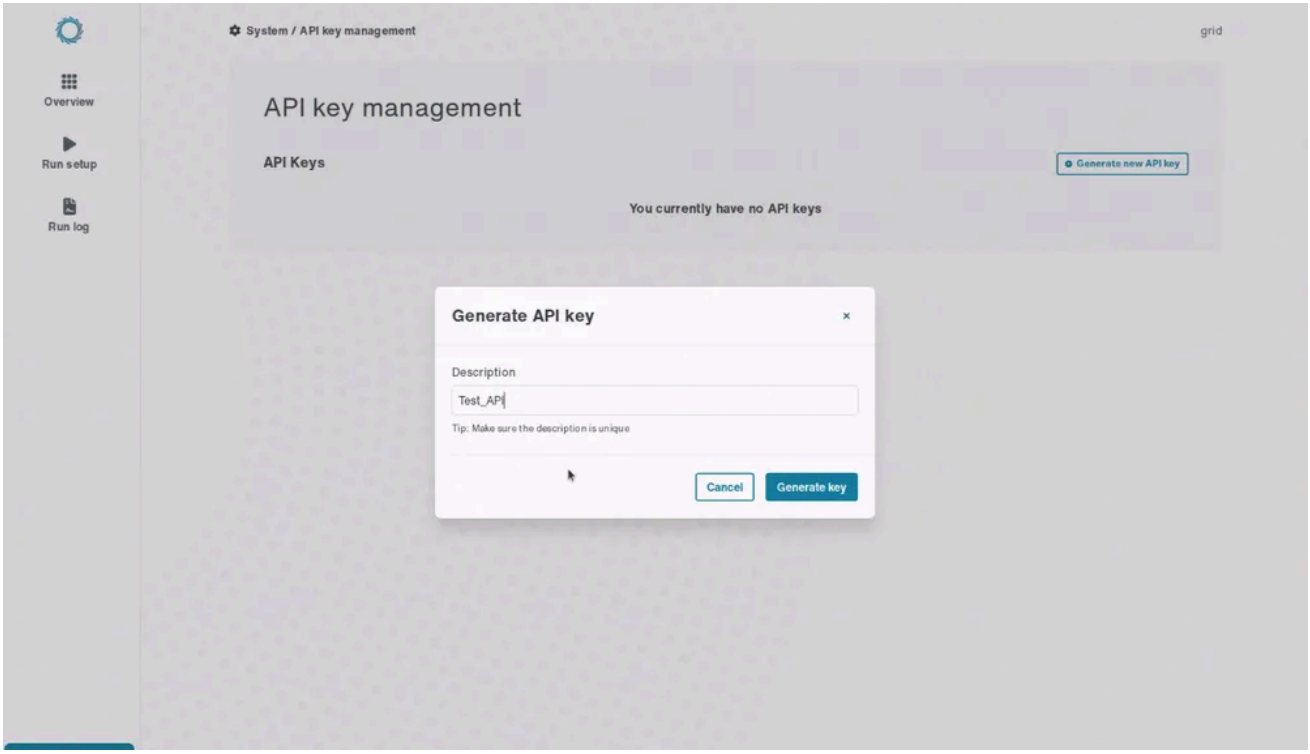
2 In the Sequencing Software, navigate to Settings and click API key management.



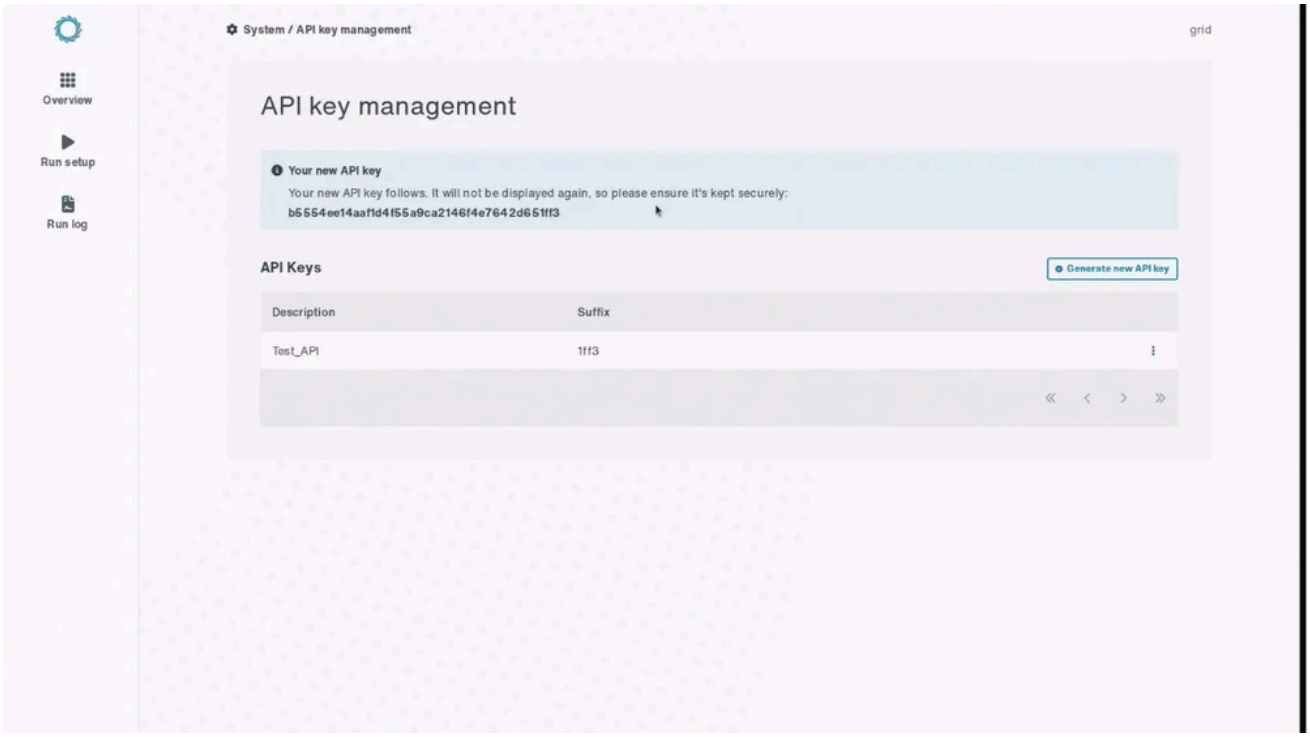
3 Click Generate new API key.



4 Enter your new API key description and click Generate key.



Important: Copy your API key and either use it immediately or save it somewhere safe. The key will not be displayed again, although you will be able to generate new ones.



