

lumiraDx™ Connect User Manual

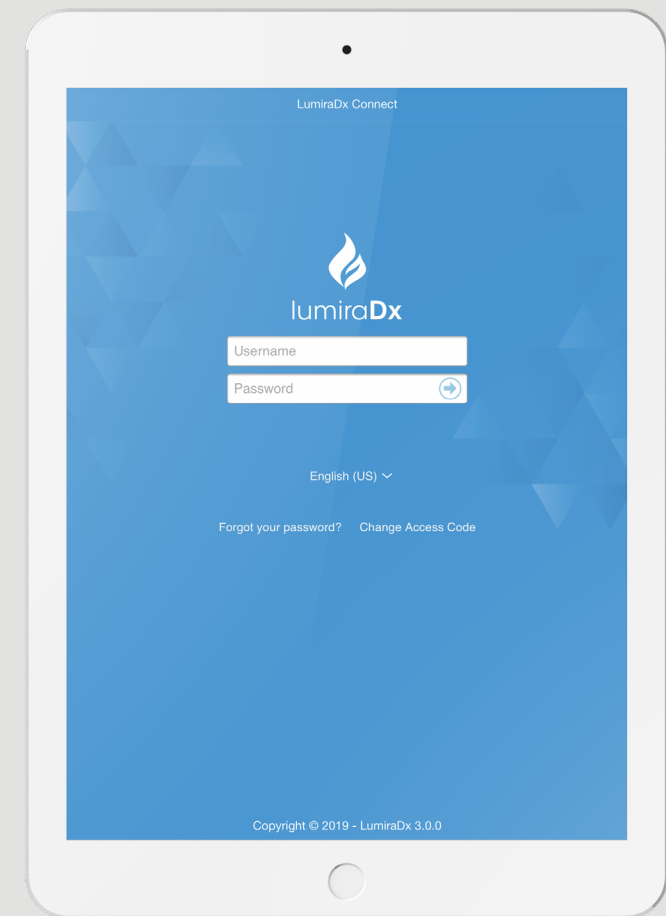


LumiraDx Group Limited,
2024 - © All rights reserved, worldwide.

LumiraDx UK Ltd
Roche House Charles Avenue
Burgess Hill
England
RH15 9RY
United Kingdom
Company Number: 09206123

ART-00300 Rev7

For product and connectivity support please contact LumiraDx
Customer Services at customerservices@lumiradx.com



Connect User Manual

Contents

1	Abbreviations	3
2	Overview of LumiraDx Connect	4
2.1	LumiraDx Connect Manager	6
2.2	LumiraDx Connect App	7
2.3	LumiraDx Connect Hub	7
2.4	EHR Connect	8
3	Getting Started	9
3.1	Unpacking the Connect Hub	9
3.2	Installing the LumiraDx Connect App	9
3.3	Powering the Connect Hub	10
3.4	Connect Hub Configuration	10
3.5	Configuration with a wired Ethernet connection	10
3.6	Configuration with a wireless connection	15
3.7	Using a mobile device as a Connect Hub	19
4	Connect Manager System	20
4.1	WorkGroups	21
4.2	Users	23
4.3	Instruments	29
4.4	Test Results	31
4.5	Personal Settings	35
4.6	Organization and Quality Control Settings	36
5	Miscellaneous	42
5.1	Logging into Connect Manager	42
5.2	Username and password requirements	43
5.3	Application updates	43
6	Customer Services	44
7	Security	45
7.1	General Data Protection Regulation (GDPR) Compliance	45
8	Privacy Notice	46
9	Legal Notices	49

1 Abbreviations

EHR	Electronic Health Record
FIPS	Federal Information Processing Standard
GDPR	General Data Protection Regulation
ID	Identification
SSID	Service Set Identifier
LIS	Laboratory Information System
HIS	Hospital Information System

2 Overview of LumiraDx Connect

LumiraDx Connect is a smart integrated connectivity platform which allows users to configure and manage LumiraDx point of care Platform Instruments remotely, and transfer test results into an existing patient's Electronic Health Record (EHR). This is powered by LumiraDx Connect Manager and EHR Connect.

To use LumiraDx Connect it is advised the following checks are completed and information acquired from your IT department prior to continuing to setup and configure LumiraDx Connect:

- Local network configuration
 - Check whether there is a preference for Ethernet or Wireless connection
 - If your IT network uses a "Proxy" you will require the following information:
 - "Hostname" of the Proxy
 - "Port" number of the Proxy
 - Username and password, if necessary.
 - If you will use Wi-Fi for connectivity, you will need to obtain the following information:
 - The 'SSID' name of the Wi-Fi
 - The password for your Wi-Fi
 - If your local IT network requires access to be granted to secure websites, you will need to allow outbound access to *.lumiradx.com on ports 80, 123 & 443.
- Installing software on mobile devices
 - You will need to be able to install an app from the public app stores on a mobile / tablet device.

Standalone

Run patient tests and quality control tests.

Store test results together with time, date and patient ID.



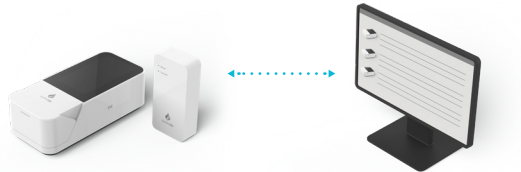
LumiraDx Instrument

Managed

Configure single or multiple Instruments.

Create WorkGroups and user login credentials.

Manage compliance and governance functions.



LumiraDx Instrument

*& LumiraDx Connect Hub
or LumiraDx Connect App*

**LumiraDx Connect
Manager**

EHR Connected

Integrate with Electronic Health Record for transfer of patient test results.

View patient test results in your LIS or HIS.



LumiraDx Instrument

*& LumiraDx Connect Hub
or LumiraDx Connect App*

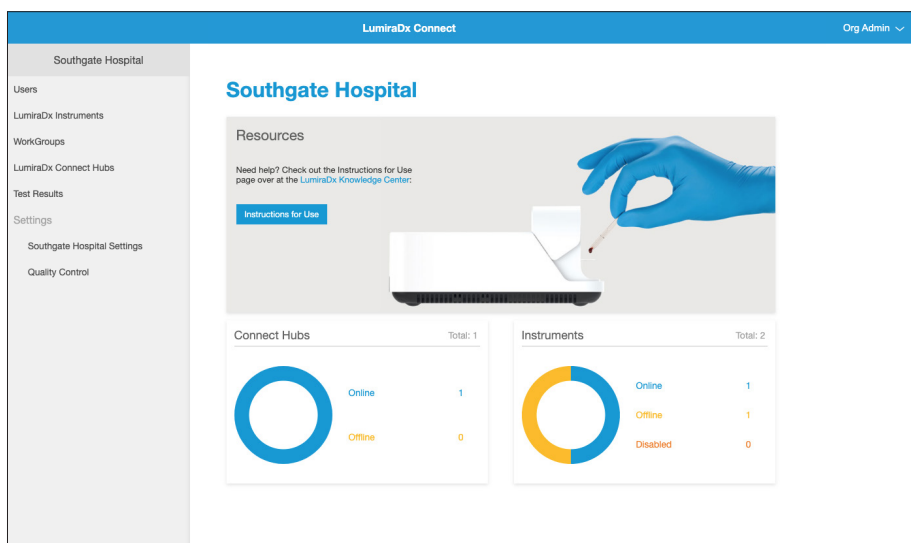
**LumiraDx Connect
Manager**

**Electronic Health
Record**

2.1 LumiraDx Connect Manager

LumiraDx Connect Manager provides an Administrator with the opportunity to oversee remote patient and quality control tests, making quality management easier. LumiraDx Connect Manager is a cloud-based website application and mobile application for native iOS and Android used for fast, accurate management of all your LumiraDx Instruments. It can be used to:

