illumina®

Security and Networking

For Illumina Instrument Control Computers

ILLUMINA PROPRIETARY
Document # 1000000085920 v02
October 2021

Revision History

Document	Date	Description of Change
Document # 1000000085920 v02	Oct 2021	Removed erroneous characters from firewall allow list URLs and added URLs for NextSeq 2000. Consolidated regional platform and instrument specific endpoints (Control Computer Firewall section). Clarified Add and Remove SRP Rules section.
Document # 1000000085920 v01	July 2021	Added URL allow list to firewall section.
Document # 1000000085920 v00	April 2021	Initial release.

Table of Contents

Instrument Control Computer Security and Networking

Each Illumina sequencing system is equipped with a control computer that operates the system. As with any computer connected to a network or the internet, following best practices limits the risk of malware (malicious software) damaging the control computer.

This guide provides guidelines for managing the security of the control computer on your sequencing system. Use these guidelines to configure your system and ensure a more secure operating environment.

Control Computer Security

This section provides 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.

- **Software restriction policies**—Increase the reliability, integrity, and manageability of computers in a domain. By restricting configurations, only identified applications can run.
- **Antivirus software**—Protect the computer and the data streaming through it.
- **Operating system settings**—Adjust settings within operating system, such as Remote Desktop Protocol, Windows updates, and user settings.

Software Restriction Policies

Windows Software Restriction Policies (SRP) use rules to allow only specified software to run. For the Instrument, SRP rules are based on certificates, file names, file extensions, and directories.

By default, SRP is turned on to prevent unwanted software from running on the control computer. An IT representative or system administrator can add and remove rules to customize the security level. If the system is added to a domain, the local Group Policy Object (GPO) might automatically modify the rules and turn off SRP.

Turning off SRP prevents the protection it provides and overrides default protections. Changing the rules overrides the default protections.

SRP Rules

Windows Software Restriction Policies (SRP) use rules to allow only specified software to run. Information on SRP can be found in the system guide for your system.

Linux SRP are managed through the SEL configuration. For information on customization, contact your local administrator.

Add and Remove SRP Rules

Add and remove SRP rules to customize system security. Modifying the rules requires turning off SRP temporarily.

For some Illumina instrument systems, for example the iSeq Sequencing System, only the administrator (sbsadmin) user can turn off SRP. The administrator account has the privileges necessary to modify SRP rules.

1. Log in to the operating system.

2. Turn off SRP as follows.
   a. Navigate to the directory `C:\Illumina\Security`.
   b. Double-click `Disable.reg`.
   c. Select **Yes** to confirm the changes.

   When using a touch-screen interface, tapping and holding for about two seconds is equivalent to right-clicking.
3. Select **Start**, and then select **Run**.
4. In the Open field, enter **secpol.msc**.
5. In the Local Security Policy dialog box, expand **Software Restriction Policies**, and then select **Additional Rules**.
6. Add a rule as follows for files, file extensions, or directory paths.
   a. On the Action menu, select **New Path Rule**.
   b. In the Path field, enter the file name, file extension, or directory that you want to allow. You can also browse to the location.
   c. In the Security level list, select **Unrestricted**.
   d. **[Optional]** In the Description field, enter a reason for creating the rule.
   e. Select **OK** to add the rule.
7. Add a rule as follows for certificates that you have previously imported.
   a. On the Action menu, select **New Certificates Rule.**
   b. Browse to the certificate file you imported
   c. In the Security level list, select **Unrestricted**.
   d. **[Optional]** In the Description field, enter a reason for creating the rule.
   e. Select **OK** to add the rule.
8. Delete a rule as follows.
   a. Select the rule you want to delete, and then select **Delete**.
   b. Select **Yes** to confirm the deletion.
9. Close the Local Security Policy dialog box.
10. ***Immediately*** reinstate SRP as follows.
    a. Navigate to the directory `C:\Illumina\Security`.
    b. Double-click `Enable.reg`.
11. If SRP rules were modified for the first time, log off and then log on again for the rules to take effect.

Third-party Software

Illumina supports only software provided at installation.

Google Chrome, Java, Box, and other third-party software, including scripts, are untested and can interfere with performance and security. Use of third-party software and scripts cause corrupt and missing sequencing data.

Antivirus Software

An antivirus software of your choice is highly recommended to protect the instrument control computer against viruses.

To avoid data loss or interruptions, configure the antivirus software as follows.

