Genome Suite Analyzer User Guide for AWS

The Sequencing Center

Date: 2024-10-01

Repository: The-Sequencing-Center/GenomeSuite-Docs

Website: www.thesequencingcenter.com

Support: support@thesequencingcenter.com

Phone: +1 877-425-2235

Contents

Getting started

GenomeSuite Analyzer runs on the Amazon Web Services (AWS) platform. If you do not have an AWS account, start with Create an AWS account. If you do have an AWS account, you can skip to the step Log into your AWS account.

Some steps are identified as a "*one-time step*". This means you should only have to perform this step once during initial setup.

GenomeSuite Analyzer can process POD5, FAST5 or BAM files. You will have to choose one filetype for each run.

Create an AWS account

This is a *one-time step.*

1. Open the AWS account creation page and **Create an AWS Account**.
2. Fill in the details and click **Verify email address**. You will receive an email with a verification code that you need to enter on the sign up page.
3. Set up your root user password and confirm it.
4. Choose between a Personal or Professional account. The features and functions are the same, but the information required might differ slightly.
5. Fill in your contact information and read the AWS Customer Agreement. Once done, click **Continue**.
6. Provide a valid payment method (credit/debit card). This step is mandatory even if you plan to use the free tier services. You may also need to verify your payment method by entering a code sent by AWS.
7. AWS will ask you to provide a phone number to verify your identity. You will receive a call or SMS with a verification code that you need to enter to proceed.
8. Select one of the available support plans (Basic, Developer, Business, or Enterprise). The Basic support plan is free.
    - After selecting your support plan, AWS will begin activating your account. This process usually takes a few minutes but can take up to 24 hours. Once activation is complete, you will receive a confirmation email.

After your account is activated, you can sign in to the AWS Management Console and start using AWS services.

Log into your AWS account

1. Open your web browser and go to the AWS Management Console login page.
2. On the login page, you will see two options:
    - **Root user:** Use this if you are logging in as the account owner or the main administrator.
        - If you are the root user, click **Root user** and enter your email address associated with the AWS account. Click **Next**.
    - **IAM user:** Use this if you have been assigned a user account within an AWS organization.
        - If you are an IAM user, click **IAM user** and enter your IAM username along with the account ID or alias. Click **Next**.
3. Enter the password for your account, and click **Sign In**.

- If Multi-Factor Authentication (MFA) is enabled for your account, you will be prompted to enter the code from your authentication device, such as a mobile app. Enter the code and proceed.

4. After successful authentication, you will be directed to the AWS Management Console, where you can start managing your AWS services.

Create an S3 bucket

This is a *one-time step.*

You will now create an AWS S3 bucket that will contain all of your Nanopore POD5 sample files.

1. From the AWS Management Console, type **S3** into the search bar at the top and select **S3** from the drop-down list. This takes you to the Amazon S3 dashboard.
2. On the S3 dashboard, click the **Create bucket** button.
3. To configure the bucket settings, enter a name for the bucket in the **Bucket** name field.
   - **Bucket name:** Bucket names must be globally unique across all existing bucket names in Amazon S3.
     - If you choose a name that is already taken, you'll have to try other names until you find a unique name.
     - The name must not contain spaces and must adhere to the bucket naming rules (e.g., lowercase letters, numbers, and hyphens).
   - **Region:** Select the region **US East (N. Virginia) us-east-1**. This is the region where the S3 bucket will be created.
4. Set the bucket options.
   - **Block public access settings:** By default, S3 buckets are set to block all public access. You can leave this option enabled unless you specifically need the bucket to be public.
   - **Bucket versioning:** To enable versioning, which keeps multiple versions of an object in the same bucket, you may optionally choose to enable this in **Bucket Versioning**.
   - **Tags, object lock, and encryption:** You may also enable additional optional settings such as adding tags, enabling object lock, and set default encryption, but these are not necessary can be configured later.
5. Review your bucket settings configuration and click **Create bucket**.
6. After the bucket is created, you are taken back to the S3 dashboard, where you will see the bucket name listed among your S3 buckets. Verify that the bucket was created successfully.

