Data Security Guidelines

DOCUMENT NUMBER:
CG-30292

DOCUMENT REVISION:
D

Effective Date:
08/03/2023

bionano

Table of Contents

Legal Notice 3

Patents 3

Trademarks 3

Revision History 4

Introduction 5

Bionano Compute On Demand 5

Saphyr Assure 5

Data Privacy Statement 6

Information Classification 7

System Design 8

Saphyr System Architecture 12

Saphyr Assure 13

Molecule Detection 15

Local Compute Cluster 17

Bionano Compute On Demand 18

Communication Channels 19

Controls 20

Risk Management 21

Common Security Considerations 22

Bionano Compute On Demand and Saphyr Assure Terms and Conditions 23

Technical Assistance 24

Legal Notice

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

Patents

Products of Bionano Genomics® may be covered by one or more U.S. or foreign patents.

Trademarks

The Bionano logo and names of Bionano products or services are registered trademarks or trademarks owned by Bionano Genomics, Inc. (“Bionano”) in the United States and certain other countries.

Bionano™, Bionano Genomics®, Saphyr®, Saphyr Chip®, Bionano Access™, VIA™ software, and Bionano EnFocus™ are trademarks of Bionano Genomics, Inc. All other trademarks are the sole property of their respective owners.

No license to use any trademarks of Bionano is given or implied. Users are not permitted to use these trademarks without the prior written consent of Bionano. The use of these trademarks or any other materials, except as permitted herein, is expressly prohibited and may be in violation of federal or other applicable laws.

Revision History

REVISION	NOTES
A	Initial release of document.
B	Added Saphyr Assure information and updated Instrument Controller information
C	Additional security features added from Access 1.7 release.
D	Revised for Access 1.8 release

Introduction

The Bionano Security Guideline document is being released in conjunction with the Bionano Compute On Demand and Saphyr Assure services, but it is relevant for all Bionano customers. This guideline outlines how data will be handled. It also outlines what responsibilities lie on the customer organization to provide a secure end-to-end solution.

Bionano Compute On Demand

Bionano Compute On Demand is a hosted solution designed to provide compute resources to perform Bionano Solve operations for customers who have no local compute resources or temporarily require additional compute resources. Bionano Compute On Demand works in conjunction with Bionano Access. Bionano Access is a web server that acts as a portal and visualization tool for Bionano data.

Saphyr Assure

Saphyr Assure is a remote service provided by Bionano that enables the Instrument Control Software (ICS) to transmit system health metrics, run diagnostics and configuration information to enable Bionano to proactively provide support to customers. Saphyr Assure analyzes run metrics and alerts the support team to potential issues so that they can reach out to the customer to address issues before data quality and run performance are impacted. Saphyr Assure enables users to install software updates for Saphyr ICS, allowing for quick and easy updates. Saphyr Assure also manages Microsoft Windows update checking to ensure the system is always running with the latest validated updates.

Data Privacy Statement

Bionano is committed to protecting the security of personal and protected data. We take reasonable physical, electronic, and administrative safeguards to help protect personal information from unauthorized or inappropriate access. We do not sell or share personal or protected data with third parties without explicit permission. Bionano Compute On Demand does not retain any protected data on the hosted systems beyond the life of the job as indicated in its terms of use. Saphyr Assure does not collect any protected data; it only collects system health and diagnostic data.

Information Classification

To understand potential security risks, we classify the data involved. Personally identifiable data is non-health information that can be traced to an individual. When personal data becomes tied to health information, it becomes protected health information, as defined by HIPAA. Bionano does not ask for, transmit, or store protected health information. Specifically, Bionano stores and transmits only de-identified genomic data. Below (**Table 1**) we have identified the types of data in the Bionano Compute On Demand and Saphyr Assure that fall into these categories. Bionano provides security features to protect all the following data.

Table 1. Information Categories

Service	Category	Data	Description
Bionano Compute On Demand	Personal	User Account	User account information, including email addresses, is used to track token and job ownership. Contact information is used to convey job and system status messages.
Bionano Compute On Demand	Personal	Jobs Metrics	General metrics regarding jobs such as the user, organization, job status, operation type, run time, and cost are tracked. This information is necessary to provide an accurate accounting of tokens spent, system health, and troubleshooting.
Saphyr Assure	Performance	Chip Metrics	General information about chip usage (i.e., throughput, data quality) is tracked to continuously improve instrument, chip performance, and provide enhanced support.
Saphyr Assure	Performance	System Alerts	Error conditions and alerts are tracked to monitor the health of the environment and to provide enhanced support.
Bionano Compute On Demand	Other	Genomic Data	De-identified genomic data is stored temporarily on the Bionano Compute On Demand service during the analysis. After the operation has been completed and downloaded the input files are deleted. All data transfers are encrypted.

System Design

Several features have been built into Bionano products to ensure the protection of user data. This section will describe the security features of our Instrument Controller, Bionano Access, Bionano Compute On Demand and Saphyr Assure. **NOTE**: While some of these features are automatic and do not require user action (i.e., data encryption), many features (i.e., HTTPS SSL certificate) do need active management by qualified personnel at the customer site.

