Configuring Virus Scanner Software on Illumina Sequencers

Safeguard sequencing instrument control computers, while maintaining system performance.

Introduction

This is a general explanation of how to set up virus scanners on instrument control computers for HiSeq®, HiScanSQ®, and MiSeq® systems, and the Genome Analyzer™, such that they do not degrade or harm system performance. Illumina recognizes the importance of customer requirements to safeguard their networks with virus detection and removal software. Internally, Illumina enforces an IT policy that deploys such software on all computers, including instrument computers. However, instrument control computers are segregated into a group with special configuration settings.

There are many popular antivirus (AV) scanners that can be set up to operate under these guidelines, including:

- Symantec (Norton)
- McAfee
- Trend Micro
- Computer Associates
- Kaspersky
- Panda
- Bit Defender
- Shield Deluxe
- ESET / NOD32
- Avira
- Avast
- AVG
- GFI Languard
- Nero
- ClamWin
- Ad-Aware
- Dr. Web
- PCTools

However, the exact settings and configuration dialogs will vary between these different products. We can only provide general guidelines and leave it up to the IT group at the customer site to configure the sequencing instrument computer accordingly.

Automatic Scanning

Disable automatic full system scans based on fixed or periodic scheduling

Full system scans degrade the performance of the instrument in terms of time to completion and data quality because of slower imaging cycles. Only perform full system scans manually, when the instrument is idle or in a maintenance protocol, such as "washing".

The instrument must perform runs that last for several days and many customers attempt to maximize throughput by minimizing the time between runs. However, it is recommended that the time between runs be used for PC maintenance, such as updating the anti-virus (AV) software libraries and system scans.

Anti-Virus Software Updates

Most AV software will automatically update the virus definitions and software. To ensure these updates do not interfere with a sequencing run, configure the software so that the updates will download, but not install without user authorization. Do not automatically reboot the computer upon software update.

Enable automatic scanning of removable media

It is a good security practice to scan media such as CD's, DVD's, floppy disks, removable hard drives, and USB thumb drives, etc. when they are loaded or connected to the HiSeq, HiScanSQ, MiSeq or Genome Analyzer computers. However, if such media are loaded and scanned during an ongoing experiment on the instrument, the user is very likely to experience unwanted performance degradation.

We highly recommend that customers implement a policy that prohibits attaching or detaching removable hard drives or thumb drives during runs because of the impact on performance if the media is scanned. We do not recommend disabling scanning of removable media, since thumb drives are a very common vector for spreading virus contamination between computers.

Enable scanning email, attachments, and web downloads (but warn operators)

It is good security practice to scan all email, attachments, and Internet downloads. Of course, any sequencing instrument computer should not be used for general email, web browsing, and downloading. But it may be convenient and more productive for customers to send emails from the instrument, or may even be part of a site's SOP for setting up or monitoring runs on the instrument. Sometimes it may be necessary for them to work on the web for similar reasons of convenience or productivity. In these isolated instances, there should be no real performance degradation. The customer should avoid processing large downloads or large email attachments when the instrument is running a protocol.

Disable scanning TCP/IP packet traffic (but warn operators)

Because the sequencing instrument PC sends several megabytes of data to the network file server every second, this packet traffic should not be slowed down for virus scanning or the run could suffer significant performance degradation. It is therefore important to disable automatic scanning of packets sent and received over a TCP/IP link. For BaseSpace enabled sequencers, the data that is copied to the network servers will also get copied to the cloud, so the AV should be set up to disable scanning of packets sent to *.illumina.com domains.

The list of items that should be scanned to safeguard networks includes email attachments and web downloads because they generally come in over TCP/IP network connections, and packets that are part of an application protocol, such as SMTP, HTTP, Telnet, and FTP, etc.

Exclude Folders

The AV software will contain a mechanism to exclude certain folders from virus detection/removal scans. Configure the AV software to use this mechanism to make sure the following folders are never scanned.

Instrument Run Folders

The run data for each experiment are normally stored under the D:\Illumina and E:\Illumina folders for HiSeq, HiScanSQ, and MiSeq systems, and the D:\Runs base folder for Genome Analyzers. In most instances the D: or E: drive is only used for temporary run data storage. There is no other purpose for the D: or E: drive in any of the protocols or operating procedures from Illumina. Therefore, it is possible to exclude both the D: and E: drives in their entirety from any virus scans.

However, if the customer is using either the D: or E: drive for other file types, they may decide to include those other folders as targets for virus scanning. In this case, the D:\Illumina, the E:\Illumina or the D:\Runs folders can be disabled instead of the entire D: or E: drive.

In any case, make sure that D:, D:\Runs, D:\Illumina or the E:, E:\Illumina folder is on the list of excluded folders on the instrument control computer.

Illumina Instrument Control Software Folder

We recommend that the C:\illumina folder and all its subfolders be excluded from virus scanning. During runs, files may be created, updated and/or deleted there.

Illumina, Inc. • 1.800.809.4566 toll-free (U.S.) • +1.858.202.4566 tel • techsupport@illumina.com • www.illumina.com

FOR RESEARCH USE ONLY

Pub. No. 970-2010-006 Current as of 02 May 2012