Chromium Connect:
Network Connectivity Guidelines

Introduction

The Chromium Connect instrument combines single cell partitioning, barcoding, and library preparation in standardized, automated workflows. This Technical Note provides an overview of network connectivity guidelines for the Chromium Connect instrument in order to describe:

- remote performance monitoring
- data collected by 10x Genomics
- live remote support
- security considerations
- additional connectivity details

The Chromium Connect instrument has a highly interactive user interface paired with network connectivity, intended to provide a seamless user experience along with efficient remote performance monitoring to minimize instrument downtime. If any unexpected instrument errors occur, the user-controlled live remote support access to the instrument allows the 10x Genomics Support team to quickly troubleshoot errors. See the following sections for detailed information.
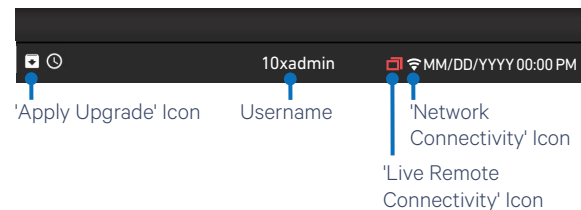
Refer to the Chromium Connect user guide (CG000180) for details regarding various instrument components, user interface navigation, and all additional features.

Chromium Connect

1A

1B

Menu > Settings > Network

Footer

'Apply Upgrade' Icon   Username   'Network Connectivity' Icon

'Live Remote Connectivity' Icon

Figure 1. The Chromium Connect (1A) has a user-friendly interface (1B) that displays the network connectivity status.

Remote Performance Monitoring

Monitoring the performance of the Chromium Connect helps ensure that the instrument is performing optimally and maximizes instrument uptime. This also gives 10x Genomics the ability to respond quickly and troubleshoot issues that may occur. While the user focuses on processing samples and data collection, the instrument will proactively collect performance data to allow the 10x Genomics Support Team to address potential instrument downtime.

Data Collected by 10x Genomics

No biological sample data is being collected by 10x Genomics. Remote data collection is limited to the following items:

• Calibration data

• Instrument operation logs

• Mechanical and fluidic system logs

• Computer system logs

Data Protection

All aforementioned collected data transferred to and stored on 10x Genomics Cloud is encrypted using TLS in transit, encrypted at rest with AES-256, and are stored within the United States (US-WEST2 and US-EAST2 on AWS). Additionally, connections to the Chromium Connect performance monitoring does not require opening any ingress ports in the user's firewall.

10x Genomics Cloud is subject to the 10x Genomics Cloud Service Terms, and data collected under this performance monitoring will be treated as Usage Data as defined under the Cloud Service Terms.

Customer-controlled Live Remote Support

Should an unexpected error occur with the Chromium Connect, 10x Genomics is committed to troubleshooting the problem as soon as possible. To enable this, a live remote support feature allows a 10x Genomics representative to remotely access the instrument and observe the problem in real-time to find and implement an appropriate solution. The live remote support option is completely user-controlled and can be locally enabled or disabled by the user at any time by using the instrument settings menu.

Firewall

Live remote support for the Chromium Connect is designed to keep the user network and the instrument safe. It does not require opening any ingress ports in the user's firewall and is conducted over an encrypted connection on a private network, protecting user data from third parties. The Chromium Connect employs a strong host firewall that blocks all inbound connections and is protected from attack on the local network and from the Internet. Outbound connections are made to trusted 10x Genomics resources only. In addition, access by 10x Genomics employees is restricted, with only the strictly necessary personnel granted access upon customer support requests.

