DxS IntelliServe Specifications

Introduction

What is the DxS IntelliServe solution?

DxS IntelliServe is a remote service and diagnostics solution based in the Microsoft Azure cloud that provides connectivity between Beckman Coulter instruments and technical experts to improve instrument availability and protect your laboratory workflow.

The DxS IntelliServe solution utilizes advanced analytical tools for predictive and preventive analytics to communicate critical device information, enable virtual issue resolution, and allow technical and application experts the ability to interact with your instrument.

The intent is to build a platform that:

- Significantly increases instrument availability by reducing emergency downtime and the time required to troubleshoot and resolve service issues.
- Improves the ease of keeping instrumentation up to date with the latest software, which provides bug fixes, new features, and assay test menus updates.
- Continually expands its innovative, remote capabilities across a growing network of eligible instruments.

General Information

What is the difference between DxS IntelliServe and DxS PRO*Service* solutions?

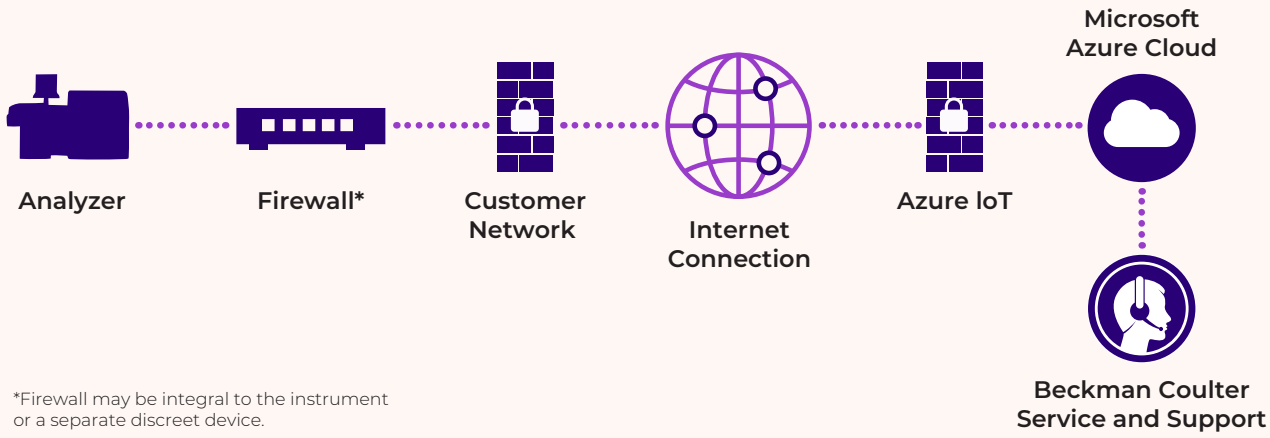
The DxS IntelliServe and DxS PRO*Service* solutions make up Beckman Coulter's remote service and diagnostics portfolio for laboratory diagnostics instruments and solutions. The DxS IntelliServe solution is the next generation of predictive monitoring, expanding upon the remote diagnostics capabilities Beckman Coulter has been providing for the last 15 years. Starting in January 2025, Beckman Coulter is incrementally transitioning PRO*Service*-supported instruments to the DxS IntelliServe platform to consolidate remote support solutions. During this transition period, some PRO*Service* instrument data will be stored in both PRO*Service* and IntelliServe infrastructures. Beckman Coulter will continue to release additional information throughout this process.

Characteristics	DxS PRO*Service*	DxS IntelliServe
Supported Disciplines	Automation, Blood Banking, Chemistry, Hematology, Immunoassay, Information Systems	Automation, Chemistry, Immunoassay†
Eligible Instruments	View Beckmancoulter.com for a complete listing of eligible instruments.	
Technology Infrastructure	Hosted Infrastructure	Microsoft Azure Cloud
Remote Desktop Sharing	Open VPN	Microsoft Azure Relay Service

†Beckman Coulter is working on expanding instrument coverage, and the most up-to-date information can be found at www.beckmancoulter.com.

BECKMAN COULTER

DxS Remote Connectivity Framework



*Firewall may be integral to the instrument or a separate discreet device.

How does the DxS IntelliServe solution work?

Each connectable Beckman Coulter instrument is configured through an integrated or a standalone firewall device, which is connected to the Internet via an ethernet port. Performance data is continuously and securely transferred from the instrument through the Internet to Beckman Coulter's Microsoft Azure Cloud servers for technical and application experts to analyze for immediate insights or action.