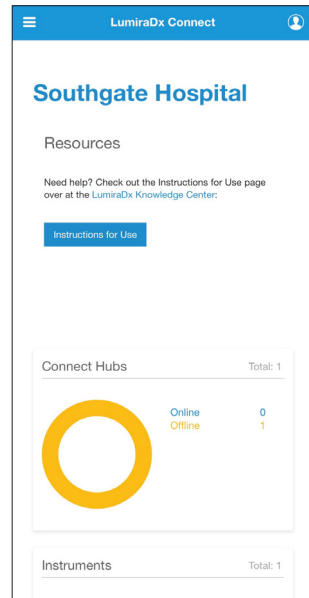
- Set up WorkGroups
- Assign users and LumiraDx Instruments to WorkGroups for ease of management
- Manage users and administrators
- Monitor and manage Instruments and Connect Hub (s)
- View Instrument test and Quality Control results
- Manage Quality Control Policy
- Manage Users training status



2.2 LumiraDx Connect App

LumiraDx Connect App is an application for native iOS and Android which acts as a mobile version of LumiraDx Connect Manager. In addition to allowing access to Connect Manager from a mobile or tablet, the LumiraDx Connect App can also be used to:

- Perform initial configuration and connection of Connect Hubs to a Wi-Fi network
- Act as an alternative method of connecting an Instrument to LumiraDx Connect when operating out of range of a Connect Hub



2.3 LumiraDx Connect Hub

LumiraDx Connect Hub is a standalone module which allows Instruments to automatically communicate with the Connect Manager application through a Bluetooth Low Energy connection.



The Connect Hub:

- Seamlessly and wirelessly transfers test results collected by LumiraDx Instruments
- Is highly secure – Instruments only communicate through designated hubs
- Automatically connects to Instruments within a 10-meter range
- Connects to a network using Wi-Fi or Ethernet
- Offers support for up to 7 Instruments from each Connect Hub simultaneously
- Has a simple interface showing power and connection status
- Is provided with interchangeable power blades which are compatible with power outlets in most geographic areas
- Is easy to set up using the LumiraDx Connect App

2.4 EHR Connect

EHR Connect is an additional service that enables seamless connection between the LumiraDx Instrument and existing Electronic Health Record systems allowing test results to be saved to patient medical records. Integration with a wide range of healthcare systems is supported and the technology is compatible with industry operation standards such as HL7, GDT and others, and is flexible to support both cloud and local based installations.

EHR Connect can provide additional support for the transfer of test results, patient positive confirmation at the time of the patient test, administration of Instrument Operators and Quality Control policy settings either through seamless integration with Connect Manager or an Organization's existing middleware system. The extent of the integration depends on the level of management supported by the middleware provider.

Further information about this additional service can be obtained from LumiraDx Customer Services.

3 Getting started

3.1 Unpacking the Connect Hub

The LumiraDx Connect Hub package includes the following contents:

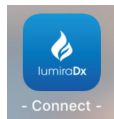
- LumiraDx Connect Hub
- LumiraDx Connect Hub power blades
- LumiraDx Connect Hub pack insert

Inspect the Connect Hub and packaging for damage before use. For safety reasons, do not plug in a damaged Connect Hub, and report any damage to Customer Services. Refer to the Customer Services chapter of this Connect User Manual for contact information.

3.2 Installing the LumiraDx Connect App

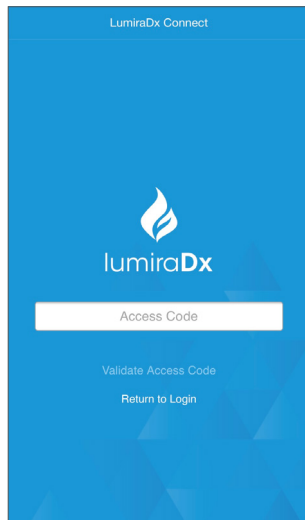
Your organization's designated administrator will oversee the LumiraDx setup and will receive initial connectivity details from LumiraDx. These details will be needed for the first-time login to Connect Manager.

The LumiraDx Connect App is available through Android and iOS app stores. To install the Connect App on to a mobile device, open the app store, search for LumiraDx Connect and install the app.



Note: On Android devices, if the app asks, "Allow Connect to access this device's location?" Select "Allow". Android devices will not allow Bluetooth to connect unless access to the device's location is allowed.

1. Open the app and enter the Access Code provided.
2. Tap/select 'Validate Access Code'.
3. Enter username, then password.
4. Tap 'Login'.



3.3 Powering the Connect Hub

Using the correct Connect Hub power blade, plug the Connect Hub into a wall socket. When the Connect Hub is powered, the 'Power' indicator will light up.


3.4 Connect Hub Configuration

Once configured, Connect Hubs will begin transferring data automatically between LumiraDx Instruments, Connect Manager and Electronic Health Record. Connect Hubs can only be configured using the LumiraDx Connect App running on a mobile device. The mobile device must be within 10 meters of the Connect Hub for successful setup.

3.5 Configuring a Connect Hub with a wired Ethernet connection

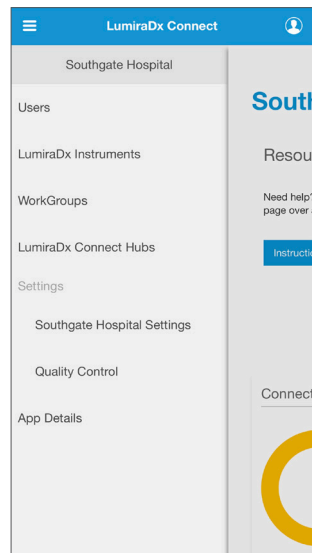
If your organization does not require use of a proxy, you may be able to start using your Connect Hub by simply connecting it to the power supply and inserting an Ethernet cable into the Connect Hub Ethernet port.

If your organization does require use of a proxy, please follow the following steps:

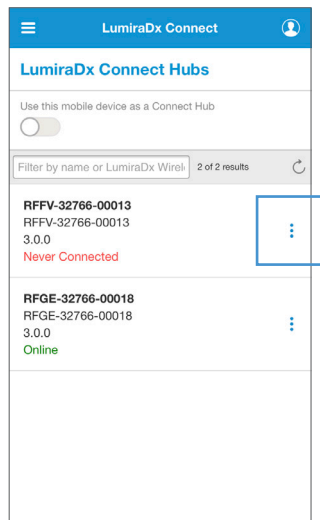
1. Login to Connect App on a mobile device and tap the menu icon  at the top left of the screen to access the menu

Note: Make sure Bluetooth is turned on for your mobile device

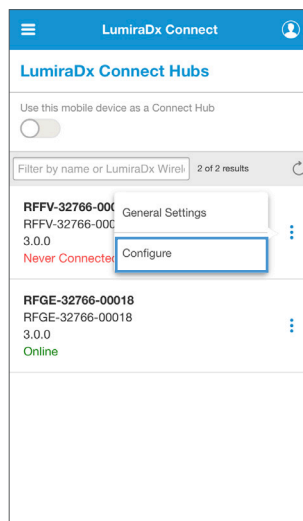
2. Tap 'LumiraDx Connect Hubs'



3. Tap the Action Menu  for the Connect Hub you wish to configure.

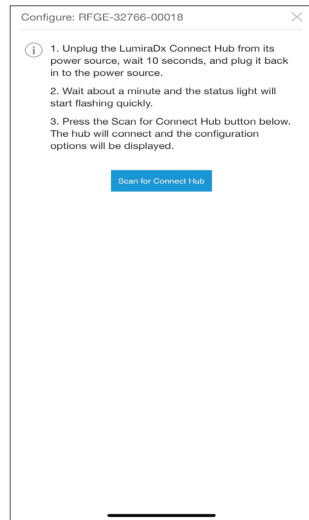


4. Tap 'Configure' from the drop-down menu.



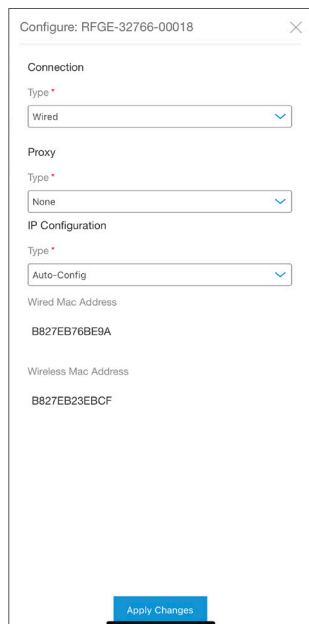
5. Unplug the LumiraDx Connect Hub from its power source, wait 10 seconds, and plug it back into the power source.
6. Insert one end of the Ethernet cable into the Connect Hub Ethernet port and the other end of the cable to either the wall socket Ethernet port or a router.
7. Wait about a minute and the Connect status light will start flashing quickly.
8. Tap 'Scan for Connect Hub'.