5 Edit the config file /home/nanoxint/nanoxint.conf with any text editor (this requires root permissions). With the file open, paste in the API Key from step 2 as shown below:

```
MINKNOW_API_CLIENT_CERTIFICATE_CHAIN=/run/secrets/ssl_certificate_chain
MINKNOW_API_CLIENT_KEY=/run/secrets/ssl_certificate_key
DEVICE_CONFIG='{
  "g1": {
    "type": "gourami",
    "host": "host.docker.internal",
    "port": 6789,
    "api_key":"PASTE-API-KEY-HERE"
  },
}'
CLIENT_CONFIG='{"lims_1":{"api_key":"SET-YOUR-NANOXINT-CLIENT-API-KEY-HERE"}}
```

In the same file, configure any client API keys that the LIMS will use (last line in the example output above). Use a key that is secure as per your institution's security/IT policies. This client key will be used by LIMS or other external systems to communicate to the LIMS interface.

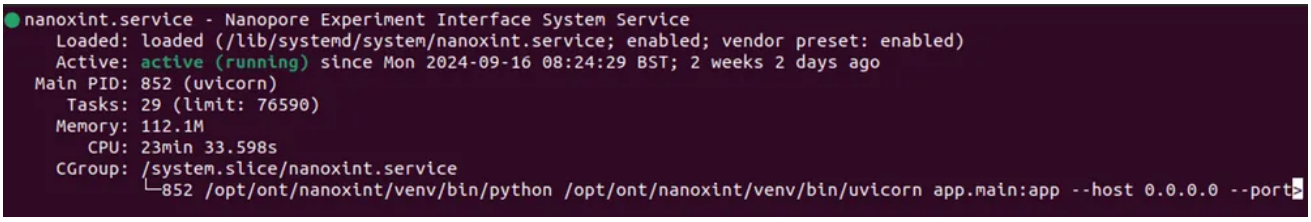
6 Restart your LIMS interface by running the command:

```
sudo systemctl restart nanoxint
```

7 To check that it has started up properly, run the command:

```
sudo systemctl status nanoxint
```

The output should look similar to the following image (note that `nanoxint` is both `loaded` and `active (running)`):



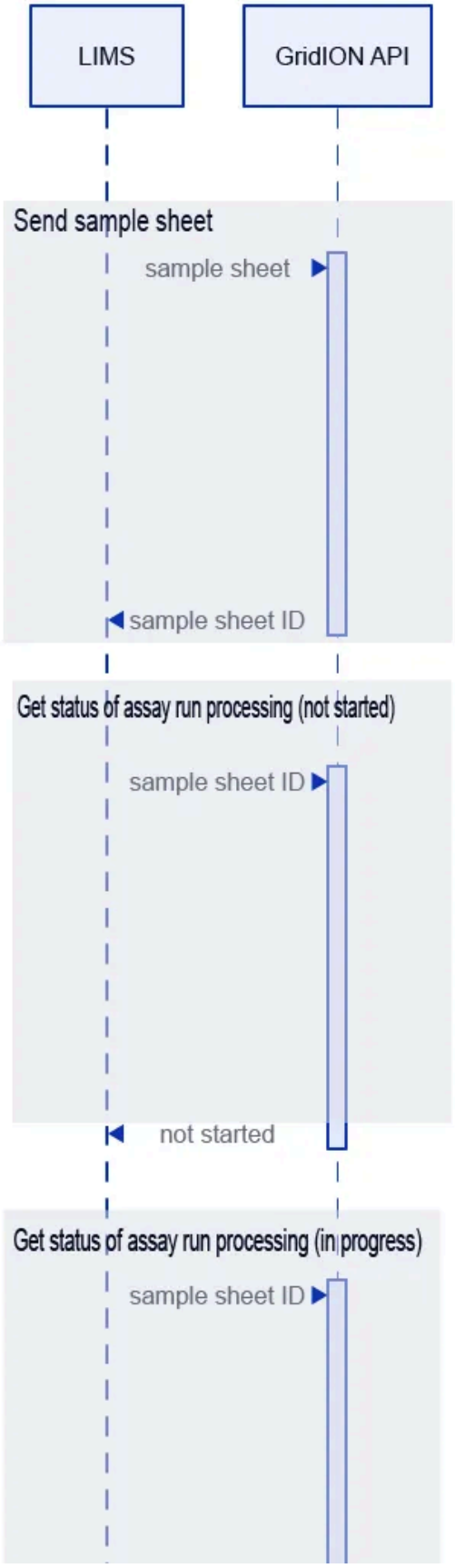
8 Integrate the device to the LIMS

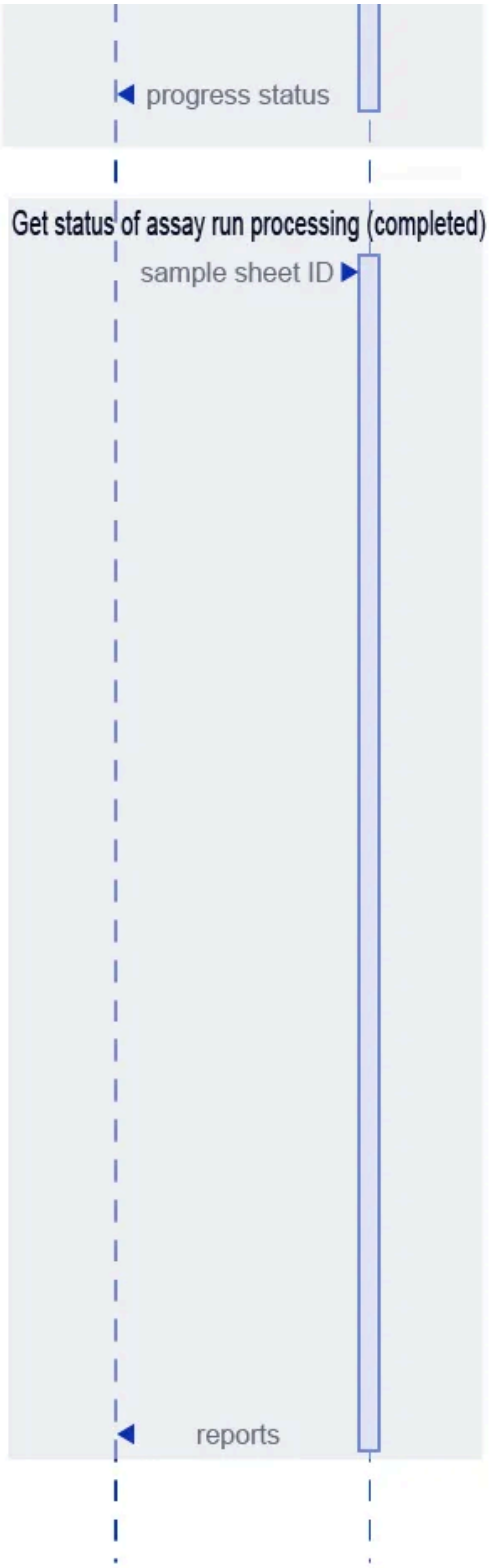
When you have enabled the LIMS interface, use the available endpoints to link to your LIMS as shown the diagram at the end of this section. The documentation on available endpoints can be accessed through a web browser at `http://<hostname>:7329/docs`. The hostname is the GridION's name on the local network if DNS routing is set up. Note that only the endpoints that are under the `dx` namespace will work in the current context.

