SINGULAR GENOMICS

TECHNICAL NOTE

Networking, Security, and Remote Access for the G4 Sequencing Platform

The G4™ Sequencing Platform by Singular Genomics™ requires access to cloud storage solutions or network-attached storage to manage the extensive amount of data generated by the instrument. The sequencing runs can be monitored remotely by the user using the G4 Platform Manager app. The instrument also sends instrument health monitoring data to Singular Genomics to improve the quality of service and to support customers. Access can be granted to Singular Genomics by the user to troubleshoot issues remotely. This document describes how the instrument must be configured to enable these features.

CONNECTIVITY PURPOSES

The G4 Sequencing Platform requires network connectivity during operation and to enable support. During operation, network connectivity is needed for the following purposes:

Purpose	Description
Data Management	The G4 instrument transfers sequencing results to a configured cloud storage provider using the internet or on-premise Network-Attached-Storage using the user's private network. For more information, see **"Connections Setup" on page 3**.
Instrument Health Monitoring	The G4 collects a small amount of instrument health data that is sent to Singular Genomics Customer Care to improve products and services and assist customers in troubleshooting issues remotely. For more information, see **"Telemetry Data for Instrument Health Monitoring" on page 4**.
Run Management	The G4 instrument can be controlled and monitored remotely using the G4 Platform Manager app.

Network connectivity is also needed to enable support for the following issues:

Purpose	Description
Technical Issues	The G4 instrument is configured to collect additional data for Singular Genomics engineers and support scientists to identify and resolve technical issues internal to the instrument, and issues related to the configuration and execution of sequencing runs.
Remote Access	Remote access may be needed to enable engineers and scientists at Singular Genomics to support technical and operational issues with the G4 instrument.

Note that Singular Genomics only collects log file information such as run configurations, timestamps, QC information and instrument sensor data. Genomic data is never included, nor any identifiable data or patient health data.

The various connectivity purposes are illustrated in Figure 1.

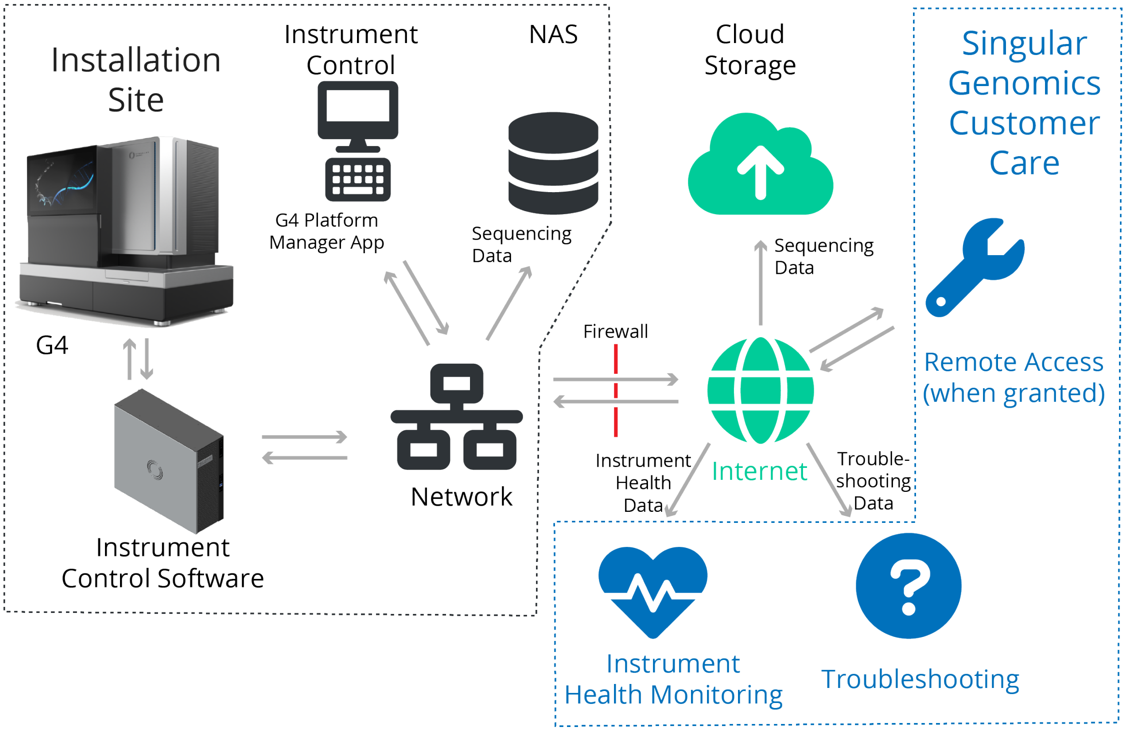


Figure 1: **G4 Connections**.

