DxS ProService
Remote Desktop Sharing

The DxS PROService solution allows Beckman Coulter service and support staff to remotely access a connected instrument's console

BECKMAN COULTER

DxS Pro*Service* Remote Desktop Sharing

Critical Security Controls to Protect Remote Sessions

The Remote Desktop Sharing (RDS) feature within Beckman Coulter's DxS PRO*Service* solution allows Beckman Coulter service and support staff to access the connected instrument's console to remotely troubleshoot service issues.

KEY BENEFITS OF RDS INCLUDE:

Maximized instrument uptime with remote support through RDS, which allows for detailed investigation and diagnosis to reduce length of service issues.

Increased remote resolution of instrument issues without waiting for onsite service—allowing your laboratory staff to focus on performing critical laboratory tests for patients.

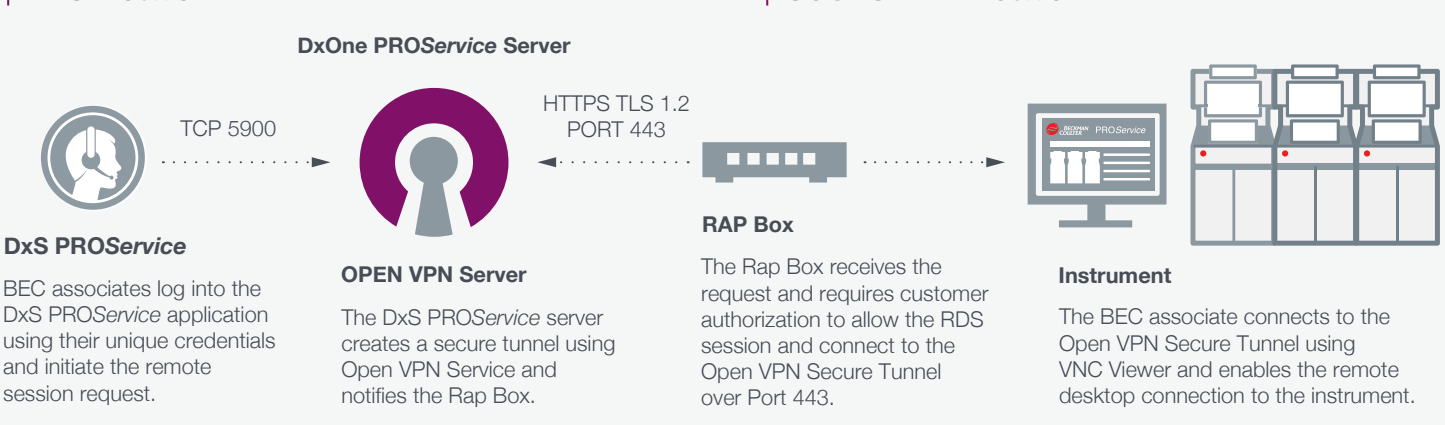
Complete control over RDS sessions, as each session requires your specific authorization before access is granted to Beckman Coulter associates.

The PRO*Service* application has been carefully designed and tested to integrate closely with your Beckman Coulter instrument and ensure there are no negative effects on the instrument workstation. This integration provides Beckman Coulter support staff with the advanced insights and tools needed to efficiently resolve issues remotely.

We understand the potential desire to use a third-party application software for remote desktop sharing capabilities. However, Beckman Coulter instruments are validated by appropriate regulatory agencies and installing or running a non-validated software on the instrument is prohibited as doing so will change the integrity of the instrument.

Therefore, Beckman Coulter policy does not allow the use or installation of any third-party software or Windows onboard applications for remote desktop sharing or other purposes. The PRO*Service* application is the only supported solution, and Beckman Coulter can provide all required technical resources to properly validate it in your environment.

RMS Remote Desktop Sharing



User Authentication & Authorization

Remote sessions adhere to multiple authentication and authorization processes to ensure that each session is initiated, established, and conducted by approved Beckman Coulter associates and with explicit customer permission.

User Authorization using RBAC

Role-based Access Control (RBAC) restricts remote session access based on the Beckman Coulter associate's role. Remote session access is only provided to Beckman Coulter associates who are involved in troubleshooting Beckman Coulter instruments.

Connection to the Beckman Coulter (BEC) Network

All Beckman Coulter associates must connect their work computer to Beckman Coulter's corporate network to access the PRO*Service* solution and establish instrument remote sessions.