__We recommend that you complete an IQ/OQ/PQ run once the LIMS has been set up to ensure the connection functions correctly and the LIMS can send valid sample sheets to the device. __

Overview of the flow of information in a LIMS integration

1. The LIMS sends sample details for a library, either as a sequencing software-compatible sample sheet or as a JSON message, to the REST API. The sample sheet is then made available during run setup. The API returns a unique sample sheet ID to the LIMS that can be used to track the library.
2. Using the sample sheet ID, the LIMS queries the REST API to determine the status of that library. If a run has started, the API will return a unique run ID.
3. Using the run ID, the LIMS can query the REST API for the status of that run from time to time, or upon a user interaction (details will vary depending on the LIMS configuration). If it is still in progress, information will be provided about the whole run and individual samples.
4. When the run completes, results can be acquired using the run ID. Results are available in reports as HTML and sometimes also PDF or directly as structured JSON data.


LIMS
GridION API
Send sample sheet
sample sheet
sample sheet ID
Get status of assay run processing (not started)
sample sheet ID
not started
Get status of assay run processing (in progress)
sample sheet ID


progress status
Get status of assay run processing (completed)
sample sheet ID
reports

9. Installing system updates

> **IMPORTANT**
>
> **This section requires IT Administrator permissions to complete.**

1. **While the GridION Q is not intended to have regular upgrades that change features, you may want to perform regular updates to the operating system of the device. The following command will update the system without affecting the sequencing software itself:**

```
sudo /opt/ont/mooneye/bin/ont-mooneye-software-update --os
```

You can run this command with a frequency decided by your IT department.

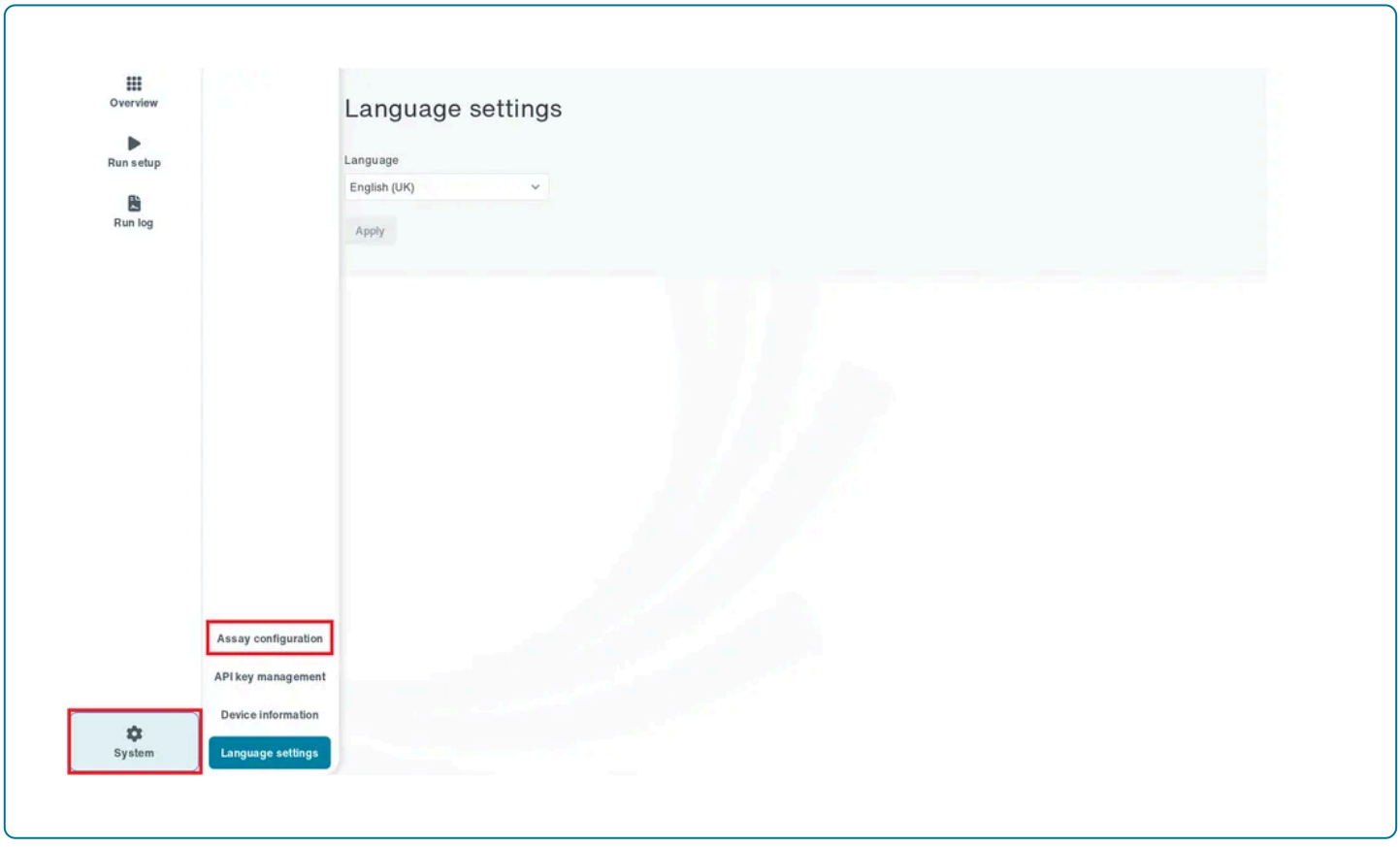
10. Configuring an assay definition file for your own assay