G4 COMPUTERS

The G4 Sequencing Platform comes with two computers in a single case, both of which require access to the intranet and the internet.

G4 Primary Computer

The G4 Primary Computer uses Windows 10 Pro as its operating system. It can connect to the intranet or the internet using Wi-Fi. Connectivity to the intranet is required to access the remote management capabilities of the G4.

The G4 Primary Computer has the following features:

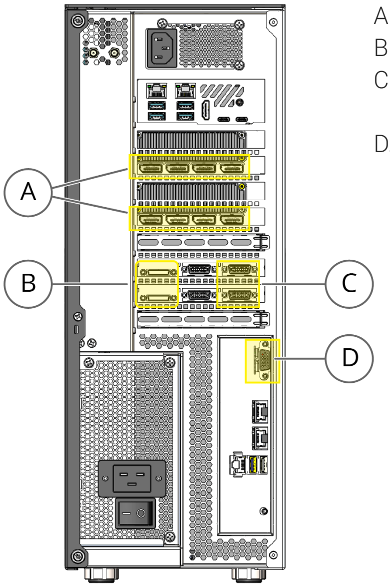
Feature	Description
Operating system	Windows 10 Pro
Wi-Fi	Supports 802.11 a/b/g/n/ac Wi-Fi
Bandwidth required	10 Mbps
Intranet access	• Required to access the G4 Platform Manager app from the intranet • 9000/9001 TCP Incoming
Internet access	• Required to provide software updates for Windows 10 Pro • Required for Singular Genomics Support using remote access software

G4 Secondary Computer

The G4 Secondary Computer uses Ubuntu 20.04 LTS and connects to the primary computer using a direct Ethernet connection. It can only connect to the intranet or the internet using an Ethernet connection. Connectivity to the intranet is required to upload results to a local storage resource (NAS) and to the internet to upload results to the user configured cloud storage provider.

The G4 Secondary Computer has the following features:

Feature	Description
Operating system	Ubuntu 20.04 LTS
Ethernet	Supports 10Gbps Ethernet using CAT-5e or CAT-6a
Required outgoing network bandwidth	Minimum 1 Gbps, 10 Gbps preferred. These speeds have the following approximate upload times of 100 GB of data: • At 1 Gbps – 15 minutes • At 10 Gbps – 2 minutes
Intranet access	Required to upload data to NAS provided by the customer (SMB)
Internet access	• Software updates for Ubuntu 20.04 LTS • Software updates for the primary analysis • Singular Genomics Support using remote access software • Ports 3000/5432/8000 TCP Incoming for the internal web interface to the primary analysis • Port 19999 TCP for netdata



A. DisplayPorts
B. DH60-27P ports
C. CameraLink HS ports on the right
D. VGA port

Figure 2: Connection ports at the back of the G4 instrument computer case that should never be used (highlighted in yellow).

G4 Computers Connection Ports

The G4 computers and their connection ports are for the G4 instrument only and should not be used for other purposes. In particular, there are a number of ports that should never be used: the eight DisplayPorts, the two DH60-27P ports, the two CameraLink HS ports on the right, and the VGA port. The locations of these ports are shown in Figure 2. Note that the two CameraLink HS ports in the middle are connected to the G4 instrument camera and are therefore in use.

CONNECTIONS SETUP

Some of the connections are already set up by Singular Genomics, others need attention from the user's IT department. This section lists the connections that need to be checked or set up, depending on your configuration:

- Data storage on the network.
- Data storage on the cloud. Use an existing account, or Singular Genomics can help setting up a new account. Recommended provider is Amazon's AWS.
- G4 Platform Manager app for instrument control.

Customer Network Information Required

In addition, the following information is required to set up the connection to the customer site network:

Connection	Required Information
Wi-Fi connection parameters	• Wi-Fi SSID • Authentication mechanism • Session credentials
Ethernet if DHCP is not used:	• Static IP address • Netmask • Default gateway

REMOTE SUPPORT

If an instrument has run problems, the Singular Genomics Customer Care team can start troubleshooting without having to be on-site. This can result in rapid issue resolution, decreased time on site, and shorter recovery times. Remote troubleshooting can be done through monitoring instrument health data, analyzing engineering data files, or through remote access to the instrument. These procedures are described below.

