TECHNISCHER HINWEIS

Einrichten der Systemdiagnose per Fernzugriff mit Illumina Proactive

illumina®

Inhaltsverzeichnis

Maximieren der Betriebseffizienz mit Illumina Proactive

Illumina bietet eine breite Palette an NGS-Geräten (Next-Generation Sequencing, Sequenzierung der nächsten Generation), die in vielen Laboren zu den wichtigsten Sequenziersystemen gehören. Ob großes Sequenzierungszentrum oder kleines Forschungslabor mit einem einzelnen Gerät – der zuverlässige Betrieb und das zuverlässige Management von Geräten sind entscheidend für die optimale Nutzung mit maximalem Durchsatz.

Damit Labore dieses Ziel erreichen können, bietet Illumina mit Illumina Proactive einen Dienst zur Systemdiagnose per Fernzugriff, bei dem Geräte-Performancedaten bei jedem Lauf an Illumina gesendet werden, um eine proaktive Wartung zu ermöglichen. Alle Illumina-Sequenzierungsgeräte erfassen Performancedaten. Welche Metriken hierbei erfasst werden, ist jedoch von der jeweiligen Softwareversion abhängig. Durch die Aktivierung von Illumina Proactive vereinfachen Anwender die Fehlerbehebung, da genauere Ausfalldiagnosen zur Verfügung stehen und Ausfallrisiken genauer ermittelt werden können. Des Weiteren kann Illumina Proactive die Betriebsdauer von Geräten verlängern, die Betriebseffizienz erhöhen und das Risiko von Ressourcenverlusten verringern (Abbildung 1). Dieser technische Hinweis erläutert die Vorteile der Überwachung der Geräte-Performance und enthält Anweisungen zur Aktivierung von Illumina Proactive sowie Antworten auf häufig gestellte Fragen zum Thema Datensicherheit.

Vorteile von Illumina Proactive

Maximieren der Betriebsdauer von Geräten

Die Erkennung von Gerätekomponenten mit erhöhtem Ausfallrisiko kann dazu beitragen, ungeplante Ausfallzeiten zu minimieren, und ermöglicht Anwendern die Abstimmung erforderlicher Komponentenwechsel auf betriebliche Anforderungen. Diese Funktion findet bei einigen Komponenten von Illumina-Geräten bereits Anwendung und wird kontinuierlich auf weitere Komponenten ausgedehnt.

Effizientere Fehlerbehebung

Müssen zur Fehlerbehebung Informationen erst zusammengestellt, heruntergeladen und versendet werden, kann es zu Verzögerungen kommen. Im Gegensatz dazu ermöglicht der direkte Zugriff auf Geräte-Performancedaten durch Illumina Proactive dem Service- und Supportteam von Illumina die schnelle Diagnose und Behebung von Geräteproblemen. Zusätzlich erhöht die Verfolgung des Performanceverlaufs die Effizienz der Fehlerbehebung und kann in einigen Fällen sogar eine präventive Reparatur ermöglichen.

Was sind Geräte-Performancedaten und wieso sind diese wichtig?

Als Geräte-Performancedaten werden alle Metriken bezeichnet, die Daten zur Betriebsperformance des Sequenzierungsgeräts enthalten, darunter Softwareprotokolle, Gerätekonfigurationen und weitere Dateitypen. Diese Kategorie umfasst keinerlei Sequenzierungsdaten. Diese sind im Rahmen des Datenverkehrs weder zugänglich, noch werden sie übermittelt. Geräte-Performancedaten tragen in mehrfacher Hinsicht zur Prognose von Fehlerrisiken, zur Fehlererkennung und zur Behebung von Performanceproblemen bei (Tabelle 1).

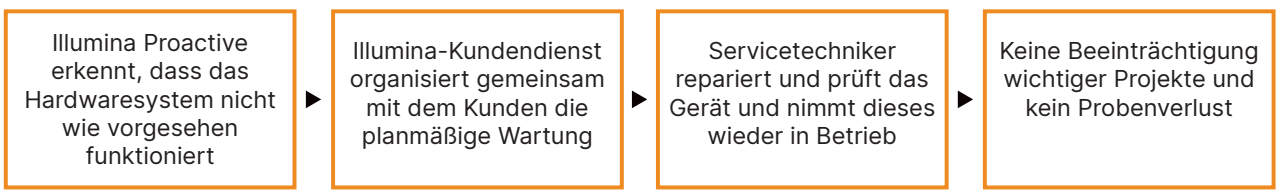

Abbildung 1: Beispiel für Illumina Proactive in der Praxis: In diesem Beispiel wird durch die Routineüberwachung von Geräte-Performancedaten ein Risiko für den Ausfall optischer Hardware ermittelt, was eine geplante Wartung im Kontext eines wichtigen Projekts ermöglicht. Diese verhindert den mit hohen Kosten verbundenen Verlust von Zeit, Aufwand und Proben.

