Security for BeckmanConnect Diagnostic Support

BeckmanConnect Diagnostic Support is customer installable on any networked instrument controller PC with access to permitted network endpoints and on which the customer has administrator access.

Features of BeckmanConnect Diagnostic Support include:

- Sync of instrument performance data to Beckman Coulter for support and predictive analytics
- Notifications of system configuration issues or instrument performance/failures
- Customer-initiated remote support via a policy- and access-restricted customized version of TeamViewer
- Checking for new available upgrades to BeckmanConnect Diagnostic Support to install new features

This document provides information about the security features of BeckmanConnect Diagnostic Support.

Components

TeamViewer Client

A customized, access-restricted, and policy-secured TeamViewer installation that permits remote support for a system **only** by local Beckman Coulter support representatives after the connection is initiated and approved by the laboratory technician. TeamViewer runs as a service and has a shortcut available within the operating system. The client is configured to always run and communicate with the TeamViewer servers.

Notification Client

A software service that provides real-time notifications to the instrument controller PC regarding software and instrument status and logs active system notifications.

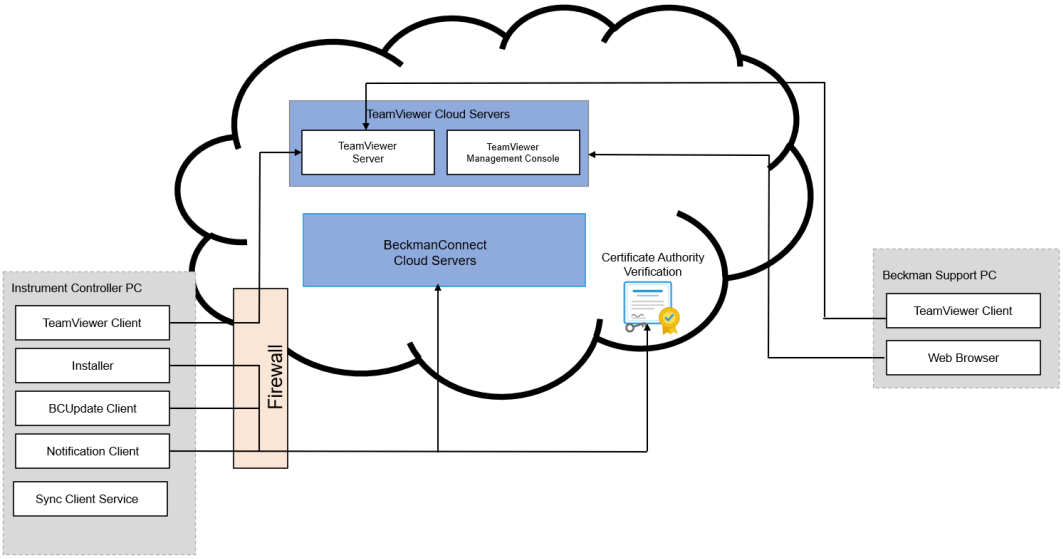
BeckmanConnect Update (BCUpdate) Client

A software service that monitors software updates to the BeckmanConnect Diagnostic Support components and notifies users when an upgrade is available for installation.

BeckmanConnect Sync (Data Collection) Client Service

A software service that collects instrument performance data and software status and uploads the data to the regional Beckman Coulter servers. No Protected Health Information (PHI) or Personally Identifiable Information (PII) is contained in data uploaded to Beckman Coulter servers.

