TECHNICAL NOTE

Setting up remote system diagnostics with Illumina Proactive

illumina®

Table of Contents

Maximizing operational efficiency through Illumina Proactive

Illumina provides a wide range of next-generation sequencing (NGS) instruments that have become the core sequencing systems for many laboratories. Whether operating a large sequencing center or a small research lab with a single instrument, reliable instrument operation and management are critical for optimal usage and maximum throughput.

To help laboratories achieve this goal, Illumina provides Illumina Proactive, a remote system diagnostics service in which instrument performance data from each run are sent to Illumina to enable proactive maintenance. All Illumina sequencing instruments are designed to capture performance data, while the type of metrics used to monitor performance depends on the software version. By enabling Illumina Proactive, users facilitate troubleshooting with more accurate diagnosis of failures and detection of failure risks. Furthermore, Illumina Proactive can increase instrument uptime, improve operational efficiency, and reduce the risk of lost resources (Figure 1). This technical note explains the benefits of instrument performance monitoring, instructs on how to enable Illumina Proactive, and answers frequently asked questions about data security.

Benefits of Illumina Proactive

Maximize instrument uptime

Detecting instrument components at elevated risk of failure can reduce unplanned downtime and allow users to schedule required component replacements at their convenience. This capability has been enabled for several Illumina instrument components and will continue to be expanded to others.

Troubleshoot runs more efficiently

Locating, downloading, and sending required information to troubleshoot a problem can cause unnecessary delays. On the other hand, direct access to instrument performance parameters through Illumina Proactive allows the Illumina Service & Support team to diagnose and troubleshoot instrument issues quickly. In addition, historical performance monitoring supports efficient troubleshooting, and sometimes, preemptive instrument repair.

What is instrument performance data and why is it important?

Instrument performance data refers to any metric that can characterize the operational performance of the sequencing instrument, including software logs, instrument configurations, and other file types. Sequencing data are not included in this category, and are not accessible or reported through the same data stream. Instrument performance data can support failure risk prediction, failure detection, and performance issue troubleshooting in various ways (Table 1).

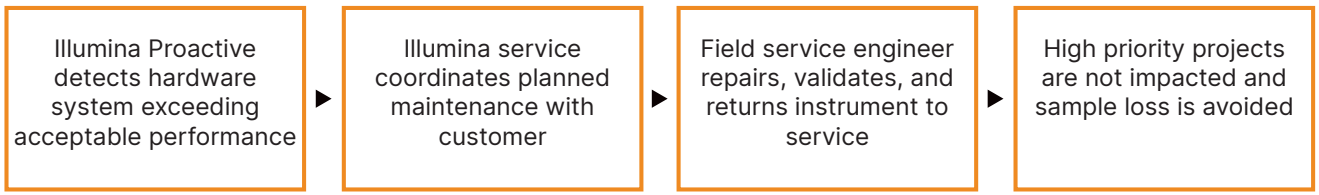

Figure 1: Example of Illumina Proactive in action—In this example, routine monitoring of system performance data results in detection of failure risk for optical hardware, resulting in planned maintenance around a high-priority project. A potentially expensive loss of time, effort, and sample is avoided.

Table 1: Different types of run performance data

Instrument performance data	Run performance data	Instrument configuration data	Run configuration data
Data collected	Q-scores, instrument operational logs	Instrument serial number, software version	Run parameters, reagent, and flow cell lot numbers
Value to Illumina service team	Failure prediction, failure detection	Run troubleshooting	Run troubleshooting
Value to user	Enables analysis of error and warning notifications regarding optical, mechanical, thermal, and fluidic system performance	Enables assessment of whether software version, instrument type, or other hardware variables may be contributing to performance issues	Informs on roles of lot numbers, experiment type, and other experimental variables that contribute to performance issues

Enabling Illumina Proactive

For each system, instrument performance monitoring is configured in the control software by the user. User guides provide details on how to enable or disable the delivery of instrument performance data. For greater detail on universal and instrument-specific network configurations, refer to the Universal Settings and Instrument-Specific Settings sections in this document.