Introduction

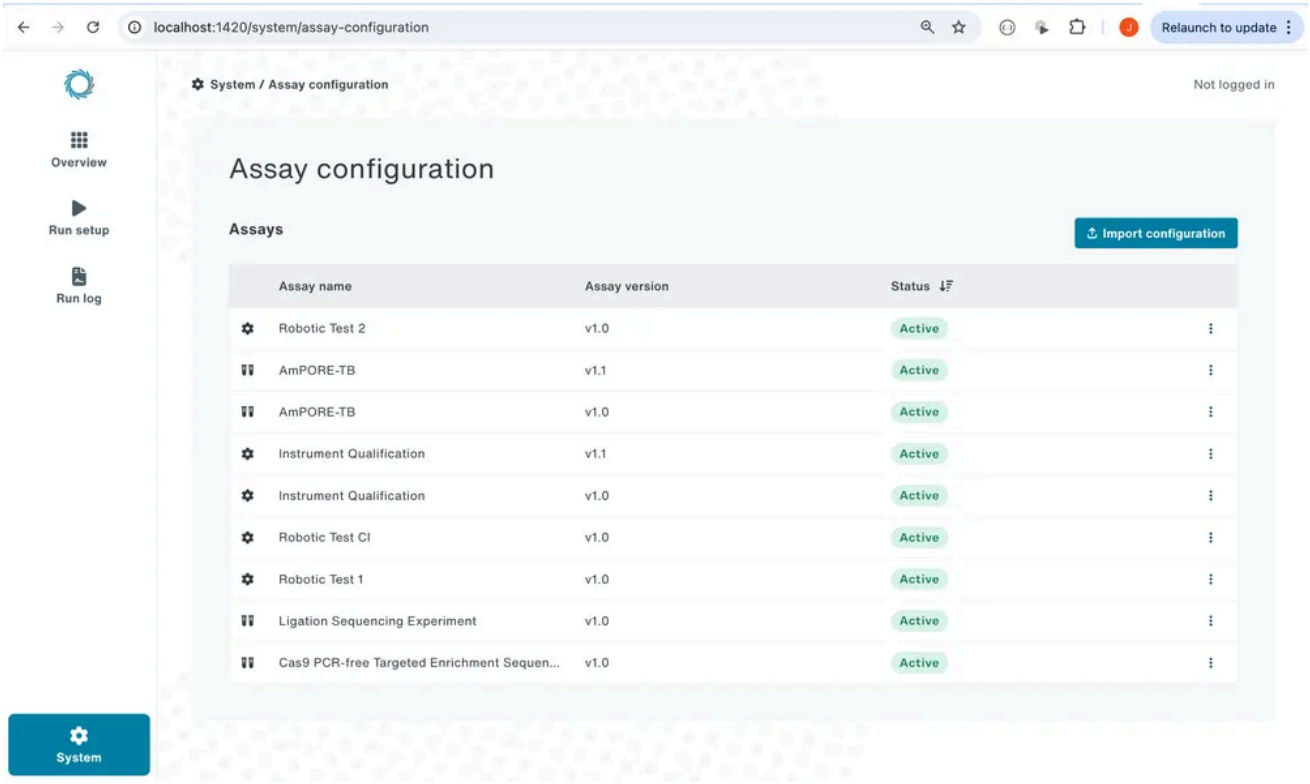
The Q-line sequencing software uses assay definition files to run each chemistry and assay type. The files provide the software with values for key sequencing parameters. If you have designed your assay on Q-line products and want to run it in a production environment, multiple adjustments will be required until it satisfies your needs.

You can only export, edit, and re-import assay definition files if you have the role of Lab Manager. **You should test your custom assay definition file to ensure it works before proceeding to scale/high-value samples.**

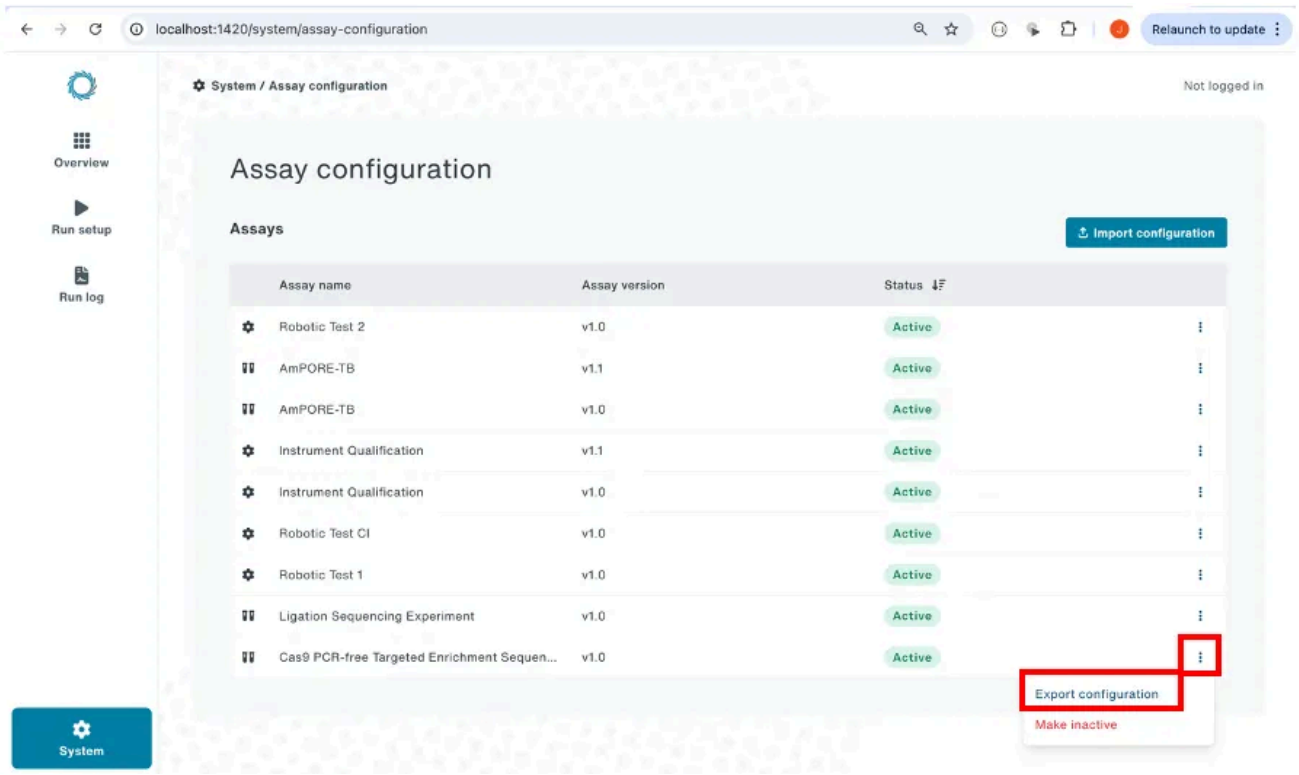
1. **In the sequencing software, click on System, then click Assay Configuration.**



2 **You will see a list of available assay definition files. Click on the three dots next to the default file for the sequencing kit you want to use for your assay. For example, if you use the Rapid Barcoding Kit (Q-SQK-RBK110.96), select the assay definition file for Rapid Barcoding Experiment 01-96.**



3 **Click Export Configuration.**



4 **Open the file in a text editor (e.g. Notepad++).**

5 **Edit the assay definition file with appropriate values for your assay. The configuration parameters are described in more detail below. You will need to edit certain parameters and leave other parameters at their default values.**

6 **Click Save As to save the assay definition file as a new .toml file.**

Assay definition parameters

The formatting of the file content is important:

- Text after a # symbol is for comments; do not change the comments.
- In cases where a line contains an =, only make edits to values after the =.
- Set text values between quotation marks (“”).
- Do not change the values contained within square brackets ([]). The exception to this is the field `minknow_parameters` .

The assay definition file is divided into six sections, each headed by lines that begin with #.