System Architecture



Security Overview

Software Component Security

	BeckmanConnect Notification Client BCUpdate Client Installer BeckmanConnect Sync Client (service)	TeamViewer Client Installer
In-Transit Encryption	SSL/TLS 1.2	AES 256-bit session encryption
Authentication	Unique AES 256-bit encrypted keys for each device	RSA 4096-bit keys for sessions
Destination Firewall Rules[1]	Beckman cloud servers Outbound: Required by all geographies connectupdate.beckman.com:443 SSL CA verification sites over port 80 or manual SSL certificate trust update[3] via ctldl.windowsupdate.com:80 Required by countries using the Africa server[4] connectenrollmentafrica.beckman.com:443 bcls-connect-prod-iothub-northsa.azure-devices.net:443 Required by countries using the Europe server[5] connectenrollmenteurope.beckman.com:443 bcls-connect-prod-iothub-westeurope.azure-devices.net:443 Required by countries using the United States server[6] connectenrollment.beckman.com:443 bcls-connect-prod-iothub-westus.azure-devices.net:443	TeamViewer cloud servers[2] Outbound: Required by all geographies download.teamviewer.com:443 webapi.teamviewer.com:443 customdesignservice.teamviewer.com:443 configdl.teamviewer.com:443 dl.teamviewer.com:443 router1.teamviewer.com:443 – router15.teamviewer.com:443 (all 15 servers)
Code Signing	DigiCert	

[1] The installer will verify successful communication to each endpoint before permitting installation.

[2] TeamViewer does not publish a list of server endpoints. Beckman has determined the endpoints necessary for proper function of BeckmanConnect, but these endpoints may be changed by TeamViewer at any time. The IPs associated with some of the endpoints are not fixed.

[3] See BeckmanConnect Frequently Asked Questions (FAQ) document for details.

[4] Includes South Africa and Botswana

[5] Includes Austria, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, French Guiana, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Montenegro, Netherlands, North Macedonia, Poland, Portugal, Republic of Cyprus, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Ukraine, United Kingdom

[6] Includes Australia, Brazil, Canada, India, Indonesia, Japan, Mexico, Puerto Rico, South Korea, Thailand, United States, Vietnam

Server Security

	Beckman Servers	TeamViewer Servers
Data Transmitted and Stored	Enrollment: Enrollee's email and name, instrument, instrument ID and serial number Ongoing: Performance data (QC, maintenance, logs), software installation status, online status All data is scanned by up-to-date malware protection software server-side. Instrument performance data transferred to Beckman does not include any PHI or PII.	Instrument ID, serial number, online status/history, session and session event log
At-Rest Encryption	256-bit AES	Sensitive data AES/RSA 2048-bit encrypted
Access Restrictions	Access to data restricted to Beckman Support associates trained in local privacy regulations (e.g., GDPR, HIPAA) via Beckman SSO	Access to data restricted to Beckman Support associates trained in local privacy regulations (e.g., GDPR, HIPAA)
Bandwidth Requirements	6 Mbit or more suggested	
Data Centers	ISO/IEC 27001 certified GDPR compliant	
Intrusion Protection	Intrusion detection software present	Authentication from new location requires email verification

Remote Desktop Sharing Security

A thorough review of our IT requirements and consent to the terms of service are required prior to activating remote support features. BeckmanConnect Diagnostic Support is configured for maximum out-of-the-box security:

- Access is restricted to authenticated Beckman Coulter associates who have undergone training to understand the data and privacy guidelines that apply to the customer's region.
- TeamViewer connection allow-listing is deployed to prevent access to instruments from sources external to the Beckman Coulter Service & Support organization.
- Outgoing TeamViewer connection requests and meeting functionality within the client have been disabled.
- TeamViewer provides a uniquely generated 8+ character password for each connection. This password changes with each new session and provides brute-force attack protection via exponential password lockout, preventing unauthorized connections.
- Following successful authentication of a secure TeamViewer session, users are required to manually approve any screen-view, remote-control, or file-transfer requests through the TeamViewer client. Connection requests and file transfers are logged on TeamViewer secure servers for audit purposes.
- Note: File transfer during remote sessions is currently not enabled for instrument controller PCs containing personal health information (Navios EX Flow Cytometer, DxFLEX Flow Cytometer, Data Innovations Instrument Manager, AQUIOS CL Flow Cytometry System, CellMek SPS, Navios Flow Cytometer). If this feature is enabled in a future release, users must download an update and authorize the new feature during installation before it will be activated.

BECKMAN COULTER
Life Sciences

© 2026 Beckman Coulter, Inc. 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.
2023-GBL-EN-100962-v4 (v4.0)

danaher