Upload POD5 files to an S3 bucket

There are several methods available for uploading POD5 files to S3 buckets. These methods are beyond the scope of this document. For human whole genome sequencing, the aggregate size of these files is quite large, ca. 1TB or more, and may need special methods to upload in reasonable time.

Please contact us at support@thesequencingcenter.com to review and discuss options for uploading large datasets.

Store POD5 files in S3 bucket

If you already have an AWS account and an S3 bucket with POD5 files in it, you have two choices. You can use the existing bucket name with GenomeSuite Analyzer or you can copy or move the files from the existing bucket to another bucket within the same AWS account.

1. In the S3 dashboard, click on the bucket that contains the POD5, FAST5 or BAM files you want to copy or move.
2. Browse the folders in your source bucket and select the files you want to copy or move.
   - You can select multiple files by holding the **Ctrl** key (or **Cmd** on Mac) while clicking.
3. After selecting the files, click the **Actions** button at the top of the screen, and choose either **Copy** or **Move**.
   - A dialog box appears asking where you want to copy or move the files.
4. In the **Destination** field, click **Browse S3** and navigate to the destination bucket. Specify the exact location within the bucket by selecting a folder or leave it blank to place the files directly in the bucket's root.
5. Once the destination is set, click **Copy** or **Move**. Depending on the size and number of files, this may take a few moments.
6. Navigate to the destination bucket and verify that the files have been successfully copied or moved.

Create a key pair

This is a *one-time step.*

1. In the AWS Management Console, type **EC2** in the search bar and select **EC2** from the drop-down menu.
2. In the EC2 Dashboard in the left-hand side menu, click on the **Key Pairs** option under the **Network & Security** section.

3. Click the **Create Key Pair** button.

4. Configure the key pair settings:

   - **Name:** Enter a name for your key pair, such as `GenomeSuite-Analyzer-keypair`. The name must be unique within your AWS region.
   - **Key pair type:** Choose the key pair type, typically **ED25519**.
   - **Private key file format:** Choose the format for the private key file. Options include: - **.pem:** For SSH clients (like OpenSSH) on Linux or macOS. - **.ppk:** For PuTTY, a popular SSH client on Windows.
   - **Tags:** (Optional) You can add tags to your key pair for easier management.

5. Click **Create key pair**. AWS will generate the key pair and automatically download the private key file to your computer.

Secure the private key

1. Save the private key.

   - The private key file will automatically download to your computer. This file is crucial for connecting to your EC2 instances securely, so store it in a safe location. If you lose this file, you will not be able to connect to your instances using this key pair.

2. To set the correct key pair permissions on a Linux or macOS system, run the following command:

   ```
   chmod 400 /path/to/your-keypair.pem
   ```

3. Store the private key in a secure location. Do not share it with anyone or commit it to version control systems like Git.

Important notice:

- **One-time download:** The private key file can only be downloaded once at the time of creation. If you lose the private key, you will need to create a new key pair and update your instances to use the new key.

- **Accessing EC2 instances:** When launching a new EC2 instance, you will be able to select this key pair for SSH access. Ensure the correct permissions are set on your private key file before attempting to connect.

Create a security group

This is a *one-time step.*

1. In the AWS Management Console, type **EC2** in the search bar and select **EC2** from the drop-down menu.

2. From the left-hand menu in the EC2 Dashboard, click the **Security Groups** option under the **Network & Security**.

3. Click the **Create security group** button to create and configure a new security group.

    - **Name:** Enter a name for your security group, such as **GenomeSuite-Analyzer-sg**.
    - **Description:** Provide a brief description of the security group, like "Security group for SSH access to EC2 instances".
    - **VPC:** Choose the appropriate VPC (Virtual Private Cloud) where you want this security group to be used. If you only have one VPC, it will be selected by default.