- **Encrypted Data Transfer**: All data transfers are encrypted. This includes all local communication between systems as well as communication to hosted Compute On Demand and Saphyr Assure services. File uploads to the Compute On Demand service do utilize HTTP, but those transfers are encrypted via the Java library used.
- **Password Protection**: User passwords stored in the system are hashed and stored in a database.
- **Password Expiration**: Administrators can set how often passwords should expire. They can also set how long previous passwords should be retained.
- **Password Complexity**: Administrators can also control password complexity. They can set the minimum length, inclusion of numbers, special characters, and case changes in a valid password.
- **Detect CAPS Lock**: The login page will display a message if CAPS lock is on.
- **First Login**: On first login the user will be prompted to change their password.
- **Forgot Password Workflow**: From the login page users can indicate they have forgotten their password. The system will allow the user to reset their password from a link sent by email. The link is valid for a limited period.
- **Password Change**: From the account profile screen, users can change their password at any time. Each password provided will be retained in their password history for the configured password expiration period.
- **Login Attempts**: Administrators can control how many login attempts are permitted before a user account is locked. Administrators can unlock accounts.
- **Session Controls**: Users are not permitted to share accounts. When the system detects a new login on a user account any previous sessions are invalidated.
- **Session Inactivity**: Sessions will be deactivated after a set period of inactivity on the website. Bionano Access can detect activity on a given page, so activity is not measured solely by page loads.
- **Active Directory Support**: It is possible to configure a Bionano Access Server to use Active Directory for authentication. Refer to the *Bionano Access Software User Guide* (CG-30142) for details.
- **Logging**: All system activity is logged. The default system configuration will roll logs each day and retain them for five days. This log files can be archived or configured to remain for longer periods of time. The logs are in JSON format so they can be parsed easily.
- **User Roles**: System privileges are controlled by the assignment of a role to a user account. There are four roles in the system: Administrator, Project Lead, User, and Read-Only. User accounts can only be assigned a single role. These roles are described in detail in the *Bionano Access User Guide*.
- **Account Deactivation**: Only accounts that have no data associated with them can be deleted. User accounts that have performed any operations cannot be deleted; they can only be deactivated. This

ensures that all records of system activity are retained properly. Only administrators can delete or deactivate accounts. Users cannot log into accounts that have been deactivated.

- **Project Based Data Access**: All data in Bionano Access is tied to projects. Project Leads can create projects and control who can access them.
- **Job Ownership Protection**: Several forms of identification are tracked with each Bionano Compute On Demand job to determine ownership. Only the instance of Bionano Access that submitted the job can download the results.
- **Code Obfuscation**: Bionano Access JavaScript source code has been obfuscated and is not legible to prevent malicious modification of the source code.
- **Token Balance Protection**: All voucher usage and token balances are managed by the Bionano Compute On Demand solution and do not reside on Bionano Access.
- **Debugging Prevention**: Bionano Access JavaScript source code is self-defending and cannot be debugged.
- **Login Banner**: Administrators can use the Bionano Access Login Banner feature to post corporate policies on the login screen related to the use of Bionano Access.
- **Input Validation**: Data files are validated to ensure required fields are not empty and data is of the correct data type and within valid ranges.
- **HTTPS Support**: All Bionano Access Servers ship with a self-signed SSL certificate as of Bionano Access version 1.6. We recommend installing a valid SSL certificate from the user organization whose certificate authority can be verified from the Bionano Access Server and Instrument Controller.
- **Firewall**: All Bionano-provided computers have their firewalls enabled and are set to only allow native traffic.
- **Diagnostic Data Scrubbing**: When instrument diagnostic data is generated, all identifiers are automatically scrubbed to remove any personal or protected data. The sanitized data set can then be shared with Bionano Support to diagnose instrument issues. All automated system health monitoring datasets that are transmitted to Saphyr Assure are also scrubbed to remove any personal or protected data.
- **Multi-Factor Authentication**: Access to system health monitoring and diagnostic data is secured via multi-factor authentication (MFA) and limited to Bionano personnel that require the data to properly support the system.
- **Enterprise Data Centers**: Bionano only contracts with certified enterprise level data centers for our hosted services. They support the following standards: ISO/IEC 27001, GDPR, FedRamp, HITRUST, HIPAA, and many others. Although subject to change, currently, those data centers are associated with Amazon Web Services (AWS) and Microsoft Azure. Datacenters used for Bionano Compute On Demand are localized in the United States and Europe (currently, Ireland, Netherlands, and Germany) and a customer may choose to point their Bionano Access to any of the supported localized datacenters. Saphyr Assure data is hosted in a datacenter in the United States.
- **Remote Support Tools**: Bionano utilizes TeamViewer to provide remote support to the Saphyr Instrument Controller and the Bionano Access Server. Bionano has enabled multi-factor authentication for its users in addition to a separate machine level password. The Instrument Controller and Bionano Access Server are locked to Bionano's TeamViewer account and cannot be accessed by any other users. Remote sessions can only be initiated with the express permission of a customer representative.