The instruments only communicate to specific Azure endpoints over port 443 (Outbound Only). These endpoints are used to communicate instrument performance data from the instrument to the Microsoft Azure Cloud for access and use by Beckman Coulter service experts. The specific endpoint URLs can be found in the Remote Connections Form.

How are the endpoints used?

Endpoint	Purpose
DPS (Device Provisioning Services) Endpoint	Used for instrument enrollment and acts as a gatekeeper, only allowing authorized instruments to connect to IntelliServe.
Azure IoT Hub	Allows Beckman Coulter to manage the instruments and view connectivity status. Heartbeat messages from the analyzer are sent to the Azure IoT Hub every 30 seconds to communicate instrument connectivity status.
Data Lake	All transmitted instrument data is stored in this data lake and then goes to structured tables in the SQL database.
Microsoft Azure Relay Service	Used for Remote Desktop Sharing functionality. Requires the use of the wildcard '*' in URL filtering due to Microsoft's use of multiple changing URLs in the relay service.
DxS IntelliServe Azure Endpoint	Used as an entry point into IntelliServe Cloud which will connect the instrument to the required cloud services like DPS, Azure IoT Hub, Data Lake, Relay Services.

What is the Microsoft Azure Cloud?

At its core, Microsoft Azure is a cloud computing platform—with solutions including Infrastructure as a Service, Platform as a Service, and Software as a Service that can be used for services such as analytics, virtual computing, storage, networking, and much more.

Why should I connect my instrument to the DxS IntelliServe solution?

The DxS IntelliServe solution has a comprehensive set of features, tools, and capabilities to maximize your instrument's availability, reduce interruptions to your laboratory workflow, and ultimately enable you to deliver lab and patient outcomes. Below are some high-level features and benefits that the DxS IntelliServe solution provides:

Features	Benefits
Predictive Monitoring & Alerts†	· Reduces unplanned interruptions to laboratory workflow · Detects emergency downtime before it occurs,† so the service issue can be avoided or planned
Realtime Monitoring	· Provides laboratory staff with immediate awareness of contingent workflow planning · Provides more immediate failure notifications† with alerts based on pre-defined measures
Remote Operation & Troubleshooting	· Decreases length of instrument downtime · Resolves service issues† without sending an engineer on-site through remote issue resolution · Increases preparation for on-site visits (when required) to reduce on-site interruption time, as well as reduction of return visits
Remote Software Updates*	· Keeps the instrument up to date · Provides remote availability of software updates upon release · Allows the laboratory to implement updates according to their schedule
Automated Metering*	· Reduces the time required for inventory management · Automatically uploads reagent data from the instrument and automatically reorders materials based on usage and inventory levels

*Some features or functionality will not be available until subsequent releases following the initial product launch and may vary by instrument.
†Depends on the instrument-specific service issue or error.

What is the cost for the DxS IntelliServe solution?

The DxS IntelliServe solution is available to all customers with eligible Beckman Coulter instruments. Some features may require warranty or service agreement coverage to be in place on the instrumentation or may require an additional fee. Please contact your Beckman Coulter sales representative for more information.

Features and Capabilities

What do I need to do to prepare to install the DxS IntelliServe solution?

Beckman Coulter's service organization works with your laboratory and IT staff to complete the Remote Connections Form (available online or hardcopy), which confirms the required installation specifications.

The set-up requires physical access to a wired network connection and some minimal IT configuration for the ethernet port.

Which Beckman Coulter instruments can connect to the DxS IntelliServe solution?

Beckman Coulter is continuously expanding the list of analyzers and solutions available for this coverage, and the most up-to-date information can be found at www.beckmancoulter.com/dxsintelliserve.

Can the DxS IntelliServe solution be added to existing Beckman Coulter or non-Beckman Coulter instruments in the lab?

The DxS IntelliServe solution is only available for specific Beckman Coulter instruments and may not be available for the existing installed Beckman Coulter instruments in your lab. Beckman Coulter is working on expanding instrument coverage, and the most up-to-date information can be found at www.beckmancoulter.com/dxsintelliserve. Currently, the DxS IntelliServe solution is not available for third-party instruments.

I am a Beckman Coulter reagent and consumables metering customer. Can the DxS IntelliServe solution process my metering information?

Yes, metering is available on select instruments. Please contact your Beckman Coulter representative for more information.

Architecture and Installation

What is the installation process for the DxS IntelliServe solution?