- Set for manual scans. Do not enable automatic scans.
- Perform manual scans only when the instrument is not in use.
- Set updates to download without user authorization, but ***not to install***.
  - Install the antivirus software only when the instrument is not in use and you can reboot the computer.
  - Do not allow the computer to reboot automatically after install.
- Exclude the application directory and data drives from any real-time file system protection.
- Windows Defender is off by default. Keep it off. This Windows product can affect the computer resources used by Illumina software.

Control Computer Firewall

The Windows firewall protects the control computer by filtering incoming traffic to remove potential threats. The firewall is enabled by default to block all inbound connections. Keep the firewall enabled and allow outbound connections.

For the instrument to connect to BaseSpace and Proactive, you will need to add regional platform endpoints and instrument specific endpoints to the allow list on your firewall.

Regional Platform Endpoints

The following table lists the endpoints that provide access from Universal Copy Service to BaseSpace and Illumina Proactive. Some Enterprise addresses include a user-defined domain field. This custom field is reserved with {domain}.

If using Illumina Connected Analytics (ICA), connect to ICA using the following endpoint:

{region}.platform.illumina.com

See the *Illumina Connected Analytics Online Help* for supported regions.

Instance	Address
US Enterprise	{domain}.basespace.illumina.com
	{domain}.api.basespace.illumina.com
	basespace-data-east.s3-external-1.amazonaws.com
	basespace-data-east.s3.amazonaws.com
	instruments.sh.basespace.illumina.com
	login.illumina.com
	use1.platform.illumina.com
EU Enterprise	{domain}.euc1.sh.basespace.illumina.com
	{domain}.api.euc1.sh.basespace.illumina.com
	euc1-prd-seq-hub-data-bucket.s3.eu-central-1.amazonaws.com
	instruments.sh.basespace.illumina.com
AUS Enterprise	{domain}.aps2.sh.basespace.illumina.com
	{domain}.api.aps2.sh.basepace.illumina.com
	instruments.sh.basespace.illumina.com
	aps2-sh-prd-seq-hub-data-bucket.s3.ap-southeast-2.amazonaws.com
US Basic and Professional	basespace.illumina.com
	api.basespace.illumina.com
	basespace-data-east.s3-external-1.amazonaws.com
	basespace-data-east.s3.amazonaws.com
	instruments.sh.basespace.illumina.com
EU Basic and Professional	euc1.sh.basespace.illumina.com
	api.euc1.sh.basespace.illumina.com
	euc1-prd-seq-hub-data-bucket.s3.eu-central-1.amazonaws.com
	instruments.sh.basespace.illumina.com
AUS Basic and Professional	aps2.sh.basespace.illumina.com
	api.aps2.sh.basepace.illumina.com
	instruments.sh.basespace.illumina.com
	aps2-sh-prd-seq-hub-data-bucket.s3.ap-southeast-2.amazonaws.com

Instance	Address
GC Basic and Professional	cnn1.sh.basespace.illumina.com.cn
	api.cnn1.sh.basespace.illumina.com.cn
	instruments.sh.basespace.illumina.com.cn
	cn-sh-cnn1-prod-seq-hub-data-bucket.s3.cn-north-1.amazonaws.com.cn

MiniSeq, NextSeq 500, NovaSeq 6000

Allow List URLs
http://instruments.sh.basespace.illumina.com:443
http://o.ss2.us
http://ocsp.rootg2.amazontrust.com
http://ocsp.rootca1.amazontrust.com
http://ocsp.sca1b.amazontrust.com
http://login.illumina.com:443
http://dpm.demdex.net:443
http://ocsp.digicert.com
http://illuminainc.demdex.net:443
http://api.basespace.illumina.com:443
http://smetrics.illumina.com:443
http://basespace.illumina.com:443
http://da1s119xsxmu0.cloudfront.net:443
http://api.iron.illumina.com:443
http://api.dashboard.my.illumina.com:443
https://fonts.googleapis.com:443
http://www.illumina.com:443
http://ocsp.pki.goog/gsr2
http://cdn3.userzoom.com:443
http://www.googletagmanager.com:443
http://illuminainc.tt.omtrdc.net:443

Allow List URLs
http://cdn.walkme.com:443
http://www.google-analytics.com:443
http://stats.g.doubleclick.net:443
http://fonts.gstatic.com:443
http://cdn.walkme.com:443
http://www.google.com:443
http://www.google-analytics.com:443
http://stats.g.doubleclick.net:443
http://basespace-data-east.s3-external-1.amazonaws.com:443
http://basespace.illumina.com:443

NextSeq 2000

Allow List URLs
api.basespace.illumina.com
instruments.sh.basespace.illumina.com
basespace.illumina.com
platform.login.illumina.com
use1.platform.illumina.com
basespace-data-east.s3.amazonaws.com
basespace-data-east.s3.us-east-1.amazonaws.com
dpm.demdex.net
illuminainc.demdex.net
cm.everesttech.net
smetrics.illumina.com

Operating System Settings

Observe the following safeguards and recommendations when configuring the operating system on the instrument control computer for maximum security.