TeamViewer is compliant with many security standards such as ISO/IEC 27001, ISO/IEC 9001:2015, GDPR, HITRUST, HIPAA, and others. See *https://www.teamviewer.com/en-us/trust-center/compliance/* for further details. Remote support may be left enabled to allow for unattended access or, at the user's discretion, can be turned on and off as needed via the Saphyr ICS interface or Bionano Access user interface to provide attended access.

- **Instrument Controller Operating System**: The Instrument Controller has been designed to limit and reduce the attack surface by disabling unnecessary operating system services, blocking user access to the operating system, blocking all applications not provided by Bionano and disabling all incoming network traffic. The Instrument Controller is preconfigured with the Saphyr Instrument Control Software (Saphyr ICS) which runs on an embedded version of the Windows 10 operating system that has been configured to run in Kiosk mode. Kiosk mode allows the user to interact solely with the Saphyr ICS application and does not present access to the operating system to the user. Systems shipped prior to the release of ICS 5.1 do not have kiosk mode enabled. Saphyr P/N 60325 and 60396 are compatible with kiosk mode and may be upgraded by contacting Bionano support.
- **Instrument Controller Operating System Access:** By default, access to the operating system on the Instrument Controller is limited. All functions that the instrument requires of the user or user's IT administrator can be accomplished within the ICS user interface. As there is no requirement for operating system access for instrument setup or operation, the default policy is to not supply operating system credentials to end users. Exceptions to this policy can be requested from Bionano Support.
- **NOTE:** The Instrument Controller is not a general-purpose PC, and the user should not modify any operating system parameters or settings, change any existing operating system user accounts or passwords, install any 3rd Party software, or modify the computer hardware without prior approval from the Bionano support team. Bionano is unable to guarantee the performance or accuracy of the Saphyr system if any unapproved modifications are made.
- **NOTE:** The user should not attempt to join the instrument controller to a domain as this will interfere with the group policy configuration that the instrument control software requires to run reliably and can also cause a failure of the kiosk mode feature.
- **Windows Updates**: Bionano is committed to providing tested and validated security updates in a timely manner. The Instrument Controller does not permit automatic Windows updates as they often cause a system restart which would interrupt instrument operations. Saphyr ICS had been designed to manage the detection, validation, and installation of Windows updates to ensure that the system is kept up to date with the latest security updates while ensuring compatibility with our systems. Saphyr ICS checks (daily) for available windows updates from Microsoft's servers. When an update is detected, it is sent to the Saphyr Assure service to check whether it has been tested and validated to function properly with the Saphyr Instrument Controller. When an update has been tested and released, the user will be notified of pending updates to install. When the instrument is idle and not processing a chip, the user can click the update icon and install pending updates (**Figure 1**).

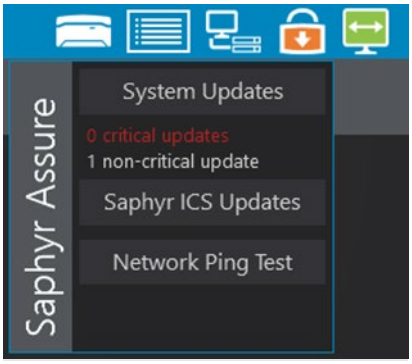

Figure 1. System Updates

- **Windows Defender**: The Instrument Controller includes the Windows Defender antivirus and malware detection program and is configured to protect the system without adversely affecting the performance of the Saphyr ICS software. Security Intelligence Updates for Windows Defender are downloaded and installed via the **Windows Update** mechanism described in the preceding section. The use of other products can interfere with the operation and performance of the Saphyr ICS application and is not recommended.
- **Download Warnings**: Administrators can add custom system messages to warn users regarding proper data handling that must be acknowledged each time they attempt to download data.
- **Proxy Support**: The Bionano Access Server can be configured to support proxy use when connecting to Bionano Compute On Demand services.
- **Logging**: Extensive logging is available from the Bionano Access Server. The log files are in Splunk compatible format. The log files roll nightly and are retained for 5 days by default. Retention can be configured, and log files can be archived daily.

Saphyr System Architecture

The diagram below (**Figure 2**) depicts the high-level architecture of the typical data solution for a Saphyr instrument installation. The Saphyr is connected via USB3, USB2 and CAN-BUS to the Instrument Controller. The Instrument Controller and the Bionano Access Server have been designed to sit adjacent to the Saphyr in the lab. The Instrument Controller is connected to the Bionano Access Server via network. We include a tether cable so chip processing can continue if there is a customer network outage. The Compute servers are installed in the customer's data center and the communication between the Bionano Access Server and the Compute servers is over the customer's network. The communication between the Instrument Controller and the Bionano Access Server is HTTPS. There is also HTTPS traffic coming from the compute nodes back to the Bionano Access Server. We provide a self-signed SSL certificate by default. We recommend a valid SSL certificate be installed by the customer on the Bionano Access Server when possible. Static IP addresses are required for the Bionano Access Server and each node in the compute cluster.

