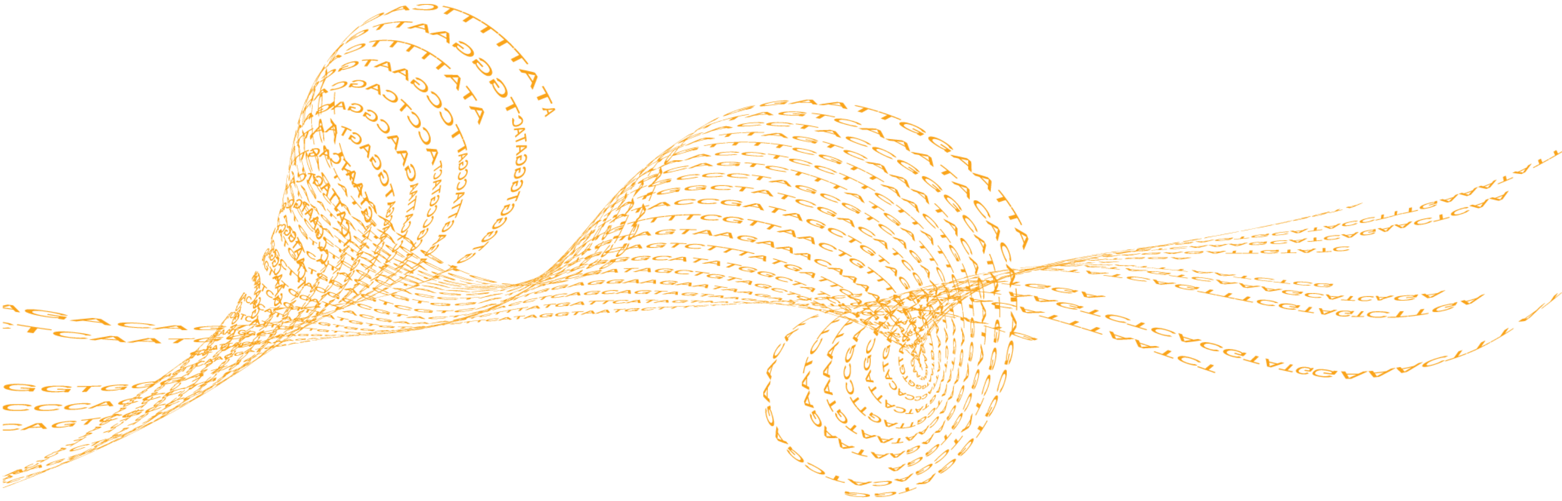
Illumina Security

Best Practices Guide

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



ILLUMINA PROPRIETARY
Pub. No. 970-2016-016
Current as of 18 April 2016

This document and its contents are proprietary to Illumina, Inc. and its affiliates ("Illumina"), and are intended solely for the contractual use of its customer in connection with the use of the product(s) described herein and for no other purpose. This document and its contents shall not be used or distributed for any other purpose and/or otherwise communicated, disclosed, or reproduced in any way whatsoever without the prior written consent of Illumina. Illumina does not convey any license under its patent, trademark, copyright, or common-law rights nor similar rights of any third parties by this document.

The instructions in this document must be strictly and explicitly followed by qualified and properly trained personnel in order to ensure the proper and safe use of the product(s) described herein. All of the contents of this document must be fully read and understood prior to using such product(s).

FAILURE TO COMPLETELY READ AND EXPLICITLY FOLLOW ALL OF THE INSTRUCTIONS CONTAINED HEREIN MAY RESULT IN DAMAGE TO THE PRODUCT(S), INJURY TO PERSONS, INCLUDING TO USERS OR OTHERS, AND DAMAGE TO OTHER PROPERTY.

ILLUMINA DOES NOT ASSUME ANY LIABILITY ARISING OUT OF THE IMPROPER USE OF THE PRODUCT(S) DESCRIBED HEREIN (INCLUDING PARTS THEREOF OR SOFTWARE).

Introduction

Illumina® sequencing systems are equipped with instrument control computers that are intended for use operating your system. As with any computer connected to a network or the Internet, following best practices limits the risk of malware (malicious software) damaging your control computer.

This guide recommends security configurations for instrument control computers on Illumina sequencing systems. Use these recommendations to manage security configurations for your system and ensure a more secure operating environment.

Intended Use

The instrument control computer is designed to operate Illumina sequencing systems. For quality and security reasons, using this computer for web browsing, checking email, reviewing documents, or other unnecessary Internet activity is discouraged.

Hardware Configuration

Use the following safeguards when configuring hardware.

- Enable a firewall.
- Disable Remote Desktop Protocol (RDP) capability.
- Change the password settings.
- Configure antivirus software.

NOTE
These recommendations do not apply to BaseSpace® Onsite or ForenSeq™ Universal Analysis Software.

Manage Firewalls

Depending on your needs and network environment, use at least 1 of the following types of firewall protection:

- **Windows firewalls**—By default, the Windows firewall is enabled in Illumina systems. This firewall blocks all inbound connections except RDP, which Illumina recommends disabling.
- **Network firewalls**—Your IT environment might provide firewall protection for Illumina systems. For system security, block all inbound connections and set up firewalls that align with the recommendations in this guide. For details on specific settings, contact your Illumina service representative.

