GeoMx® DSP Cybersecurity Guidelines

The NanoString GeoMx DSP system is an integrated environment with an embedded server. Aside from a thin client accessible from your desktop computer via the Chrome browser, all computing resources are resident on the instrument.

To help answer common questions from customers using GeoMx DSP systems, we have prepared this guideline document intended for lab managers and IT administrators.

IT requirements

As an integrated environment, the GeoMx DSP instrument can perform its core functionality in an offline or partially-offline state. However, the instrument is designed to use external resources via its 1GB Ethernet port. If the instrument is offline, it will be highly limited. NanoString has configured the onboard firewall and anti-malware tools to secure the instrument.

Limitations of offline use

- Access to analysis tools and data upload tools will only be available by being physically present at the instrument. Third party applications like Microsoft Excel are and cannot be installed on the system and therefore cannot be used to directly view and work with exported (data) files on the system itself.
- You will not be able to run a sample and perform data analysis at the same time.
- If a backup system is not established (backup to corporate file share via SMB is recommended below), the system will **stop working** when the hard-drive is full.
- NanoString will not be able to perform remote support or update the instrument remotely, causing longer turnaround times.
- You will not be able to run the Data Analysis Suite with NGS data in offline use mode.

Features requiring network connectivity

There are three features that require network connectivity:

- Desktop clients access the web interface via the Google Chrome browser for remote ROI selection and data analysis.
- Establishing an **automatic data backup system** is *highly recommended*. If no SMB backup location is established, the instrument will **stop working** when the hard-drive is full. The instruments ships with a 10TB hard drive for OS and GeoMx DSP software installation and storage. On average, 20 GB per scan will be used for storage. At medium throughput, the instrument could run out of hard drive space after 6-8 months if no external storage is established. The effective storage can be expanded by allowing the instrument to connect to a corporate file share via SMB. When connected to external storage, the instrument will backup data to the network share.
- NanoString includes remote support with the instrument, which allows for faster resolution of issues with the ability for NanoString support to diagnose, configure, and update components remotely. To

accomplish this, the Instrument must have WAN/internet access for NanoString support personnel to access the instrument.

- Processing NGS data in the Data Analysis Suite is a feature only enabled once online.

Storage requirements

The mounted file share must have enough space to store all scan images. We estimate a storage need of 20GB/scan.

Client computers

The web browser on client computers can be used for remote ROI selection and data analysis. The system has been designed to work with Google Chrome web browser. Other browsers will not work.

Other requirements

To maintain optimal system performance, NanoString does not permit installing additional software on the instrument or joining the instrument to a Windows domain.

Remote support

The instrument must have WAN/Internet access to allow for remote support, which is included with the support contract. NanoString is using LogMeIn Rescue (LMI) to provide this remote support, and the instrument is preconfigured with a LogMeIn Rescue Calling Card to provide this functionality. NanoString has not configured unattended access without customer's permission; NanoString cannot connect without a user on the instrument's side initiating and accepting the connection. In addition, NanoString technicians authenticate to LogMeIn Rescue using SSO.
If your instrument is behind a firewall, you will need to whitelist the following URLs:

http://secure.logmeinrescue.com:443
http://secure.logmeinrescue.com:80

Remote Desktop Protocol (RDP) is an alternative remote access strategy should LMI fail. RDP is prepackaged in the Microsoft OS allowing computers on the same network to take remote control from each other. RDP is not enabled on instruments by default; it is only enabled with permission from the customer. While LMI is a direct pathway from an external network to the DSP, RDP requires an intermediary. NanoString Support will take control of a networked computer using Zoom (Skype, WebEx, etc.) and then leverage RDP to take control of the Instrument to access engineering scripts to further troubleshoot and provide remote support. To reiterate, NanoString has not configured unattended access without customer's permission, NanoString cannot connect to GeoMx DSP without a user on the instrument initiating and accepting the connection. In addition, NanoString technicians authenticate to Zoom using SSO.

Network traffic

Windows Defender Firewall on the GeoMx DSP system instrument is enabled to control incoming LAN-based network traffic. It is configured to deny both inbound and outbound communications except that which is required for proper operation of the system.

Included anti-virus & anti-malware

Windows Defender anti-virus is configured and will receive anti-virus definitions as long as the instrument has a network route to retrieve updates.

In addition to using Windows Defender, we use Windows AppLocker. AppLocker is a whitelisting program that only allows NanoString-approved applications and processes to execute in Windows. As a result, AppLocker also provides robust protection from viruses and malware by blocking execution and enforces a high degree of overall change control of the DSP system state. In contrast to traditional security software that relies on blacklisting, which is inherently vulnerable to zero-day attacks and situations where the blacklist happens to not be updated in a timely manner, AppLocker blocks everything except that which has been specifically allowed to run on the instrument.

AppLocker allows us to maintain a static, robust, and secure application execution environment and protects the instruments from any unauthorized software or manipulation while at the same time ensuring that the machine remains in an unchanged and securely validated state.