Requirements for enabling Illumina Proactive:

- No inbound ports are required
- Outbound Port 443
- BaseSpace™ Domains for each region
- Network connection with bandwith as specified in the site prep guides for specific instruments
- Software must be configured to enable performance monitoring

For details on endpoint requirements and networking recommendations, see support-docs.illumina.com/SHARE/NetworkSecurity/Content/SHARE/NetworkSecurity/SecurityIntro

Instructions for enabling Illumina Proactive:

1. Make sure that any concerns regarding information security are addressed by appropriate IT representatives, and that all institutional requirements are met.

2. Confirm current system instrument performance monitoring settings. Some instruments may already be enabled by default. See instrument performance monitoring settings.

3. Select “Send Instrument Performance Data to Illumina” checkbox before starting a run. All Illumina instruments should provide this option in the user interface, although the exact wording may vary.

Data security considerations

Data security is a top priority for Illumina customers. Illumina recognizes the increased focus in our community on the privacy of genomic and other health data and we design our products to meet these evolving standards. As a result of consistent effort, security profiles for Illumina operating systems improve over time as new systems are designed and new threats to information are identified. Illumina continually assesses and enhances our system security profiles as new threats are identified to maintain a strong cybersecurity posture and support continuous innovation in health care. Protecting the privacy of customer personal information, including genomic data, is fundamental to Illumina practices.

No inbound ports

Illumina sequencing systems do not require inbound ports from the internet. Illumina recommends blocking these ports, reducing the possibility of reaching the login screen via the internet. This security measure reduces access to the operating system from remote locations.

Software restriction policy

Many Illumina systems have a feature called software restriction policy (SRP) that limits the applications run on Illumina computers to those that Illumina has approved (allow-listed). This restriction reduces the likelihood of any malware from being executed, even if it infiltrates the system, because SRP protection will not allow execution, regardless of how files appear to the user (ie, malware may appear as an image file, or excel spreadsheet).

Security in transit

Instruments communicate with BaseSpace Sequence Hub through a web-based application program interface (API). All traffic between the sequencing instrument and BaseSpace Sequence Hub uses Transport Layer Security (TLS 1.2), an internet standard that encrypts sensitive communications as they pass over the internet. All service methods require API key signatures, and service is refused to all others.

Encryption at rest

Data stored in persistent storage systems are referred to as being “at rest.” BaseSpace Sequence Hub uses Advanced Encryption System (AES)-256 to protect data at rest. AES-256 is a specification for the encryption of electronic data established by the US National Institutes of Standards and Technology (NIST).[2]

Data center security

Illumina Proactive integrates with the existing Illumina cloud infrastructure provided by Amazon Web Services (AWS). Secure access to data is managed using Illumina BaseSpace Sequence Hub, whose suite of cloud applications have achieved annual ISO 27001:2013 audit certification[3] and Health Insurance Portability and Accountability Act (HIPAA) attestation (AT101). [4,5] Illumina Proactive does not require a BaseSpace Sequence Hub account.

Illumina software as a service (SaaS) products are designed and operated in keeping with best practices and laws around data protection and data handling, including General Data Protection Regulation (GDPR). Customers should determine GDPR responsibilities for use of their own personal data. More details on Illumina's cloud data security and privacy practices can be found on the Illumina cloud data security page. For cloud service provider data security practices, see the AWS Data Protection Page.

Frequently asked questions about data security

Q: Will my sequence data be sent to Illumina if I enable Illumina Proactive?

A: No. Only instrument performance data, which includes software logs and instrument configurations as previously described, are sent by the instrument to Illumina. Sequencing run data are not sent and are not accessible through this service. Various features distinguish the connectivity between instrument performance monitoring and sequence data analysis (Table 2).

Table 2: BaseSpace Sequence Hub connectivity options

Attribute	Illumina Proactive mode	Run monitoring mode	BaseSpace Sequence Hub Analysis mode
Connection type	One-time instrument configuration	Pre-run user connection	Per-run user connection
Requires internet connection	✓	✓	✓
Includes instrument configuration and operational logs[a]	✓	✓	✓
Requires BaseSpace Sequence Hub login		✓	✓
Includes sequence data (BCL) files			✓

a. For details around specific instrument configuration and operational logs, refer to the instrument-specific settings section in the Appendix.

Q: Will sending my instrument performance data to Illumina enable all types of failure risk to be detected proactively?

A: No. Instrument performance monitoring has successfully enabled proactive maintenance in multiple cases to date. As more data become available, the capabilities of this service will continue to expand and improve across the Illumina portfolio of sequencing products.

