

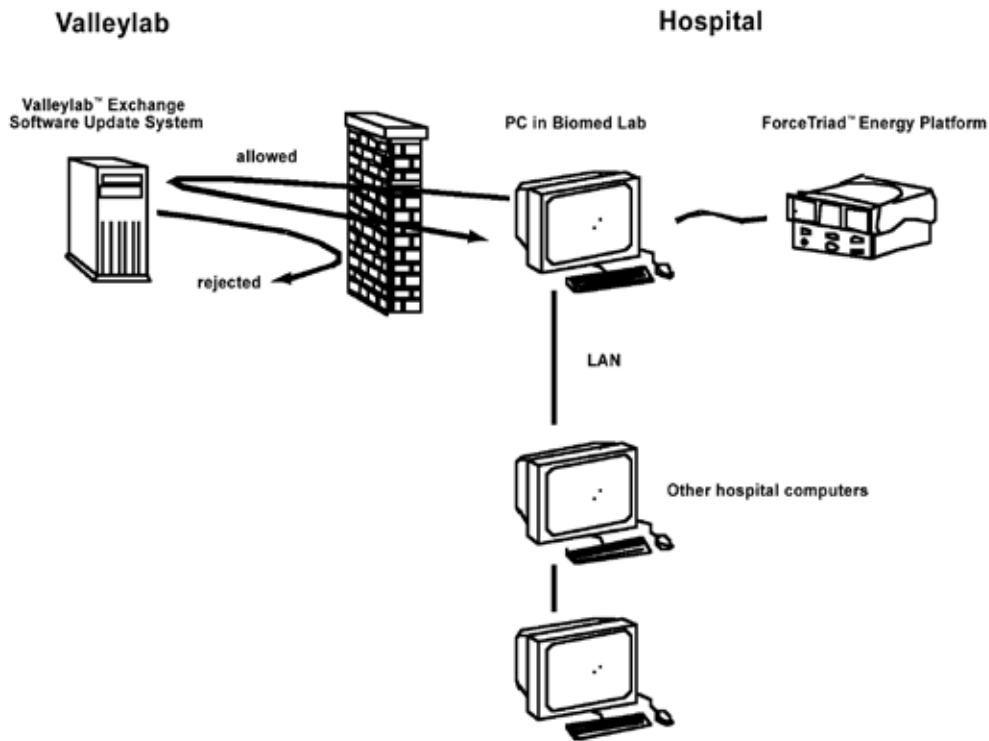
# An Overview of Valleylab™ Exchange Software Update System Features

Valleylab, Boulder, CO

The Valleylab™ Exchange Software Update System allows Valleylab to remotely upgrade ForceTriad™ energy platform software as new features and energy-delivery profiles become available. The remote upgrade capability eliminates the need to return the ForceTriad™ energy platform to Valleylab for software upgrades.

The Valleylab™ Exchange Software Update System is based on intelligent device management (IDM) technology from Qestra Corporation. The technology is designed to work with existing firewalls and security procedures. To enable your equipment to communicate with the Valleylab™ Exchange Software Update System enterprise server at our support center, the clinical engineering technicians install an “agent”— a small piece of software that can connect to the Valleylab ForceTriad™ energy platform into the PC being used for the communication. The hospital IT department will need to grant each Valleylab™ Exchange Software Update System-enabled PC the same standard Internet-access capabilities as other PCs. The software agent connects to Valleylab from behind the safety of your corporate firewall, adhering to all the security policies set up by the hospital network administrator and IT department. With Valleylab™ Exchange Software Update System, the clinical engineering technician’s PC operates like any other PC on the local area network.

Many other types of remote access solutions provide remote service connect over a variety of data communications, and may require virtual private networks (VPNs), dedicated telephone lines or special network connections. The Valleylab™ Exchange Software Update System does not require special connections. It uses the existing hospital security infrastructure, and works with your existing hospital firewalls and security policies.



### Protection from the Outside World

***The Valleylab™ Exchange Software Upgrade System does not come into the hospital network, but rather the software agent sends any necessary data out — the hospital PC network addresses are never revealed to the outside world. Since all communication is outbound, the hospital corporate network does not need to accept any connections from the outside or open up ports in order for the Valleylab™ Exchange Software Update System to do its job. Computers that are Valleylab™ Exchange Software Update System-enabled simply will not accept connections from any system or user outside the corporate firewall.***

Furthermore, whenever the software agent establishes a connection, it is via a standards-based tunnel not visible to unauthorized users who “listen in” at standard network ports. In fact, the only applications that can communicate with the Valleylab™ Exchange Service Agent are other Valleylab™ Exchange Software Update System applications or a Valleylab support technician using the Valleylab™ Exchange Software Update System management software. This means unauthorized entities cannot use the connection even if they “see” it.

