



Beckman Coulter Instrument PC Networking Requirements

Overview

This document describes the minimum technical criteria required to connect a Beckman instrument PC to your local network and/or the internet. By following all the suggestions below, your instrument can safely be connected to the network; even for systems where networking was not previously recommended.

This guidance is intended to be shared with your computer administrator or IT department to ensure your instruments are secure prior to connecting your instrument PC to the network.

Before Connecting to the Network

Prior to making changes to the configuration of your instrument PC, it is recommended to backup any critical files.

Ensure your instrument PC meets the following requirements:

- Configure automatic backups, if possible.
- Software and/or institutional firewall is enabled for all network types.
 - **TIP:** If you have Biomek Method Launcher installed and are using a product other than Microsoft® Windows Firewall, you must add a process exception for “C:\Program Files (x86)\Biomek Method Launcher\BiomekRuntime.exe” to use remote features.
- Antivirus software is installed with the following directories excluded from real-time scanning:

Product	Supported OS	Folders
Biomek Liquid Handlers (FX ^P , NX ^P , 4000)	Windows 7, 10	C:\Users\Public\Documents\Biomek
		C:\Users\Public\Documents\SAMI4.1
		C:\ProgramData\Beckman Coulter
		C:\ProgramData\Beckman Coulter Inc
Biomek i-Series Liquid Handlers	Windows 10	C:\Users\Public\Documents\Biomek5
		C:\Users\Public\Documents\SAMI5.0
		C:\ProgramData\Beckman Coulter
		C:\ProgramData\Beckman Coulter Inc
CytoFLEX Flow Cytometers	Windows 7, 8, 8.1, 10	None

Vi-CELL BLU CellMek SPS Aquios CL	Windows 10	Systems are configured with McAfee Application control. Software should not be modified or removed. Refer to IFU for additional information.
Data Innovations Instrument Manager	Windows 7, 10	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
Navios EX Navios	Windows 10	C:\WINDOWS\system32\sx32w.dll file (if available)
		Systems are configured with McAfee Application control. Software should not be modified or removed. Refer to IFU for additional information.
DxFlex CytoFlex SRT	Windows 10	McAfee Application Control is the suggested malware protection software. Refer to IFU for additional information.

- Microsoft® Windows AutoPlay disabled
- Microsoft® Windows Update enabled for critical updates
 - **TIP:** If updates have not been previously downloaded, perform a one-time download of the Cumulative Update package from a secure machine and install on each system prior to connecting to the network. Ensure all updates are downloaded and installed prior to connecting to the internet for the first time.

For Navios EX, Navios, CellMek SPS, DxFLEX, Aquios CL, and Data Innovations Instrument Manager automatic updates should remain disabled. Cumulative security updates should be manually applied after they are validated and approved by Beckman Coulter (Navios EX, Navios, CellMek SPS, DxFLEX, Aquios CL, CytoFLEX SRT) or Data Innovations (Instrument Manager).

For Vi-CELL BLU analyzers, OS updates are installed as part of software upgrades.

- Check with your IT department and review the security appendix in the IFU to ensure any additional requirements are configured.

If the preceding firewall and/or antivirus requirements are not already implemented through 3rd party software on the instrument PC and there are no security recommendations in your IFU, the following free firewall and antivirus software is included with Microsoft® Windows:

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

After implementing the above network security requirements, the machine may be safely connected to the local network and/or internet.

Additional Recommendations

In addition to the required steps detailed above, instrument owners/operators should consider taking additional measures to safeguard their data. These steps may include physical access controls to restrict instrument/lab access, digital access controls to restrict access to the PC, employee training to avoid preventable incidents, regular backups of critical data and auditing measures to ensure compliance with the above policies. to avoid preventable incidents and auditing measures to ensure compliance with the above policies.



© 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. All other trademarks are the property of their respective owners.

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

MULTI-648402.20