The Connect App will now connect to the Connect Hub and you will now see the configuration settings for the Connect Hub.



9. In 'Connection' section, select 'Wired'.
10. You may need to contact your IT department for your 'Proxy' details. If your organization does not require use of a proxy, select 'None' in the 'Proxy' menu.
11. If your organization requires use of a proxy, select 'Manual' in the 'Proxy' menu then complete the fields below.
12. You may also need to contact your IT department for 'Static IP (IPv4)' configuration details. If your organization does not require a Static IP for internet access, select 'Auto-config' in the IP Configuration menu.

Note: If you do not know what values to enter in these fields, ask your Network Administrator.



13. If your organization requires registering the MAC Address of the Connect Hub to gain internet access, the address is now displayed on the configuration screen. Note there are separate Addresses for Wired versus WiFi Connections.
14. Tap 'Apply Change'.

Configure: RFGE-32766-00018

Connection

Type *

Wired

Proxy

Type *

Manual

Hostname *

URL or IP Address

Port *

0

Username

Password

IP Configuration

Type *

Auto-Config

Wired Mac Address

B827EB76BE9A

Wireless Mac Address

B827EB23EBCF

Apply Changes

15. A confirmation message will show that the configuration settings have been applied.
16. The Connect Hub "Connect" light will change from a flashing green light to a solid green light within 60 seconds.

Configure: RFFV-32766-00013

Connection

Type *

Wi-Fi

SSID *

LumiraDx

Password

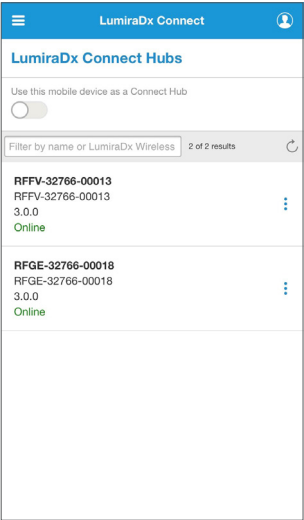
Proxy

Type *


None

Apply Changes

17. The Connect App will now show that the Connect Hub is online.

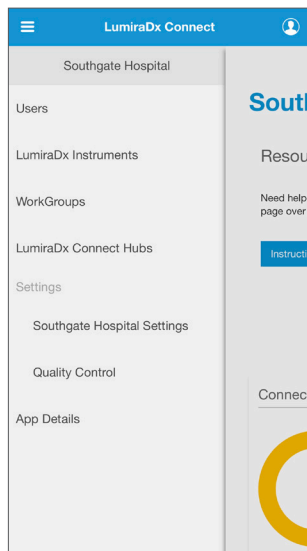



3.6 Configuring a Connect Hub with a wireless connection

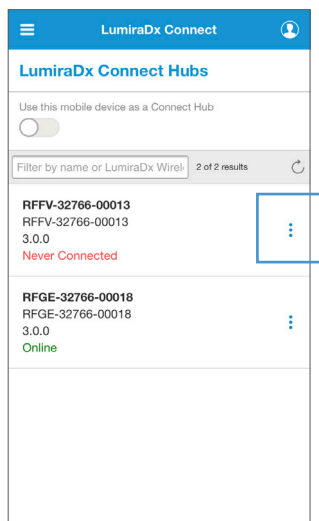
1. Login to Connect App on a mobile device and tap the menu button  at the top left of the screen to access the menu.

Note: Make sure Bluetooth is turned on for your mobile device.

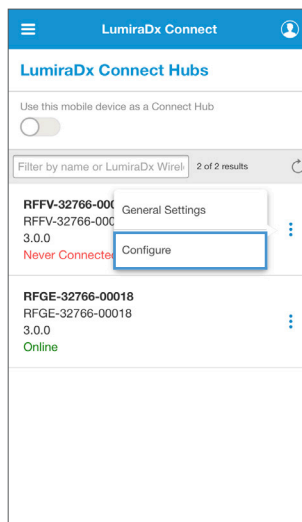
2. Tap 'LumiraDx Connect Hubs'.



3. Tap the Action Menu  for the Connect Hub that you wish to configure.

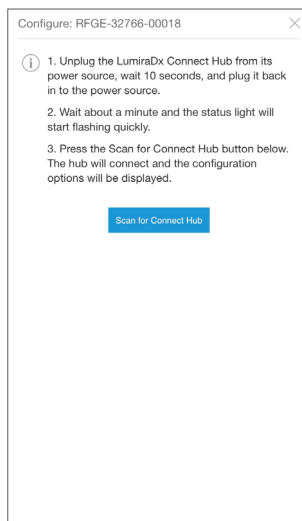


4. Tap 'Configure' from the drop-down menu.



5. Unplug the LumiraDx Connect Hub from its power source, wait 10 seconds, and plug it back into the power source.
6. Wait about a minute and the Connect status light will start flashing quickly.
7. Tap 'Scan for Connect Hub'.

The Connect App will now connect to the Connect Hub and you will see the configuration settings for the Connect Hub.



8. In 'Connection' section, select 'Wi-Fi'.
9. In 'SSID', enter the Service Set Identifier (SSID or network name) for the Wi-Fi network.
Note: if you do not know what the SSID is, ask your Network Administrator.
10. Enter the Wi-Fi 'Password'.
11. You may need to contact your IT department for your 'Proxy' details. If your organization does not require use of a proxy, select 'None' in the 'Proxy' menu.
12. If your organization requires use of a proxy, select 'Manual' in the 'Proxy' menu then complete the fields below.
13. You may also need to contact your IT department for 'Static IP (IPv4)' configuration details. If your organization does not require a Static IP for internet access, select 'Auto' in the IPv4 menu.

Configure: RFGE-32766-00018

Connection

Type *
Wi-Fi

SSID *

Password

Proxy

Type *
None

IP Configuration

Type *
Auto-Config

Wired Mac Address
B827EB76BE9A

Wireless Mac Address
B827EB23EBCF

Apply Changes

Note: If you do not know what values to enter in these fields, ask your Network Administrator.

Important: IP and Subnet information should be entered with a slash separating the values (no spaces). The Subnet should be entered in CIDR notation instead of the full address.

Ex. 192.4.0.0/24

The above example equates to an address of 192.4.0.0/255.255.255.0

14. If your organization requires registering the MAC Address of the Connect Hub to gain internet access, the address is now displayed on the configuration screen. Note there are separate Addresses for Wired versus WiFi Connections.
15. Tap 'Apply changes'.

Configure: RFGE-32766-00018

Connection

Type *
Wi-Fi

SSID *

Password

Proxy

Type *
Manual

Hostname *
URL or IP Address

Port *
0

Username

Password

IP Configuration

Type *
Auto-Config

Wired Mac Address
B827EB76BE9A

Wireless Mac Address
B827EB23EBCF

Apply Changes

16. A confirmation message will show that the configuration settings have been applied.
17. The Connect Hub "Connect" light will change from a flashing green light to a solid green light within 60 seconds.

