



# Anforderungen bei der Vernetzung des PC eines Beckman Coulter-Geräts

## Überblick

Dieses Dokument beschreibt die technischen Mindestanforderungen zur Verbindung des PC eines Beckman-Geräts mit Ihrem lokalen Netzwerk und/oder dem Internet. Indem Sie den unten genannten Vorschlägen Folge leisten, kann Ihr Gerät sicher mit dem Netzwerk verbunden werden. Dies gilt sogar für Systeme, für die Vernetzung bisher nicht empfohlen war.

Dieser Leitfaden soll an Ihren Administrator bzw. Ihre IT-Abteilung weitergegeben werden, um sicherzustellen, dass Ihre Geräte vor der Verbindung Ihres Geräte-PC mit dem Netzwerk geschützt sind.

## Vor der Verbindung mit dem Netzwerk

Es wird empfohlen, dass Sie wichtige Dateien sichern, bevor Änderungen an den Konfigurationen des PC Ihres Geräts vorgenommen werden.

Stellen Sie sicher, dass der PC Ihres Gerätes die folgenden Anforderungen erfüllt:

- Wenn möglich die automatische Datensicherung aktivieren.
- Software- und/oder institutionelle Firewall ist für alle Netzwerktypen aktiviert.
  - **TIPP:** Falls Sie den Biomek Method Launcher installiert haben und ein anderes Produkt als die Microsoft® Windows Firewall verwenden, müssen Sie eine Prozessausnahme für „C:\Programme (x86)\Biomek Method Launcher\BiomekRuntime.exe“ hinzufügen, um die Remote-Funktionen zu verwenden. Falls Sie den Vi-CELL BLU Analysator verwenden, empfiehlt Beckman Coulter, nur die vorkonfigurierte Microsoft Windows Firewall zu verwenden.
- Antivirus-Software ist in den folgenden Verzeichnissen, die von der Echtzeit-Überprüfung ausgeschlossen sind, installiert:

Produkt	Unterstütztes Betriebssystem	Ordner
<b>Biomek-Pipettierroboter (FX<sup>P</sup>, NX<sup>P</sup>, 4000)</b>	<b>Windows 7, 10</b>	C:\Users\Public\Documents\Biomek
		C:\Users\Public\Documents\SAMI4.1
		C:\ProgramData\Beckman Coulter
		C:\ProgramData\Beckman Coulter Inc
<b>Pipettierroboter der Biomek i-Serie</b>	<b>Windows 10</b>	C:\Users\Public\Documents\Biomek5
		C:\Users\Public\Documents\SAMI5.0
		C:\ProgramData\Beckman Coulter
		C:\ProgramData\Beckman Coulter Inc

<b>CytoFLEX-Durchflusszytometer</b>	<b>Windows 7, 8, 8.1, 10</b>	None
<b>Vi-CELL BLU CellMek SPS Aquios CL</b>	<b>Windows 10</b>	Die Systeme werden mit der McAfee Application Control konfiguriert. Die Software darf nicht verändert oder entfernt werden. Weitere Informationen finden Sie in der Gebrauchsanweisung.
<b>Data Innovations Instrument Manager</b>	<b>Windows 7, 10</b>	C:\instrument manager
		C:\intersystems
		C:\Program Files (x86) or Program Files\Common Files\Data Innovations\Instrument Manager
		C:\Program Files (x86) or Program Files\Common Files\InterSystems
		C:\WINDOWS\system32\sx32w.dll file (if available)
<b>Navios EX Navios</b>	<b>Windows 10</b>	Die Systeme werden mit der McAfee Application Control konfiguriert. Die Software darf nicht verändert oder entfernt werden. Weitere Informationen finden Sie in der Gebrauchsanweisung.
<b>DxFlex CytoFlex SRT</b>	<b>Windows 10</b>	McAfee Application Control ist die empfohlene Malware-Schutzsoftware. Weitere Informationen finden Sie in der Gebrauchsanweisung.

- Microsoft® Windows AutoPlay deaktiviert
- Microsoft® Windows Update für wichtige Updates deaktiviert
  - **TIP:** Wenn zuvor keine Updates heruntergeladen wurden, führen Sie von einem geschützten Gerät aus einen einmaligen Download des Kumulativen Updatepakets durch und installieren Sie dieses vor der Verbindung mit dem Netzwerk auf jedem System. Stellen Sie sicher, dass alle Updates heruntergeladen und installiert wurden, bevor Sie zum ersten Mal eine Internetverbindung herstellen.

Für Navios EX, Navios, CellMek SPS, DxFLEX, Aquios CL und Data Innovations Instrument Manager sollten automatische Updates deaktiviert bleiben. Kumulative Sicherheitsupdates sollten manuell ausgeführt werden, nachdem sie von Beckman Coulter (Navios EX, Navios, CellMek SPS, DxFLEX, Aquios CL, CytoFLEX SRT) oder Data Innovations (Instrument Manager) validiert und genehmigt wurden.

Bei Vicell Blu-Analysensystemen werden Aktualisierungen des Betriebssystems als Teil der Software-Upgrades installiert.

- Wenden Sie sich an Ihre IT-Abteilung und lesen Sie den Sicherheitsanhang in der IFU, um sicherzustellen, dass alle zusätzlichen Anforderungen konfiguriert sind.

Wenn die vorangegangenen Firewall- und/oder Antivirenanforderungen nicht bereits über Software von Drittanbietern auf dem Geräte-PC installiert wurden und keine Sicherheitsempfehlungen in Ihrer Gebrauchsanweisung enthalten sind, ist die folgende kostenlose Firewall- und Antivirensoftware in Microsoft© Windows enthalten:

- Microsoft® Windows Firewall
- Microsoft® Windows Defender (antivirus)

Nach Erfüllung der oben genannten Anforderungen für die Netzwerksicherheit kann das Gerät sicher mit dem lokalen Netzwerk und/oder dem Internet verbunden werden.

### **Zusätzliche Empfehlungen**

Über die oben genannten erforderlichen Schritte hinaus sollten Gerätebesitzer/-betreiber zusätzliche Maßnahmen zum Schutz ihrer Daten in Betracht ziehen. Diese Schritte können u. a. sein: physische Zugriffssteuerung zur Begrenzung des Zugriffs auf Geräte/Labore, digitale Zugriffssteuerung zur Begrenzung des Zugriffs auf den PC, Mitarbeiterschulungen zum Verhindern vermeidbarer Zwischenfälle, regelmäßige Sicherung wichtiger Daten sowie regelmäßige Prüfungsmaßnahmen zur Sicherstellung der Einhaltung der oben genannten Richtlinien, um vermeidbare Zwischenfälle zu verhindern.



© 2021 Beckman Coulter Life Sciences. All rights reserved. Beckman Coulter, the stylized logo, and the Beckman Coulter product and service marks mentioned herein are trademarks or registered trademarks of Beckman Coulter, Inc. in the United States and other countries.

For Beckman Coulter's worldwide office locations and phone numbers, please visit Contact Us at [beckman.com](https://www.beckman.com)

MULTI-648402.20