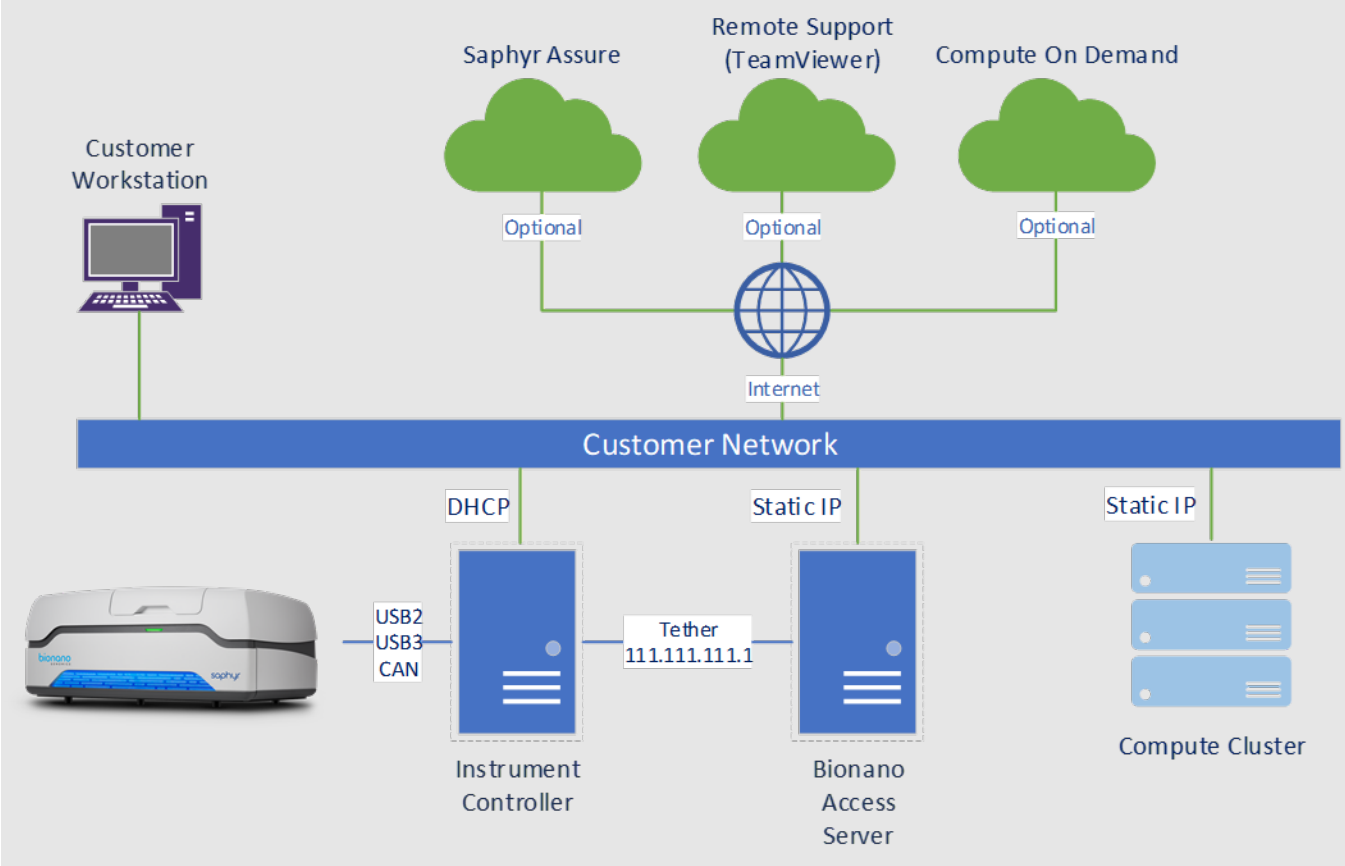

Figure 2. Saphyr System Architecture

The Instrument Controller has been designed to limit and reduce the attack surface by disabling unnecessary operating system services and disabling all unsolicited incoming network traffic. Saphyr can be configured to run in kiosk mode which blocks user access to the operating system and only allows interaction with the Instrument Control software. This is the recommended operating mode in high security settings.

Saphyr Assure

Saphyr Assure is a remote service provided by Bionano that enables the Instrument Control Software (ICS) to:

- Perform remote health monitoring by analyzing instrument performance data, configuration, and logs (Requires opt-in)
- Automate user-initiated diagnostic request submission.
- Enable user-initiated download and installation of software updates for Saphyr ICS
- Retrieve validated Windows Security Updates and Defender anti-virus definition updates.

NOTE: Even if the user is not going to opt-in to the heath monitoring features, network access to Saphyr Assure should still be configured to allow OS Updating, Saphyr ICS software updates and user-initiated diagnostics.

