



# BeckmanConnect Security Highlights

## Overview

This document highlights the privacy and security features in the BeckmanConnect remote management solution. This solution is designed to enable our Service and Support organization to provide real-time service via a secure remote connection to Beckman Coulter instruments in your lab.<sup>1</sup> This document is intended to be reviewed by the local IT administrator for the instrument PCs and network infrastructure at your facility as part of the approval process for BeckmanConnect.

Supporting the Beckman Coulter remote management platform is TeamViewer GmbH, a global leader in secure online remote support and collaboration. At the forefront of remote software development, TeamViewer GmbH is a recognized provider of cloud-based technologies receiving a five-star quality seal by the Federal Association of IT Experts and Reviewers.<sup>2</sup> TeamViewer is a provider-of-choice for many data sensitive sectors including healthcare institutions, government, banking and finance.<sup>3</sup>

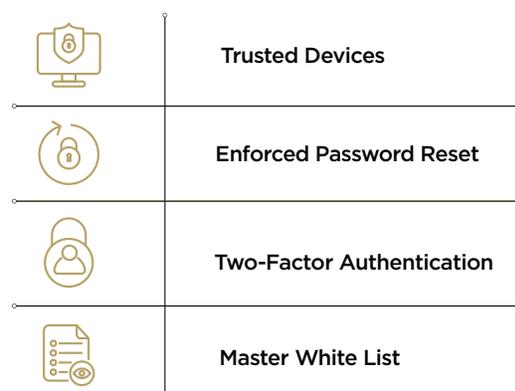
## Technical Summary

The TeamViewer tool provides a secure remote screen and file sharing platform to enable Beckman Coulter Service & Support experts to securely connect to Beckman Coulter instruments located in customer facilities. All TeamViewer traffic is secured via RSA public/private key exchange and AES (256 bit) session encryption. Additionally, the platform is configured to prevent 'man-in-the-middle' and brute force attacks. More detail is available in the TeamViewer security statement, located [here](#).<sup>3</sup>

## Security Measures

To operate, TeamViewer requires an internet connection. Before connecting any Beckman Coulter instrument PC to the network for the first time, please be sure to read the BeckmanConnect Instrument PC Networking Requirements document and ensure the instrument PC is secure. Thorough review of our IT requirements and consent to the terms of service are required prior to activating remote support features.

BeckmanConnect is configured for maximum out-of-the-box security:



**Figure 1.** Two-factor authentication, trusted devices and the use of whitelists ensure only authorized Beckman Coulter support agents can gain remote access to Beckman Coulter instruments in your lab.

<sup>1</sup> BeckmanConnect currently supports all Biomek instruments running Windows 7 or Windows 10 and CytoFLEX series flow cytometers.

<sup>2</sup> Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.

<sup>3</sup> TeamViewer security statement, <https://dl.tvcdn.de/docs/en/TeamViewer-Security-Statement-en.pdf>

- TeamViewer connection white-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.
- Users are required to provide a unique connection password to initiate all connection sessions. This password changes with each new session to prevent 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. Users may authorize the transfer of any file for the duration of the support session or request unique prompts for each file transfer. Connection requests are logged locally and on TeamViewer secure servers for audit purposes.
- The TeamViewer client is configured to automatically obtain and install critical security updates and updates to company TeamViewer policies.
- Access to the Beckman Coulter TeamViewer management portal is restricted by username and complex password. Access is restricted to Beckman Coulter employees who have undergone training to understand the data and privacy guidelines that apply to the customer's region.

### Firewall Requirements

BeckmanConnect is designed to enable a secure remote connection without the need for any special firewall configuration. In select situations, a firewall might be set up to block unknown outbound connections. In such cases, the firewall must be configured to facilitate the connection.

BeckmanConnect will use port 443 to establish an outbound TCP connection. Port 443 is required for the client software to:

- auto-update
- set required group policy settings for security purposes
- allow remote connections from Beckman Coulter Service & Support personnel

**NOTE: The service will not function properly without outbound access to port 443.**

BeckmanConnect makes connections to secure servers located around the world. These servers use a number of different IP addresses, which may change over time. All IP addresses used by BeckmanConnect resolve to either \*.teamviewer.com or \*.beckman.com domains. You can use this information to restrict the destination IP addresses you allow through your firewall or proxy server.