4. To configure the inbound rules for SSH access, click **Add Rule** from the **Inbound rules** section.

    - **Type:** From the drop-down list, select **SSH**. This will automatically set the **Port Range** to 22.
    - **Source:** You can choose **My IP** to allow SSH access only from your current IP address.
        - Alternatively, select **Anywhere** (0.0.0.0/0) to allow SSH access from any IP address, but note that this is less secure and should be used with caution.
        - You can also specify a custom IP range if you only want to allow SSH access from specific IP addresses or ranges.

5. Review the rules you added to ensure they match your requirements. Once satisfied with the configuration, click **Create security group**.

6. Attach the security group to an EC2 instance.

    - **During EC2 instance launch:** When launching a new EC2 instance, you can select this security group under the **Configure Security Group** section.

    - **For existing instances:** If you want to assign this security group to an existing instance, go to the **Instances** section, select your instance, click **Actions** > **Networking** > **Change Security Groups**, and then select the **analyzer-sg** security group.

Important notice:

- **Security considerations:** Allowing SSH access from any IP address (0.0.0.0/0) is convenient, but can expose your instance to potential attacks. It is recommended to restrict access to specific IP addresses whenever possible.

- **Firewall settings:** Ensure that any local firewalls on your machine or network allow outbound connections on port 22. # Launch GenomeSuite Analyzer on EC2

To launch the GenomeSuite Analyzer AMI (Amazon Machine Image) using EC2:

Select an EC2 region

1. Navigate to the EC2 Dashboard and confirm you are in the correct region.
2. In the top-right corner of the EC2 Dashboard, click on the **Region** selector drop-down.
3. Select one of the four regions from the list of regions GenomeSuite Analyzer is available in four AWS regions.
    - US East (N. Virginia) us-east-1
    - US East (Ohio) us-east-2
    - US West (Oregon) us-west-2
    - Canada (Central) ca-central-1

Launch the GenomeSuite Analyzer AMI

1. In the left-hand menu under **Images**, click on **AMIs**.
2. At the top of the AMIs page, click **Owned by me** and choose **Public images** from the drop-down list.
3. In the search bar, type **GenomeSuite__Analyzer__v.1.3.0** and press Enter.
4. From the results, select the checkbox next to the **GenomeSuite__Analyzer__v.1.3.0** AMI to highlight the row.
5. With the AMI row selected, click on the **Launch instance from image** button at the top right of the page to launch the instance.

Configure the instance

1. On the **Launch an Instance** page, enter a name for your instance in the **Name** field.
2. Under **Instance Type**, select one of the following options:

    For human exome, use these instance types:

    - `p3.2xlarge`
    - `p3.8xlarge`
    - `p3.16xlarge`

    For human whole genome, use this instance type:

    - `p4d.24xlarge`

    These instance types are optimized for high-performance computing tasks using Nvidia GPU's.

3. Under **Key Pair (login)**, select the key pair you created earlier (e.g., `GenomeSuite-Analyzer-keypair`).
4. Under **Network Settings** > **Edit**, choose **Select existing security group** and select the security group you created earlier (e.g., `GenomeSuite-Analyzer-sg`).
5. Under **Configure Storage**, set the storage size to **2048 GiB**. Ensure the storage type is set to **gp3** (General Purpose SSD).

Launch the instance

1. Review the configurations to ensure everything is set correctly.
2. Click the **Launch Instance** button at the bottom of the page.
   - If you get an error message `Insufficient Capacity`, this means all of the available computing resources are in use.
3. At this point, you have two options:
   1. Wait a few minutes and try to launch the instance again.

   2. Choose a different region and try to launch the instance again.

   Typically, there are computing resources available in one of the regions.
4. Once launched, you will be taken to a page showing the status of your instance. The instance will take a few minutes to initialize.
5. After the instance is running, you can find it under **Instances** in the EC2 Dashboard. Make sure the instance status is **Running** before attempting to connect. # Configure the EC2 instance

There are a couple ways to configure and connect to an EC2 instance depending on your operating system. Follow the applicable instructions below.