All communications are **encrypted** using 256-bit secure socket layer (SSL) protocol.

## **Security for Data Privacy**

The Valleylab service team is interested only in receiving data about equipment performance and configuration to help maximize the productivity of the ForceTriad™ energy platform. The software agent therefore collects only diagnostic information relevant to service issues as well as configuration information to determine the compatibility of the software upgrade. Valleylab does not collect any customer or proprietary corporate information. Equipment performance data is stored for diagnostic use in a database accessible only by certified Valleylab support-team engineers with special authorization and permission.

## **Technical Details**

### *The Valleylab™ Exchange Software Upgrade System Does Not Require Changes to Existing IT Security*

The software agent supports dynamic host configuration protocol (DHCP), so there is no need to assign fixed IP addresses to each Valleylab™ Exchange Software Update System-enabled PC. Each PC communicates through the firewall via the agent, who initiates all communication with the Valleylab™ Exchange Software Update System server visible to the agent via a known IP address. Therefore, the clinical engineering technician's PC can communicate as a client in the same way that a Web browser accesses a Web site. By complying with the hospital's existing network security, firewalls and proxy servers, no changes to established procedures are needed to support remote software upgrade for the Valleylab™ Exchange Software Update System.

### *VPNs Not Required*

Since the agent is responsible for initiating two-way communication in a manner compliant with the secure computing environment at the device site, there is also no need for a virtual private network. The only requirement is an Internet connection.

### *Data Transmission*

The service agent communicates with the Valleylab™ Exchange Software Update System server via transmissions that require password authentication to validate the identity of devices exchanging information with the enterprise. The Valleylab™ Exchange Software Update System server supports transmission via proxy servers, and all data transmissions are encrypted using 128-bit (or higher) secure socket layer (SSL) protocol.

### *Data Collection*

Secure data transmission begins at the source with control over the types of data being collected for transmission. The agent software is set up to have access only to ForceTriad™ energy platform's performance and configuration data, and is not able to access any other data.

### *Remote Access*

For applications such as remote desktop or software management, the equipment operators and system administrators behind the corporate firewall have the protection of full control over file uploads, downloads and remote desktop access to their devices. Operators can grant or deny access to remote access sessions, software updates and applications access. If an issue arises, the clinical engineering technician can request a remote access session from Valleylab service personnel. The Valleylab™ Exchange Software Update System allows only authorized users at Valleylab to log in with username and password authentication. As further security, user login profiles control which customers and equipment the support technician can view, as well as the level of access allowed. All Valleylab user and system interactions are logged for audit purposes.

## Summary

The remote service solution from Valleylab is designed to meet hospitals' need for highly secure communication. As previously described, all data communications are secure and generated from behind customer firewalls. No changes to existing security procedures or costly VPNs are required. For more information, please do not hesitate to contact your Valleylab technical service team.

## Technical Specifications

The Valleylab™ Exchange Software Update System was built using Qestra's SecureLink technology specifically designed for secure, efficient intelligent device management (IDM) communications. The features include a hardened software design for application and data security with support for widely used industry standards such as TCP/IP, HTTP, SOAP and XML for the widest set of integration options. Browser interfaces are also based on industry-standard Java and HTML, while the enterprise software is built using J2EE for portability and extensibility.

### The Qestra technology supports:

#### Device Layer

- Built as an application intended for 24x7 operations in production environments with automatic restart in event of system or software failure
- Supports 128-bit (or higher) SSL encryption
- Requires password authentication for all communication with the enterprise
- Supports auditing of system events locally as well as on the enterprise, allowing local access to logs and audit files

#### Network Layer

- Supports 128-bit SSL encryption
- Uses polling server-based communications (to operate within the boundaries set by corporate firewalls)
- Supports load-balancing of network traffic

#### Enterprise Layer

- Provides SSL encryption as a default for all communications
- Requires username and password authentication
- Supports digital certificates for non-repudiation with human user and devices
- Supports user-level authorization for application functionality (limiting access to device and data views and interaction)
- Supports robust auditing of device and user interactions and system events