Operating System Updates

To appropriately install and configure your control computer operating system updates, follow the site prep guidelines for your system. You can access the latest version of site prep documentation from the Illumina Support Site.

If your instrument control computer uses Linux as the operating system, execute security updates using CLI (terminal) and user-interface (desktop) to make sure your data is secure.

If your instrument control computer uses Windows as the operating system, make sure your data are secure by manually installing Windows critical security updates when available. By default, Windows security updates are not enabled. For information on enabling Windows security updates, see the Security Update Guide available on the Microsoft website. When installing updates, your system must be idle. Some updates require a full system reboot.

If you are unable to install security updates, the following are recommended alternatives,

- Increase firewalling and network isolation (virtual LAN).
- Network isolation of network attached storage (NAS) that still allows data to sync to the network.
- Apply the appropriate permission-based controls to users.
- Make sure that instrument control computer is only used as intended. For more information, see User Behavior.

Turn Off Remote Desktop Protocol

Remote Desktop Protocol (RDP) is a Windows desktop sharing application that allows remote login. RDP may or may not be disabled on your system. If necessary, use the following instructions to disable it.

1. In Control Panel, select **System**.
2. Select **Remote settings**.
3. In the System Properties dialog box, select **Don't allow connections to this computer**, and then select **OK**.

Enabling Remote Desktop Protocol is highly discouraged. RDP is a common entry point for cyber attacks.

User Accounts

Illumina instrument control computers running Windows 10 or later support two types of accounts: administrator and user. Permissions for each type are shown in the following table.

Permissions	Administrator	User
Set up, start, and monitor sequencing runs.	X	X

Permissions	Administrator	User
Download and update software.	X	
See status for active run started by other user.	X	
Terminate unresponsive UCS process.	X	

Instrument control computers running Windows 7 support only administrator accounts.

Update User Passwords Using Windows

1. Press Ctrl+Alt+Delete, and then select **Change a password**.
2. In the Old password field, type the default password.
3. In the New password field, type the new password.
   For security, the password must be at least 10 characters long, comply with local policies, and contain numbers, letters, and symbols.
4. In the Confirm password field, reenter the new password.
5. Press Enter to confirm the reset and return to the desktop.
6. In the search box, type **netplwiz**, 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. Select **Apply**, and then select **OK**.

Reset User Passwords Using Linux

This section details how to reset the ilmnuser, ilmnadmin, or root password using Linux. Password recovery is not available. Resetting your password does not bypass account lockout after too many incorrect password attempts. You must wait 10 minutes before you can reset your password or try to log in.

Reset ilmnuser Password

You can reset the ilmnuser password if you know the ilmnadmin or root password.

1. Log in to ilmnadmin.
2. Open terminal.
3. Enter `sudo passwd ilmnuser`.
4. Enter the ilmnadmin password at the prompt.
5. Enter a new ilmnuser password at the prompt.
6. Retype the new ilmnuser password at the prompt to confirm the new password.

Reset ilmnadmin Password

You can reset the ilmnadmin password if you know the root password.

1. Log in to root.
2. Open terminal.
3. Enter `passwd ilmnadmin` to change the ilmadmin password, or enter `passwd ilmnuser` to change the ilmnuser password.
4. Enter the new password at the prompt.
5. Retype the new password at the prompt to confirm the new password.

Reset Root Password

To reset the root password, use one of the following options:

- If you know the password from the time the last OS image was captured, restore to that saved image.
- If you do not remember the password, contact Illumina Tech Support.

Password Requirements

You are required to set a password upon initial setup of your system. The following table identifies the required password policies for the control computer.

Policy	Security Setting
Enforce password history	5 passwords remembered
Maximum password age	180 days
Minimum password age	0 days
Minimum password length	10 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Illumina does not store or maintain customer login credentials, and unknown passwords cannot be reset. An unknown password requires that an Illumina representative restore the factory default, which removes all data from the system and extends the necessary support time.