Option 1: Install and configure the AWS CLI on Mac

This is a *one-time step.*

To connect to your EC2 instance using a Mac Terminal, you will first need to install the AWS CLI and then configure it.

Install the AWS CLI on Mac

1. On your Mac, open the **Terminal** application. This should be located in the **Applications** directory.
2. Homebrew is a package manager for macOS that simplifies the installation of software. If you do not have Homebrew installed, run the following command in Terminal and follow the on-screen instructions:

```
/bin/bash -c **$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/ins
```

3. Once Homebrew is installed, install the AWS CLI by running the following command:

   ```
   brew install awscli
   ```

4. Verify that the AWS CLI is installed correctly by running the following command:

   ```
   aws --version
   ```

   You should see output showing the installed version of the AWS CLI.

Configure the AWS CLI on Mac

1. In Terminal, configure the AWS CLI by running the following command:

   ```
   aws configure
   ```

2. When prompted, enter the following AWS credential information:

   - **AWS Access Key ID:** Enter your AWS Access Key ID.
   - **AWS Secret Access Key:** Enter your AWS Secret Access Key.
   - **Default region name:** Enter your preferred region (for example, `us-east-1`).
   - **Default output format:** Enter **None**.

Option 2: Install and configure the AWS CLI on Windows

This is a *one-time step.*

To configure the AWS CLI on a Windows machine and connect to an EC2 instance, follow these steps:

Install AWS CLI on Windows

1. Open PowerShell or Command Prompt by searching for it in the **Start** menu.

2. Download and run the .msi AWS CLI installer for Windows.

   - Follow the on-screen instructions to complete the installation. The installer will automatically install the AWS CLI to your system.

3. In PowerShell or Command Prompt, verify that the AWS CLI is installed correctly by running the following command :

   ```
   aws --version
   ```

   You should see output showing the installed version of the AWS CLI, confirming that it is ready to use.

Configure the AWS CLI on Windows

1. In PowerShell or Command Prompt, configure the AWS CLI by running the following command:

   ```
   aws configure
   ```

2. When prompted, enter the following AWS credential information:

   - **AWS Access Key ID:** Enter your AWS Access Key ID.
   - **AWS Secret Access Key:** Enter your AWS Secret Access Key.
   - **Default region name:** Enter your preferred region (for example, us-east-1).
   - **Default output format:** Enter **None**.

Optional steps

Set environment variables

If you want to make sure the AWS CLI is accessible from any directory, ensure that the installation path is included in your system's environment variables. This is typically done automatically by the installer.

Connect to EC2 instance using SSH

To connect to your EC2 instance using SSH from Windows, you can use PuTTY or the Windows Subsystem for Linux (WSL) with an SSH client. Ensure that you have your `.pem` key file and that it is converted to `.ppk` if using PuTTY. # Connect to GenomeSuite Analyzer on EC2

You can now access the GenomeSuite Analyzer instance that is running on AWS EC2.

Connect to your EC2 instance

1. Ensure you have the `.pem` key pair file that was created when you launched your EC2 instance.

2. Set the correct permissions for the key pair file by running the following command:

   ```
   chmod 400 /path/to/your-keypair.pem
   ```

   Replace `/path/to/your-keypair.pem` with the actual path to your `.pem` file.

3. Connect to your EC2 instance by running the following command in Terminal:

   ```
   ssh -i /path/to/your-keypair.pem ubuntu@your-instance-public-dns
   ```

Replace `/path/to/your-keypair.pem` with the path to your .pem file and `your-instance-public-dns` with the Public DNS address of your EC2 instance. You can find the Public DNS in the AWS Management Console under the **Instances** section.

4. **Access your EC2 instance:**
   - Once connected, you will have shell access to your EC2 instance, allowing you to manage it as needed.