AUTOMATED HEALTH MONITORING BENEFITS

Saphyr Assure is designed to maximize the performance and availability of the Saphyr instrument. By continually monitoring run performance, Saphyr Assure can detect future performance issues before they impact customer workflow and data quality. If any potential issues are identified, the Bionano support team will proactively contact the customer and determine a time to service the instrument before system performance is compromised. Depending on the nature of the issue, support personnel can connect to the system remotely (if enabled) and perform real-time repairs eliminating downtime.

DATA COLLECTION

Saphyr Assure is designed to collect only information related to instrument and chip performance that is useful in determining current instrument health and predicting future servicing needs. The service has been carefully designed to ensure that no protected Personal Information is collected. This information detailed below is also collected when a user initiated diagnostic request is generated (**Table 2**).

Table 2. Types of information collected.

Information Type	Description of Collected Data
Instrument configuration	Saphyr ICS version number, Instrument serial number, part number, hardware configuration (component serial numbers, firmware versions), calibration information
Run setup	Sample unique ID (random, machine generated unique identifier), Enzymes, Fluorescent Label, Genome Type (human, or non-human)
Chip	Chip serial number, barcode, chip registration data
Run performance	Operation start / end time DNA Loading recipe and electrophoresis trace data Chip cleaning metrics Hardware performance metrics (i.e., focus, uniformity, lasers, stages) DNA quantity and distribution statistics Mapping metrics (Map Rate, NLV/PLV rate, BPP …)

Saphyr Assure does **not** collect protected Personal Information and does **not** collect any optical genome map data or any other identifying information (**Table 3**).

Table 3. Types of information not collected.

Information Type	Description of Uncollected Data
Sample	Sample Name, Sample Description, User ID
Genome Reference	Reference Name, Reference File Name
Project	Project Name
Run	Operator ID
Chip Setup	Chip Name
Molecule	Individual DNA molecule data (BNX)

All communication with the Saphyr Assure service is performed over an encrypted https connection using Transport Layer Security (TLS) V1.2. All data stored in the Saphyr Assure service is encrypted using 256-bit AES encryption using the Microsoft Azure infrastructure. Access to health monitoring and diagnostic data is secured via multi-factor authentication (MFA).

Molecule Detection

The Instrument Controller (**Figure 3**) is connected to the Saphyr Instrument via USB3. The Instrument Controller will take the captured images and convert them to BNX files. BNX is a proprietary Bionano data format that describes the molecules detected and the label locations on them. Refer to Bionano.com for current specifications on all our proprietary data formats. The Instrument controller will also generate molecule metrics (i.e., the count of molecules detected, label density, etc.).