Configure: RFFV-32766-00013

Connection

Type *

Wi-Fi

SSID *

LumiraDx

Password

Proxy

Type *

None

Apply Changes

18. The Connect App will now show that the Connect Hub is online.

LumiraDx Connect

LumiraDx Connect Hubs



Use this mobile device as a Connect Hub

Filter by name or LumiraDx Wireless 2 of 2 results

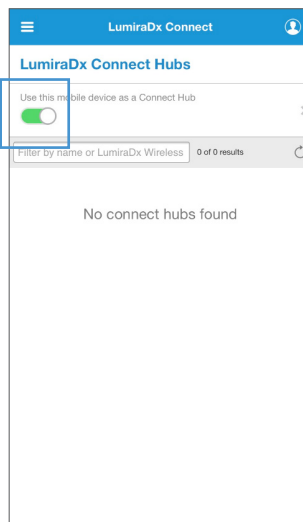
RFFV-32766-00013 RFFV-32766-00013 3.0.0 Online	⋮
RFG-32766-00018 RFG-32766-00018 3.0.0 Online	⋮

3.7 Using a mobile device as a Connect Hub

If a LumiraDx Instrument is out of range of a Connect Hub but needs to be managed by Connect Manager or to send test results to Connect Manager, a mobile device can be used as an alternative to the LumiraDx Connect Hub.

1. Login to Connect App on a mobile device and tap the menu button  at the top left of the screen to access the menu.
2. Tap 'LumiraDx Connect Hubs'.
3. On the Connect Hubs page, enable the mobile device to act as a Connect Hub by using the slider.
4. Tap the  icon to see what Instruments the mobile device is connected to.

Note: The mobile device as a Connect Hub feature is now available to all user roles.



4. Connect Manager system

The Connect Manager website or Connect App can be used to create the administrative infrastructure of the LumiraDx Platform.

Users of Connect Manager and Instruments can have different types of roles:

- **Organization Admin** is an administrator for the entire organization. They can login to Connect Manager, create new users, edit existing users, create WorkGroups and edit the settings of every WorkGroup.
- **WorkGroup Admin** is an administrator for one or more selected WorkGroups. They can login to Connect Manager and add Instrument operators to their specific work groups.
- **Instrument Admin** can login to LumiraDx Instruments, perform setup and upgrades and perform tests.
- **Instrument Operators** can login to LumiraDx Instruments to perform tests.

4.1 WorkGroups

Instruments and Users can be assigned to Workgroups (e.g. Cardiology). This allows control of which Users can use which Instruments. The WorkGroup settings area will be not be available and hidden if Instrument Operators are being managed through a middleware provider.

Note: Instruments may only appear in one WorkGroup while Users can be assigned to one or more.

To add a new WorkGroup:

- 1. Organization Admin must login to Connect Manager.
- 2. Tap 'WorkGroups' to display the list of existing WorkGroups.
- 3. Tap +

LumiraDx ConnectAdmin Account

WorkGroups

Filter by workgroup name

2 of 2 results

NAME	DESCRIPTION
Unassigned	Unassigned Instruments
Cardiology	

- 4. Enter the name of the new WorkGroup.
- 5. Optionally, enter a brief description of the new WorkGroup. This description appears next to the WorkGroup name when selected.
- 6. Each WorkGroup is set to the Organization's Time Zone by default. Select 'Override Organization's Time Zone' to choose a different Time Zone for the WorkGroup. Select the correct time zone from the drop-down list.
- 7. Tap 'Apply Changes'.

Create WorkGroup

Name *

Description

☐ Override Organization's Time Zone

Time Zone *

(GMT-05:00) Eastern Time (US & Canada)

Apply Changes

To view the Settings, Instruments and Users who belong to a WorkGroup, select the WorkGroup from the list.

Select 'Users' or 'Instruments' tabs to view the list of Users and Instruments in the WorkGroup. Select the 'Settings' tab to view the WorkGroup settings and override the organization's Quality Control Policy if required. Administrators can also override the organization's time zone to enable each WorkGroup to use a local time zone. Refer to the "Organization and Quality Control Settings" chapter of this Connect User Manual for more information.

Southgate Hospital

← WorkGroups

Users

Cardiology

Users

Instruments

Settings

Filter by name or username

3 of 7 results

NAME

USERNAME

FILES

Active

User 1, Nurse

operator1

Instrument Operator

User 2, Nurse

operator2

Instrument Operator

Admin, WorkGroup

wgadmin

Instrument Administrator, WorkGroup Administrator

4.2 Users

To edit or create a new User:

Organization Admin must login to Connect Manager.

From the Users page, select any User from the list to edit or tap + to create a new User.

Users			+
	Filter by name or username	6 of 6 results	
NAME	USERNAME	ROLES	
Active			
Last Name, First Name	admin	Instrument Administrator, Organization Administrator	
Admin, Org	root.94efa	Organization Administrator	
Smith, Steven	stevensmith	Instrument Operator, Organization Administrator	
Training Expiring Soon			
Doe, Jane	jd	Instrument Operator	
Training Expired			
Doe, John	jdoe	Instrument Administrator, Organization Administrator	
Disabled			
Doe, Jeff	jeffd	Instrument Operator, Organization Administrator	

Tap the filter icon to filter the list of users in view.

Users

Filter by name or username 11 of 11

Filters [Clear Filters](#)

Roles

Instrument Operator ☒

Instrument Administrator ☒

WorkGroup Administrator ☒

Organization Administrator ☒

Status

Active ☒

Training Expired ☒

Training Expiring Soon ☒

Disabled ☐

Sort

Username (default)

☒ Ascending

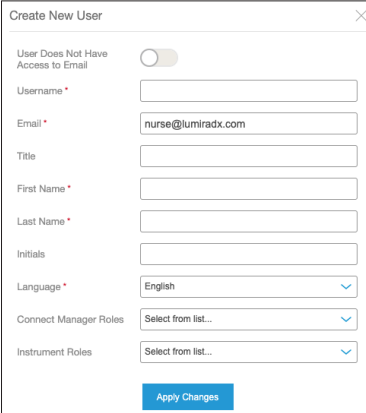
☐ Descending

Highlighted fields must be completed.

'Username' will be used for logging in to an Instrument or Connect Manager.

Note: Usernames are case sensitive.

An email address can only be used once by a single user within an organisation.



The 'Create New User' form has a toggle switch at the top labeled 'User Does Not Have Access to Email', which is currently turned off. Below the toggle are several input fields: 'Username' (empty), 'Email' (containing 'nurse@lumiradx.com'), 'Title' (empty), 'First Name' (empty), 'Last Name' (empty), 'Initials' (empty), 'Language' (a dropdown menu showing 'English'), 'Connect Manager Roles' (a dropdown menu showing 'Select from list...'), and 'Instrument Roles' (a dropdown menu showing 'Select from list...'). At the bottom right is a blue button labeled 'Apply Changes'.

If a new User does not have an e-mail account use the slide button to set a username and password for them.

Note: This feature is not available for all organizations. Contact LumiraDx Customer Services at customerservices@lumiradx.com for more information.

Connect Manager Roles – select one of the following:

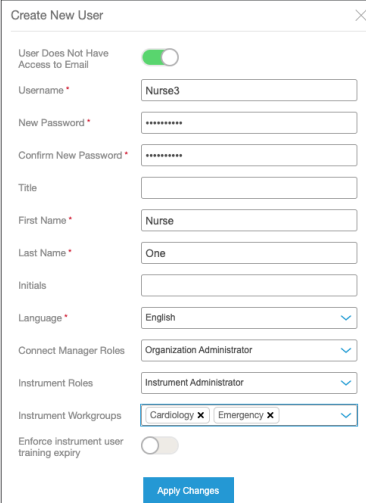
- None
- Organization Administrator
- WorkGroup Administrator

Note: If you select WorkGroup Administrator, you must select the WorkGroups to which the administrator belongs.