Windows administrator accounts

NanoString does not permit Windows administrator access to the system aside from qualified NanoString technicians.

All the software that runs on our instruments has been through a rigorous verification and validation process; we carefully control how each piece of software works and how it interacts with the entire system. Any system changes must be verified and validated before being released to the instrument to ensure it remains in a validated state.

Application accounts

Instrument accounts are distinct from Windows accounts. There are two types of accounts – admin and user. Admin accounts can see all data in the system and perform administrative tasks, including user management and some instrument maintenance. We recommend that admin roles be assigned only to application administrators.

Access control for users is based around groups. Objects belong to one or more groups; users belong to one or more groups. Admins see all, without restriction. If a user and an object have a group in common, the user sees the object; if they don't have a group in common, the user doesn't see the object at all. If a user sees a folder, they see the slides and scans in the folder; if a user sees a slide or scan, they can do whatever their role says they can. If a regular user isn't in a group, they have no way of knowing that the group exists.

System integration

- Do not join the GeoMx DSP system to your Windows domain. NanoString does not permit joining the system to a Windows domain or applying a different group policy to the instrument. Any system changes must be verified and validated before being released to the instrument to ensure it remains in a validated state.
- Do not update Windows on the instrument. NanoString release system updates only after rigorous validation and verification. Any system changes must be verified and validated before being released to the instrument to ensure it remains in a validated state. NanoString releases OS system updates along with the regular software updates on a quarterly cycle. If a critical Windows security patch is released, NanoString will validate it and release an out-of-cycle hot fix. Contact your NanoString representative or geomxsupport@nanostring.com for updates or requests for critical patches.
- Do not install other anti-virus software on the instrument. Windows Defender is already installed and running. AppLocker is also configured to whitelist only the applications needed by the instrument to provide an additional anti-malware protection. Installing any other AV product would not provide an additional level of security and could potentially contribute to degraded and/or unpredictable system performance.

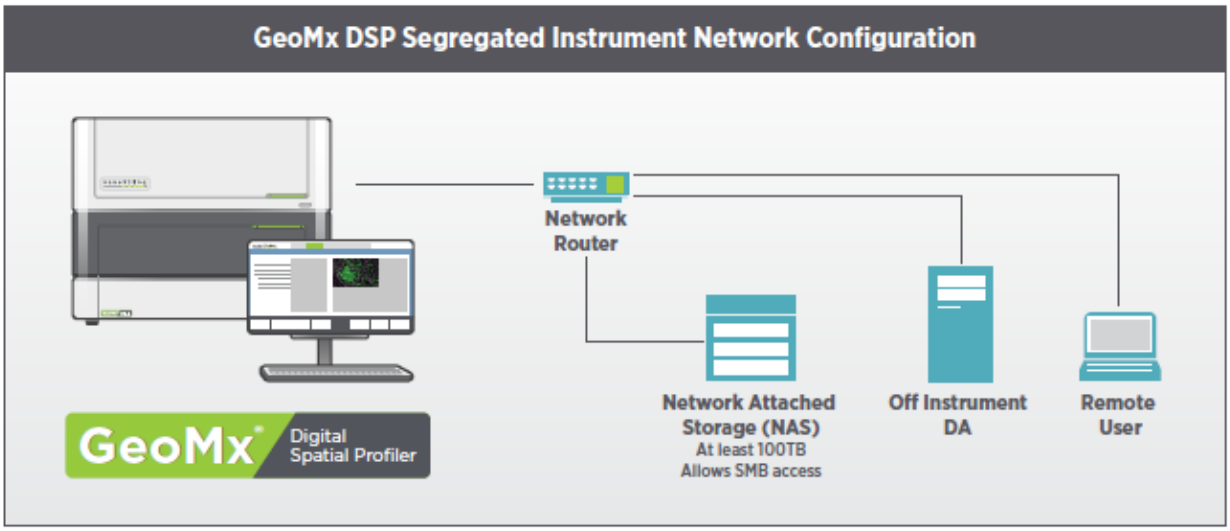
Network settings

The instrument is configured to use DHCP to obtain an IP address. You may also reserve a static IP for the instrument; your NanoString technician can provide you the MAC address of the instrument to reserve its IP address. If you have a static IP for the instrument and prefer not to use DHCP, please provide the IP address, Default Gateway and DNS servers to the NanoString technician prior to installation, and this will be configured during installation.

GeoMx DSP Segregated Network (Optional)

Because of the custom software running on the embedded operating system, NanoString completes a rigorous validation and verification process on all software running on the GeoMx instrument. The instrument cannot be joined to an existing Windows domain, and no additional software can be installed on the system.

To enable data archiving and off-instrument data analysis, a requirement of NGS readout, networking of the GeoMx instrument is required. Where it is not possible to mount GeoMx DSP to the institutional network, a segregated network can be deployed as illustrated below.



Additional questions

Please contact GeoMx support at geomxsupport@nanostring.com if you have additional questions.