PRO*Service* REMOTE SERVICE APPLICATION

RMS technology, architecture and security information for IT professionals

BECKMAN COULTER

Move healthcare forward.

INCREASE UPTIME, IMPROVE PRODUCTIVITY

Medical diagnostics are a vital part of the modern healthcare system, and instrument uptime is critical to diagnostics throughput and profitability.

Improved instrument uptime can be attained by:

- Reducing unscheduled service through remote and proactive monitoring of instrument trends
- Allowing some service "visits" to be done remotely
- Making service visits more efficient through knowledge of mass trends across the installed base
- Ensuring that the technician has the right parts for on-site visits

These are all worthwhile goals, and Beckman Coulter can support your organization's need for secure, efficient instrument management through PRO*Service*.

PRO*Service*: Enhancing instrument performance

PRO*Service* features*	Benefits
Service Dashboard Remote Desktop Sharing (RDS) Remote Upload	Maximize uptime and productivity Reduce unscheduled downtime Make troubleshooting and service more efficient
Remote Download	Update software remotely Update database remotely Update online "Help" file remotely Update reagent file/settings remotely Immediately access documents (e.g., customer notifications)
Triggers	Avoid/Reduce unscheduled downtime with proactive and predictive support to solve issues before they affect instrument performance Reduce customer-initiated service calls Improve system uptime and efficiency
Remote Setup/Configuration	Shorten on-site visit time for instrument/middleware setup Eliminate on-site visit to configure add-on test Accelerate revenue generation for add-on tests
mPRO*Service*	Increase service efficiency with mobile PRO*Service* Service Dashboard

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

PRO*Service* design highlights

PRO*Service* utilizes RMS—a secure, proprietary data pipeline—to connect Beckman Coulter instruments in customer laboratories with Beckman Coulter's service and support department. This encrypted interface can connect multiple instruments simultaneously with little impact to customers' IT systems.

- The RMS Remote Application Process (RAP) box connects to the instrument Transmission Control Protocol/Internet Protocol (TCP/IP) port and creates a firewalled subnet for the connected instruments. It does not touch the laboratory information system (LIS) data connection unless a customer requests the Network Connectivity feature
- Instrument status is sent via Hypertext Transfer Protocol Secure (HTTPS)/Secure Sockets Layer (SSL) to PRO*Service*
- Remote management is available and performed through an outbound-initiated virtual private network (VPN) tunnel

Using firewall-friendly technology, the RMS RAP box securely transfers information pertinent to instrument health to Beckman Coulter servers via the Internet.

PRO*Service* is enabled by a small, headless computer that links your Beckman Coulter instruments to servers, software and a support team at Beckman Coulter. This computer, also known as an RMS RAP box, is installed in your laboratory and connects to your Beckman Coulter instruments via TCP/IP.

The RMS RAP box coordinates secure, encrypted communication between your instruments and the secure Beckman Coulter servers.

Architecture

The PRO*Service* application uses the RMS RAP box, the Internet and sophisticated enterprise software to connect your Beckman Coulter instruments to support staff.

RMS RAP box

At the client

The RMS RAP box is a dedicated communications processor that buffers and forwards status reports from software agents on each instrument to Beckman Coulter servers. It also provides authentication and VPN services to support remote instrument management.

En route

All data is encrypted with 128-bit Advanced Encryption Standard (AES) and sent over the Internet via SSL.

PRO*Service* uses the popular open source SSL/Transport Layer Security (TLS) VPN called OpenVPN. OpenVPN utilizes OpenSSL cryptographic modules for data encryption, which is used for RDS.

At Beckman Coulter

Beckman Coulter's dedicated database and servers handle data collection and analysis. The system (Figure 1) supports sophisticated reporting and triggers, which alert Beckman Coulter service and support staff to potential instrument issues. Access to instrument data and status is controlled according to the training, role and location of the Beckman Coulter staff.