Instrument Roles – indicate whether the user is an Instrument Operator or Instrument Administrator.

Assign User appropriate WorkGroups.

Select whether enforced training compliance is required and the training expiration date.



The 'Create New User' form has the 'User Does Not Have Access to Email' toggle switch turned on. The input fields are: 'Username' (containing 'Nurse3'), 'New Password' (containing '*****'), 'Confirm New Password' (containing '*****'), 'Title' (empty), 'First Name' (containing 'Nurse'), 'Last Name' (containing 'One'), 'Initials' (empty), 'Language' (a dropdown menu showing 'English'), 'Connect Manager Roles' (a dropdown menu showing 'Organization Administrator'), 'Instrument Roles' (a dropdown menu showing 'Instrument Administrator'), and 'Instrument Workgroups' (a dropdown menu showing 'Cardiology' and 'Emergency' with 'x' icons). At the bottom right is a blue button labeled 'Apply Changes'.


Note: If 'Instrument Operator' is selected, the user will be able to login to Instruments and administer tests. If 'Instrument Administrator' is selected the user will be able to login to Instruments, perform setup and upgrades, and administer tests. Choose the appropriate WorkGroups for this User from the check list that appears.

Users cannot change their WorkGroup or Instrument roles themselves. Changes must be made by another Organization Administrator.

Note: If Instrument Operators are being managed through a middleware provider, the WorkGroup and Instrument Roles will not be available. Instrument Operators will need to be set up through the middleware connected system. Connect Manager Users can still be created and managed through Connect Manager.

Once a new User has been created, an automatic email will be sent to the User's email address containing their initial password which will expire within 24 hours.

If a username and password have been set for the User by an Administrator, the User will be required to change their password after their first login.

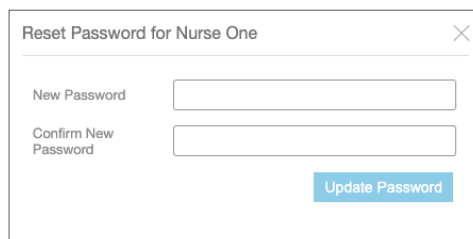
To disable or enable a User or to reset a User's password tap the action menu  for that User.

If a User account has been set up without an e-mail address the menu will show:

- Disable User
- Set New Password

Admin2, Org	admin2	Instrument Operator, Organization Administrator	<div>Disable User</div>
One, Nurse	nurse2	Instrument Administrator, Organization Administrator	<div>Set New Password</div>
User 1, Nurse	operator1	Instrument Operator	

Selecting 'Set New Password' will allow the Organization Admin to create a new password for the User.




The screenshot shows a dialog box titled "Reset Password for Nurse One" with a close button (X) in the top right corner. Inside the dialog, there are two text input fields. The first field is labeled "New Password" and the second field is labeled "Confirm New Password". Below these fields is a blue button labeled "Update Password".

If a User account has been set up with an e-mail address login the menu will show:

- Disable User
- Send Password Reset E-mail
- Set New Password

Users			
Filter by name or username			7 of 10 results
NAME	USERNAME	ROLES	
Active			Disable User
Admin, Org	admin	Instrument Operator, Organization Administrator	Send Password Reset Email
Admin2, Org	admin2	Instrument Operator, Organization Administrator	Set New Password
One, Nurse	nurse2	Instrument Administrator, Organization Administrator	

Selecting 'Send Password Reset E-mail' will result in an automated e-mail being sent to the User with their new password.



Admin User

Are you sure you want to reset this user's password? A new password will be emailed to the email address on the account.

Reset Password

Cancel

Instrument Operator Training

The Instrument Operator Training status can be viewed from the home screen.

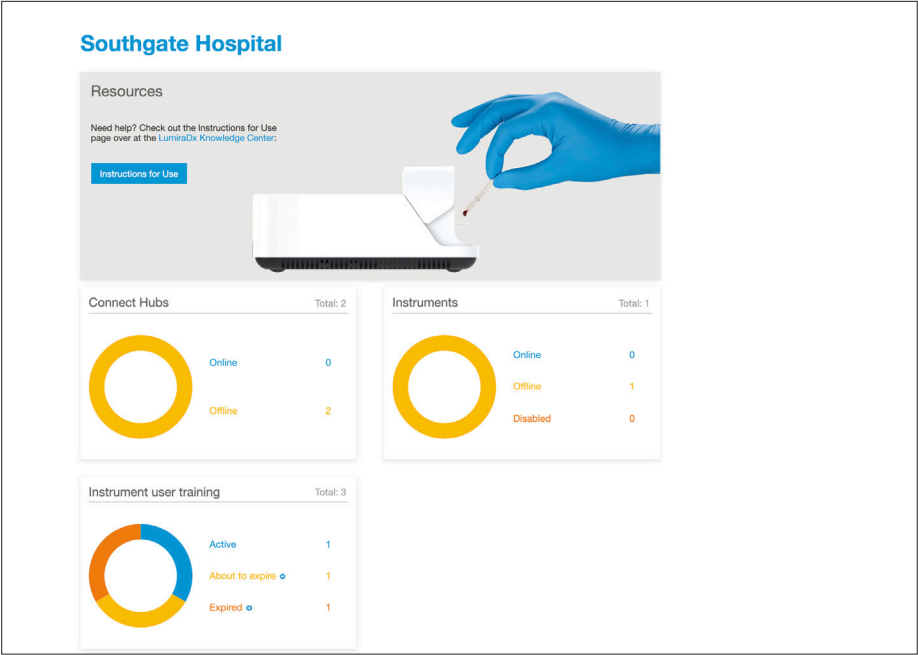
Active – Users who are within their training expiration date

About to expire – Users who are within 14 days of training expiration

Expired – Users who have passed their training expiration date. These users are unable to perform patient tests until their training has been updated and a new training expiration date set.

Click on a user status to see a filtered view of those users.


Note: User accounts without an e-mail address will not be notified if training has expired. Administrators must monitor the home screen dashboard and notify Users when training is about to expire.






4.3 Instruments

An organization's Instruments can be designated to a particular WorkGroup. This is useful if an organization prefers to restrict the use of any Instruments to certain departments. An Instrument's WorkGroup and other settings can be updated via the Instruments page in Connect Manager.

To update an Instrument's general settings:

- 1. Organization or WorkGroup Admin must login to Connect Manager.
- 2. Tap 'LumiraDx Instruments'.
- 3. Tap the action menu button  and 'General Settings' to view and edit the Instrument settings.

Instruments			
 Filter by name or serial number		1 of 1 results	
NAME	SERIAL NUMBER	STATUS	
REHH-32765-00553	REHH-32765-00553	Online	<div><div>General Settings</div><div>Test Results</div><div>Quality Control Report</div></div> <div></div>

- 4. 'Instrument name' – enter a name other than the default for the Instrument.
- 5. 'WorkGroup' – select the WorkGroup to which the Instrument is assigned.

Note: Instruments are assigned to the "Unassigned" WorkGroup by default. Move the Instruments to a WorkGroup created by (or for) your organization.

Warning: If the WorkGroup assignment of an Instrument is changed, all settings and operators will be cleared from the Instrument and new settings sent based on the new WorkGroup.

General Settings

Instrument Name *

REJH-32765-00569

WorkGroup *

Unassigned

Serial Number

REJH-32765-00569

LumiraDx Wireless Id

REJH-32765-00569

Software Version

1.2.0.1d94dee

Hardware Version

5.4

Apply Changes

A prompt will ask the User whether any test data should be deleted from the Instrument when changing WorkGroups or whether the test data should be kept.

Warning: Selecting 'Delete Data and reboot the Instrument' means that test data will only be visible in Connect Manager.

- 6. Tap 'Apply Changes'.

Note: The WorkGroup menu will be hidden for organizations that are managing Instrument Operators through a middleware provider.

