Security for BeckmanConnect Diagnostic Support

Overview

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
- Check for 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 to 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 systems. The client is configured to always run and communicates 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.

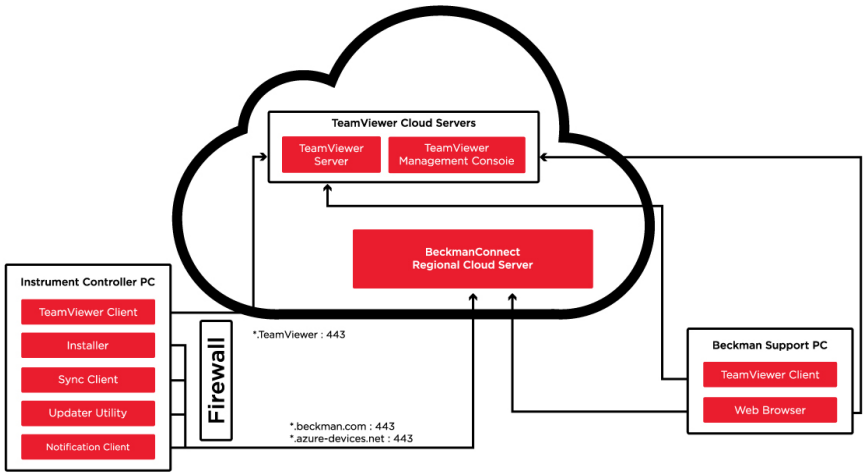
BeckmanConnect upgrade utility

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

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

	Sync Client **Notification Client** **Updater Utility** **Installer**	**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	Beckman cloud servers Outbound: *.beckman.com:443 (outside China) *.azure-devices.net:443 (outside China) *.azure-devices.cn:443 (China) *.mybeckman.cn:443 (China) *.blob.core.chinacloudapi.cn:443 (China)	TeamViewer cloud servers Outbound *.teamviewer.com:443
Code Signing	Digicert	

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 scanned by up-to-date malware protection software server-side. Instrument performance data transferred to Beckman does not include any PHI or PHI	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

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.
- Remote support users are required to provide 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 request 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, DxFLEX, Data Innovations Instrument Manager, AQUIOS CL, CellMek SPS, Navios). 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

For Beckman Coulter's worldwide office locations and phone numbers, please visit Contact Us at beckman.com

2023-GBL-EN-100962-v1