Customer Authorization

Customer authorization and permission are required before each remote session can be established. When the Beckman Coulter associate initiates a remote session with the instrument, the software on the instrument console displays an authorization request which must be accepted by the lab operator before the connection can be established.

The remote session is established after the customer allows the remote session. If the authorization request is denied or ignored, then the remote session cannot be conducted by the Beckman Coulter associate.

User Authentication using Azure AD FS

Beckman Coulter associates who want to initiate a remote session to instrument console need to first log in to the PRO*Service* solution, which is protected by Beckman Coulter's corporate Active Directory Federation Service (AD FS) authentication process.

The user authentication requires a unique username and password for every Beckman Coulter associate to log into the application.

RAP Box as a Firewall Device

Each Beckman Coulter instrument enrolled in the PRO*Service* solution is connected via an ethernet cable to a proprietary IoT Gateway device called a RAP Box. This device acts as a firewall to all the connected instruments to control incoming and outgoing traffic. It has built-in intelligence and security hardening that securely enables remote sessions with Beckman Coulter associates.

RMS Remote Application Processor (RAP) Box

No Inbound connection

The RAP Box is configured not to accept any inbound connections, making instruments unreachable to the unauthorized attempts.

TLS 1.2 over 443

Only outbound TLS 1.2 communication over Port 443 is enabled on the RAP Box, which makes the remote session communication secure and encrypted.

FIPS 140-2 Compliance

Communication between the OpenVPN Server and the RAP Box is over TLS 1.2 and uses only FIPS 140-2 Compliant cryptographic algorithms for data in transit encryption.

Intrusion Detection and Audit Logs

The RAP box is set up using auditd and snort for audit logging and intrusion-detection, respectively, which takes care of monitoring, logging, and preventing malicious network activities.

ClamAv AntiVirus Engine

ClamAV antivirus engine scans all the incoming and outgoing files from the RAP Box, removing malicious files reaching RAP Box.

Open VPN as Secure Tunnel Service

OpenVPN is an open-source connection protocol that establishes a secure tunnel between the Beckman Coulter associate's work computer and the instrument console to ensure that the data communicated between the two is encrypted and private over the internet.

Why OpenVPN?

OpenVPN, with its open-source code, strong encryption, and strong community support, is one of the best tunneling protocols to keep data secure. The OpenVPN tunneling protocol uses AES 256-bit encryption to protect data packets. Because the protocol is open source, the code is vetted thoroughly and regularly by the security community, which constantly looks for potential security flaws. New versions are available for upgrade.

How is OpenVPN Server Protected from security risks?

Intrusion Detection by Guardicore

The OpenVPN server is protected with Guardicore, a Cybersecurity Intrusion Detection product that monitors and prevents any suspicious network activities and ensures that the remote sessions. It also ensures that the remote sessions are secure and only conducted by authorized Beckman Coulter associates.

McAfee – Solidcore

The OpenVPN server is protected with McAfee Solidcore, which allows the execution of only whitelisted and approved software and blocks unauthorized executable files, libraries, drivers, ActiveX controls, scripts, and specialty code on the VPN server.

Mutual Certificate Authentication

Communication between the OpenVPN server and the RAP Box is protected by mutual certificate authentication using a unique CA-signed SSL certificate.

IPTables Firewall Rules

IPTables Firewall rules are applied at runtime on the RAP Box and OpenVPN servers to ensure that the Beckman Coulter associate's work computer only connects to the instrument console through the RAP Box. The following rules are configured in the RAP Box and OpenVPN Servers.

- The OpenVPN server will be configured with IPTables firewall rules at runtime during the remote session to only allow traffic between the designated RAP Box and the Beckman Coulter associate's work computer. The firewall rule is removed once the remote session is completed.
- The RAP Box will be configured with IPTables firewall rules at runtime during the remote session to only allow traffic from the OpenVPN Secure Tunnel to pass through to the instrument console.

Remote Session Audit Reports

Audit logs are created for each remote session initiated by the Beckman Coulter associate and include details of the user who performed the remote session, the IP Address of the user's work computer, the date, and duration time of the remote session, and the customer log-in that approved the remote session. Remote session audit logs are stored for three years. Due to the possibility of sensitive *PHI* data being displayed, video recordings are not captured for any remote sessions.

External PEN Testing

An external organization performs Security Penetration Testing before releasing any major or critical features to ensure that the software does not have any weaknesses that hackers can exploit.