Tabelle 1: Unterschiedliche Arten von Lauf-Performancedaten

Daten zur Geräte-Performance	Daten zur Lauf-Performance	Daten zur Gerätekonfiguration	Daten zur Laufkonfiguration
Erfasste Daten	Q-Scores, Gerätebetriebsprotokolle	Geräteseriennummer, -softwareversion	Laufparameter, Reagenzien- und Fließzellenchargennummern
Vorteile für das Serviceteam von Illumina	Ausfallvorhersage, Fehlererkennung	Fehlerbehebung	Fehlerbehebung
Vorteile für den Benutzer	Ermöglicht Fehleranalyse und Warnungen hinsichtlich der Performance des optischen, des mechanischen, des thermischen sowie des Fluidiksystems	Ermöglicht die Beurteilung, ob die Softwareversion, der Gerätetyp oder andere Hardwarevariablen zu Performanceproblemen beitragen können	Informiert darüber, inwiefern Chargennummern, Versuchstyp sowie andere Versuchsvariablen zu Performanceproblemen beitragen

Aktivierung von Illumina Proactive

Die Überwachung der Geräte-Performance wird vom Anwender in der Steuerungssoftware des jeweiligen Geräts aktiviert. Das jeweilige Benutzerhandbuch enthält ausführliche Informationen zur Aktivierung bzw. Deaktivierung der Bereitstellung von Geräte-Performancedaten. Ausführliche Informationen zu universellen und gerätespezifischen Netzwerkkonfigurationen finden Sie im vorliegenden Dokument in den Abschnitten „Universelle Einstellungen“ und „Gerätespezifische Einstellungen“.

Anforderungen für die Aktivierung von Illumina Proactive:

- Keine Ports für eingehende Verbindungen erforderlich
- Port 443 für ausgehende Verbindungen
- BaseSpace™-Domänen für die einzelnen Regionen
- Netzwerkverbindung mit der im Handbuch zur Standortvorbereitung zum jeweiligen Gerät angegebenen Bandbreite
- Software muss zur Überwachung der Performance konfiguriert sein

Einzelheiten zu Anforderungen an Endpunkte und Empfehlungen bezüglich Netzwerken finden Sie unter support-docs.illumina.com/SHARE/NetworkSecurity/Content/SHARE/NetworkSecurity/SecurityIntro.

Anweisungen zur Aktivierung von Illumina Proactive:

1. Stellen Sie sicher, dass die IT-Abteilung alle Maßnahmen zur Gewährleistung der Informationssicherheit trifft und dass alle Anforderungen der jeweiligen Einrichtung erfüllt sind.

2. Überprüfen Sie die derzeitigen Einstellungen zur Überwachung der Geräte-Performance. Bei einigen Geräten ist diese standardmäßig aktiviert. Siehe „Einstellungen zur Überwachung der Geräte-Performance“.

3. Wählen Sie das Kontrollkästchen „Send Instrument Performance Data to Illumina“ (Geräte-Performancedaten an Illumina senden), bevor Sie einen Lauf starten. Diese Option ist in der Benutzeroberfläche aller Illumina-Geräte vorhanden, die genaue Bezeichnung kann jedoch abweichen.

Gewährleistung der Datensicherheit

Datensicherheit hat für Illumina-Kunden oberste Priorität. Illumina ist sich bewusst, dass dem Schutz genomischer und weiterer Gesundheitsdaten in unserem Tätigkeitsfeld immer größere Bedeutung zukommt. Wir entwickeln unsere Produkte im Hinblick auf Konformität mit den entsprechenden, veränderlichen Standards. Mit der Entwicklung neuer Systeme und der Ermittlung neuer Bedrohungen in Bezug auf Daten verbessern wir fortlaufend die Sicherheit von Illumina-Betriebssystemen. Illumina wertet kontinuierlich die Sicherheitsprofile seiner Systeme aus und verbessert diese, wenn neue Bedrohungen erkannt werden. Damit gewährleisten wir hohe Cybersicherheit und unterstützen die fortlaufende Weiterentwicklung im Gesundheitswesen. Der Schutz personenbezogener Daten von Kunden, einschließlich genomischer Daten, steht für Illumina an erster Stelle.

Keine Ports für eingehende Verbindungen

Illumina-Sequenziersysteme erfordern keine Ports für eingehende Verbindungen aus dem Internet. Illumina empfiehlt die Sperrung all dieser Ports, was die Wahrscheinlichkeit verringert, dass der Anmeldebildschirm über das Internet aufgerufen werden kann. Diese Sicherheitsmaßnahme schränkt den Fernzugriff auf das Betriebssystem ein.

Richtlinien für Softwareeinschränkung

Zahlreiche Illumina-Systeme sind mit einer als Richtlinie für Softwareeinschränkung (SRP, Software Restriction Policy) bezeichneten Funktion ausgestattet, dank der nur von Illumina genehmigte (auf die Zulassungsliste gesetzte) Anwendungen auf Illumina-Computern ausgeführt werden können. Diese Einschränkung verringert die Wahrscheinlichkeit der Ausführung von Schadsoftware, selbst bei Infiltration des Systems, da SRP die Ausführung immer verhindert, unabhängig von der Form, die die Schadsoftware gegenüber dem Anwender vortäuscht. (Schadsoftware kann sich beispielsweise als Bilddatei oder Excel-Tabelle tarnen.)