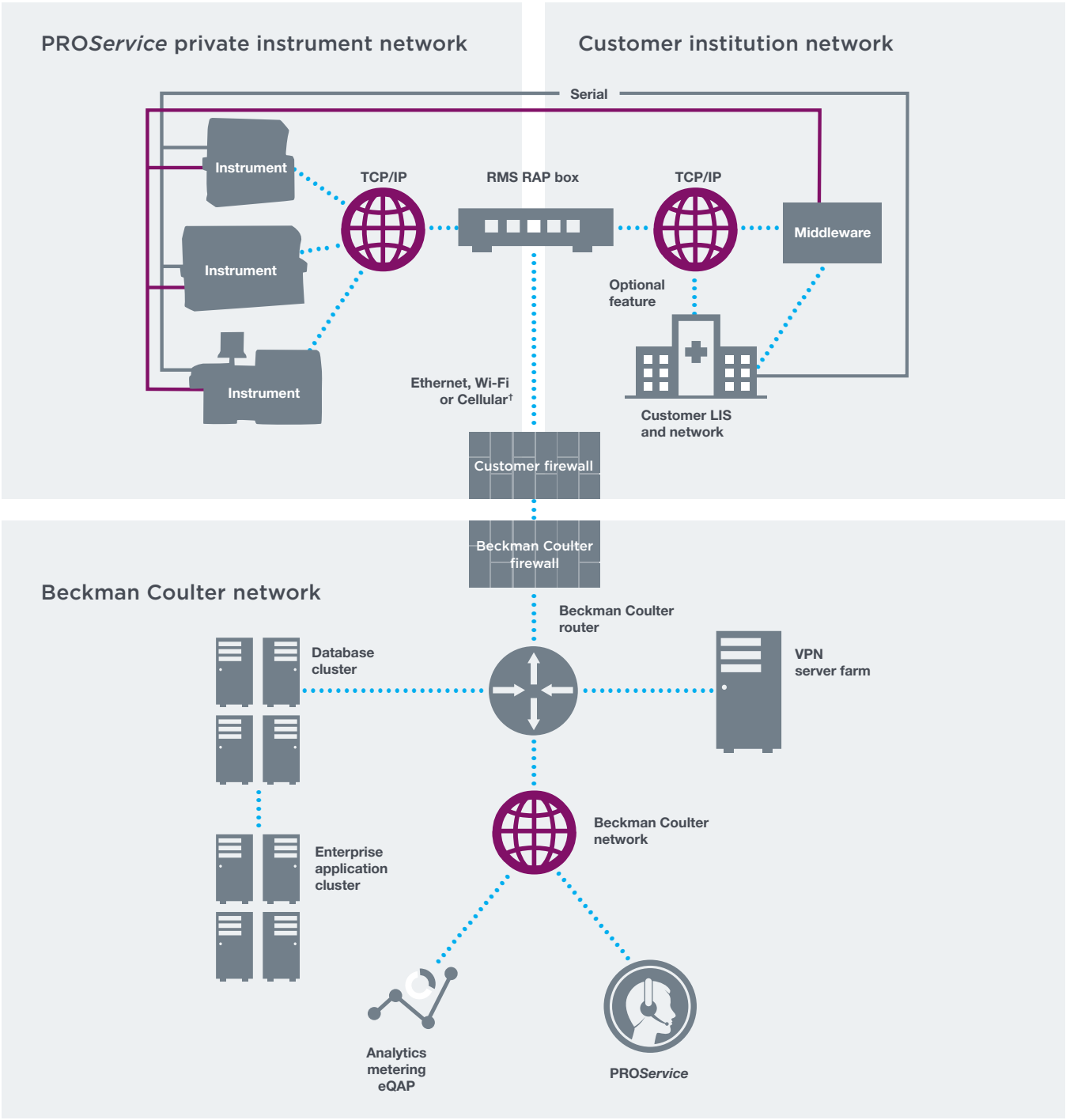


Figure 1. Standard RMS connection

Hardware

The RMS RAP box is a small, custom computer running Red Hat Enterprise Linux (RHEL). For reliability, it has a solid-state drive (SSD), fanless cooling and no moving parts. It has Ethernet ports for each connected instrument plus one for the network/Internet connection. Beckman Coulter performs all RMS RAP box software updates and maintenance, most of which is done remotely.

†Availability of Wi-Fi and cellular Internet connectivity varies by geography.