Vulnerability Scans and Security Patch Updates

Vulnerability scans are run at the RAP Box, OpenVPN, and other cloud servers regularly to identify critical vulnerabilities in the software. Patches are applied to address open critical vulnerabilities to ensure that the entire platform is safe and has no weaknesses that hackers can exploit.

Remote Session — Auto Log Off

Remote sessions automatically terminate after 30 minutes of inactivity to ensure that unauthorized users are unable to access the remote session.

Critical security controls such as user authentication with RBAC, customer authorization for each remote session, End-End encryption over TLS1.2, FIPS 140-2 compliance, and dynamic firewall rules allow traffic exclusively between remote session endpoints. Auto log-off, key monitoring, and audit controls (like intrusion detection and vulnerability scans at a regular cadence) ensure the remote session is protected, eliminating the likelihood of a successful cyber-attack.

Overall Key Features of RDS

User Authentication & Authorization

- User authentication using Azure AD FS
- User authorization using RBAC
- Customer RDS Authorization
- PRO*Service* can only be accessed from Beckman Coulter's corporate network

Firewall Protection

- RAP Box as another layer firewall device
- No Inbound connection
- TLS 1.2 over 443
- FIPS 140-2 compliance
- Intrusion detection and audit logs - auditd and Snort
- ClamAv AntiVirus Engine

Secure Tunnel Service

- OpenVPN server is protected with Guardicore
- OpenVPN server is protected with McAfee
- IPTable Firewall rules are applied at runtime on RAP Box and OpenVPN
- Communication between OpenVPN Server and the RAP box is protected by mutual certificate authentication

Additional Security Measures

- Audit logs for every remote session initiated by the Beckman Coulter associate are captured
- Security penetration testing planned and performed by an external organization
- Vulnerability scans are run at the RAP Box, OpenVPN, and other cloud servers at a regular cadence
- A remote session initiated by the Beckman Coulter associate will be automatically terminated after 30 minutes of inactivity

DxS Pro*Service* Remote Desktop Sharing

DxS PRO*Service* enables the secure transmission of instrument status information to Beckman Coulter so you can focus on patient care.

Conforms to Information Security standards established by the industry and VA.

Reduces unscheduled downtime by enabling proactive, preventive action to be taken by you or Beckman Coulter.

Minimizes interruptions when service is needed by expediting issue isolation and readiness of parts.

Glossary

TERM	DEFINITION
AD FS	Active Directory Federation Service (AD FS): A software component created by Microsoft that uses claim-based authentication to provide single sign-on (SSO) capabilities to users of multiple applications across organizational boundaries.
Auditd	Auditd generates log entries to record information about the events happening on the system. The recorded information is used to analyze what went wrong with the security policies and improve them further by taking additional measures.
External PEN Testing	Penetration Testing, also known as PEN Testing: a security assessment by a third-party organization which simulates a cyber-attack against your network to check for exploitable vulnerabilities.
FIPS	Federal Information Processing Standards: publicly announced standardizations developed by the U.S. federal government for use in computer systems by all non-military government agencies and by government contractors, when properly invoked and tailored on a contract; ensures that all federal government agencies adhere to the same guidelines regarding security and communication.
FIPS 140-2	A U.S. government computer security standard that specifies the minimum cryptographic modules requirement for data encryption and is validated by the National Institute of Standards and Technology.
RAP box	The hardware (i.e., a small, headless computer) responsible for facilitating the communication between connected Beckman Coulter instruments and the Beckman Coulter data center via its trusted subnet; responsible for deciding when to use local storage, dispatching and executing local commands, and controlling the VPN tunnel, including starting and authentication.
RBAC	Role Based Access Control (RBAC): restricts network access based on a person's role within an organization.
Snort	Snort is open-source intrusion prevention system used to define malicious network activity.
SSL Certificate	Secure Sockets Layer (SSL) Certificate: A digital certificate that authenticates a website's identity and enables an encrypted connection between a web browser and a web server.
TLS	Transport Layer Security: a session layer security protocol used on the Internet to secure web pages and transactions by means of public key cryptography.
Triggers	A set of conditions that, when matched to instrument data, alerts the DxS PRO*Service* support team.
VA	U.S. Department of Veterans Affairs

DxS PRO*Service* availability or features vary by instrument/system platform.

For Beckman Coulter's worldwide office locations and phone numbers, please visit www.beckmancoulter.com/contact

FL-436200 | 2022-10782

BECKMAN COULTER