Q: Will I need to log in to my BaseSpace Sequence Hub to enable this service?

A: No. For instrument performance data mode, only a network connection to Illumina is needed. Because instrument performance data and sequencing data are sent independently of each other, a BaseSpace Sequence Hub login is not required.

Q: My Information Security team requires additional technical information before enabling this service. Are there additional resources available?

A: Yes. Additional resources are available that address data security considerations for Illumina's instruments and Proactive software and provide general data security best practices. Illumina Technical Support can be reached at techsupport@illumina.com.

For more information on Illumina data security practices, visit the Illumina Security web page or review our Corporate Privacy Policy. See the Appendix for data security documentation specific to our NGS systems and cloud-based SaaS products.

Q: Is Illumina Proactive compliant with GDPR laws?

A: Yes. Illumina SaaS products are designed and operated to comply with global laws, including GDPR.

Q: Are there other best practices that Illumina recommends concerning data security?

A: Secure deployment of research use only instruments and diagnostic medical devices depends on layers of security. Illumina strongly recommends that instruments and devices are deployed in the smallest network subnet or security context, with trusted devices. Firewalls and other network policies should be used to restrict inbound and outbound access. Sample-specific information should be also be omitted from the names of experiments or sample IDs to keep sensitive data protected.

Appendix

The remaining sections contain information on requirements that your IT department needs to know to implement Illumina Proactive.

Network configuration

Several integration settings are common to all Illumina systems for implementing Illumina Proactive or integrating with BaseSpace Sequence Hub, but each platform may also have requirements specific to that platform, depending on intended use case. Illumina provides an updated location for both universal connection requirements (connections that are common to all ILMN platforms) and settings specific for each platform.

For more information, including other recommendations for networking, visit support-docs.illumina.com/SHARE/NetworkSecurity/Content/SHARE/NetworkSecurity/SecurityIntro

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 more information on the needed endpoints, visit support-docs.illumina.com/SHARE/NetworkSecurity/Content/SHARE/NetworkSecurity/WindowsFirewall

Inbound ports are not required, or recommended, except for Local Run Manager. Remote Desktop Protocol (RDP) may be enabled on some systems, by default, and the recommendation is to close all inbound ports, including RDP, unless Local Run Manager is noted as a requirement for local allow-listing. Local Run Manager does not require internet access, only access to local storage and management resources. The Illumina Security Best Practices Guide provides more information on firewalls and RDP.

Antivirus configuration

User-selected antivirus software 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 allow automatic scans
- Perform manual scans only when the instrument is not in use
- Set updates to download without user authorization, but not install
- Do not update during instrument operation; update only when the instrument is not running and when it is safe to reboot the instrument control computer
- Do not reboot the computer automatically upon update
- Exclude the application directory and data drives from any real-time file system protection; apply this setting to the C:\Illumina and Z:\ilmn directories
- Disable Windows Defender; this Windows product can affect the operating system resources used by Illumina software

Operating system configurations

Illumina instruments are tested and verified to operate within specifications before shipping. After installation, changes to settings can create performance or security risks. The following configuration recommendations mitigate performance and security risks for the operating system:

- Configure a password that is at least 10 characters, and use local ID policies for additional guidance; keep a record of the password
- Illumina does not keep 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
- Configure Automatic Updates in Windows to prevent updates
- When connecting to a domain with Group Policy Objects (GPOs), some settings might affect the operating system or instrument software; if the instrument software operates incorrectly, consult your facility IT administrator about possible GPO interference.
- Use the Windows firewall or a network firewall (hardware or software) and disable the Remote Desktop Protocol (RDP); for more information on firewalls and RDP, refer to the Illumina Security Best Practices Guide[5]
- Maintain administrative privileges for users; Illumina instrument software is configured to allow user permissions when the instrument is shipped
- The system has fixed internal IP addresses, which can cause system failure when conflicts occur
- The control computer is designed to operate Illumina sequencing systems; web browsing, checking email, reviewing documents, and other nonsequencing activity creates quality and security problems

Windows updates

Illumina recommends the application of critical security updates only. To control configuration and operation of the instrument control computer and deliver a more robust operating environment, the default Windows OS has Windows Update turned off. Feature or general updates on the system can put the system operating environment at risk and is not supported. The Illumina Security Best Practices Guide provides more information on Windows update alternatives.