Telemetry Data for Instrument Health Monitoring

Every G4 Sequencing Platform can automatically send telemetry data for instrument health monitoring (instrument health data) to Singular Genomics. This allows Singular Genomics to pro-actively identify a reduction in instrument performance. This results in a more reliable instrument and minimization of sample, reagent, and time loss.

The telemetry data consists of log files that provide general information about runs, and information about the optical system, fluidics, and thermal and mechanical data. Genomic data is never included, nor any identifiable data or patient health data.

Push Engineering Data for Troubleshooting

For remote troubleshooting, Singular Genomics may request engineering data files to be sent to Singular Genomics. When supporting data files are requested for troubleshooting, the data needs to be pushed to Singular Genomics, which means users have full control over when these files get sent.

The files contain more specific information of the optical system, fluidics, and thermal and mechanical data. Again, genomic data, identifiable data, or patient health data is never included.

Remote Access for Troubleshooting

In other cases, remote access to the instrument is the most efficient way to troubleshoot through remote access software. Remote access is turned off by default, you will have to explicitly grant Singular Genomics engineers access through the remote access software. Once control has been granted, Singular Genomics engineers have full admin control of both the Windows and Linux installs on the instrument computer, as long as the remote access software stays enabled.

SECURITY

The network should at a minimum adhere to the security standards UL 2900 parts 1, 2-1, and 2-2. In addition, security best practices, firewall settings, and anti-virus configuration settings are listed below.

Security Best Practices

Singular Genomics expects the following security best practices:

- Only use the instrument for its intended purpose.
- Never go on the internet from the instrument, or directly expose the instrument to the internet, beyond necessary for its intended purpose specified by Singular Genomics.
- Never install software that is not approved by Singular Genomics.
- Only change system settings if explicitly instructed by Singular Genomics, either in the User Guide or through communication.
- Do not connect USB devices not approved by Singular Genomics.
- If the instrument starts to behave anomalously, contact Singular Genomics Customer Care.

Firewall Settings

The G4 requires an internet connection for monitoring and data transfer, and has a firewall set up to restrict incoming traffic. If the instrument is behind an additional firewall, whitelist the following URLs for incoming traffic:

- *.corp.singulargenomics.com

Singular Genomics does not recommend restricting outgoing traffic, but if needed, make sure to whitelist the following addresses:

- *.corp.singulargenomics.com
- The external cloud storage location, if used (for example, Amazon's AWS).

Whitelist by URL and not by IP address, as IP addresses can change over time.

Ports

The following ports should be left open:

Port	Purpose
G4 Primary Computer ports 9000/9001	TCP incoming for access for the G4 Platform Manager app.

Operating System Updates

To make sure your data is secure, adhere to the following operating system updates best practices:

- Only install updates when the system is idle.
- For the Windows operating system on the G4 Primary Computer, make sure to manually install Windows critical security updates when available. See also the Security Update Guide available on the Microsoft website.
- For the Linux operating system on the G4 Secondary Computer, execute security updates using CLI (terminal) or user-interface (desktop).
- By default, security updates are not enabled automatically.
- Some updates require a full system reboot.

CONFIGURE ANTIVIRUS SOFTWARE

Protect the instrument control computer from viruses and other malware with antivirus software of your choice. Follow the antivirus software vendor's instructions, as well as the following guidelines to configure the antivirus software:

- Set up for manual scans. Do not allow automatic scans.
- Only scan when the instrument is not in use.
- Do not automatically install updates. You can download updates automatically, but implementation should be started manually when the instrument is not in use.
- Do not reboot automatically after installation.
- Make sure the Singular Genomics application directories and data drives are excluded from real-time protection.

CUSTOMER CARE

For any questions regarding this document, or for further assistance, contact Singular Genomics Customer Care.

SINGULAR
GENOMICS

For Research Use Only.
Not for use in diagnostic procedures.

CUSTOMER CARE
Our Singular focus is you.

Email: **care@singulargenomics.com**
Call: +1-442-SG-CARES (1-442-742-2737)
Website: **www.singulargenomics.com**

Lit No 000-000-003, Aug. 25, 2022