The instrument detail view now indicates if the Instrument is in sync with the server for Operators, Test Result offloads and Instrument Settings.

General Settings

Instrument Name *

REJH-32765-00569

WorkGroup *

Cardiology

Workgroup modified

Would you like to delete all test data on the instrument?

Delete Data and reboot the instrument

Keep Data

Serial Number

REJH-32765-00569

LumiraDx Wireless Id

REJH-32765-00569

Software Version

1.2.0.1d94dee


Hardware Version

5.4

Apply Changes

To view the sync statuses for an Instrument:

- 7. Organization or WorkGroup Admin must login to Connect Manager.
- 8. Tap 'LumiraDx Instruments'.

Tap the action menu button  and 'General Settings' to view the instrument status.

Note: For Middleware customers that offload to a local electronic health record and use the Middleware system to manager Instrument Operators, would see Operators and Test Results show as "Not Synced". This is expected as these are managed outside of Connect Manager.

General Settings

Instrument Name *

REVF-00256-13657

WorkGroup

Unassigned

Serial Number

REVF-00256-13657

LumiraDx Wireless Id

REVF-00256-13657

Software Version

1.29.0.d9088b3

Hardware Version

50505

Registered

21 Oct 2024 14:45

Sync Statuses

Operators

Synced

Test Results

Not Synced

Instrument Settings

Synced

Apply Changes

4.4 Test Results

Patient Test results and Quality Control test results can be viewed from the Test Results dashboard or from the Instruments page. Results can also be exported to a .CSV file if required.

Note: LumiraDx recommends keeping Instruments connected during daily testing. If this cannot be achieved, the instruments should be connected at least once a day. Routinely connecting the instruments will ensure the transmission of test results to Connect Manager and any configured third-party systems.

To view Test Results dashboard:

1. Organization or WorkGroup Admin must log in to Connect Manager
2. Tap 'Test Results' to view Patient Test and QC Test dashboard

Southgate Hospital

Users

LumiraDx Instruments

WorkGroups

LumiraDx Connect Hubs

Test Results

Settings

Southgate Hospital Settings

Quality Control

Test Results

showing 8 results

Export Results

Filters

Clear Filters

Show All Data

Last Name

Serial Number

WorkGroup

Test Type

Date Range

Cancel

Apply

QC TESTS

QC tests

QC errors

QC errors (%)

Failed QC tests

Failed QC tests (%)

QC overrides

0

0

0%

0

0%

3

	RESULT	STATUS	OPERATOR	WORKGROUP	SERIAL NUMBER	
	PASS	Accepted	20 chars	Unassigned	REJH-32765-00569	
	PASS	Accepted	20 chars	Unassigned	REJH-32765-00569	
Mar 18, 2021 2:13 pm	INR	1.1	Accepted	20 chars	Unassigned	REJH-32765-00569
Mar 18, 2021 2:13 pm	SARS-CoV-2 Ag	POSITIVE +	Accepted	Jones, M.	Unassigned	REJH-32765-00569
Mar 15, 2021 5:44 pm	SARS-CoV-2 Ag	POSITIVE +	Accepted	Jones, M.	Unassigned	REJH-32765-00569
Mar 15, 2021 5:41 pm	SARS-CoV-2 Ag	NEGATIVE -	Accepted	Jones, M.	Unassigned	REJH-32765-00569
Mar 15, 2021 5:38 pm	SARS-CoV-2 Ag	NEGATIVE -	Accepted	Smith, J.	Unassigned	REJH-32765-00569
Mar 15, 2021 5:35 pm	SARS-CoV-2 Ag	PASS	Accepted	Clone, P.	Unassigned	REJH-32765-00569

3. Tap the filter icon to filter the list of Test Results
4. Filter results by surname, serial number, WorkGroup, Test Type and Date Range

Test Results

showing 8 results

Filters [Clear Filters](#)

Show All Data ☐

Last Name

Serial Number

WorkGroup

Test Type Select One

Date Range All time

[Cancel](#) [Apply](#)

5. Tap on any Test result to view further details of that test

Patient Test SARS-CoV-2 Ag

Workgroup
Unassigned

Tested By
Jones, M.

Tested On
Mar 18 2021 2:13pm

Sample Type
Nasal Swab

Serial #
REJH-32765-00569

Lot #
5000010

Test Strip
301581

Expiry
Jan 01 2022 6:59pm

Control
Unknown

POSITIVE +
SARS-CoV-2 Ag

Accepted


6. Tap 'Export' to send the list of results to a .CSV file


[Export Results](#)


Patient and Quality Control test results can also be viewed for each Instrument in your organization from the Instruments page.

1. From the Instrument page select the action menu  for the Instrument whose test results you want to view, and select 'Test Results'.

Instruments



1 of 1 results


NAME	SERIAL NUMBER	STATUS	
REHH-32765-00553	REHH-32765-00553	Online	<div> <div>General Settings</div> <div>Test Results</div> <div>Quality Control Report</div> </div> 

2. Select date range for when the tests were performed.
3. Select 'Test Type' to filter by Test type.
4. Tap on any Test result to view further details of that test.
5. Tap 'Export' to send the list of results to a .CSV file.

Test Results | REHH-32765-00553

From

Jul 01 2020




To

Nov 10 2020

Test Type

All

Export

TIME OF TEST	TEST TYPE	STATUS
 Aug 27 2020 6:24pm	SARS-CoV-2 Ag	Accepted >
 Aug 27 2020 6:06pm	SARS-CoV-2 Ag	Accepted >
 Aug 27 2020 6:04pm	SARS-CoV-2 Ag	Accepted >

The following warning will appear as a pop-up on screen.

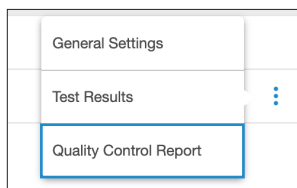
Warning: All data and information is displayed for viewing purposes only. The user acknowledges that any exportation of the data from the Connect Manager display function may result in corruption of that data. The user, on behalf of the Organization, shall accept sole responsibility for the use of any data or information extracted from the display function.

Note: Organizations managing the LumiraDx Platform through a middleware provider may choose to disable Test results being sent to Connect Manager. In this case the 'Test Results' option will not be available from the Instruments page in Connect Manager.

Quality Control Reports

A PDF report of Quality Control Tests can be produced for each Instrument.

Tap 'Quality Control Report' from the Instrument action menu.



Select the Test Type and enter the Sample Type, date range and optionally enter the address of the testing location.

Note: Sample Type refers to the type of patient sample(s) used when performing a specific Patient Test.

Tap 'Download Report' to create a PDF of the Quality Control Report.

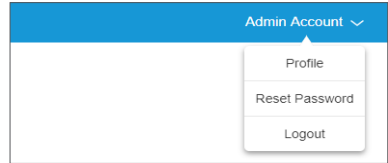
A screenshot of a mobile application form titled 'Quality Control Report for REVY-00000-00048'. The form contains the following fields: 'Test Type' with a dropdown menu showing 'Select Test Type...'; 'Sample Type' with a text input field; 'From' with a date picker showing 'Jul 09 2021'; 'To' with a date picker showing 'Aug 09 2021'; and 'Street Address on Report' with a large text input area. Each date field has a calendar icon to its right. The form has a close button (X) in the top right corner.

4.5 Personal Settings

Updates to name, contact information, and password can be made.

To update your personal information:

1. Login to Connect Manager.
2. In the top right corner of the page tap your Name and select "Profile" from the drop-down menu.
3. Edit all of the relevant profile information fields.
4. Tap 'Apply Changes'.

A screenshot of the "Profile" form in the Connect Manager application. The form has a white background and a close button (X) in the top right corner. It contains several input fields: "Username" (pre-filled with "admin2"), "Email" (pre-filled with "admin@lumiradx.com"), "Title" (empty), "First Name" (pre-filled with "Org"), "Last Name" (pre-filled with "Admin2"), "Initials" (empty), and "Language" (a dropdown menu set to "English"). At the bottom right of the form is a blue button labeled "Apply Changes".