The installation process is designed to be seamless but does require key actions from you (as a customer) as well as from Beckman Coulter:

STEP ONE

Your laboratory IT must prepare your site and configure your network to IntelliServe's specifications

STEP TWO

Once your instrument is on-site and your network is prepared, Beckman Coulter's service engineer configures the instrument to your network to enable communication over the internet to BEC Microsoft Azure Cloud servers

STEP THREE

Once remote connectivity is established, your instrument can be enrolled in the DxS IntelliServe system

Engagement from your IT counterparts is critical for a seamless and timely implementation.

To help ensure a smooth installation process, the site preparations must be completed before the instrument installation. Otherwise, installing the DxS IntelliServe solution will require a return visit.

How does the DxS IntelliServe solution use my network?

The integrated instrument firewall or a standalone Beckman Coulter firewall is connected to your network using a static or Dynamic Host Configuration Protocol IP address. The instrument, via a Beckman Coulter firewall, communicates through your existing network to Beckman Coulter Azure cloud endpoints (URLs) only. These URLs must be whitelisted within your network to allow this communication.

Additionally, you must also allow http connect plain text requests on Port 443, and bypass SSL inspection to the identified endpoints. The internet connection between the analyzer and Azure Cloud is secured using the Transport Layer Security (TLS) standard v1.2.

The Remote Desktop Sharing session between the instrument and the Microsoft Azure cloud is securely established over port 443 (outbound only).

What if my network has a proxy server for internet or wireless internet access?

Customer network proxy servers are supported for DxS IntelliServe connections. You will be required to whitelist additional endpoint URLs to support these types of connections, and these can be found in the Remote Connections Form.

What bandwidth will my network need to support the DxS IntelliServe solution?

No additional resources should be necessary to support the data transmitted by the DxS IntelliServe solution. Typical data packets are 2 KB or fewer at intervals of approximately 30 seconds. For Remote Desktop Sharing and software updates, 1 Mbps bandwidth is required.

How do I get started?

For new instruments, this is part of the instrument installation planning process. We will proactively work with you and your team to initiate, manage, and complete this process.

However, for any other requests or questions, please email RemoteSolutionsInstalls@beckman.com or contact your Beckman Coulter sales representative or field service engineer to begin the installation process.

Security, Privacy & Confidentiality

How safe and secure is the DxS IntelliServe solution?

Azure core services used by the DxS IntelliServe solution are compliant with the following standards[1]:

- ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and for international security, reliability, data privacy, and business continuity management standards,
- SOC 1 Type 2, SOC 2 Type 2, and SOC 3 for applications in which confidentiality and privacy of information stored and processed in the cloud is critical,
- Health Insurance Portability and Accountability, Business Associate Agreement for the United States healthcare applications, and General Data Protection Regulationfor European Union,
- Canadian Standard Association Star Attestation Level 2 for cloud security across multiple control areas. https://azure.microsoft.com/en-us/resourcesmicrosoft-azure-and-data-compliance-in-the-internet-of-things-iot-context/

The DxS IntelliServe solution follows Danaher and Beckman Coulter security policies and procedures, and continuously conducts internal and external penetration tests. In addition, it uses:

- TLS v1.2 to establish a connection and port 443 for outbound traffic.
- DigiCert SSL/TLS certificate for enrolling instruments.

What firewall protection is being used to support this solution?

An instrument-integrated or standalone firewall is used to support this solution in conjunction with the Microsoft Azure cloud firewall.

Does this solution open my instruments or lab to additional risks (including malware or viruses)?

The instrument can only communicate to defined Azure endpoints whitelisted in the network firewall. There is no need to open any ports for inbound connections.

All file uploads and downloads are scanned with antivirus software.

Can HTTP Connect plain text requests over port 443 to the cloud proxy server cause any security threat to my network?

No. The DxS IntelliServe Azure Endpoint is configured to only accept Connect requests to the whitelisted endpoints over port 443 and all other port forwarding is disabled in the cloud proxy server. A Connect request to any malicious endpoints cannot be exploited through the cloud proxy server. In addition, the Connect request is a plain text request over port 443. Once the proxy establishes the connection, then the entire communication between the Beckman Coulter instrument to Cloud Servers are end-to-end encrypted.

Can bypassing SSL inspection create any security risks?

No. Beckman Coulter's instrument communication with the Azure cloud is done by mutual certificate authentication to make sure that only genuine Beckman Coulter instruments are communicating with the proper Azure cloud server.