Additional tips

Using SSH config file: If you frequently connect to the same instance, consider setting up an SSH config file to simplify the connection command.

Security considerations: Ensure your `.pem` file is kept secure, as it provides access to your EC2 instance.

Configure AWS Credentials

This is a one-time step.

After logging into the EC2 instance, you must configure your AWS credentials by following these steps:

1. Ensure you are connected the EC2 instance using SSH as previously explained.
2. In your EC2 instance, configure the AWS CLI by running the following command:

   ```
   aws configure
   ```

3. **Enter Your AWS Credentials:**
   - The CLI will prompt you to enter the following information:
     - AWS Access Key ID: Enter your AWS Access Key ID (see below).
     - AWS Secret Access Key: Enter your AWS Secret Access Key (see below).
     - Default region name: Enter the region where your S3 bucket is located (e.g., us-east-1).
     - Default output format: Enter None.
4. When prompted, enter the following AWS credential information:
   - **AWS Access Key ID:** Enter your AWS Access Key ID.
   - **AWS Secret Access Key:** Enter your AWS Secret Access Key.
   - **Default region name:** Enter your preferred region (for example, us-east-1).
   - **Default output format:** Enter **None**.

Important Note: By configuring your AWS credentials directly on the EC2 instance, you enable the instance to interact with S3 buckets. This is essential for performing operations like uploading or downloading files from an S3 bucket. # How to get your AWS Access Key ID and AWS Secret Access Key

For new users

1. Sign in to the AWS Management Console and navigate to the **IAM (Identity and Access Management) Console**.

2. To create a New IAM User:

    1. In the IAM Dashboard, click **Users** in the left-hand menu.
    2. Click **Add user**.
    3. Provide a username and check the **Programmatic access** checkbox to generate an access key.
    4. Click **Next: Permissions** to assign appropriate permissions, either directly or by attaching a policy (e.g., AmazonS3FullAccess if you need S3 access).
    5. Follow the remaining prompts and then click **Create user**. You will see a page with the Access Key ID and Secret Access Key.

3. Download the credentials as a `.csv` file or view them directly on the page.

    Important: This is the only time you'll be able to view the Secret Access Key, so make sure to store it securely.

For existing users

1. Sign in to the AWS Management Console and navigate to the **IAM Console**.

2. In the IAM Dashboard, click **Users** in the left-hand menu.

3. Click on your username to access the details.

4. Create a New Access Key (if none exists or if you need a new one):

    1. Go to the **Security credentials** tab.
    2. Scroll down to the **Access keys** section.
    3. Click on **Create access key**. AWS will generate a new Access Key ID and Secret Access Key for you.

5. Download the credentials as a `.csv`file or view them directly on the page. Ensure it is stored securely.

6. Verify your configuration by listing the S3 buckets or EC2 instances:

    ```
    aws s3 ls
    ```

    or `aws ec2 describe-instances` If configured correctly, this returns a list of your S3 buckets or EC2 instances. # Run GenomeSuite Analyzer

To run GenomeSuite Analyzer on the EC2 instance, follow these steps:

1. When you are logged into your EC2 instance with your AWS credentials, you should already be in the `/home/ubuntu` directory. Confirm this by running the following command:

   ```
   cd /home/ubuntu
   ```

   If you are already there, this command won't change anything.

2. Change into the GenomeSuite Analyzer distribution directory by running the following command:

   ```
   cd analyzer/dist
   ```

3. Start GenomeSuite Analyzer by running the following command:

   ```
   ./analyzer -b bucketname -s samplename -f filetype -m modelname
   ```

   - Replace `bucketname` with the name of the S3 bucket where your POD5, FAST5 or BAM files are stored.
   - Replace `samplename` with an arbitrary name of your choice for the sample being processed.
   - Replace `filetype` with `pod5`, `fast5` or `bam`. This parameter specifies the file format of the sample files. All sample files must be the same filet
   - Replace `modelname` with a dorado basecaller model name.