To change your password:

1. Login to Connect Manager.
2. In the top right corner of the page tap your Name and select "Reset Password" from the drop-down menu.
3. Enter 'Current password' and 'New password' in the required fields. See section 5.2 for password requirements.
4. Tap 'Update Password'.

A screenshot of the "Reset Password" form in the Connect Manager application. The form has a white background and a close button (X) in the top right corner. It contains three input fields: "Current Password" (pre-filled with "*****"), "New Password" (pre-filled with "****" and a red error icon), and "Confirm Password" (pre-filled with "*****"). A "Password requirements" pop-up window is overlaid on the form, listing the following requirements: "At least 8 characters in length" (marked with a red X), "At least one number" (marked with a green check), "At least one lowercase letter" (marked with a green check), "At least one of these special characters: [.,/] (marked with a green check), "At least one uppercase letter" (marked with a green check), "Does not use unsupported characters" (marked with a green check), and "Does not match your previous passwords" (marked with a green check).

4.6 Organization and Quality Control Settings

Organization administrators can update setting for the whole organization from the settings menu.

Organization settings

Tap 'Organization Settings' to update the time zone and contact details for the organization.

Once the settings have been updated tap 'Apply Changes'.

Southgate Hospital Settings


Region

United States

Language

English

Time Zone *

(GMT-05:00) Eastern Time (US & Canada) 

Contact Name *

Organizational Administrator

Contact Email *

administrator@yourorganization.org

Contact Phone *

5551234567


Apply Changes

Time Zone Setting by WorkGroup

Each WorkGroup is set to the Organization's Time Zone by default. The settings can be overridden for an individual WorkGroup within the WorkGroup settings. Select 'Override Organization's Time Zone' and choose the correct time zone from the drop-down list. Tap 'Apply Changes'.


[← WorkGroups](#)

Emergency Room

Users	Instruments	Settings
<div>Name *<input type="text" value="Emergency Room"/></div> <div>Description<input type="text"/></div> <div> The WorkGroup time zone setting will be enforced for all instruments in Emergency Room</div> <div><input checked="" type="checkbox"/> Override Organization's Time Zone</div> <div>Time Zone *<input type="text" value="(GMT-08:00) Pacific Time (US & Canada)"/></div>		

Quality Control Settings

Quality Control


 The quality control policy can be overridden at the workgroup level.

Quality Control

Quality Control Policy *

Policy Interval

☒

Days 

Require for each new lot

☒

The following features can be configured to determine the Organization's Quality Control Policy.

Quality Control

- **Off**
- **Mandatory** – If the Quality Control policy has expired users are unable to perform a patient test, until a Quality Control Test has been performed with a status of PASS.
- **Advisory** – If the Quality Control policy has expired a warning is displayed on the Instrument. Users can acknowledge the warning and proceed with testing.
- **Mandatory with Override** – If the Quality Control policy has expired, users are required to either run a Quality Control Test or override the expired Quality Control policy and run a patient test by entering a comment to explain the reason for the override.

Quality Control

i The quality control policy can be overridden at the workgroup level.

Quality Control

Require for each new lot

✓ Off
Mandatory
Advisory
Mandatory With Override

Apply Changes

Policy

- **By Lot** – Users will be required to perform a Quality Control test when using a new Test Lot on an Instrument for the first time.
- **By Type** – Users will be required to perform a Quality Control test when using a new Test Type on an Instrument for the first time.

Policy Interval

Set a Policy Interval by moving the 'Policy Interval' slider to 'on'. Enter a number and select 'Tests' or 'Days' to determine how frequently a Quality Control test is required for each Lot or Test Type on each Instrument.

Require for each new lot

Use the slider to determine if a Quality Control test should be required for each new lot of Test Strips. This defaults to 'on' when the Policy is set to By Lot. The setting is editable when the Policy is set to By Type.

Quality Control Policy by WorkGroup

Each WorkGroup is set to the Organization's Quality Control policy by default. The settings can be overridden for an individual WorkGroup within the WorkGroup settings. A WorkGroup level Quality Control Policy can be set even if the Organization Quality Control is set to 'Off'.

[← WorkGroups](#)

Emergency Room

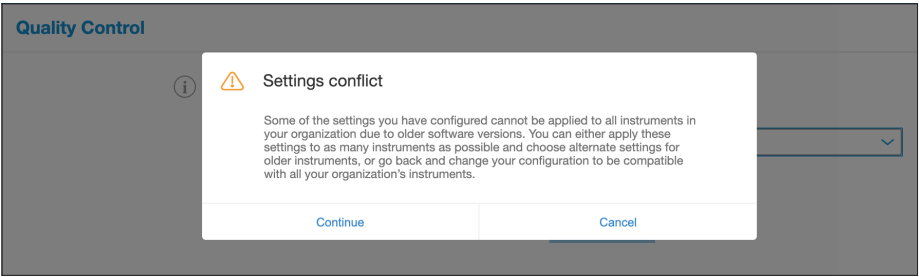
Users	Instruments	Settings
<div>Name *<input type="text" value="Emergency Room"/></div> <div>Description<input type="text"/></div> <div><div><div></div></div> The WorkGroup time zone setting will be enforced for all instruments in Emergency Room</div> <div><input checked="" type="checkbox"/> Override Organization's Time Zone</div> <div>Time Zone *<input type="text" value="(GMT-08:00) Pacific Time (US & Canada)"/></div>		
<div>Quality Control</div> <div><input checked="" type="checkbox"/> Override Organization's Quality Control Policy</div> <div>Quality Control<input type="text" value="Mandatory"/></div> <div>Quality Control Policy *<input type="text" value="By Lot"/></div> <div>Policy Interval<div><div><div></div></div><div>20</div><div>Days</div></div></div> <div>Require for each new lot<div><div><div></div></div></div></div> <div>Apply Changes</div>		

Note: If the organizations Quality Control policy is being managed by a middleware provider, the Quality Control settings in Connect Manager will be 'read only'. The user will be able to view the Quality Control policy settings sent by the middleware provider but will not be able to edit them within Connect Manager.

Mixed Instrument software versions

If some Instruments in the Organization are running on an old software version, they may not be compatible with all the configurable settings in Connect Manager. In this case, Connect Manager will display a message to highlight that settings are not supported on all Instruments and what steps can be taken to resolve the issue.

Quality Control Policy example



Quality Control

The quality control policy can be overridden at the workgroup level.

Quality Control

Mandatory With Override

Quality Control Policy *

By Lot

Policy Interval

20

Days

Require for each new lot

Quality Control support warning

The Quality Control Policy that you have selected cannot be applied to all instruments in your Organization. Please select a fallback setting which shall be applied to all remaining instruments.

PARENT SETTINGS

FALLBACK SETTINGS

Applies to the 1 instrument running the latest software version

QUALITY CONTROL

Mandatory With Override

Off

QUALITY CONTROL POLICY

By Lot

POLICY INTERVAL

20

Days

REQUIRE FOR EACH NEW LOT

Apply Changes

User training example

Edit User

Username *

jd

Email *

instrument@operator.com

Title

First Name *

Jane

Last Name *

Doe

Initials

Language *

English

Connect Manager Roles

Select from list...

Instrument Roles

Instrument Operator

Instrument Workgroups

Emergency Room x

Enforce instrument user training expiry

☒

Training valid until *

Nov 13 2020

Apply Changes

5. Miscellaneous

5.1. Logging in to Connect Manager

To login to Connect Manager:

1. Either:
 - Open the Connect App on your mobile device; or
 - Using a web browser, navigate to connect.lumiradx.com.
2. Enter the organization access code if accessing Connect Manager for the first time.
Note: Organization Access code is only needed for first time visitors. The next time you visit this site you will access the login screen directly.
3. Enter 'Username' and 'Password' in the relevant fields.
4. Tap 'Login'.