Sicherheit während der Übertragung

Geräte kommunizieren über eine webbasierte API (Application Program Interface) mit BaseSpace Sequence Hub. Der gesamte Datenverkehr zwischen dem Sequenzierungsgerät und BaseSpace Sequence Hub wird mit TLS 1.2 (Transport Layer Security) verschlüsselt, einem Standardprotokoll für die Übertragung sensibler Daten im Internet. Alle Servicemethoden erfordern API-Schlüsselsignaturen. Sind diese nicht vorhanden, wird der Servicezugriff verweigert.

Verschlüsselung bei Speicherung

Als gespeichert werden Daten bezeichnet, die sich in Dauerspeichersystemen befinden. BaseSpace Sequence Hub schützt gespeicherte Daten mit AES-256-Verschlüsselung (Advanced Encryption System). Bei AES-256 handelt es sich um eine Spezifikation des US National Institute of Standards and Technology (NIST) für die Verschlüsselung elektronischer Daten.[2]

Rechenzentrumssicherheit

Illumina Proactive ist in die vorhandene Illumina-Cloudinfrastruktur integriert, die von Amazon Web Services (AWS) bereitgestellt wird. Der sichere Datenzugriff erfolgt über Illumina BaseSpace Sequence Hub, dessen Cloudanwendungssuite in einem jährlichen Audit auf die Einhaltung von ISO 27001:2013[3] geprüft wird und einen Nachweis der HIPAA-Konformität (AT101) erhalten hat.[4, 5] Für Illumina Proactive ist kein BaseSpace Sequence Hub-Konto erforderlich.

Bei der Entwicklung und Nutzung der Software-as-a-Service(SaaS)-Produkte von Illumina werden Best Practices und Gesetze hinsichtlich Datenschutz und Datenbearbeitung berücksichtigt, einschließlich der Datenschutz-Grundverordnung (DSGVO). Kunden sollten eigene Maßnahmen hinsichtlich der Einhaltung der DSGVO in Bezug auf von ihnen verarbeitete personenbezogene Daten treffen. Weitere Informationen zur Sicherheit von Clouddaten sowie den Datenschutzmaßnahmen bei Illumina finden Sie auf der Illumina-Seite zur Datensicherheit in der Cloud. Informationen zu den Datenschutzmaßnahmen des Cloudanbieters finden Sie auf der Seite zum Datenschutz bei AWS.

Häufig gestellte Fragen zum Thema Datensicherheit

F: Werden Sequenzdaten an Illumina gesendet, wenn ich Illumina Proactive aktiviere?

A: Nein. Wie oben bereits erläutert, werden nur Geräte-Performancedaten wie Softwareprotokolle und Gerätekonfigurationen vom Gerät an Illumina gesendet. Es werden keine Daten zu Sequenzierungsläufen gesendet und auf diese besteht im Rahmen des Service auch kein Zugriff. Die Verbindung für die Überwachung der Geräte-Performance und der Sequenzdatenanalyse unterscheiden sich in mehrfacher Hinsicht (Tabelle 2).

Tabelle 2: Optionen für die BaseSpace Sequence Hub-Verbindung

Attribut	Illumina Proactive-Modus	Laufüberwachungsmodus	BaseSpace Sequence Hub-Analysemodus
Verbindungstyp	Einmalige Gerätekonfiguration	Laufspezifische Benutzerverbindung	Laufspezifische Benutzerverbindung
Erfordert eine Internetverbindung	✓	✓	✓
Umfasst Gerätekonfigurations- und Betriebsprotokolle[a]	✓	✓	✓
Erfordert BaseSpace Sequence Hub-Anmeldung		✓	✓
Enthält Dateien mit Sequenzdaten (BCL)			✓

a. Informationen zu spezifischen Gerätekonfigurations- und Betriebsprotokollen finden Sie im Abschnitt zu den gerätespezifischen Einstellungen im Anhang.

F: Werden alle Arten von Ausfallrisiken proaktiv erkannt, wenn ich Geräte-Performancedaten an Illumina sende?

A: Nein. Die Überwachung der Geräte-Performance ermöglicht bislang nicht in allen Fällen die Veranlassung einer proaktiven Wartung. Mit der Verfügbarkeit weiterer Daten wird dieser Service jedoch für alle Sequenzierungsprodukte von Illumina kontinuierlich ausgebaut und verbessert.

F: Muss ich mich bei BaseSpace Sequence Hub anmelden, um diesen Service zu aktivieren?

A: Nein. Für den Geräte-Performancedaten-Modus ist nur eine Netzwerkverbindung mit Illumina erforderlich. Da Geräte-Performancedaten und Sequenzierungsdaten unabhängig voneinander gesendet werden, ist keine Anmeldung bei BaseSpace Sequence Hub erforderlich.

F: Mein Informationssicherheitsteam benötigt zusätzliche Informationen, bevor der Service aktiviert werden kann. Sind weitere Ressourcen verfügbar?

A: Ja. Es stehen zusätzliche Ressourcen zu den Themen Datensicherheit in Zusammenhang mit Illumina-Geräten und der Proactive-Software sowie allgemeine Best Practices zur Datensicherheit zur Verfügung. Den technischen Support von Illumina erreichen Sie unter techsupport@illumina.com.