Third-party software

Illumina does not support software beyond what is provided at installation. Do not install Chrome, Java, Box, or any other third-party software that was not provided with the system. Third-party software is untested and can interfere with performance and security. For example, RoboCopy or other synchronization and streaming programs can cause corrupt or missing sequencing data because it interferes with streaming performed by the control software suite.

User behavior

The instrument control computer is designed to operate Illumina sequencing systems. It should not be used as a general-purpose computer. For quality and security reasons, using the control computer for web browsing, checking email, reviewing documents, or other unnecessary activity is discouraged, as it can result in degraded performance or loss of data.

Group policy application

When connecting to a domain with Group Policy Objects (GPOs), some settings might affect the operating system or instrument software (Table 3). If the instrument software operates incorrectly, consult your facility IT administrator about possible GPO interference.

Password management

Configure a password that is at least 12 characters and use local ID policies for additional guidance. Keep a record of the password. For customer security, Illumina does not keep 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.

Administrative rights and privileges

Maintain administrative privileges for users. Illumina instrument software is configured to allow user permissions when the instrument is shipped.

Table 3: Universal approval requirements for internal system operation

Connection	Value	Purpose
Domain	localhost:*	All ports for localhost-to-localhost communication, which are needed for interprocess communication
Port	8081	Real-time analysis
Port	8080	Control software
Port	8090	Remote copy service

Instrument-specific settings

In addition to settings previously mentioned, there are the settings that need to be considered for each platform, representing internal settings that need to be allow-listed (Table 4, Table 5).

Table 4: Information security specifications for Illumina sequencing systems

System	SRP	EMET	Default IPD setting	Opt-in or Opt-out	IPD setting at software upgrade
NovaSeq 6000	Yes	Yes	On	Opt-out	Retain previous setting
HiSeq series	No	No	On	Opt-out	Reset to On
NextSeq 550	No	No	On	Opt-out	Retain previous setting
NextSeq 550Dx - Research Mode	Yes	Yes	Off	Opt-in	Retain previous setting
NextSeq 1000 and NextSeq 2000	No	No	On	Opt-out	Retain previous setting
MiSeq	No	No	On	Opt-out	Retain previous setting (per user basis)
MiSeqDx	No	No	Off	Opt-in	Retain previous setting
MiSeqDx - Research Mode	No	No	On	Opt-out	Retain previous setting
MiniSeq	No	No	On	Opt-out	Retain previous setting
iSeq 100	Yes	No	On	Opt-out	Retain previous setting
iScan	No	No	On	Opt-out	Retain previous setting (per user basis)

Systems with the Local Run Manager module require Port 80 or 443 to be inbound for the local network only.

Table 5: Internal communication requirements by system

System	Ports and IP addresses	Purpose	Bandwidth requirement
NovaSeq 6000	5555	Hardware controller interface	200 Mb/system
	22, 80, 111, 443, 623, 2049, 5900, 8889, 9980, 169.254.x.x, fddc:65e5:66fa::1/48, fddc:65e5:66fa::2/48	Internal data transfer	200 Mb/system
HiSeq series	The HiSeq System has no internal IP communication processes		100 Mb/system
NextSeq 550	192.168.113.*:*	Allow All Ports; this is the communication link with firmware on the internal network card	50 Mb/system
NextSeq 550Dx	192.168.113.*:*	Allow All Ports; this is the communication link with firmware on the internal network card	50 Mb/system
	Port 80 or 443	Local Run Manager; required local inbound (no internet access)	50 Mb/system
NextSeq 1000 and NextSeq 2000	21, 22, 4647, 5458, 5555, 5647, 7359, 7360, 169.254.*.*.*	Allow All Ports; this is the communication link with firmware on the internal network card	200 Mb/system
MiSeq	Port 80 or 443	Local Run Manager; required local inbound (no internet access)	10 Mb/system
MiSeqDx	Port 80 or 443	Local Run Manager; required local inbound (no internet access)	10 Mb/system
MiniSeq	192.168.113.*:*	Allow All Ports; this is the communication link with firmware on the internal network card	10 Mb/system
	Port 80 or 443	Local Run Manager; required local inbound (no internet access)	10 Mb/system
iSeq 100	Port 80 or 443	Local Run Manager; required local inbound (no internet access)	10 Mb/system
iScan	6030, 888	AutoLoader	10 Mb/system

The IP listed is critical; it is the interface for the hardware controller.