   GenomeSuite Analyzer will start processing the data. You should see output in the terminal indicating the progress of the operation. Depending on the size of the dataset, this may take some time.

Example commands

Use the following command to show help:

```
./analyzer --help
```

If your S3 bucket is named GenomeSuite-Analyzer-sample, and you are using POD5 files, the command would look like this:

```
./analyzer -b GenomeSuite-Analyzer-sample -s sample1 -f pod5
```

If your S3 bucket is named GenomeSuite-Analyzer-sample, and you are using FAST55 files, the command would look like this:

```
./analyzer -b GenomeSuite-Analyzer-sample -s sample1 -f fast5
```

If your S3 bucket is named GenomeSuite-Analyzer-sample, and you are processing a BAM file, the command would look like this:

```
./analyzer -b GenomeSuite-Analyzer-sample -s sample1 -f bam
```

If you want to see a list of available Nanopore Dorado basecalling models:

```
./analyzer -m
```

Create a New AMI

This is a *one-time step.*

When the GenomeSuite Analyzer job is done, and before terminating the running EC2 instance, it is **VERY IMPORTANT** that you create a new AMI. By creating a new AMI you will save all your configuration settings from above. You can then use this new AMI for all future runs.

To create a new AMI from a running EC2 instance using the EC2 console, follow these steps:

1. In the AWS Management Console, type **EC2** in the search bar and select **EC2** from the drop-down menu.
2. In the EC2 Dashboard, click on **Instances** in the left-hand menu under the **Instances** section. This displays a list of all running EC2 instances.
3. Find the running instance from which you want to create an AMI.
4. Click the checkbox next to the instance to select it.
5. With the instance selected, click on the **Actions** drop-down menu at the top right of the page.
6. From the **Actions** drop-down menu, navigate to **Image and templates** and then select **Create image**. This opens the **Create Image** dialog box.
7. Configure the image settings.
   - **Image Name:** Enter a name for your AMI in the **Image name** field.
   - **Image Description (optional):** You can provide a description of the AMI for future reference.
8. Once you have configured all the settings, click on the **Create image** button at the bottom of the dialog box. AWS will start creating the AMI.
9. To monitor its progress, click on **AMIs** in the left-hand menu under the **Images** section.
   - You will see your new AMI listed with a status of **Pending**. Once the status changes to **Available**, the AMI is ready to use.

Terminate the EC2 instance

When the GenomeSuite Analyzer job is finished, it is very important that you terminate the running GenomeSuite Analyzer EC2 instance. You do not want to accumulate unnecessary charges by letting the instance continue running.

To terminate an EC2 instance, follow these steps:

1. On the EC2 Dashboard, in the left-hand menu, click on **Instances** under the **Instances** section.
2. Find the instance you want to terminate. You can use the search bar at the top to filter instances by name, instance ID, or other attributes.
3. Click the checkbox next to the instance you want to terminate to select it.
4. With the instance selected, click on the **Instance state** button at the top of the page.
5. From the dropdown menu, select **Terminate instance**. A confirmation dialog will appear asking if you are sure you want to terminate the instance.
6. Click **Terminate** to confirm.
   - The instance will begin shutting down and its state will change to **shutting-down** and then to **terminated**. Once terminated, the instance will no longer incur charges. # Download the VCF File

GenomeSuite Analyzer will generate a VCF file and store it in your S3 bucket. To download the VCF file from the S3 bucket, follow these steps:

1. Open your web browser and sign into the AWS Management Console with your AWS account credentials.
2. In the AWS Management Console, type **S3** into the search bar and select **S3** from the dropdown list to navigate to the S3 service.
3. In the S3 Dashboard, find and click on the bucket name where the VCF file is stored (e.g., `GenomeSuite-Analyzer-sample`).
4. **Locate the VCF File:**
   - Search for the VCF file using the naming convention `sample_name.vcf.gz`, where `sample_name` is the name you provided in the `-s` parameter when running GenomeSuite Analyzer. For example, if the sample name was `sample1`, look for the file named `sample1.vcf.gz`.
5. Once you find the `sample_name.vcf.gz` file, click on the checkbox next to the file name to select it.
6. With the file selected, the **Download** button. The file will begin downloading to your local machine. # Reference genome