Weitere Informationen zu Datenschutzpraktiken bei Illumina finden Sie auf der Illumina-Webseite zum Thema Sicherheit und in der Datenschutzrichtlinie des Unternehmens. Angaben zur Datensicherheitsdokumentation für spezifische NGS-Systeme und cloudbasierte SaaS-Produkte finden Sie im Anhang.

F: Ist Illumina Proactive DSGVO-konform?

A: Ja. SaaS-Produkte von Illumina werden unter Berücksichtigung weltweiter gesetzlicher Regelungen entwickelt, einschließlich der DSGVO.

F: Empfiehlt Illumina weitere Best Practices zur Datensicherheit?

A: Die Sicherheit des Einsatzes von nur für Forschungszwecke bestimmten Geräten und Medizinprodukten für die Diagnostik beruht auf unterschiedlichen Sicherheitsebenen. Illumina empfiehlt dringend, Geräte und Produkte im kleinstmöglichen Netzwerksubnetz bzw. Sicherheitskontext mit vertrauenswürdigen Geräten einzusetzen. Firewalls und andere Netzwerkrichtlinien sollten zur Beschränkung des internen und externen Zugriffs verwendet werden. Zum Schutz vertraulicher Daten sollten Namen von Versuchen und Proben-IDs zudem keine probenspezifischen Informationen enthalten.

Anhang

Die verbleibenden Abschnitte enthalten Informationen zu Anforderungen, die Ihre IT-Abteilung bei der Implementierung von Illumina Proactive benötigt.

Netzwerkkonfiguration

Einige Integrationseinstellungen für die Implementierung von Illumina Proactive oder die Integration in BaseSpace Sequence Hub sind bei allen Illumina-Systemen gleich. Abhängig von der vorgesehenen Anwendung gelten u. U. jedoch auch plattformspezifische Anforderungen. Illumina stellt aktuelle Informationen sowohl zu allgemeingültigen Verbindungsanforderungen (Verbindungen, die für alle ILMN-Plattformen gelten) als auch zu plattformspezifischen Einstellungen bereit.

Weiterführende Informationen, einschließlich weiterer Empfehlungen zu Netzwerken, finden Sie unter support-docs.illumina.com/SHARE/NetworkSecurity/Content/SHARE/NetworkSecurity/SecurityIntro.

Firewall des Steuerungscomputers

Die Windows-Firewall schützt den Steuerungscomputer durch das Filtern von eingehendem Datenverkehr, um potenzielle Bedrohungen auszuschließen. Die Firewall ist standardmäßig aktiviert, um alle eingehenden Verbindungen zu blockieren. Lassen Sie die Firewall aktiviert und lassen Sie ausgehende Verbindungen zu.

Weitere Informationen zu den erforderlichen Endpunkten finden Sie unter support-docs.illumina.com/SHARE/NetworkSecurity/Content/SHARE/NetworkSecurity/SecurityIntro.

Ports für eingehende Verbindungen sind nicht erforderlich und werden nicht empfohlen, ausgenommen für Local Run Manager. Remote Desktop Protocol (RDP) ist auf bestimmten Systemen womöglich standardmäßig aktiviert. Die Empfehlung lautet, alle Ports für eingehende Verbindungen (auch für RDP) zu schließen, falls Local Run Manager nicht für die lokale Zulassungsliste als erforderlich gilt. Local Run Manager benötigt keinen Internetzugriff, sondern lediglich Zugriff auf lokale Speicher- und Managementressourcen. Weitere Informationen zu Firewalls und RDP finden Sie im Sicherheitshandbuch mit den Best Practices von Illumina.

Virenschutzkonfiguration

Eine vom Benutzer ausgewählte Virenschutzsoftware wird dringend empfohlen, um den Gerätesteuerungscomputer vor Viren zu schützen. Um Datenverluste und Unterbrechungen zu vermeiden, konfigurieren Sie die Virenschutzsoftware wie folgt:

- Legen Sie fest, dass Virenprüfungen manuell und nicht automatisch ausgeführt werden sollen.
- Führen Sie manuelle Virenprüfungen nur aus, wenn sich das Gerät nicht in Verwendung befindet.
- Legen Sie fest, dass Updates zwar ohne Autorisierung durch den Benutzer heruntergeladen, jedoch nicht installiert werden sollen.
- Aktualisieren Sie die Software nur, wenn das Gerät nicht in Betrieb ist und wenn der Gerätesteuerungscomputer sicher neu gestartet werden kann.
- Lassen Sie den Computer nach einer Aktualisierung nicht automatisch neu starten.
- Schließen Sie das Anwendungsverzeichnis und die Datenlaufwerke ggf. von einem Echtzeit-Dateisystemschutz aus. Wenden Sie diese Einstellung auf die Verzeichnisse C:\Illumina und Z:\ilmn an.
- Deaktivieren Sie Windows Defender. Dieses Windows-Produkt kann negative Auswirkungen auf die Ressourcen des Betriebssystems haben, die von der Illumina-Software verwendet werden.