Basic parameters

You will need to change some of the fields described in this section to create your own assay definition file. Changes to these fields may affect sequencing performance if you are changing the flow cell and kit product

codes. Incompatible values will result in the assay not being imported properly, halting during setup, or sequencing runs failing to start.

Assay definition core fields

This section provides information for how the sequencing software identifies the assay and how the assay is displayed in the UI.

You will need to decide on a naming and versioning convention for values in “key” and “version”. Appropriately controlling these values ensures that the sequencing software can identify your assay as a unique assay. When compiling a sample sheet for your sequencing experiment, you will need to use the same values in “key” and “version” as those in the assay definition file for the sequencing experiment to proceed correctly.

Field	Restrictions	Description
name	text	How the assay is displayed in the UI, including on the Assay Selection screen.
key	alphanumeric characters and -	A unique name for your assay, which will be used in certain back-end processes and in the sample sheets for your assay. Only one assay import is allowed per key/version combination. The sample sheet must match the key when setting up a run.
version	“v#.#”	Allows for versioning of assays. Appears on the Assay Management screen in the sequencing software. Only one assay import is allowed per key/version combination. The sample sheet must match the version number when setting up a run.
description	text	A description that accompanies the assay name on the Assay Selection screen.
symbol	“test_tube” or “cog”	A symbol that accompanies the assay in some places on the UI. You can use either symbol depending on your preference.
estimated_seconds_to_result	integer	A value in seconds that the assay is expected to complete in. Should be an approximation of sequencing time + analysis time. The time to result is shown on the status bar for each position in the software user interface.

Flow cell details

This section provides information about the flow cell types and kits that are going to be used in the assay. It also tells the software if the assay involves barcoded libraries and the highest barcode number that can be expected across all experiments that use this assay. You can then specify barcodes on a per-experiment basis via the sample sheet.

The value for compatibility is a 3-character code that is written into the flow cell memory once the flow cell has been run with a particular assay. We recommend maintaining unique compatibility code for different assays to avoid unexpected interactions if the flow cell recalibration process fails to remove all previous library from a different assay.

Field	Restrictions	Description
product_code	Must be a known Oxford Nanopore Technologies product code	The product code for the flow cell. The software recognises the product code without the Q- prefix, so the prefix should be omitted. Since you will be starting from a pre-existing assay definition file, you will not need to edit this field.
kit	Must be a known Oxford Nanopore Technologies product code	The product code for the parent sequencing kit. For example, if using the Native Barcoding Expansion Kit, use the product code for the Ligation Sequencing Kit (SQK-LSK109). The software recognises the product code without the Q- prefix, so the prefix should be omitted. If the product code contains a '.' this will need to be replaced with '-'. E.g. SQK-RBK110.96 will become SQK-RBK110-96. Since you are starting from a pre-existing assay definition file, you will not need to edit this field.
compatibility	3 alphanumeric characters	Compatibility enforcement means only assays with the same compatibility key can share a flow cell. Must not exceed 3 characters in length.
barcoded_run	true/false	true if the assay will contain barcoded samples. false if the assay will not contain barcoded samples. Since you will be starting from a pre-existing assay definition config file, you will not need to edit this field.
last_barcode	integer highest available barcode number	The highest barcode that the software should expect to see. When setting a sample sheet for an experiment, do not use barcodes higher than this number. Can be omitted if the above field is set to false. Since you will be starting from a pre-existing assay definition file, you will not need to edit this field.

Flow cell check criteria

This section specifies threshold values for pore counts at flow cell check, allowing you to set assay-specific limits for flow cell quality depending on your sequencing output requirements. This also allows for different minimum pore limits to be set for different numbers of samples. **These values do not imply that the flow**

cell meets/does not meet warranty; they only specify whether the flow cell meets the requirement of the specific assay.

Changes to these fields may lead to a higher-than-expected failure rate in flow cell checks.

Field	Restrictions	Description
limit_type	“warn” or “fail”	“fail” will not allow a flow cell to be used for this assay if the pore count at flow cell check is below the given threshold. “warn” will provide an on-screen warning if the pore count at flow cell check is below the given threshold. The flow cell can still be used at your discretion.
maximum_samples	integer	Allows for different thresholds to be set depending on the number of samples to be loaded.
minimum_pores	integer **Note:** Do not set to <100.	The threshold value for the minimum number of pores found at flow cell check that will allow the assay set-up to proceed. You can set different pore minima for different numbers of samples. Flow cell check will proceed against the lowest threshold. Higher thresholds are then checked at the point of sample sheet input.

Sample sheet requirements

This section provides information on sample sheet composition that will be checked at sample sheet import for the correct compatibility.

Field	Restrictions	Description
initial_upload_barcodes_needed	true/false	true if the assay will contain barcoded samples. false if the assay will not contain barcoded samples.

You can classify samples according to their type. We suggest several types below:

- sample
- no_sample
- no_template_control
- positive_control
- negative_control

You can specify the number of samples that can or must belong to each category of sample. A category section always begins with `[sample_sheet.types.<category>]` where `<category>` is the name of your category.

Field	Restrictions	Description
kind	“sample”, “no sample”, or “control”	Groupings for sample types.
mix	integer minimum number of barcodes available	There must be at least this many samples of this type provided in the sample sheet. You can set the value to 0 if this sample type is optional.
max	integer ≤ maximum number of barcodes available	There must be no more than this many samples of this type provided in the sample sheet.

Advanced parameters

Changes to these fields will affect sequencing performance and are only recommended for experienced Nanopore users.

Sequencing configuration

This section sets parameters for the sequencing software to perform sequencing.

Changes to these fields may affect sequencing performance. You must independently verify the performance of sequencing runs that use custom settings on a per-assay basis.

Field	Restrictions	Description
space_required_bytes	integer	The number of bytes of disk space required to start a sequencing run. If less space than this is available at assay selection, a warning will be shown asking a manager to clear disk space. The assay setup cannot proceed until enough disk space has been cleared. We recommend setting this to the largest amount of data you have seen generated by a run of your assay plus a substantial margin. If you set this number too low, this could result in assay failure and the failure of other assays running at the time.
initial_pore_scan_healthy_count	integer	The number of pores that need to be seen at first scan to be sure that no major issues have been introduced between flow cell check and sequencing. If fewer than this number of pores are found, an on-screen warning is shown.
initial_strand_activity_healthy_percent	float <1	The % of time that active channels must spend sequencing strands of DNA to be sure that no major issues have been introduced between flow cell check and sequencing. We strongly recommend not changing this value.
minknow_parameters	varied	See section below.
maximum_samples	integer ≤maximum number of barcodes available	Allows for different run times to be set depending on the number of samples to be loaded.
runtime_hours	number	The length of sequencing time for libraries with up to the above number of samples.