GenomeSuite Analyzer includes the T2T human reference genome, the most complete human genome at this time: T2T-CHM13v2.0

T2T human genome.
Sergey Nurk *et al.* , The complete sequence of a human genome. Science 376, 44-53(2022).
DOI:10.1126/science.abj6987

T2T human Y chromosome.
Rhie A, Nurk S, Cechova M, Hoyt SJ, Taylor DJ, Altemose N, Hook PW, Koren S, Rautiainen M, Alexandrov IA, Allen J, Asri M, Bzikadze AV, Chen NC, Chin CS, Diekhans M, Flicek P, Formenti G, Fungtammasan A, Garcia Giron C, Garrison E, Gershman A, Gerton JL, Grady PGS, Guarracino A, Haggerty L, Halabian R, Hansen NF, Harris R, Hartley GA, Harvey WT, Haukness M, Heinz J, Hourlier T, Hubley RM, Hunt SE, Hwang S, Jain M, Kesharwani RK, Lewis AP, Li H, Logsdon GA, Lucas JK, Makalowski W, Markovic C, Martin FJ, Mc Cartney AM, McCoy RC, McDaniel J, McNulty BM, Medvedev P, Mikheenko A, Munson KM, Murphy TD, Olsen HE, Olson ND, Paulin LF, Porubsky D, Potapova T, Ryabov F, Salzberg SL, Sauria MEG, Sedlazeck FJ, Shafin K, Shepelev VA, Shumate A, Storer JM, Surapaneni L, Taravella Oill AM, Thibaud-Nissen F, Timp W, Tomaszkiewicz M, Vollger MR, Walenz BP, Watwood AC, Weissensteiner MH, Wenger AM, Wilson MA, Zarate S, Zhu Y, Zook JM, Eichler EE, O'Neill RJ, Schatz MC, Miga KH, Makova KD, Phillippy AM. The complete sequence of a human Y chromosome. Nature. 2023 Sep;621(7978):344-354. doi: 10.1038/s41586-023-06457-y. Epub 2023 Aug 23. PMID: 37612512; PMCID: PMC10752217. # Notice

THE SEQUENCING CENTER SUITE (INCLUDING, WITHOUT LIMITATION, THE GENOMESUITE ANALYZER SOFTWARE AND ANY RELATED DOCUMENTATION AND MATERIALS) ARE PROVIDED "AS IS" WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND; AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SEQUENCING CENTER HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS, IMPLIED, STATUTORY OR OTHER, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE IN TRADE, OR THAT THE SYSTEM (INCLUDING, WITHOUT LIMITATION, THE PRODUCTION CARD, THE SOFTWARE AND ANY RELATED DOCUMENTATION AND MATERIALS) WILL MEET USER'S REQUIREMENTS OR THAT ITS OPERATION WILL BE SECURE, UNINTERRUPTED OR ERROR- FREE, OR SUITABLE FOR THE PARTICULAR NEEDS OF USER OR ANY OTHER PERSON.

Information furnished is believed to be accurate and reliable. However, The Sequencing Center Inc. assumes no responsibility for the consequences of use of such information or for any infringement of patents or other rights of third parties that may result from its use. No license is granted by implication or otherwise under any patent or patent rights of The Sequencing Center Inc. Specifications mentioned in this publication are subject to change without notice. This publication supersedes and replaces all information previously supplied.

Document ID: TSC-001-08132024-v.1.3.0

Product ID: GenomeSuite-Analyzer-TSC-001-08092024-v-1-3-0

GenomeSuite Analyzer Version: v.1.3.0