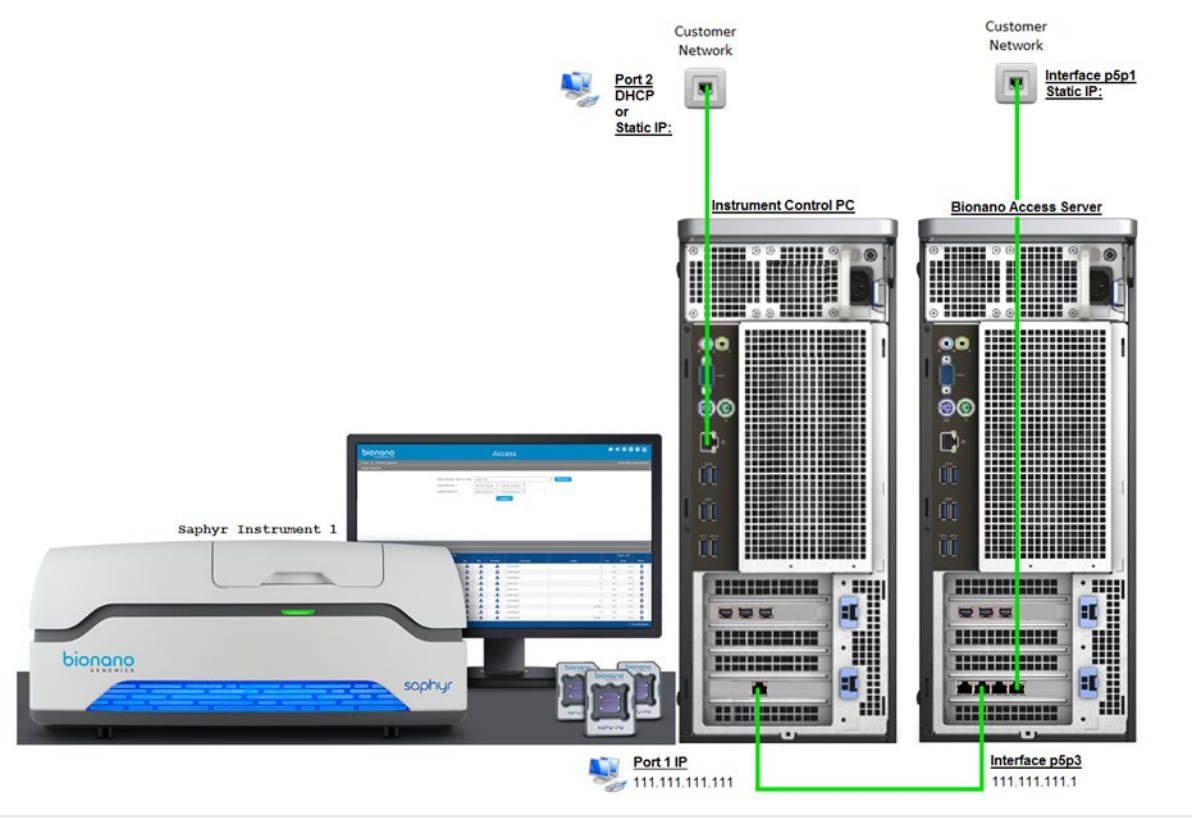

Figure 3. Instrument Controller

There are two ways the instrument controller can be connected to the Bionano Access Server. Typically, the Instrument Controller and Bionano Access Server are tethered with a network cable. This allows chip runs to be processed even if the customer's network is down. The Bionano Access Server is accessible to the Instrument Controller with the IP address of 111.111.111.1. To tether the Bionano Access Server it must sit in proximity to the Instrument Controller in the lab. When it is not possible to place the Bionano Access Server in the lab it can be reached over the customer's network. The customer must assign a static IP address to the Bionano Access Server. 1GB bandwidth on the network is sufficient for transferring molecule data to the Bionano Access Server.

Chip run data is grouped into cohorts. There are eight cohorts per scan per flowcell. For each cohort, the Instrument Controller will send a BNX file with molecule metrics to the Bionano Access server over HTTPS (port 3005). The Bionano Access Server will then generate mapping metrics such as the map rate. The Instrument Controller will pull mapping metrics for each cohort over HTTPS (port 3005). Both ICS and Bionano Access will

dashboard the molecule and mapping metrics so the operator can monitor the chip run at the instrument or from their workstation. When the chip run is completed the individual cohort BNX files for a flowcell (assuming users are not multiplexing) are merged and the resulting BNX file is inserted into the selected Bionano Access project as a new Molecules Object.

Local Compute Cluster

The Bionano Compute cluster will consist of at least one Saphyr Compute system. Each Saphyr Compute server consists of four individual servers inside a single 2U rack mount chassis. Detailed information about the server configuration is provided in the *Saphyr® Networking and Setup Guide* (CG-30251) . To launch jobs and transfer files the Bionano Access Server will communicate with the Saphyr1a over SSH. The Bionano Access Server will not communicate with any other nodes in the compute cluster. The Saphyr1a node must be assigned a static IP and be accessible to the Bionano Access Server. The Compute systems are rack mount so they are often in data center that can be distant from the lab. 1GB band with is sufficient, but 10GB is recommended if possible. The size and complexity of the files transferred has continued to grow over time. When a node finishes a compute job it will do two things. First, it will curl an HTTPS post (port 3005) to the Bionano Access Server to semaphore that the job has been completed. Second, it will output a file with the completion status. Every 5 minutes the Bionano Access Server will SSH to the Saphyr1A node and check for completion marker files for each active job. After the Bionano Access Server receives a semaphore or finds a completion marker file it will download the result files from the Saphyr1A node via SSH. Once the results have been downloaded the Bionano Access Server will email the user who launched the job to let them know the results are available. By default, the Bionano Access Server will relay emails through Amazon SES services. Bionano Access Server can be configured to use local SMTP email services within the customers infrastructure instead if desired. Contact Bionano Support to learn how to change SMTP settings. A chron job on Saphyr1a will delete job files that are older than 2 weeks automatically.

4

Bionano Compute On Demand

The flow of data for a Bionano Compute On Demand job is like how they are processed locally. Data is just being routed to the hosted Bionano Compute On Demand service instead of the local compute cluster. All communication to and from the Bionano Compute On Demand service is encrypted. To use the Bionano Compute On Demand service the organization's Bionano Access Server must have Internet access. The Bionano Access Server can be configured to work with a proxy that does not require authentication credentials if necessary. Bionano Compute On Demand can be configured to use only regional datacenters to process the data to ensure the data does not leave those regional boundaries. Contact Bionano Support for more information about the regional datacenters.

Before launching each job, the Bionano Compute On Demand service is contacted to provide a token estimate. When the job is launched the tokens needed are reserved. Then the input files are uploaded serially. Once all the files have been uploaded the analysis will start. Each analysis job runs on its own independent compute environment. When the job is finished it can be downloaded back to the local Bionano Access Server. The Bionano Compute On Demand service tracks what instance of Bionano Access launched the job and will only allow that instance to retrieve the results. Once the results have been successfully downloaded the input and result files on the Bionano Compute On Demand service are deleted. If the job does not successfully complete any input and result files will still be deleted automatically after 30 days. End users only ever interact with their local Bionano Access Server to use the Bionano Compute On Demand service. They do not ever directly access the Bionano Compute On Demand service. After completion, the Bionano Compute On Demand services will reconcile the cost of the job and refund any unused tokens that were not consumed. The user will receive a refund email in this case from the Bionano Compute On Demand service.