Access Permissions & Limitations

Live remote support enables a 10x Genomics representative to locally access the instrument (similar to onsite support). 10x Genomics representatives will not access or transfer any experimental data or sample images without the user's permission. Once the needed support has been provided, the user can disable live remote support, which can also be re-enabled only by the user if needed at a later time.
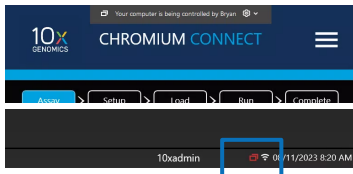
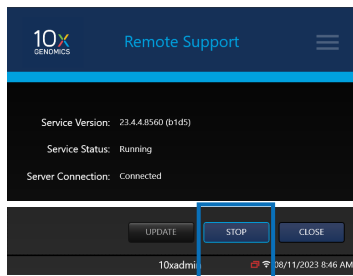## Live Remote Support Connectivity

Menu
Select Remote Support
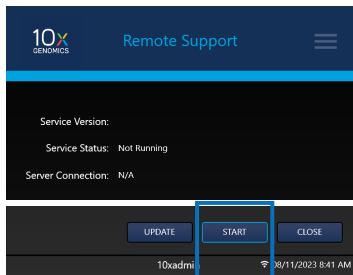
Start Remote Support

Banner
displays Remote Support connectivity

Footer
displays connectivity icons

Stop Remote Support

Additionally, a status icon in the Chromium Connect interface will always keep the user informed about the status of live remote support (enabled or not) thereby empowering the user to control access:

The following connectivity icons may be found in the lower right corner of the screen:

- Icon present: Remote connection feature is turned ON and Technical Support is connected to the remote server.
  - Icon not present: User has turned OFF the remote connection feature.
- Icon has a small red dot (lower right corner): Live remote support is enabled but the local host is not connected to the server.
- Icon has a yellow warning (lower right corner): Live remote support is enabled but the local host experienced an error connecting to the server.

During live remote support, a screen banner in the header notifies the user that the screen is currently shared and remotely controlled.

Security Considerations & Features

Allow outbound TCP port 443 for 10x Genomics Cloud access. As an additional (optional) level of security, the instrument can be isolated on its own network VLAN with Internet-only access.

Topic	Feature
Data NOT collected	Biological sample data, personal health information
Required inbound ports	10x Genomics servers: 80, 8080, 443, 4195
	Email servers: 587, 465, 25, 2525
	ConnectWise servers: 8040, 8041
	Shared Drive: 445, 139
Data center encryption at rest	Encrypted at rest with AES-256
Data encryption in transit	Encrypted with TLS
Instrument firewall	Blocks all inbound connections
	Windows Firewall ON
	Incoming ports and outgoing ports limited (see above)
On instrument restrictions	No installed browser, account runs with restricted permissions
Virus Detection	Windows Defender
Operating System	Windows 10 IOT build 1607 (used as an Embedded OS)
	Custom Window Manager (no Windows Explorer)
User Accounts	One master account (full admin permissions)
	User is not authorized to add any new OS accounts. The user can only create and modify UI accounts.
Updates & Patches	Provided by 10x Genomics directly to the instrument

Additional Technical Details

In order to connect, navigate to Settings > Network > Connections. Note that Wi-Fi configuration may not be available in your region. LAN is recommended for optimal performance.
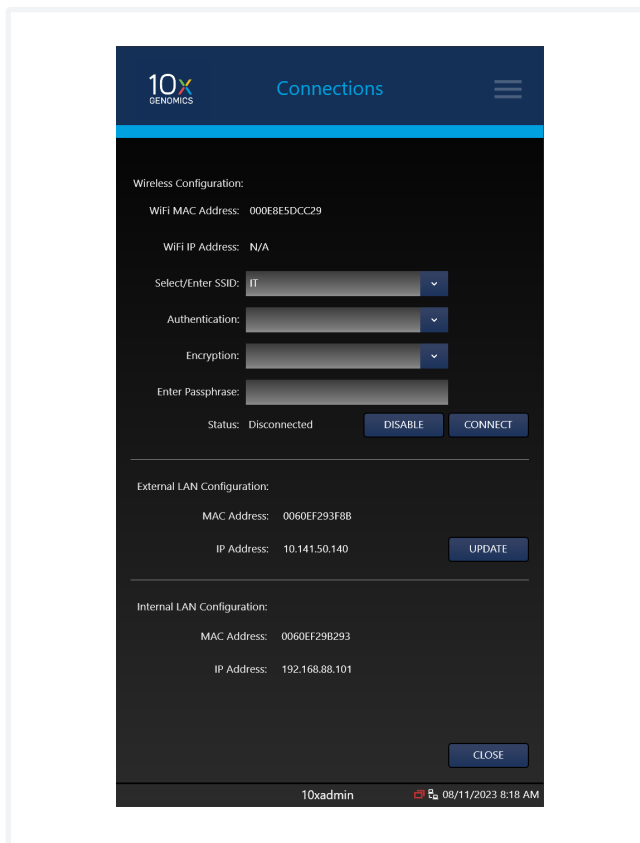
Connectivity