Betriebssystemkonfigurationen

Illumina-Geräte wurden auf den korrekten Betrieb innerhalb der Spezifikationen vor der Lieferung getestet und verifiziert. Nach der Installation können Änderungen an den Einstellungen ein Risiko der Performanceminderung oder Sicherheitsrisiken verursachen. Die folgenden Konfigurationsempfehlungen verringern das Risiko einer Performanceminderung sowie Sicherheitsrisiken:

- Konfigurieren Sie ein Kennwort, das aus mindestens 10 Zeichen besteht, und wenden Sie die lokalen ID-Richtlinien als zusätzliche Sicherheit an. Notieren Sie sich das Kennwort.
- Illumina bewahrt keine Kundenanmeldedaten auf und unbekannte Kennwörter können nicht zurückgesetzt werden.
- Ist das Kennwort unbekannt, muss ein Illumina-Mitarbeiter die werksseitigen Einstellungen wiederherstellen, wodurch alle Daten aus dem System gelöscht werden und sich die Wartung verlängert.
- Deaktivieren Sie automatische Windows-Updates.
- Beim Verbinden mit einer Domäne über Gruppenrichtlinienobjekte (GPO, Group Policy Objects) können manche Einstellungen Auswirkungen auf das Betriebssystem oder die Gerätesoftware haben. Wenn die Gerätesoftware nicht ordnungsgemäß funktioniert, fragen Sie den IT-Administrator Ihrer Einrichtung nach einer möglichen GPO-Störung.
- Verwenden Sie die Windows-Firewall oder eine Netzwerkfirewall (Hardware oder Software) und deaktivieren Sie das Remotedesktopprotokoll (RDP, Remote Desktop Protocol). Weitere Informationen finden Sie im Sicherheitshandbuch mit den Best Practices von Illumina.[5]
- Behalten Sie die Administratorberechtigungen für die Benutzer bei. Die Illumina-Gerätesoftware ist bei Lieferung so konfiguriert, dass das Zuweisen von Benutzerberechtigungen möglich ist.
- Das System weist feste interne IP-Adressen auf, die zu Systemfehlern führen können, wenn Konflikte auftreten.
- Der Steuerungscomputer ist für den Betrieb von Illumina-Sequenziersystemen bestimmt. Das Surfen im Internet, das Abrufen von E-Mails, das Anzeigen von Dokumenten und andere nicht zur Sequenzierung gehörige Aktivitäten stellen Qualitäts- und Sicherheitsrisiken dar.

Windows-Updates

Illumina empfiehlt ausschließlich die Anwendung wichtiger Sicherheitsupdates. Um die Konfiguration und den Betrieb des Gerätesteuerungscomputers steuern zu können und eine zuverlässigere Betriebsumgebung zu erreichen, ist im Windows-Standardbetriebssystem Windows Update deaktiviert. Funktionsupdates oder allgemeine Updates auf dem System können ein Risiko für die Systembetriebsumgebung darstellen und werden nicht unterstützt. Im Sicherheitshandbuch mit den Best Practices von Illumina finden Sie weitere Informationen über Alternativen zu Windows Update.

Software von Drittanbietern

Illumina unterstützt keine andere Software als die, die bei der Installation bereitgestellt wird. Installieren Sie nicht Chrome, Java, Box oder eine andere Drittanbietersoftware, die nicht mit dem System ausgeliefert wurde. Drittanbietersoftware wurde nicht getestet und kann die Leistung und die Sicherheit beeinträchtigen. So können beispielsweise RoboCopy oder andere Synchronisierungs- und Streamingprogramme dazu führen, dass Sequenzierungsdaten beschädigt werden oder verloren gehen, da sie die Streamingfunktion der Steuerungssoftwaresuite stören.

Benutzerverhalten

Der Gerätesteuerungscomputer ist für den Betrieb von Illumina-Sequenziersystemen bestimmt. Der Computer darf nicht als Computer für allgemeine Anwendungen verwendet werden. Aus Qualitäts- und Sicherheitsgründen wird dringend davon abgeraten, auf dem Steuerungscomputer im Internet zu surfen, E-Mails abzurufen, Dokumente anzuzeigen oder andere nicht erforderliche Arbeiten zu erledigen, da dadurch die Performance beeinträchtigt werden kann und möglicherweise Daten verloren gehen.

Anwenden von Gruppenrichtlinien

Beim Verbinden mit einer Domäne über Gruppenrichtlinienobjekte (GPO, Group Policy Objects) können manche Einstellungen Auswirkungen auf das Betriebssystem oder die Gerätesoftware haben (Tabelle 3). Wenn die Gerätesoftware nicht ordnungsgemäß funktioniert, fragen Sie den IT-Administrator Ihrer Einrichtung nach einer möglichen GPO-Störung.

Kennwortmanagement

Konfigurieren Sie ein Kennwort, das aus mindestens 12 Zeichen besteht, und wenden Sie die lokalen ID-Richtlinien als zusätzliche Sicherheit an. Notieren Sie sich das Kennwort. Illumina bewahrt zur Gewährleistung der Kundensicherheit keine Kundenanmeldedaten auf und unbekannte Kennwörter können nicht zurückgesetzt werden. Ist das Kennwort unbekannt, muss ein Illumina-Mitarbeiter die werksseitigen Einstellungen wiederherstellen, wodurch alle Daten aus dem System gelöscht werden und sich die Wartung verlängert.