For more information and details on communication requirements, refer the Site Prep Guide for the specific system (Table 6). User guides for each specific system contain information on steps to enable IPD through instrument software (Table 6).

Table 6: User guides and site prep guides for Illumina systems

System	System/reference guide	Site prep guide
NovaSeq 6000	1000000019358	1000000019360
HiSeq 1000	15023355	15006407
HiSeq 1500	15035788	15006407
HiSeq 2000	15011190	15006407
HiSeq 2500	15035786	15006407
HiSeq 3000	15066493	15066492
HiSeq 4000	15066496	15066492
HiSeq X	15050091	15050093
NextSeq 500	15046563	15045113
NextSeq 550	15069765	15045113
NextSeq 550Dx	1000000009513	1000000009869
NextSeq 1000 and NextSeq 2000	1000000109376	1000000109378
MiSeq	15027617	15027615
MiSeqDx	15070067	15038351
MiniSeq	1000000002695	1000000002696
iSeq 100	1000000036024	1000000035337
iScan	11313539	1000000000661

If a hyperlink becomes inactive due to updates, the provided document number can be used to search the Illumina website for a newer version of the guide.

Instrument performance data types

Table 7: Instrument performance data types (instrument configuration files)

File name	File description	iScan	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
Effective.cfg	Software system configuration total parameters	X	X	X	X		X	X	X	X	X	X	X
FirmwareVersions.txt	Firmware version on instrument hardware						X			X	X		X
*Calibration.cfg	Software system calibration parameters	X					X	X		X	X	X	X
*Override.cfg	Software system configuration override parameters	X	X	X	X		X			X	X	X	X
RTAStart.bat	Primary analysis start file					X	X			X	X		
Options.cfg	Software system configuration override parameters												X
*HardwareHistory.csv	Instrument hardware configuration history						X			X	X		
*CurrentHardware.csv	Instrument hardware current configuration						X			X	X		
Sequencing Configuration.xml	Instrument system configuration parameters					X							
Channel*cc.txt	Camera calibration file	X											

a. HiSeq 1000, 1500, 2000, and 2500 Systems.

Table 8: Instrument performance data types (instrument operational logs)

File name	File type	File description	iScan	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
*.jpg	Run specific operational images	Thumbnail image for each tile and color channel if option has been turned on in software (off by default), usually turned on by FAS/FSE						X	X	X	X	X		
Samplesheet.csv	Run specific sample configuration file	Sequencing sample sheet												X[b]
Recipe file (XML)	Run specific configuration file	Sequencing recipe used in run					X					X	X	X
Logs.zip		Zipped folder of human readable files; all file readily accessible by customer on instrument					X	X	X	X	X	X	X	X
CompressedLogs .zip		Zipped collection of log files; all files readily accessible by customer on instrument	X											

a. HiSeq 1000, 1500, 2000, and 2500 Systems.
b. Sample sheet is no longer uploaded in NovaSeq 6000 v1.6 software..

Table 9: Instrument performance data types (instrument analytics configuration files)

File name	File description	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
RTAConfiguration.xml	RTA configuration	X	X	X	X	X	X	X		X		
RTA3.cfg	RTA configuration										X	X
RTAerror.txt	Primary analysis error log file					X	X					

a. HiSeq 1000, 1500, 2000, and 2500 Systems.

Table 10: Instrument performance data types (miscellaneous file types)

File name	File description	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
*.IMF logs	Software operational log files		X	X		X				X	X	X
*Results.zip	Service software test results; this is sent only if triggered by a Service & Support personnel in service software					X			X	X	X	

a. HiSeq 1000, 1500, 2000, and 2500 Systems.

Table 11: Instrument performance data types (run-specific operational logs)

File name	File description	iScan	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
*Firmware_Logs	Firmware operation log files (.csv)						X			X	X		
PreRunDiagnostic Files	Pre-sequencing run check results and log files (.csv and .xml)					X	X			X	X	X	X
Cycle Logs	Troubleshooting logs for operational data generated per cycle (.txt and .xml form)						X	X	X	X	X	X	X
Error.log	Troubleshooting logs for operational data		X	X	X							X	X
CycleTimes.txt	Cycle duration time during a sequencing run		X	X	X								
UCS Logs	Copy service log file (.json and .csv)												X
CycleTime.tsv	Cycle and scan duration log file	X											
*.scrst	BeadChip scan setting configuration file	X											

a. HiSeq 1000, 1500, 2000, and 2500 Systems.