User Behavior

The instrument control computer is designed to operate Illumina sequencing systems. Do not consider it a general-purpose computer. For quality and security reasons, do not use the control computer for web browsing, checking email, reviewing documents, or other unnecessary activity. These activities

can result in degraded performance or loss of data.

Network Connections

Illumina systems are designed to stream data at a regular cadence during the sequencing activity. Depending on the off-load rate, this data transmission may persist for some time after the completion of sequencing. Illumina instruments assume a mostly-up network. Network outages may impact data transmission. In the event of a network outage, the instruments are designed to cache all data locally, however such caching may delay the start of the next sequencing run, depending on storage space on instrument. The instruments are designed to reinitiate data transfer upon restoration of the network. Refer to the site prep guide for your instrument for specific bandwidth requirements.

Review network maintenance activities for potential compatibility risks with the Instrument System.

Use the following guidelines to install and configure a network connection:

- Use a dedicated connection between the instrument and data management system. Make this connection directly or through a network switch.
- Managed switches are recommended.
- Calculate the total capacity of the workload on each network switch. The number of connected instruments and ancillary equipment, such as a printer, can impact capacity.
- If possible, isolate sequencing traffic from other network traffic.
- Illumina recommends the use of CAT-6 cables (minimum requirement is CAT-5e). A shielded network cable that is 3 meters (9.8 feet) long is provided with the instrument for network connections.

Internal Connections

For more information about ports and other connections, consult the system guide for your Illumina sequencing system.

Outbound Connections

All Illumina instruments use ports 80, 8080, and 443 for communicating with Illumina Proactive Services. These ports are designed for outbound communication only. Always keep the Windows firewall enabled.

Refer to Control Computer Firewall for information on configuring access to BaseSpace domains, Illumina Proactive, and Illumina Connected Analytics.

Consult the system guide for your Illumina sequencing system for detailed information on IP addresses and ports for your specific system.

Data Output and Storage

Illumina sequencing systems are designed for use with a network. The system is not intended to store run data. Therefore, performing a run in standalone mode requires a network connection to transfer run data to a network location. Do not save run data to a local hard drive. The system hard drive is intended for temporary storage before data are transferred automatically. Data saved on the hard drive that are not used by the current run can compromise performance. Refer to Network Connections for information on the transferring run data to network locations.

When data transfer to external storage is complete, the following files appear in the output folder:

- `RTAComplete.txt`
- `CopyComplete.txt`
- `SequenceComplete.txt`

To confirm successful data transfer, make sure that `CopyComplete.txt` is present and the Process Management screen displays green checkmarks for all processes.

Example Data Usage

The following tables provide example storage data representing a variety of Illumina sequencing systems. Because actual data retention is subject to local policies, confirm conditions before calculating storage needs.

Run sizes and other details vary depending on multiple factors. The numbers provided are intended to be a guide to the relative range of the data footprint.

NextSeq 1000 and 2000 Systems

Read Length (bp)	BCL Files Output (GB)	BAM Files Output (GB)	CRAM Files Output (GB)	FASTQ Files Output (GB)
2x50	20	50	15	75
2x100	40	75	30	150
2x150	55	150	60	300

NovaSeq 6000 System

File Type	S1 * (GB)	S2 (GB)	S4 (GB)
CBCL	470	930	2800
Interop folder	1.2	2.3	7.0
FASTQ	570	1125	3387
BAM	530	1050	3160
gVCF/VCF	14	28	84

NextSeq 500 and 550 Systems

Flow Cell Configuration*	Read Length (bp)	Output (GB)	Required Input
High-output flow cell[1]	2x150	100-120	100 ng – 1 µg (with TruSeq Library Prep Kits)
	2x75	50-60	
	1x 5	25-30	
Mid-output flow cell[2]	2x150	32-39	
	2 x 75	16-19	

[1]Maximum 400 million single reads and 800 million paired-end reads.
[2]Maximum 130 million single reads and 260 million paired-end reads.