Communication Channels

Below (**Table 4**) is an inventory of the communication protocols used between systems.

Table 4. Communication Protocols

Originating From	Target	Protocol
Bionano Access Server	Saphyr1a Compute Node	SSH (port 22)
Bionano Access Server	Amazon SES Email service	SMTP (port 587)
Saphyr Instrument Controller Customer Workstations Compute Servers	Bionano Access Server	HTTPS (port 3005 or 3006)
Saphyr Instrument Controller	Saphyr Assure Service	HTTPS (port 443)
Bionano Access Server	Compute On Demand	HTTPS (ports 443 and 3000) HTTP (port 3001)
TeamViewer	Bionano Access Server	TCP port 5938

Controls

While Bionano products have been designed to provide data security, protection of data also depends on security policies in use by the customer's organization. The following security controls should be considered.

- **Information Security Policy**: the organization should have formal security policies established.
- **Access Authorization**: If formal approval or authorization is needed for a Bionano Access user account, a procedure is needed to document the authorization for each account created. Bionano Access does not have the means to track this approval process.
- **Remote Support**: Bionano support may require remote access to the system to troubleshoot issues. Understand the organization's guidelines for external access and work within those regulations. Establish connectivity for support personnel in advance to avoid operational interruptions.
- **Disaster Recovery**: Establish procedures for backup, data retention, emergency operation, and recovery for the environment that is compliant with the organization's regulations. These policies will vary within each organization depending on the criticality of the Bionano system and the tolerance for data loss.
- **Record Retention**: Bionano Access does not have a mechanism to expire, retire, or delete expired data. We do track the date each object was created. If there are specific policies about record retention procedures will be required to manually delete them.
- **De-identification**: Various data elements within the system require a name. These include projects, samples, experiments, and objects. The organization should have a procedure for de-identification or pseudonymization of these data elements to prevent the identification of protected data.
- **Shared Accounts**: Shared accounts are not allowed and Bionano Access features prevent their use. Under no circumstances should accounts or account credentials be shared.
- **Unattended Access**: The system will deactivate accounts after a period of inactivity. If leaving a workstation log out before walking away.
- **Clear Desk Policy**: Most organizations have a clear desk policy that prohibits leaving any personal or protected data out on the desk or workstation where it is plainly visible. It is a good practice to prevent the loss of protected data or give an easy mechanism to defeat the system's de-identification.
- **System Updates**: Each Bionano software release includes important security patches in addition to new and improved functionality. It is important to upgrade as soon as possible the latest version when it is released.
- **Patching**: Customer must consider how often they want to patch their Centos operating system. At a minimum we recommend patching the system when installing updated versions of Bionano software. Some sites with tightened security patch more frequently. Bionano Access includes a security page that indicates the current patching status at Bionano and if there are any known patching issues. Users can also sign up for security patching notifications from this page.
- **User Audits**: An audit of user accounts should be conducted on a regular basis. Accounts that are no longer necessary should be deactivated.
- **Default User Account**: The default user account provided with the initial Bionano Access installation should be deactivated once true administrator accounts have been created and tested.
- **Banners**: Banners can be added to login and download screens to warn users regarding appropriate use and related policies.

Risk Management

Bionano has activities that are conducted as part of each software release. This section outlines some of the activities being conducted to harden Bionano security offerings.

- **Ticketing System**: A ticketing system is used in-house to track all defects and feature requests. The ticketing system ensures that all changes are visible to the Bionano Software Quality Assurance (SQA) team. The ticketing system also enforces and documents the workflow necessary to validate every system change completed.
- **System Validation**: All features of Bionano systems are tested for each release. Regression testing ensures that existing security features are not compromised due to code changes. Test cases are generated for each user story. A Validation Plan is generated for each release to document what was tested.
- **Threat Mitigation**: Testing is conducted with security in mind. Defects, usability issues, and security concerns are logged as tickets for development to address.
- **Change Control**: All Bionano systems are under source control. Code check-ins reference the ticket driving the change and tickets are given the commit numbers so they can be cross-referenced.
- **Security Patches**: Bionano reviews all libraries and packages in use and determines which need to be updated. Tools such as retire.js for Nodejs or Safety for Python are used to automate this review where possible. Libraries are then updated in our code base and tested during development to ensure stability.
- **Security Scans**: Tools such as Qualys are used to perform security scans on our configured systems for each release cycle. Security issues identified are ticketed for resolution. We also support customers who choose to perform their own security scans.

Common Security Considerations

This section describes some typical security concerns encountered during installation.