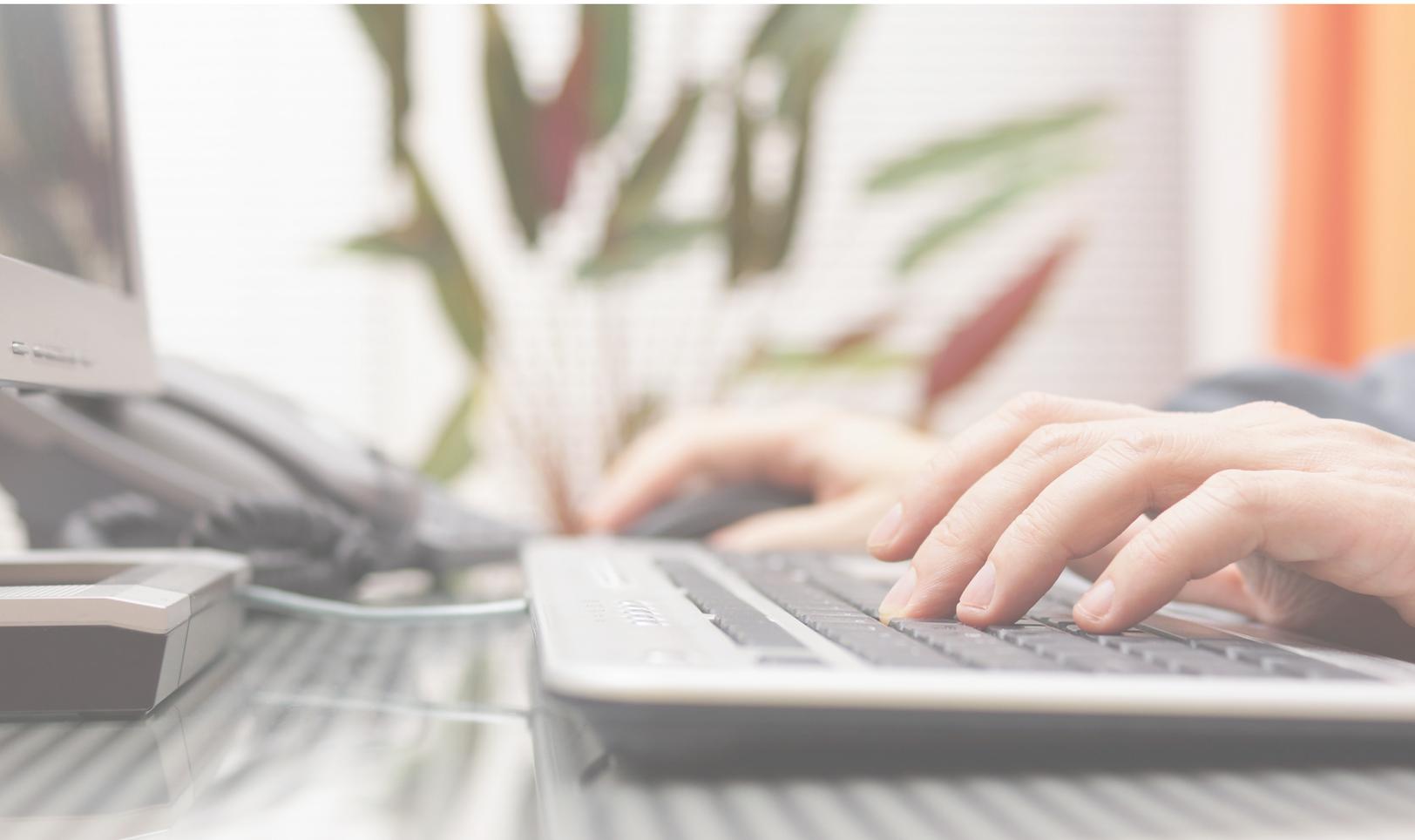
As the BeckmanConnect service only initiates outgoing data connections through a firewall, blocking incoming connections and allowing only outgoing TCP connections over port 443 to \*.teamviewer.com and \*.beckman.com domains will suffice.

## Summary

BeckmanConnect is a secure system which allows Beckman Coulter Service and Support personnel to remotely access certain instruments for technical support purposes. The end-to-end tunnel is encrypted and measures are taken to keep customers safe and ensure that access is only available to properly-trained Beckman Coulter employees.

Learn more or get connected today.

[connect@beckman.com](mailto:connect@beckman.com) | 800-369-0333



© 2018 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](http://beckman.com)

MULTI-3606WP04.18