Software

The RMS RAP box includes a custom software stack running RHEL with appropriate updates. It uses OpenSSL for data in transit and a Federal Information Processing Standards (FIPS) 140-2 validated protocol.

The PRO*Service* enterprise software gathers and analyzes inputs from all connected instruments and performs lookups and comparisons to provide instrument status and health dashboards for the PRO*Service* support team. Instrument performance is compared against the body of evidence to raise alerts to the Beckman Coulter service and support staff for timely action.

Security

Appropriate configuration standards are applied to achieve and ensure data security (Figure 2). Specific areas include operating system configuration and security enhancements, web server security enhancements and message-processing security.

RMS RAP box operating system security enhancements

Security Technical Implementation Guides (STIGs)[1] are applied for RHEL version 5 and Desktop, including the following actions:

- Update all installed RHEL version 5 software Common Vulnerabilities and Exposures (CVE)
- Enhance physical access security
- Disable unnecessary user accounts and software
- Limit access to RMS RAP box files
- Enhance password to meet the U.S. Department of Defense (DoD) requirement by using FIPS 140-2 approved hashing algorithm
- Enhance network security per DoD requirement
- Disable interactive, unencrypted communication to RMS RAP Box
- Configure RHEL auditing per DoD requirement
- Enable remote audit logging
- Enable FIPS 140-2 approved ciphers for remote shell
- Enable basic input/output system (BIOS) authentication

RMS RAP box web server security enhancements

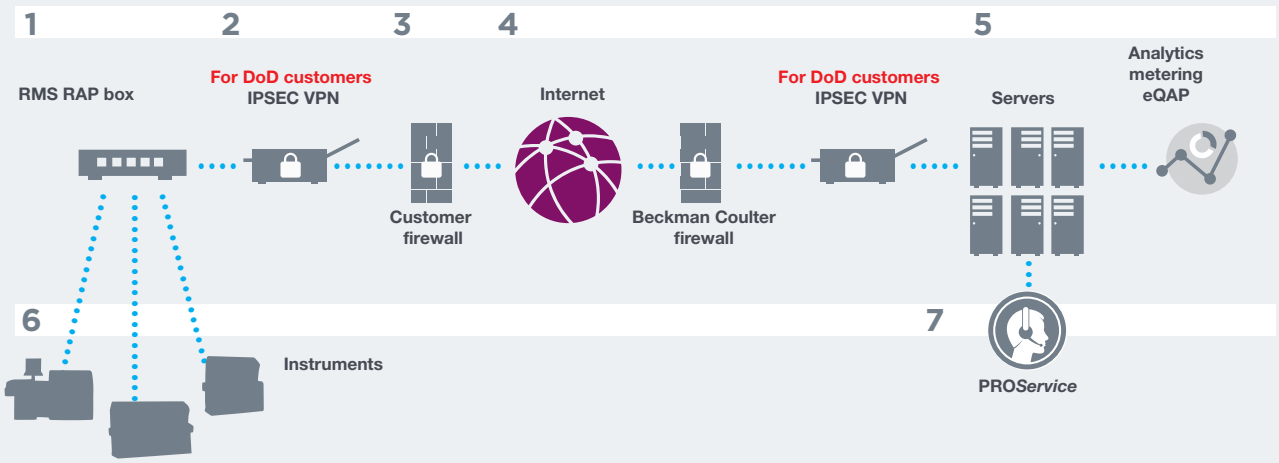
Applied STIGs for web servers include the following actions:

- Enable SSL to local web server
- Disable unnecessary Apache modules from loading
- Enable complete web server logging
- Display DoD network warning on all served pages (e.g., configuration pages, etc.)
- Restrict access to served pages
- Enhance network security per DoD requirement
- Disable all Common Gateway Interface scripts

RMS RAP box message processing security

The Application Security and Development (ASD) STIG[2] is applied, which includes the following:

- Enable FIPS 140-2 approved algorithm for data encryption using Java SunPKCS11 provider in FIPS mode
- Collect audit logs and update to remote server



1. RMS RAP box protects connected systems from network
2. IPSEC VPN provides additional security features for DoD customers
3. Communications pass through both customer and Beckman Coulter firewalls
4. Industry-standard encryption protects communications. RDS is protected from interception with VPN tunnel
5. Dual certificate authentication helps prevent unauthorized access to transmitted data
6. RDS requires manual, on-site approval
7. Beckman Coulter service and support staff access is customized by training, role and location. Three levels of access controls are used to authenticate users

Figure 2. Security features with IPSEC VPN option for Department of Defense (DoD)

Communications

There are two main forms of communication: regular status messaging and remote management sessions. Other features (benefits) are below.