Administratorberechtigungen und -privilegien

Behalten Sie die Administratorberechtigungen für die Benutzer bei. Die Illumina-Gerätesoftware ist bei Lieferung so konfiguriert, dass das Zuweisen von Benutzerberechtigungen möglich ist.

Tabelle 3: Universelle für den internen Systembetrieb erforderliche Genehmigungen

Verbindung	Wert	Zweck
Domäne	localhost:*	Alle Ports für die Localhost-zu-Localhost-Kommunikation, die für die Kommunikation zwischen den Prozessen benötigt werden
Port	8081	Real-Time Analysis
Port	8080	Steuerungssoftware
Port	8090	Remote Copy Service

Gerätespezifische Einstellungen

Zusätzlich zu den bereits erwähnten Einstellungen gibt es Einstellungen, die bei den einzelnen Plattformen unterschiedlich sind. Hierbei handelt es sich um interne Einstellungen, die auf die Zulassungsliste gesetzt werden müssen (Tabelle 4, Tabelle 5).

Tabelle 4: Informationssicherheitsspezifikationen für Illumina-Sequenziersysteme

System	SRP	EMET	Standardmäßige IPD-Einstellung	Opt-in oder Opt-out	IPD-Einstellungen für Software-Upgrade
NovaSeq 6000	Ja	Ja	Ein	Opt-out	Vorherige Einstellung beibehalten
HiSeq-Serie	Nein	Nein	Ein	Opt-out	Zurückgesetzt auf „Ein“
NextSeq 550	Nein	Nein	Ein	Opt-out	Vorherige Einstellung beibehalten
NextSeq 550Dx – Forschungsmodus	Ja	Ja	Aus	Opt-in	Vorherige Einstellung beibehalten
NextSeq 1000 und NextSeq 2000	Nein	Nein	Ein	Opt-out	Vorherige Einstellung beibehalten
MiSeq	Nein	Nein	Ein	Opt-out	Vorherige Einstellung beibehalten (benutzerspezifisch)
MiSeqDx	Nein	Nein	Aus	Opt-in	Vorherige Einstellung beibehalten
MiSeqDx – Forschungsmodus	Nein	Nein	Ein	Opt-out	Vorherige Einstellung beibehalten
MiniSeq	Nein	Nein	Ein	Opt-out	Vorherige Einstellung beibehalten
iSeq 100	Ja	Nein	Ein	Opt-out	Vorherige Einstellung beibehalten
iScan	Nein	Nein	Ein	Opt-out	Vorherige Einstellung beibehalten (benutzerspezifisch)

Systeme mit Local Run Manager-Modul erfordern Port 80 oder 443 ausschließlich für eingehenden Datenverkehr über das lokale Netzwerk.

Tabelle 5: Anforderungen bezüglich der internen Kommunikation nach System

System	Ports und IP-Adressen	Zweck	Anforderungen an die Bandbreite
NovaSeq 6000	5555	Schnittstelle der Hardware-Controller	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	Interne Datenübertragung	200 MB/ System
HiSeq-Serie	Beim HiSeq-System erfolgt keine interne IP-Kommunikation		100 MB/System
NextSeq 550	192.168.113.*:*	Alle Ports zulassen. Das ist die Verbindung für die Kommunikation mit der Firmware auf der Netzwerkkarte	50 MB/System
NextSeq 550Dx	192.168.113.*:*	Alle Ports zulassen. Das ist die Verbindung für die Kommunikation mit der Firmware auf der Netzwerkkarte	50 MB/System
	Port 80 oder 443	Local Run Manager; erforderliche lokale eingehende Verbindung (kein Internetzugriff)	50 MB/System
NextSeq 1000 und NextSeq 2000	21, 22, 4647, 5458, 5555, 5647, 7359, 7360, 169.254.*.*.*	Alle Ports zulassen. Das ist die Verbindung für die Kommunikation mit der Firmware auf der Netzwerkkarte	200 MB/ System
MiSeq	Port 80 oder 443	Local Run Manager; erforderliche lokale eingehende Verbindung (kein Internetzugriff)	10 MB/System
MiSeqDx	Port 80 oder 443	Local Run Manager; erforderliche lokale eingehende Verbindung (kein Internetzugriff)	10 MB/System
MiniSeq	192.168.113.*:*	Alle Ports zulassen. Das ist die Verbindung für die Kommunikation mit der Firmware auf der Netzwerkkarte	10 MB/System
	Port 80 oder 443	Local Run Manager; erforderliche lokale eingehende Verbindung (kein Internetzugriff)	10 MB/System
iSeq 100	Port 80 oder 443	Local Run Manager; erforderliche lokale eingehende Verbindung (kein Internetzugriff)	10 MB/System
iScan	6030, 888	AutoLoader	10 MB/System

Die aufgeführte IP-Adresse ist zwingend erforderlich. Es handelt sich um die Schnittstelle für den Hardware-Controller.

Weitere und ausführliche Informationen zu Kommunikationsanforderungen finden Sie im Handbuch zur Standortvorbereitung für das jeweilige System (Tabelle 6). Das Benutzerhandbuch für das jeweilige System enthält die erforderlichen Schritte zur Aktivierung von IPD über die Gerätesoftware (Tabelle 6).