If SSL inspection is being used on your network, the certificate presented by our instrument will be rejected by the cloud and this will cause the instrument communication to fail as the cloud cannot identify the client. We have the below security controls in place to make sure that the source and destination can identify each other and communicate securely:

1. All the communication to the above-mentioned endpoints is encrypted over port 443 over TLS1.2.
2. Every endpoint is protected and enabled with mutual certificate authentication or SAS tokens to ensure that the source is identified, authenticated, and authorized to exchange data with the Azure cloud.

What information is sent from my instruments to Beckman Coulter through the DxS IntelliServe solution? How is the information used?

The data parameters transferred to Beckman Coulter servers vary by instrument model. In general, the instrument transfers data related to instrument performance, including:

- Instrument status and events
- Instrument subsystem's vital signs, such as temperatures, pressures, and voltages
- Subsystem / module-specific parameters, including analytical system components, motion controls, and fluidic systems
- Calibration and quality control performance
- Some analytical results are needed for troubleshooting, with sample ID only
- System identifiers and statistics: software versions, instrument configurations, and metering data, if applicable

During Remote Desktop Sharing sessions, whatever is visible on the instrument console is visible to the Beckman Coulter service and support staff. **The analyzers with IntelliServe software blocks patient health information.** Each Remote Desktop Sharing session requires the customer's manual authorization from the instrument console.

How and where is my information stored?

There are two locations for data storage depending on your physical location. The Beckman Coulter Azure cloud servers are located in Germany or the United States. All data is stored in compliance with the following standards:

- ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and for international security, reliability, data privacy, and business continuity management standards
- SOC 1 Type 2, SOC 2 Type 2, and SOC 3 for applications in which confidentiality and privacy of information stored and processed in the cloud is critical
- Health Insurance Portability and Accountability, Business Associate Agreement for the United States healthcare applications, and General Data Protection Regulation for European Union
- Canadian Standard Association Star Attestation Level 2 for cloud security across multiple control areas

What security methods are in place to secure the transfer of information from my instrument?

Encryption methods:

- Data in Transit – TLS v1.2
- Data at Rest - Microsoft-managed encryption key or Transparent Data Encryption

Connection security details:

- SSL/TLS Certificate-based authentication

Firewall/solution infrastructure:

- On-site (Instrument Integrated or Stand-alone) Firewall, Microsoft Azure cloud firewall

All file uploads and downloads are scanned for viruses and malicious software.

Is any protected patient health information transferred to Beckman Coulter? Is any patient health information visible through the DxS IntelliServe solution?

Beckman Coulter Service and Support staff stay current with annual training requirements on Health Insurance Portability and Accountability Act and General Data Protection Regulation that govern the handling of patient health information.

During all operations, including remote desktop sharing sessions, the instrument transmits system performance data pertinent to mechanical and analytical functions to the DxS IntelliServe solution for immediate review by the Beckman Coulter service and support staff. Although some analyzers transmit the sample ID field for rapid identification of assay issues, Beckman Coulter recommends not including patient names or other medical information in the sample ID field. During the remote desktop sharing session, patient health information is blocked.

Who can access my instruments and their information?

The DxS IntelliServe solution is used by Health Insurance Portability and Accountability Act and General Data Protection Regulation-trained Beckman Coulter Service and Support staff (including customer technical support specialists and field service engineers) and authorized agents.

Access control management for users of the DxS IntelliServe solution is defined by the user's support role and geographic location. Additionally, DxS IntelliServe utilizes federated authentication which allows only Beckman Coulter or Authorized Service Provider associates access to the DxS IntelliServe solution using their corporate user credentials and Multifactor Authentication (MFA). The user authentication requires a unique username and password for every Beckman Coulter or Authorized Service Provider associate to log into the application.

Unauthorized third parties or users cannot access your instruments or information.

Are third-party remote desktop sharing applications supported?

No.

My instrumentation is serviced by an Authorized Service Provider (not by Beckman Coulter directly). Do they have access to the IntelliServe solution, and how is their access controlled?

Yes, Authorized Service Providers can access the IntelliServe application through federated authentication to support Beckman Coulter instruments remotely. This method allows their users to log in using corporate credentials and restricts their access to the IntelliServe application.

The DxS IntelliServe solution utilizes advanced analytical tools for predictive and preventive analytics to communicate critical device information, enable virtual issue resolution, and allow technical and application experts the ability to interact with your instrument.

Contact your local Beckman Coulter representative for more information or visit www.beckmancoulter.com/dxsintelliserve

DxS IntelliServe

BECKMAN COULTER

The DxS IntelliServe solution may not be available in all geographies. Please contact your local Beckman Coulter representative for more information.

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

DS-706900 | 2025-14184

danaher