- Regular status messages are sent from the RMS RAP box using HTTPS POST
- Remote management uses VPN sessions
- The system uses minimal bandwidth for messaging and only needs 128 kbps for a remote management session
- Communications are encrypted and only established between known, authorized addresses
- Remote service must be authorized by a user at the instrument in order to be addressed. A secure VPN tunnel is established only for the duration of that session
- The RMS RAP box's firewall rejects external communication requests
- The system can accommodate HTTP and Socket Secure (SOCKS) proxy servers. It requires Internet access with port 443 available, except in IPSEC VPN connections

ISA/
MOU

Communications security

Security features include two-way SSL authentication to secure all communication between your Beckman Coulter instruments and the Beckman Coulter data center.

Beckman Coulter leverages third-party certification authority to issue digital SSL certificates for verification of RMS RAP box identity.

The software encryption modules are National Institute of Standards and Technology-compliant, ensuring they are securely developed and maintained throughout the system's life cycle.[3]

VPN uses OpenVPN with OpenSSL in FIPS mode as well as two-way SSL authentication.

Interconnection Security Agreement and Memorandum of Understanding (ISA/MOU)

Beckman Coulter also completed the ISA/MOU with the U.S. Department of Veterans Affairs (VA) to connect and utilize all PRO*Service* features at all VA sites.

Summary

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

- Conforms to Information Security standards established by the industry, VA and DoD[4]
- 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
ASD STIG	The Application Security and Development Security Technical Implementation Guide: a series of application security requirements that apply to "all DoD developed, architected, and administered applications and systems connected to DoD networks"[4]
DoD	U.S. Department of Defense
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
IA	Information Assurance: DoD Information Assurance actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality and nonrepudiation
ISA/MOU	Interconnection Security Agreement and Memorandum of Understanding memorializes the agreement between the VA and Beckman Coulter regarding the management, operation and security of a connection between the Beckman Coulter RMS RAP box connected to laboratory instruments, owned by the VA, and PRO*Service*, owned by Beckman Coulter
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
SSL	Secure Sockets Layer: a session layer security protocol used on the Internet to secure web pages and transactions by means of public key cryptography
STIGs	Security Technical Information Guides: the Defense Information Systems Agency, part of the DoD, provides STIGs in various areas as guidance in best security practices. STIGs are configuration standards for the DoD IA and IA-enabled devices/systems. STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack
Triggers	A set of conditions that, when matched to instrument data, alerts the PRO*Service* support team
VA	U.S. Department of Veterans Affairs

References

[1] STIGs used to validate the PRO*Service* RMS RAP box system (iase.disa.mil/stigs/a-z.html):

- Red Hat Enterprise Linux 5
- Application Security and Development
- Apache Server for Unix
- Apache Site for Unix
- Network Policy
- Anti-malware
- Desktop Applications General

[2] Department of Defense. (2014) Application Security and Development Security Technical Implementation Guide, Version 3, Release 6, January 24, 2014. Retrieved from http://iase.disa.mil/stigs/app_security/app_sec/app_sec.html

[3] NIST (2014). Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules. Retrieved from http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm (1320 and 1384 Cryptographic Modules)

[4] NIST (2014). FIPS PUB 140-2 - Effective 15-Nov-2001: Security Requirements for Cryptographic Modules. Retrieved from http://csrc.nist.gov/groups/STM/cmvp/standards.html

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

ISA/MOU memorializes the agreement between VA and Beckman Coulter regarding the management, operation, and security of a connection between the Beckman Coulter RAP box connected to laboratory instruments, owned by VA, and PRO*Service*, owned by Beckman Coulter.

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

BR-52467

BECKMAN COULTER

Move healthcare forward.