Tabelle 6: Benutzerhandbücher und Handbücher zur Standortvorbereitung für Illumina-Systeme

System	System-/Referenzhandbuch	Handbuch zur Standortvorbereitung
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 und NextSeq 2000	1000000109376	1000000109378
MiSeq	15027617	15027615
MiSeqDx	15070067	15038351
MiniSeq	1000000002695	1000000002696
iSeq 100	1000000036024	1000000035337
iScan	11313539	1000000000661

Wenn ein Hyperlink aufgrund von Aktualisierungen nicht mehr funktioniert, kann mithilfe der angegebenen Dokumentnummer auf der Illumina-Website nach einer aktuellen Fassung des Handbuchs gesucht werden.

Arten von Geräte-Performancedaten

Tabelle 7: Arten von Geräte-Performancedaten (Gerätekonfigurationsdateien)

Dateiname	Beschreibung der Datei	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	Gesamtparameter für die Konfiguration des Softwaresystems	X	X	X	X		X	X	X	X	X	X	X
FirmwareVersions.txt	Firmwareversion der Gerätehardware						X			X	X		X
*Calibration.cfg	Parameter für die Kalibrierung des Softwaresystems	X					X	X		X	X	X	X
*Override.cfg	Parameter zur Überschreibung der Konfiguration des Softwaresystems	X	X	X	X		X			X	X	X	X
RTAStart.bat	Startdatei für die Primäranalyse					X	X			X	X		
Options.cfg	Parameter zur Überschreibung der Konfiguration des Softwaresystems												X
*HardwareHistory.csv	Konfigurationsverlauf der Gerätehardware						X			X	X		
*CurrentHardware.csv	Derzeitige Konfiguration der Gerätehardware						X			X	X		
Sequencing Configuration.xml	Konfigurationsparameter des Gerätesystems					X							
Channel*cc.txt	Datei für die Kamerakalibrierung	X											

a. HiSeq 1000, 1500, 2000 und 2500 System.

Tabelle 8: Arten von Geräte-Performancedaten (Gerätebetriebsprotokolle)

Dateiname	Dateityp	Beschreibung der Datei	iScan	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
*.jpg	Laufspezifische Betriebsbilder	Miniaturbilder für alle Platten und Farbkanäle, wenn die Option in der Software aktiviert wurde (standardmäßig deaktiviert). Wird in der Regel vom FAS/FSE aktiviert.						X	X	X	X	X		
Samplesheet.csv	Laufspezifische Proben-konfigurationsdatei	Sequenzierungsprobenblatt												X[b]
Rezeptdatei (XML)	Laufspezifische Konfigurationsdatei	Für den Lauf verwendetes Sequenzierungsrezept					X					X	X	X
Logs.zip		ZIP-Ordner mit Klarschriftdateien; alle Dateien für den Kunden im Gerät zugänglich					X	X	X	X	X	X	X	X
CompressedLogs.zip		ZIP-Ordner mit Protokolldateien; alle Dateien für den Kunden im Gerät zugänglich	X											

a. HiSeq 1000, 1500, 2000 und 2500 System.
b. In der NovaSeq 6000 v1.6-Software wird kein Probenblatt mehr hochgeladen.

Tabelle 9: Arten von Geräte-Performancedaten (Geräteanalysekonfigurationsdateien)

Dateiname	Beschreibung der Datei	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-Konfiguration	X	X	X	X	X	X	X		X		
RTA3.cfg	RTA-Konfiguration										X	X
RTAerror.txt	Fehlerprotokolldatei zur Primäranalyse					X	X					

a. HiSeq 1000, 1500, 2000 und 2500 System.

Tabelle 10: Arten von Geräte-Performancedaten (sonstige Dateitypen)

Dateiname	Beschreibung der Datei	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
*.IMF logs	Protokolldateien zum Softwarebetrieb		X	X		X				X	X	X
*Results.zip	Testergebnisse der Service-Software; wird nur gesendet, wenn von Service- und Supportmitarbeitern in der Service-Software festgelegt					X			X	X	X	

a. HiSeq 1000, 1500, 2000 und 2500 System.

Tabelle 11: Arten von Geräte-Performancedaten (laufspezifische Betriebsprotokolle)

Dateiname	Beschreibung der Datei	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	Protokolldateien zum Firmwarebetrieb (CSV)						X			X	X		
PreRunDiagnosticFiles	Dateien mit Ergebnissen des Tests vor dem Sequenzierungslauf und Protokollen (CSV und XML)					X	X			X	X	X	X
Cycle Logs	Fehlerbehebungsprotokolle für bei jedem Zyklus generierte Betriebsdaten (TXT und XLM)						X	X	X	X	X	X	X
Error.log	Fehlerbehebungsprotokolle für Betriebsdaten		X	X	X							X	X
CycleTimes.txt	Zyklusdauer während eines Sequenzierungslaufs		X	X	X								
UCS Logs	Copy Service-Protokolldatei (JSON und CSV)												X
CycleTime.tsv	Protokolldatei zu Zyklus- und Scandauer	X											
*.scrst	Konfigurationsdatei mit Einstellungen für den BeadChip-Scan	X											

a. HiSeq 1000, 1500, 2000 und 2500 System.