- **Anti-Virus Software / Hard Disk Encryption**: It is common for customers to have rules that dictate corporate standardized anti-virus and/or hard disk encryption software be installed on all workstations including the Instrument Controller. We do not recommend doing this. The Instrument Controller is already equipped with anti-virus software which updates automatically and has been tested with our solution. Thousands of individual files can be created during a typical chip run and adding anti-virus software is certain to have a significant performance impact, which may lead to a loss of sample or data. The Instrument Controller should be considered part of the instrument and not a typical workstation.
- **Active Directory**: The Instrument Controller cannot be joined to the customers Active Directory. Doing so would cause customer security policies to override the security settings that have already been carefully set on the system to provide the optimum environment for running the instrument. Non-validated security settings may lead to a loss of sample or data. Please contact Bionano support for any specific security setting concerns.
- **Internet Access**: Some sites prefer to limit Internet access where possible. Internet access is required to use the Bionano Compute On Demand and or Saphyr Assure services. Internet access is also required for Bionano to provide remote support. Internet access is also required to perform some system updates. Internet access can be limited, but these service offerings would be impacted.
- **VLANs**: We support a configuration for the local Compute cluster where all the nodes except the submission node are in a VLAN. This can be helpful where the customer has limited static IP addresses.
- **Customer Clusters**: This document only pertains to the use of Bionano validated systems. It does not extend to customer resources used to provide compute resources. Contact Bionano Support for concerns regarding using customer compute resources.
- **Web Server in the Data Center**: Some customers require all web servers to be secured in the data center and do not allow their placement in the lab. The Bionano Access Server can support this configuration, but network outages could interrupt the operation of the Saphyr. When placing the Bionano Access Server in a data center, we recommend a 10 GB ethernet connection if possible.

Bionano Compute On Demand and Saphyr Assure Terms and Conditions

The terms and conditions agreed to by the system administrator on behalf of the organization to enable a connection to Bionano Compute On Demand and/or Saphyr Assure are below. By using Bionano Compute On Demand and/or Saphyr Assure, the organization is bound by these terms and conditions.

- Only Bionano Compute On Demand and Saphyr Assure that is owned, licensed, or lawfully obtained by the organization can be used to process data.
- Compliance with the current Bionano technical documentation applicable to the data sent to the Bionano Compute On Demand must be in place. Noncompliance with this technical documentation may result in failure of operations that is not reimbursable by Bionano.
- Genomic data (i.e. BNX files) will be transferred from the local server to a hosted Bionano Compute On Demand resource for the purpose of computing in the cloud. These resources exist in AWS and/or Microsoft Azure data centers and not on Bionano-owned infrastructure. The data is encrypted during transit to those datacenters.
- Upon successful completion, data are returned to the organization's Bionano Access Server and are deleted from Bionano Compute On Demand.
- When operations fail in Bionano Compute On Demand, data are retained temporarily within the Bionano Compute On Demand servers. Users may authorize Bionano Support to view this data for the sole purpose of troubleshooting the failure. Whether or not Bionano is contacted, this temporary data will be deleted pursuant to Bionano procedures in effect at that time.
- Tokens provided from Bionano are required to run operations in Bionano Compute On Demand. Users will act ethically in procuring and using tokens. No attempt to misuse or otherwise attempt to subvert the use of tokens will be tolerated.
- System health metrics will be transferred from the Saphyr system to Saphyr Assure that is hosted in a Microsoft Azure data center. The data is encrypted during transit to this datacenter. Refer to Saphyr Assure section for details of the data that is transmitted.
- By enabling Bionano Compute On Demand and Saphyr Assure, Bionano is authorized to collect summary metrics to support billing, support, and product improvement. These metrics include information on the status of the Bionano Access and Saphyr system and are not shared with third parties. Bionano does not collect any protected health information nor the actual run data or pipeline results. Saphyr Assure Only without Bionano Compute On Demand can be selected. This enables the collection of the same summary metrics, but not allowing organizational genomic data (i.e., BNX file) to be sent to Bionano Compute On Demand.
- The organization agrees to receive emails from Bionano pertaining to Bionano Compute On Demand and Saphyr Assure system maintenance and upgrade events. Bionano does not share email information with any third parties. These emails will be sent to the email addresses registered in the organization's Bionano Access server and/or associated with accounts within Bionano's systems.
- Bionano, at its sole discretion and without prior notice, may terminate access to Bionano Compute On Demand and Saphyr Assure if compliance with the terms of use are not met or if otherwise illegal or unethical behavior is detected.

Technical Assistance

For technical assistance, contact Bionano Technical Support.

You can retrieve documentation on Bionano products, SDS's, certificates of analysis, frequently asked questions, and other related documents from the Support website or by request through e-mail and telephone.

TYPE	CONTACT
Email	support@bionano.com
Phone	Hours of Operation: Monday through Friday, 9:00 a.m. to 5:00 p.m., PST US: +1 (858) 888-7663
Website	www.bionano.com/support
Address	Bionano, Inc. 9540 Towne Centre Drive, Suite 100 San Diego, CA 92121