To reset your password:

1. Either:
 - Open the Connect App on your mobile device; or
 - Using a web browser, navigate to connect.lumiradx.com.
2. Tap 'Forgot your password?'
3. 'Email' – enter your email address. A temporary validation code will be sent to your email address.
4. Set your new password
 - 'Email' – enter your email address.
 - 'Validation Code' – enter the temporary validation code sent to your email address.
 - 'New Password' – enter your new password.
 - 'Re-enter Password' – enter your new password.

Note: If a User account has been set up without an e-mail address the user will be prompted to set a new password after first time login.

To set your new password

- 'Current Password' – enter your current password.
- 'New Password' – enter your new password.
- 'Re-enter Password' – enter your new password.

5.2. Username and password requirements

Username requirements:

- Maximum username length is 20 characters
- Username must be unique to all other users in the organization
- Not case sensitive

User Password requirements:

- Case sensitive
- Minimum length of 8 characters
- Requires at least 1 numeric character
- Must contain a special character (allowable characters are -, . /)
- Requires at least one lower case character
- Requires at least one upper case character
- After 10 failed attempts, the user will be temporarily locked out of Connect Manager for 30 minutes. The Connect Manager Organization Administrator should be contacted if password reset is needed.

5.3. Application updates

The LumiraDx Connect App updates automatically through the phone's app store. The web version of the app also updates automatically and requires no action from your organization.

6 Customer Services

For product and connectivity support please contact LumiraDx Customer Services at customerservices@lumiradx.com.

For your local customer services phone number please visit the customer services page at lumiradx.com.

7 Security

LumiraDx provides and enforces security and data protection within the Connect system architecture in addition to policy and process. To do this, we make the following precautions with regards to data protection:

- All data in-transit or at rest in the system is encrypted to FIPS 140 standards.
- Endpoints and protocols employ data authentication and integrity mechanisms to prevent hacking.
- End-to-end encryption is used between secured endpoints to protect data when traveling over public or unsecured networks.
- Data travels through the system de-identified until it reaches the Electronic Health Record where it can be re-identified to a patient.
- Identifiable and pseudonymized data is only stored where information security and data protection controls are compliant with the legislative and regulatory requirements relevant to the geographic region of the patient.
- Only fully anonymized data is sent to LumiraDx for performance monitoring and analysis.

7.1. General Data Protection Regulation (GDPR) Compliance

Along with its security protections, LumiraDx has ensured that it complies with every principal of GDPR.

8 Privacy Notice

An administrator or user using LumiraDx Connect Manager and EHR Connect for the first time will be required to read and accept the following privacy notice.

This Privacy Notice

This privacy notice explains the purposes for which LumiraDx will collect, hold and use your personal data. It also explains your rights under EU and UK data protection laws to access your data or seek to have it rectified or deleted.

LumiraDx operates a global Data Protection Policy which takes into account data protection legislation and regulations in all the markets in which the business operates. The framework we uphold is based on UK and EU GDPR principles and is adapted to comply with local legislation where these apply.

Personal information we collect

We may collect the following types of personal information from you when you use LumiraDx services or products:

1. Account details: when you use the application, an account will be created for you by LumiraDx or by your organization's administrator. The account will include a user name, email address, password, work group and full name.
2. When you use the application: We will record details of application usage to maintain an audit trail. This will include information relating to where the application is used (which organization), when you used the application and what tasks you performed using it.
3. Patient details. To ensure the patient can be identified and the correct test results associated with the patient in your Electronic Health Record.
4. Test results. What tests were performed on which patients and the results when using EHR Connect.

What we use your personal information for?

Purpose:

- Provide our services to you and maintain your account.
- Ensuring users have access to information relevant to their role and only to their role.
- Ensure regulatory compliance.
- Data analytics and statistical research to help us better understand how our products are used.
- Investigating misuse of your account, fraud and debt collection.

We may anonymize and aggregate any of the personal information we hold (so that it does not directly identify you). We may use anonymized and aggregated information for purposes that include testing our IT systems, for research, data analysis, improving and developing our products and services.

Who we share your personal information with?

We may share personal information with the following parties:

- Companies in the same group of companies as us: for the purpose of providing a service to you and understanding our use of our products and services.
- Other service providers and advisors: such as companies that support our IT or help us analyze the data we hold.
- The Government or our regulators: where we are required to do so by law or to assist with their investigations or initiatives.
- Police and law enforcement: to assist with the investigation and prevention of crime when legally required.

We do not disclose personal information to anyone else except as set out above. We may provide third parties with aggregate statistical information and analytics about users of our products and services, but we will make sure no one can be identified from this information before we disclose it.

Transferring your personal information internationally

The personal information we collect may be transferred to and stored in countries outside of the European Union or the UK. Some of these jurisdictions require different levels of protection in respect of personal information and, in certain instances, the laws in those countries may be less protective than the jurisdiction you are typically resident in. We will take all reasonable steps to ensure that your personal information is only used in accordance with this privacy policy and applicable data protection laws and is respected and kept secure.

How long do we keep personal information?

We will keep your personal information for a period determined by national guidelines and regulatory requirements.

Your rights in relation to personal information

You have the following rights in relation to your personal information whether you are a user of LumiraDx Connect services as healthcare professional or a patient:

- the right to be informed about how your personal information is being used;
- the right to access the personal information we hold about you;
- the right to request the correction of inaccurate personal information we hold about you;
- the right to request the blocking or deletion of your personal information where the processing does not comply with applicable data protection laws.

To exercise any of the above rights, or if you have any questions relating to your rights, please contact us by using the details set out in the 'Contacting us' section below.

If you are unhappy with the way we are using your personal information you can also complain to your local data protection regulator. If you are a citizen of an EU member state, you have a right to lodge a complaint with your national data protection supervisory authority. If you are a citizen of the UK, you have the right to lodge a complaint with the UK Information Commissioner's Office (www.ico.org.uk). We are here to help and encourage you to contact us to resolve your complaint first.

Changes to this notice

We may update this privacy notice from time to time. When we change this notice in a material way, we will update the version date at the bottom of this page. For significant changes to this notice we will try to give you reasonable notice unless we are prevented from doing so. Where required by law we will seek your consent to changes in the way we use your personal information.

Contacting us

Full details of the LumiraDx privacy policy can be found on our website lumiradx.com. In the event of any query or complaint in connection with the information we hold about you, please email us at: privacy@lumiradx.com

9 Legal Notices

Access and Use of LumiraDx Connect Manager and EHR Connect is subject to the terms of use and software and/or end user license agreements signed up to as part of accessing these systems. LumiraDx and/or its licensors (who are third party owners of intellectual property rights use in any provided software) own all intellectual property rights in the provided software and related documentation. Other than rights provided to use the system as part of agreed software and/or end user license agreements, no rights are granted to, or in, patents, copyrights, database rights, trade secrets, trade names, trademarks (whether registered or unregistered), or any other rights or licences in respect of the software.

Any warranty to the systems provided shall be in line with the accepted terms of software and/or end user license agreements. The warranty does not apply the extent of any defect or fault in the software which is caused by use of the software contrary to LumiraDx's instructions, or modification or alteration of the software by any party other than LumiraDx or LumiraDx's duly authorised contractors or agents.

Intellectual Property: LumiraDx Connect Manager and EHR Connect and all provided LumiraDx documentation are protected by law. The intellectual property of the LumiraDx services and products remains at LumiraDx. Details of relevant Intellectual Property regarding our products can be found at lumiradx.com/IP.

Legal Notices: Copyright © 2024 LumiraDx Inc and LumiraDx UK. All rights reserved. LumiraDx, the LumiraDx Logo and certain LumiraDx product names are the trademarks of LumiraDx UK or its Affiliates, registered in the UK, U.S and other countries.