Tabelle 12: Arten von Geräte-Performancedaten (laufspezifische Analysedateien)

Dateiname	Beschreibung der Datei	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
RTAComplete.txt	Datei weist darauf hin, dass die gesamte Primärverarbeitung abgeschlossen wurde	X	X	X	X	X	X	X	X	X	X	X
RTARead*Complete.txt	Datei weist darauf hin, dass der wichtigste Schritt der Primärverarbeitung abgeschlossen wurde				X							
RunParameters.xml	Parameter der Laufkonfiguration, die zu Beginn des Laufs im XML-Format ausgegeben werden	X	X	X	X	X	X	X	X	X	X	X
RunInfo.xml	Für Sequencing Analysis Viewer verwendete Parameter der Laufkonfiguration, die zu Beginn des Laufs im XML-Format ausgegeben werden	X	X	X	X	X	X	X	X	X	X	X
RunCompletionStatus.xml	Datei, die auf den Abschluss der gesamten Sequenzierung hinweist	X	X	X		X	X	X	X	X	X	X
SequenceComplete.txt	Datei, die auf den Abschluss der gesamten Sequenzierung hinweist											X
*MetricsOut.bin	Binäre Berichtsdateien für Sequencing Analysis Viewer; ohne zusätzliche Software für den Kunden nicht lesbar	X	X	X	X	X	X	X	X	X	X	X
AlignmentMetricsOut.bin					X						X	X
BasecallingMetricsOut.bin					X						X	X
CorrectedIntMetricsOut.bin	Durchschnittliche Intensität, korrigierte Kanalintensität, korrigierte Call-Intensität, Call-Zählung	X	X	X	X	X	X	X	X	X	X	X
EmpiricalPhasingMetricsOut.bin	Phasierung, Vorphasierung pro Zyklus	X	X	X	X	X	X	X	X	X	X	X
ErrorMetricsOut.bin	Fehlerrate, Read-Fehler	X	X	X	X	X	X	X	X		X	X
EventMetricsOut.bin	Zeitdaten für: RTA gestartet, Zyklus gestartet, Matrizenbildung gestartet/abgeschlossen, max. Cluster-Init. nach Matrize, verfügbarer Systemspeicher in Gigabyte, Registrierung und Extraktion, Neighbor-Korrektur, Farbmatrix-Korrektur, Matrizenbildung, Base-Calling und Qualitäts-Scoring, Sequenz-Alignment, BCL-Erstellung, Read gestartet/abgeschlossen, Filter-Alignment gestartet/abgeschlossen, Zyklus abgeschlossen, RTA abgeschlossen	X	X	X	X	X	X	X	X	X	X	X
ExtendedTileMetricsOut.bin					X						X	X
ExtrationMetricsOut.bin	Fokuswerte, Intensitäten, Zeit	X	X	X	X		X	X	X	X	X	X
FWHMGridMetricsOut.bin					X						X	X
ImageMetricsOut.bin					X						X	X
IndexMetricsOut.bin	Name, Probenname, Projektname				X		X				X	X
OpticalModeMetricsOut.bin											X	X
PFGrtidMetricsOut.bin	Clusterzählung, PF-Clusterzählung, Bereich 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-Histogramm	X	X	X	X		X	X	X		X	X
RegistrationMetricsOut.bin	Versatz unterhalb der Plattenebene, affine Abbildung	X	X	X			X	X	X		X	X
TileMetricsOut.bin	Clusterdichte, Clusterdichte PF, Clusterzählung, Clusterzählung PF, Prozent aligniert, Prozent Phasierung, Prozent Vorphasierung, zuletzt extrahierter Zyklus, letzter Call-Zyklus, letzter Q-Score-Zyklus, letzter Fehlerzyklus	X	X	X	X		X	X	X	X	X	X
TSV oder TXT	TSV- oder TXT-Protokolldateien für RTA-Dateikopieprotokolle, allgemeine Protokolle und Wartungsprotokolle; für den Kunden in Klarschrift zugänglich				X		X	X	X	X		
QGridMetricsOut.bin					X							
ReconstructionMetricsOut.bin											X	

Quellen

1. Microsoft Security Response Center. msrc.microsoft.com. Aufgerufen am 12. April 2023.
2. National Institute of Standards and Technology. Advanced Encryption Standard (AES). csrc.nist.gov/publications/detail/fips/197/final. Veröffentlicht am 1. November 2001. Aufgerufen am 12. April 2023.
3. Amazon. AWS: ISO/IEC 27001:2013. aws.amazon.com/compliance/iso-27001-faqs/. Aufgerufen am 12. April 2023.
4. Illumina. (2018) BaseSpace Sequence Hub Security and Privacy. (illumina.com/content/dam/illumina/gcs/assembled-assets/marketing-literature/basespace-security-and-privacy-security-brief-m-gl-01959/basespace-security-and-privacy-security-brief-m-gl-01959.pdf). Aufgerufen am 8. November 2022.

illumina®

+1.800.809.4566 (USA, gebührenfrei) | +1.858.202.4566 (Tel. außerhalb der USA) | techsupport@illumina.com | www.illumina.com

M-GL-01092 DEU v1.0