LAN and Wi-Fi connectivity to a network are possible through Dynamic Host Configuration Protocol (DHCP). DHCP is available on the Chromium Connect instrument. To confirm that DHCP is working properly, connect the instrument to the network via LAN or Wi-Fi and confirm that an IP address is populated. If the instrument detects a valid LAN connection, it will connect automatically and an IP address will be visible in the instrument user interface.

- Wi-Fi connected icon
- LAN connected icon

The following authentication protocols are supported for Wi-Fi connection:

Wi-Fi Authentication	Encryption
open	none
shared	TKIP
WPA	AES
WPAPSK	WEP
WPA2	
WPA2PSK	

Automated Software Download

Network-connected instruments can automatically receive instrument updates over their network connection. An "upgrade" includes software updates to the Chromium Automated Controller's firmware and software, improvements to the assay, and user interface improvements. The software upgrade process is a two step process:

a. "Transfer" the software packages provided by 10X Genomics to the instrument host.

b. The selected package will be scanned and validated by the application. If the package is deemed invalid, the package will not allow the download.

c. Before applying any software package, the instrument must be power cycled to ensure it is in a proper state to install all components.

d. Once the download is complete, a popup will appear in the user interface. The user must click "Apply" to allow the administrator to install the transferred package. The installation will upgrade all appropriate application and instrument components included in the package.

Email Notifications

Email notifications can be sent at the following points: the start of a run, when a stopping point is reached, if an error is detected, and at the completion of a run. Enable email notifications as follows:

a. Configure the remote email server: Obtain the Server Address and Server Port from the institution's network administrator. Navigate to Email Server in the menu options. Specify a username and password for a sender email account. The Display Name will appear in the "From" field of emails sent from the instrument.

b. Select a security protocol and press "Test" to send a test email to the server. If successful, the Status field will read "Connected."

c. Ensure the email accounts listed are valid.

Drives (Local Connectivity)

The Network Shared Drive function enables the instrument to remotely transfer run data or support packages to a designated storage location over a network connection. Consult an IT professional to assist in setting up this function:

a. Connect to the shared drive by clicking "Add."

b. Obtain the device ID path and credentials from the institution's network administrator (syntax must be entered correctly to verify proper connections). The software will designate a drive letter.
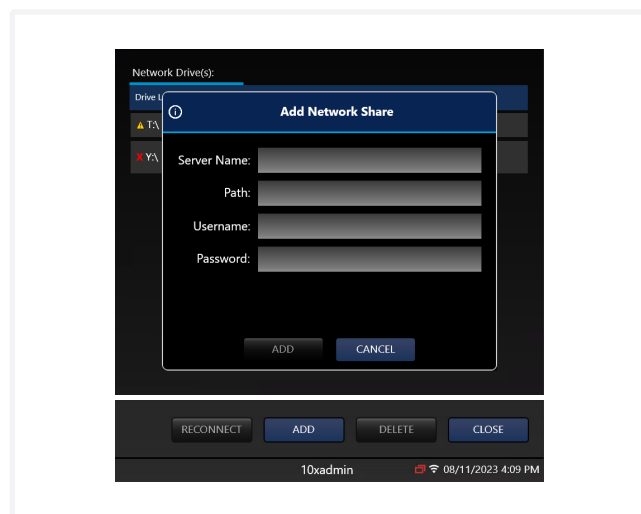
Document Revision Summary

Document Number	CG000699
Title	Chromium Connect: Network Connectivity Guidelines
Revision	Rev A
Revision Date	October 2023

Specific Changes:

N/A

General Changes:

N/A

Contact:

support@10xgenomics.com

10x Genomics
6230 Stoneridge Mall Road
Pleasanton, CA 94588 USA