Table 12: Instrument performance data types (run-specific analytics files)

File name	File description	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
RTAComplete.txt	Indicator file that all primary processing has completed	X	X	X	X	X	X	X	X	X	X	X
RTARead*Complete.txt	Indicator file that primary processing has completed key step				X							
RunParameters.xml	Run set up configuration parameters output in XML form at the beginning of the run	X	X	X	X	X	X	X	X	X	X	X
RunInfo.xml	Run set up configuration parameters output in XML form at the beginning of the run used for the Sequencing Analysis Viewer	X	X	X	X	X	X	X	X	X	X	X
RunCompletionStatus.xml	Indicator file that all sequencing is complete	X	X	X		X	X	X	X	X	X	X
SequenceComplete.txt	Indicator file that all sequencing is complete											X
*MetricsOut.bin	Binary reporting files for Sequencing Analysis Viewer; not readable by customer without additional software	X	X	X	X	X	X	X	X	X	X	X
AlignmentMetricsOut.bin					X						X	X
BasecallingMetricsOut.bin					X						X	X
CorrectedIntMetricsOut.bin	Average intensity, corrected channel intensity, corrected called intensity, called counts	X	X	X	X	X	X	X	X	X	X	X
EmpiricalPhasingMetrics Out.bin	Phasing, prephasing per cycle	X	X	X	X	X	X	X	X	X	X	X
ErrorMetricsOut.bin	Error rate, read errors	X	X	X	X	X	X	X	X		X	X
EventMetricsOut.bin	Timing data for RTA started, cycle started, template generation started/completed, posttemplate max clusters init, system memory available gigabyte, registration and extraction, neighbor correction, color matrix correction, template generation, base calling and quality scoring, sequence alignment, bclwriting, read started/completed, filter align started/completed, cycle completed, RTA completed	X	X	X	X	X	X	X	X	X	X	X
ExtendedTileMetricsOut.bin					X						X	X
ExtrationMetricsOut.bin	Focus scores, intensities, time	X	X	X	X		X	X	X	X	X	X
FWHMGridMetricsOut.bin					X						X	X
ImageMetricsOut.bin					X						X	X
IndexMetricsOut.bin	Name, sample name, project name				X		X				X	X
OpticalModeMetricsOut.bin											X	X
PFGrtidMetricsOut.bin	Cluster count, PF cluster count, Locs area in mm^2	X	X	X	X		X	X	X	X	X	X
QMetrics2030Out.bin					X		X					X
QMetricsByLaneOut.bin					X		X					X
QMetricsOut.bin	Q-score histogram	X	X	X	X		X	X	X		X	X
RegistrationMetricsOut.bin	Subtile offsets, affine transform	X	X	X			X	X	X		X	X
TileMetricsOut.bin	Cluster density, cluster density PF, cluster count, cluster count PF, percent aligned, percent phasing, percent prephasing, latest extracted cycle, latest called cycle, latest Q-scored cycle, latest error cycle	X	X	X	X		X	X	X	X	X	X
*.tsv or *.txt	TSV or TXT log files generated for RTA file copy logs, global logs, and warning logs; accessible by the customer in human readable form				X		X	X	X	X		
QGridMetricsOut.bin					X							
ReconstructionMetricsOut. bin											X	

References

1. Microsoft Security Response Center. msrc.microsoft.com. Accessed July 12, 2022.
2. National Institute of Standards and Technology. Advanced Encryption Standard (AES). csrc.nist.gov/publications/detail/fips/197/final. Published November 1, 2001. Accessed July 12, 2022.
3. Amazon. AWS: ISO/IEC 27001:2013. aws.amazon.com/compliance/iso-27001-faqs/. Accessed July 12, 2022.
4. Illumina. (2018) BaseSpace Sequence Hub Security and Privacy. illumina.com/content/dam/illumina-marketing/documents/products/whitepapers/basespace-sequence-hub-security-and-privacy-white-paper-970-2016-020.pdf. Accessed July 12, 2022.

illumina®

1.800.809.4566 toll-free (US) | +1.858.202.4566 tel
techsupport@illumina.com | www.illumina.com

M-GL-01092 v1.0