Sequencing software parameters: Output

Field	Restrictions	Description
--fast5= --pod5= --fastq= --bam=	on/off	Specifies the desired output(s). Note: changing outputs can dramatically change the disk space required.
--fastq_reads_per_file=	integer	Requires --fastq=on The number of reads to write to each FASTQ file. Changing from the default (4000) will likely affect compute performance and could lead to delays to outputs or crashes.
--fastq_data compress	N/A	Turns on compression of FASTQ files (on by default). Remove to turn off compression. Note: This will dramatically change disk space required.
--base_calling=	on/off	Switches basecalling off or on. Must be on for FASTQ or BAM outputs. We strongly recommend not changing this value.
--guppy_filename=	basecaller files	Requires –base_calling=on Specify the basecaller filename. Changing to a more intensive basecaller could affect compute performance and lead to a delay or crashes.

Sequencing features

Field	Restrictions	Description
--mux_scan_period=1.5	number	ADVANCED Changes the time between pore scans, in hours. Changing from the default (1.5) could affect sequencing performance.

Barcoding

The barcoding section is only required if barcoding is a requirement of your assay. If your libraries will not be using barcoded reads, you can remove the `--barcoding` line and subsequent lines in the section.

The barcoding section requires escape characters () in some places. Only change the word `off` or `on`; do not change the format of the lines.

Field	Restrictions	Description
barcoding_kits=["$kit"]"	N/A	DO NOT CHANGE If you have started from the correct assay definition file, there is no need to change this parameter.
require_barcodes_both_ends=	on/off	For a read to be classified as such, a barcode must be detected at each end of the read. Switch this **on** if using the Native Barcoding Expansion and switch this **off** if using the Rapid Barcoding Kit.
detect_mid_strand_barcodes=	on/off	The read will be classified as Failed if a barcode is found mid-read. This applies only when the mid-read barcoding score is above the specified confidence score.
min_score_mid=	integer, 1-100	The confidence score needed to find a barcode mid-read. The default value is 50.
ignore_unspecified_barcodes=	on/off	The sequencing software will look for barcodes that were not specified in the sample sheet when performing demultiplexing.

Other

Parameters in this section affect the filtering of reads and/or final outputs. Changes to this section are only recommended for experienced Nanopore users.

Field	Restrictions	Description
--read_filtering min_qscore=9	number	ADVANCED Sets the threshold for the q-score. Reads with a q-score below this value will be placed into “fail” output folders.
--read_splitting enable=on min_score_read_splitting=60	on/off number	ADVANCED Allows the basecaller to detect adapters in the middle of reads and therefore split them into separate reads.
--min_read_length=	integer (choose from 20, 200, or 1000)	ADVANCED Reads estimated to be below this length will not be passed to the basecaller for basecalling. They will not be written to output files and cannot be recovered at a later time.

Analysis configuration

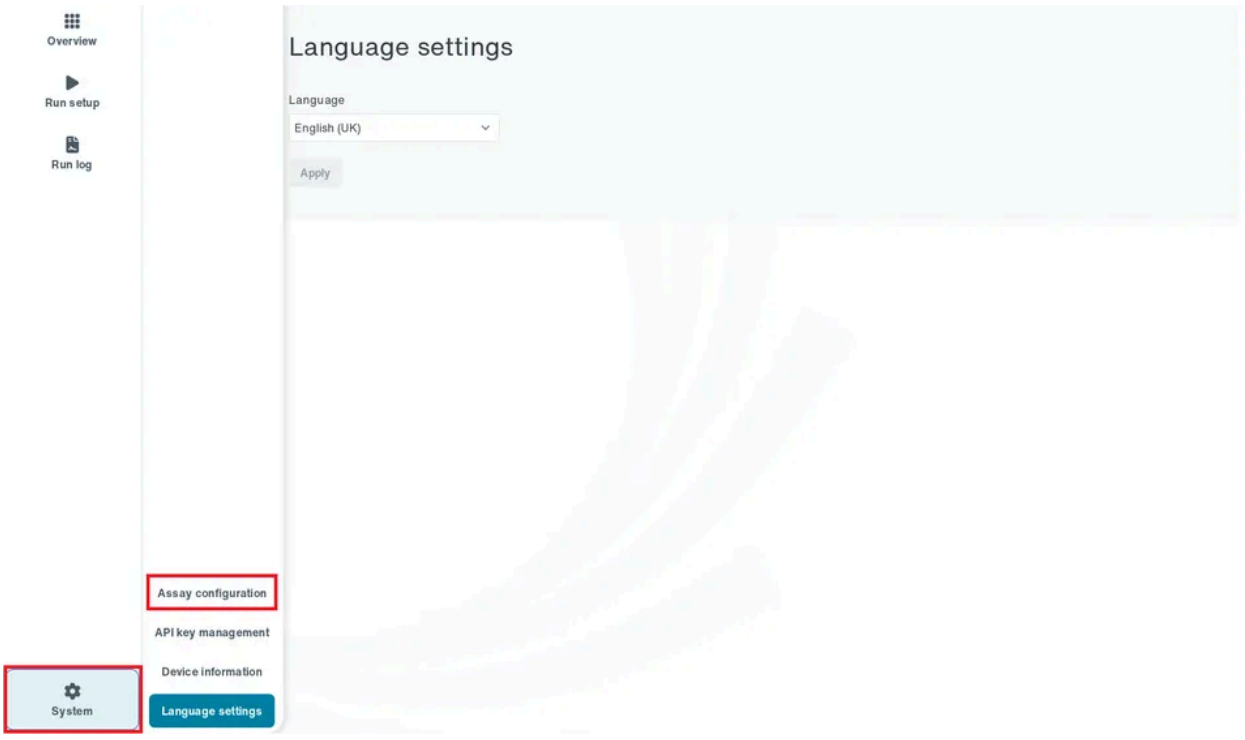
At present, some assays come with a post-basecalling analysis workflow that is configured for use with the assay. If this is a requirement for you, please contact Oxford Nanopore Technologies.