Disable RDP

RDP is a Windows desktop sharing application that allows remote login. Although RDP is convenient for monitoring run performance, it is a common entry point for cyber attacks. For system security, disable RDP in network environments that do not compensate for this potential weakness.

NOTE
You can use BaseSpace Sequence Hub for remote monitoring.

1. Click the **Start** button, and then click **Control Panel**.
2. In Control Panel, click **System**, and then click **Remote Settings**.
3. In the System Properties dialog box, click **Don't allow connections to this computer**, and then click **OK**.
   RDP is disabled.

Change Password Settings

To prevent unintended access to the operating system, use the following instructions to change the default password and update settings to require that all users enter a user name and password to log on. After changing the default password, keep the new password secure.

After the default password is changed, Illumina service representatives need assistance accessing the system. Illumina does not maintain records of customer security parameters, so each visit from Illumina requires unlocking the system or sharing the login credentials. If these steps are not taken, the representative must reimage the system, which deletes data and customer information and requires reconfiguring the system to the laboratory domain. These processes can extend the time required for system service and repair.

1. Press Ctrl+Alt+Delete, and then click **Change a password**.
2. Type the default password, **sbs123**, in the Old password field.
3. Type a new password in the New password field.
   Consult your IT administrator for guidance on password complexity. Illumina recommends a password that is at least 10 characters and contains numbers, letters, and symbols.
4. Reenter the new password in the Confirm password field.
5. Press Enter to confirm the reset and return to the desktop.
6. Click the **Start** button, type **netplwiz** in the Search field, and then press Enter.
7. In the User Accounts dialog box, select the **Users must enter a user name and password to use this computer** checkbox.
8. Click **Apply**, and then click **OK**.

Configure Antivirus Software

Antivirus software protects the instrument control computer from viruses and other forms of malware. To avoid data loss or interruptions, use the following guidelines to configure an antivirus software of your choice:

- Set for manual scans.
  - Scan only when the instrument is not in use.
  - Do not allow automatic scans.
- Set updates to download without user authorization, but not install.
  - Install the antivirus software only when the instrument is not in use and the computer can be rebooted.
  - Do not allow the computer to reboot automatically after install.
- Exclude the application directory and data drives from any real-time file system protection.

For details on configuring antivirus software for your system, see the site prep guide for your instrument. Contact your antivirus software vendor for software-specific instructions.

Domain Configuration

Before adding an Illumina system to a domain, make sure that the domain settings do not override the recommendations for hardware configuration. Operating system changes can disrupt the proprietary software on Illumina systems, so evaluate any Group Policy Objects (GPOs) for interference with software processes.

Windows Updates

To install and configure Windows appropriately, follow the instructions in the site prep guide for your instrument. The following site prep guides are available for download from the Illumina website.

System	Resource
HiSeq®	*HiSeq 4000 and HiSeq 3000 Systems Site Prep Guide (document # 15066492)* *HiSeq 2500, 1500, and 2000 Systems Site Prep Guide (document # 15006407)*
HiSeq X®	*HiSeq X System Lab Setup and Site Prep Guide (document # 15050093)*
MiniSeq™	*MiniSeq System Site Prep Guide (document # 1000000002696)*
MiSeq®	*MiSeq System Site Prep Guide (document # 15027615)* *MiSeqDx® Site Prep Guide (document # 15038351)* *MiSeq FGx™ Instrument Site Prep Guide (document # 15050525)*
NextSeq®	*NextSeq System Site Prep Guide (document # 15045113)*

Notes

Technical Assistance

For technical assistance, contact Illumina Technical Support.

Table 1 Illumina General Contact Information

Website	www.illumina.com
Email	techsupport@illumina.com

Table 2 Illumina Customer Support Telephone Numbers

Region	Contact Number	Region	Contact Number
North America	1.800.809.4566	Japan	0800.111.5011
Australia	1.800.775.688	Netherlands	0800.0223859
Austria	0800.296575	New Zealand	0800.451.650
Belgium	0800.81102	Norway	800.16836
China	400.635.9898	Singapore	1.800.579.2745
Denmark	80882346	Spain	900.812168
Finland	0800.918363	Sweden	020790181
France	0800.911850	Switzerland	0800.563118
Germany	0800.180.8994	Taiwan	00806651752
Hong Kong	800960230	United Kingdom	0800.917.0041
Ireland	1.800.812949	Other countries	+44.1799.534000
Italy	800.874909		

Safety data sheets (SDSs)—Available on the Illumina website at support.illumina.com/sds.html.

Product documentation—Available for download in PDF from the Illumina website. Go to support.illumina.com, select a product, then select **Documentation & Literature**.

🏭

Illumina
5200 Illumina Way
San Diego, California 92122 U.S.A.
+1.800.809.ILMN (4566)
+1.858.202.4566 (outside North America)
techsupport@illumina.com
www.illumina.com