HiSeq: 3000 and HiSeq 4000 Systems: Single Flow Cell

Read Length	Reads PF (M)	Output (GB)	Q30	Run Time
1x50	2.1-2.5 billion	105-125	≥85%	<1-3.5 days
2x75		325-375	≥80%	
2x150		650-750	≥75%	

HiSeq: 3000 and HiSeq 4000 Systems: Dual Flow Cell

Read Length	Reads PF (M)	Output (GB)	Q30	Run Time
1x50	4.3-5 billion	210-250	≥85%	<1-3.5 days
2x75		650-750	≥80%	
2x150		1300-1500	≥75%	

HiSeq X System: Single Flow Cell

Read Length	Reads PF (M)	Output (GB)	Q30	Run Time
2x150	2.6-3 billion	800-900	≥75%	<3.0 days

HiSeq X System: Dual Flow Cell

Read Length	Reads PF (M)	Output (TB)	Q30	Run Time
2x150	5.3-6 billion	1.6-1.8	≥75%	<3.0 days

MiniSeq System: System Sequencing Performance[1]

Flow Cell Configuration	Read Length (cycles)	Output (GB)	Run Times[4] (hours)	Data Quality[5] (% bases higher than Q30)	Required Input
High-output kit[2]	300	~7.5	~24	>80	1 ng-1 ug with Illumina Library Prep Kits
	150	~4	~13	>85	
	75	~2	~7	>85	
Mid-output kit[3]	300	~2.5	~17	>80	

[1]Actual performance parameters may vary based on sample type, sample quality, and clusters passing filter.
[2]Maximum 25 million single reads and 50 million paired-end reads.
[3]Maximum 8 million single reads and 16 million paired-end reads.
[4]Run times for the MiniSeq System include cluster generation, sequencing, and base calling with quality scores.
[5]The percentage of bases > Q30 is averaged over the entire run.

MiSeq System: Reagent Kit v2

Read Length (bp)	Total Time (hours)	Output	Quality Scores (% bases higher than Q30)	Single Reads (M)	Paired-End Reads (M)
2x25	5.5	750-850 MB	>90	12-15 M	24-30
2x150	24	4.5-5.1 GB	>80		
2x250	39	7.5-8.5 GB	>75		

MiSeq System: Reagent Kit v2 Micro

Read Length (bp)	Total Time (hours)	Output (GB)	Quality Scores (% bases higher than Q30)	Single Reads (M)	Paired-End Reads (M)
2x150	19	1.2	>80	4	8

MiSeq System: Reagent Kit v2 Nano

Read Length (bp)	Total Time (hours)	Output (MB)	Quality Scores (% bases higher than Q30)	Single Reads (M)	Paired-End Reads (M)
2x150	17	300	>80	1	2
2x250	28	500	>75	2x250	28

MiSeq System: Reagent Kit v3

Read Length (bp)	Total Time (hours)	Output (GB)	Quality Scores (% bases higher than Q30)	Single Reads (M)	Paired-End Reads (M)
2x75	21	3.3-3.8	>85	22-25	44-50
2x300	56	13.2-15	>70	2x300	56

iSeq 100 System

Output File Type	Approximate Size (MB)
BAM	600
BCL	850
FASTQ	850
gVCF/VCF	<10
InterOp	2.5

Troubleshooting

Use the following troubleshooting procedures for common instrument control computer issues. For additional support, contact Illumina Technical Support.

Mapped Drive and Network Storage Location Troubleshooting

Issue	Solution
User cannot see mapped drive or network storage location in control software (but can see them in Windows/File Explorer)	The control software on Illumina sequencing systems requires Universal Naming Convention (UNC) file paths, as demonstrated by the example below. `\\Server\Shared_Folder\`
Cannot see mapped drive or network storage location in Windows/File Explorer	Illumina sequencing systems can connect to network drive locations via several different protocols. If SMB protocol is being used, SMB2 or higher must be used, due to known vulnerabilities in SMB1. It is strongly recommended that you upgrade your network connection to SMB2 or higher, if that is not an option, contact Illumina Technical Support. Control computers using Windows 10 use the user name and password that were used for logging into the instrument as the default credentials for the network storage location as well. So, confirming with your network storage administrator that this user name and password combination is expected by the network drive may also resolve this situation.

BaseSpace Sequence Hub Troubleshooting

Issue	Solution
Cannot connect to BaseSpace Sequence Hub from instrument control software	If the desired BaseSpace option (either instance or workgroup) is not available in the control software, this may be due to the instrument lacking the network access it requires to connect. It is recommended to first check if you can access BaseSpace Sequence Hub from a browser on the instrument and log in there. Check that the correct domains and ports are open on the instrument. Reference the site prep guide for your Illumina sequencing system.
Cannot see BaseSpace Sequence Hub instances	Check that the correct domains and ports are open on the instrument. Check that the firewall allow list includes the required endpoints. For details, see Control Computer Firewall.
Cannot locate BaseSpace Sequence Hub login screen	

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

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

illumina®