Import the assay definition file into the sequencing software

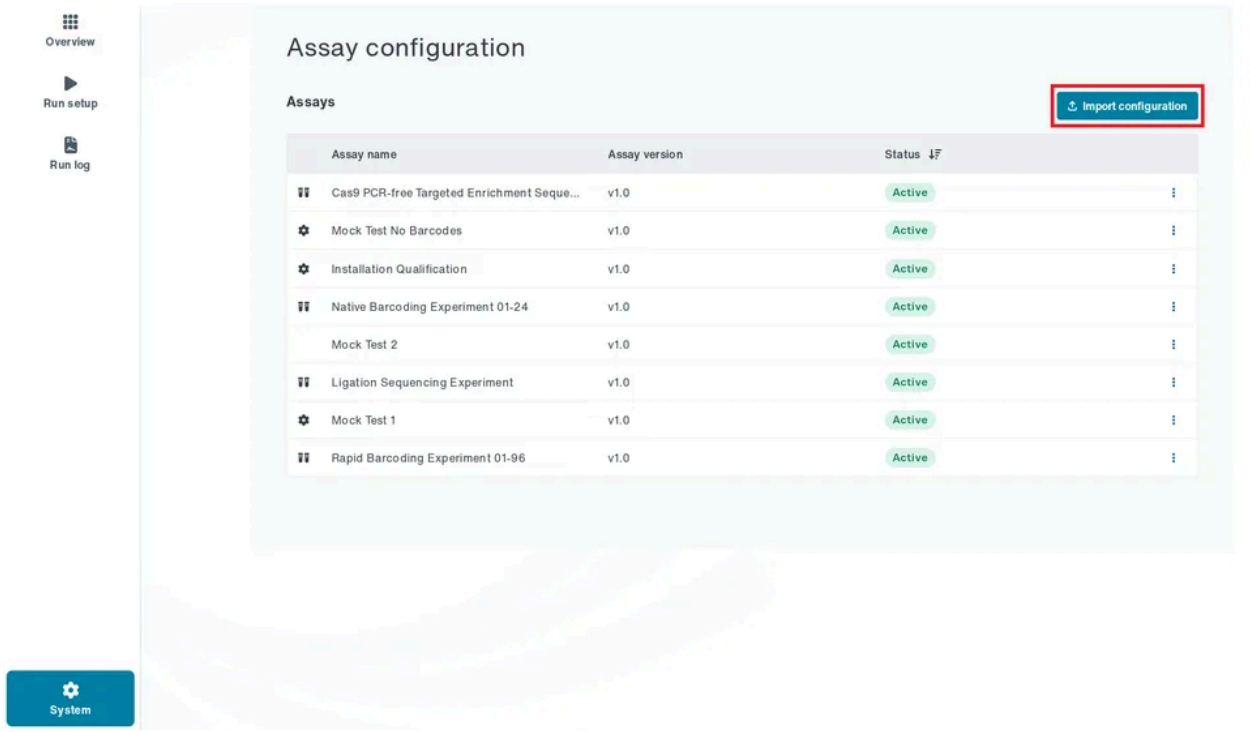
You will only see this option if you are logged in as a Lab Manager.

7 Open the sequencing software.

8 Navigate to Settings, then click Assay configuration.

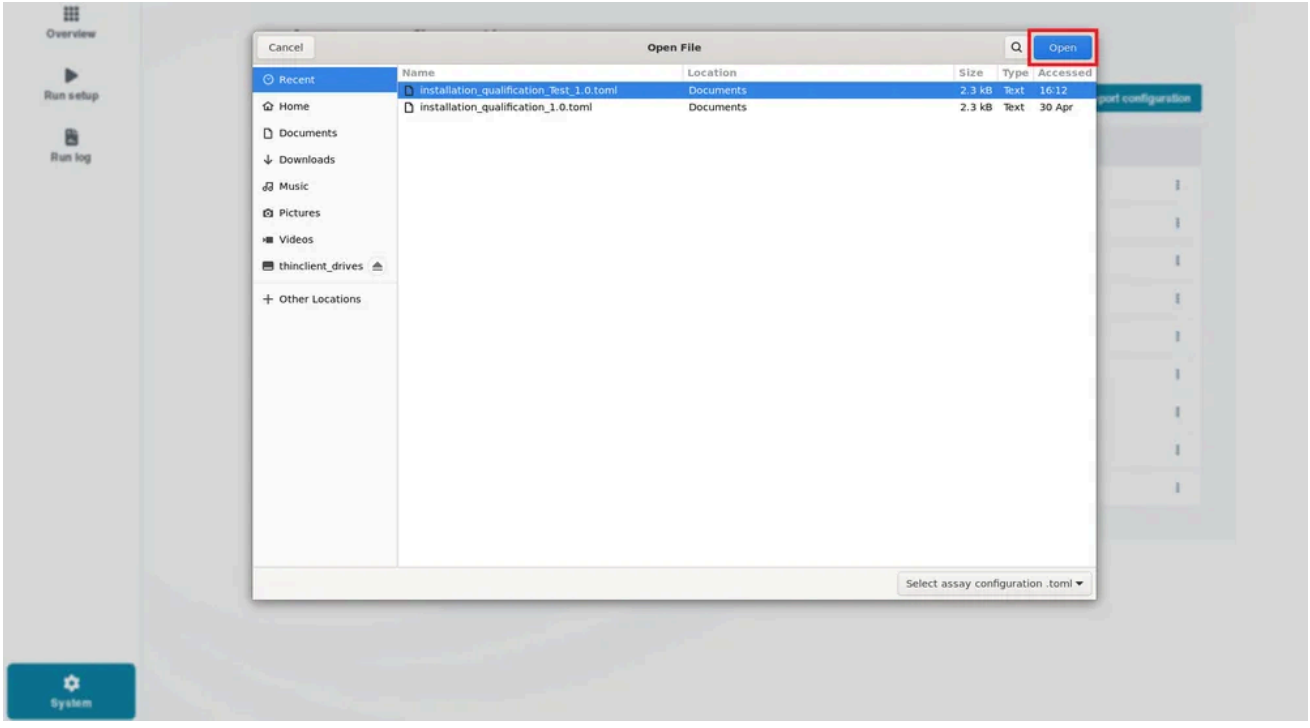


9 Click Import configuration.



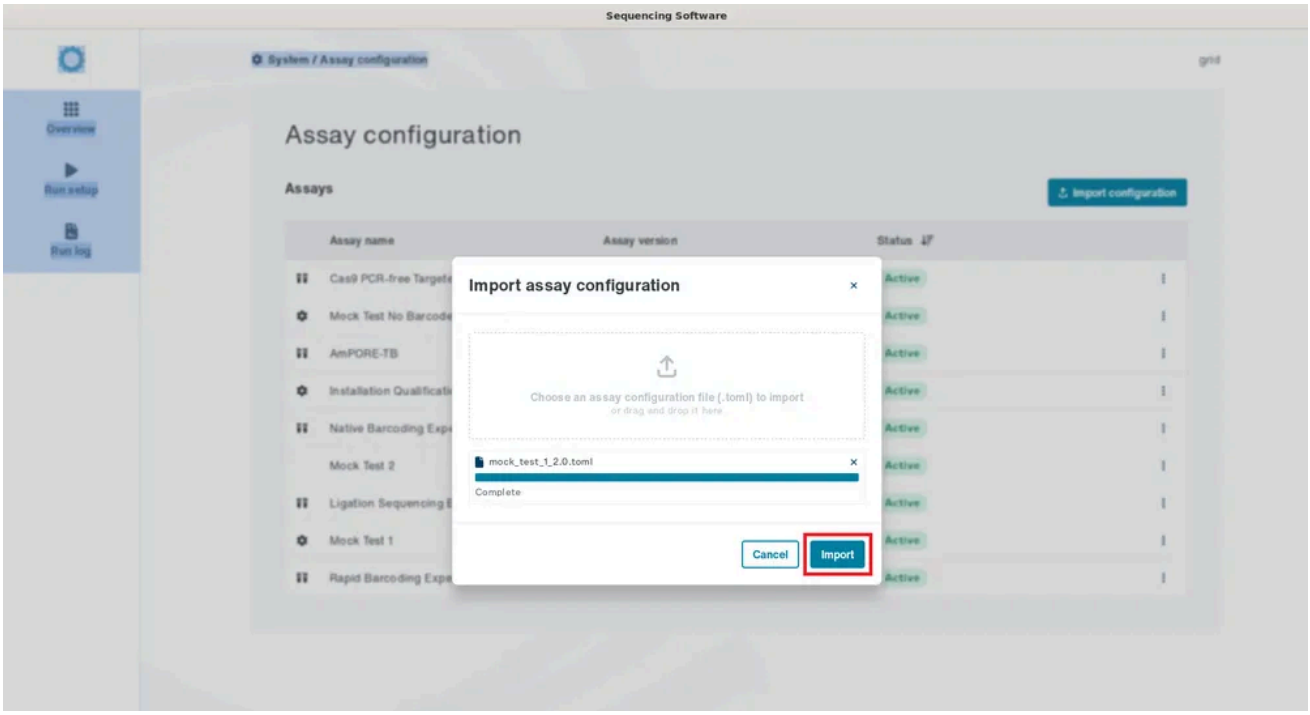
10 Navigate the file system to the location where you have saved your assay definition .toml file. Click on your saved file.

11 Click Open.



Note: If the assay definition file is incorrectly filled out, the sequencing software will fail to import the assay and will list the errors to correct.

12 Click Import.



13 Check that your assay is present in the list with the correct version.

14 Check that your assay is set to Active. If it is Inactive, click the three dots and then click Set Active.

15 After proceeding to a sequencing tests of the new assay, you will be able to decide whether to leave it as Active or make it Inactive.

16 If applicable, set any older versions of the assay to Inactive.

Your assay should now be selectable from the Assay Selection screen for all users.

Note: Switching assays from Active to Inactive is the archiving system of the Sequencing software: deleting assays is indeed not possible.

11. Configuring audit log

Enabling and configuring auditing

The Linux Audit system provides a framework to track security-sensitive information by recording events and mapping them to users as they occur. These events are recorded locally and can be sent, as they occur, to remote log destinations using syslog RFC 5424: The Syslog Protocol

Audit does not provide additional security to the platform; rather, it can be used to discover violations of its security policies.

The following events are explicitly recorded:

- All processes started by any logged-in user
- All file deletions, renames, ownership, permissions and attribute changes
- All commands run with elevated privileges
- Hostname changes
- System clock changes
- The kernel module loads and unloads
- All user logins and privilege level changes
- Configuration changes related to user identities and elevated privileges (`sudo`)
- Configuration changes related to user login access and the recording of logins
- Changes to attributes (a.k.a. permissions and ownerships) and writes to the files in the following directories:
  - /opt/ont/minknow
  - /opt/ont/gourami
  - /opt/ont/gourami-local-auth
  - /opt/ont/guppy
  - /opt/ont/mooneye
  - /opt/ont/nanoxint
  - /opt/ont/platform
  - /opt/ont/reception

Note that audit log procedures should be performed by your IT department.

Enable, disable and configure the Linux audit subsystem

The tool `ont-platform-security-audit` is used to enable, disable and configure audit.

__Important: while Linux audit is enabled at the time of installation, it will not log to syslog until enabled by this tool. __

After being enabled, audit will log to its own log file (/var/log/audit/audit.log) and to syslog. Syslog may be configured to send audit and other messages to a remote syslog server using the Oxford Nanopore Technologies tool `ont-platform-security-syslog` .

Usage examples:

Enable auditing and lock the setting to enabled. The lock means that audit will remain active until it is disabled (note: a reboot is required after disabling the audit tool).

```
sudo /opt/ont/platform/bin/ont-platform-security-audit --enable --lock
```

Unlock the audit and disable it on the next boot. For the change to take effect, reboot the system after this.

```
sudo /opt/ont/platform/bin/ont-platform-security-audit --disable --unlock
```

Display the current status of the audit subsystem:

```
sudo /opt/ont/platform/bin/ont-platform-security-audit --status
```

Configuring Syslog

Syslog is a widely used standard for message logging. It is used for various tasks, including system management and security auditing. On the GridION, syslog is implemented via the subsystem `rsyslogd` and configured using the tool `ont-platform-security-syslog` . Syslog is enabled by default and stores messages locally in the file `/var/log/syslog` .

For effective system management and auditing, we recommend that syslog messages be sent to a remote syslog server to store them and to apply additional filtering and monitoring. This remote store is considered an essential security measure within many organisations.

Syslog is enabled at system installation which can be configured to use for a remote syslog server, as outlined in the examples below. The remote server must have been configured to receive these messages, and the network between the two must be capable of propagating the messages. The transport protocol (UDP/TCP) can be configured, and the port number can be specified. By default, port #514 and TCP transport protocol will be used.

Usage examples:

To configure syslog to send messages to the remote server 192.168.1.10:

```
sudo /opt/ont/platform/bin ont-platform-security-syslog --enable --server 192.168.1.10
```

To configure syslog to send messages to the remote server 192.168.1.10 using the UDP and on port number #765:

```
sudo /opt/ont/platform/bin ont-platform-security-syslog --enable --server 192.168.1.10 --
protocol udp --port 765
```

To configure syslog to send messages to the remote server 192.168.1.10 and to schedule the cronjob to run six times per hour:

```
sudo /opt/ont/platform/bin ont-platform-security-syslog --enable --server 192.168.1.10 --
cronjob 6
```

To disable syslog sending to the current remote server:

```
sudo /opt/ont/platform/bin/ont-platform-security-syslog --disable
```

To disable the scheduled cronjob:

```
sudo /opt/ont/platform/bin/ont-platform-security-syslog --cronjob 0
```

12. GridION security

GridION security

Encryption is supported via LUKS (v1 and 2) for local drives. Please note that the technique implemented by LUKS only protects data at rest.

For network drives to access the platform, both NFS and SMB (via Samba) protocols must be supported. Data encryption on data transfers is only supported in SMB3. NFS does not provide encryption on data transfer, whereas encryption for authentication requests is standard for SMB protocol versions 2 upwards. We recommend that SMB version 1 be disabled. NFS supports authentication encryption in NFSv3 with GSS and in NFSv4.

System updates are normally via ISO images supplied by Oxford Nanopore Technologies. Online updates for individual and batch updates of Linux are available, though these may introduce compatibility issues for the installed version of the sequencing software. For those cautious of security, automatic system package updates can be set up, with the understanding that there may occasionally be compatibility issues with the installed sequencing software version.