AN OVERVIEW OF THE SECURITY FEATURES OF **VALLEYLAB™ EXCHANGE**

DESCRIPTION

The Valleylab™ Exchange is a software tool based upon standard web services and cloud technology. The purpose of Valleylab™ Exchange is to enable Medtronic and healthcare facility personnel to upgrade Medtronic medical device software, administer licensed features, and collect service logs for performance monitoring, defect troubleshooting, and failure surveillance. Furthermore, Valleylab™ Exchange is designed to support future and existing Medtronic medical devices as they become available or are enabled for such support.

Valleylab™ Exchange comprises a hosted cloud services component (Server) and a PC/Laptop application component (Client).

The Server part of Valleylab™ Exchange maintains and tracks the medical device software/firmware upgrades, verifies the hardware and software compatibility, and provides a management console for system administrators. The Server is developed and maintained by Medtronic.

The Client part of Valleylab™ Exchange is a software application which is installed on the end-user's computers and is capable of communicating with Medtronic medical devices. The Client is the broker of communication between the Medtronic device and Valleylab™ Exchange, receiving data from the Server to upgrade the Medtronic medical device, and retrieving data from the device to forward to the Server. The Client is developed and maintained by Medtronic entities which develop Medtronic medical devices. Medtronic may supply different Clients for different medical device families.

DEVELOPMENT

The Valleylab™ Exchange was developed using Medtronic's experiences in Remote Medical Device Management (RMDM) — a solution to healthcare facilities to support the service requirements of ForceTriad™ electrosurgical generators. Medtronic is now extending this service to other devices in its portfolio.

The medical industry is highly regulated and extremely sensitive regarding information security and patient privacy. For this reason, Medtronic has leveraged its extensive enterprise IT security knowledge, and Class C level software development experiences, to design the technology behind Valleylab™ Exchange to meet strict commercial requirements for security.

SECURITY CONSIDERATIONS

Deployment

Valleylab™ Exchange is designed to have minimal impact on healthcare facility network security by utilizing any existing, healthcare facility firewalls and security procedures. To enable healthcare facility equipment to communicate with Valleylab™ Exchange, personnel, who are authorized by the healthcare facility, install a lightweight software Client on a PC or laptop which can be connected to Medtronic medical devices.

Healthcare facility IT department then grants each Valleylab™ Exchange-enabled computer the same, standard internet access capabilities given to other PCs. The software Client makes connections to Valleylab™ Exchange from behind the safety of the healthcare facility corporate firewall, adhering to all the security policies set up by the healthcare facility network administrator and IT department. This means that computers enabled for Valleylab™ Exchange can be configured the same as other facility computers to operate on the healthcare facility network. Since it is likely that healthcare facility computers have already been provisioned in a manner compatible with Valleylab™ Exchange, there is little work for the healthcare facility IT department to deploy Valleylab™ Exchange, other than install the Client on designated healthcare facility computers.

Medtronic
Further, Together

Unlike other remote management solutions that connect over a variety of data communications, Valleylab™ Exchange does not require use of virtual private networks (VPNs), dedicated telephone lines, cell network, or other special network connections. It's designed to be compliant with the healthcare facility's existing security infrastructure and policies. If the hospital firewall prevents packages from being downloaded, the software in the generator cannot be updated. For further assistance, please contact Medtronic Technical Support at: **valleylab.technicalservice@covidien.com**

PROTECTION FROM THE OUTSIDE WORLD

When the software Client communicates with the Server, it does so in a safe manner, consistent with standard secure web application design.

The existing, healthcare facility firewall remains the first line of defense against unauthorized users. In addition, the secure nature of the Valleylab™ Exchange communication flow, which acts as a second layer of defense, further defends against unauthorized users.

Valleylab™ Exchange does not initiate connection to devices on the healthcare facility network. Instead, the Client residing on a healthcare facility computer initiates the connection to Valleylab™ Exchange. The result is that healthcare facility network addresses are never revealed outside the existing healthcare facility firewall. Since all Valleylab™ Exchange communication initiation is outbound, the healthcare facility network does not need to allow any connections from the outside world nor open up additional ports to allow Valleylab™ Exchange to fulfill its function. Computers that are Valleylab™ Exchange-enabled will not accept connections from any system or user outside the existing facility firewall.

Furthermore, Client connections to the Server are implemented via a standards-based tunnel that is not visible to unauthorized entities, who may attempt to eavesdrop. Only healthcare facility or Medtronic personnel that have appropriate authorization and permission can access Valleylab™ Exchange. This means unauthorized entities cannot use the connection even if they "see" it.

Additionally, all communications between the Client and the Server are encrypted, using 1024-bit Secure Socket Layer (SSL) protocol. Valleylab™ Exchange also uses bidirectional digital certificates to authenticate the sender and recipient at both ends before any data are exchanged.

Finally, all Client software is updated via this secure network connection, thus ensuring that only Medtronic supplied software is used to access this service.

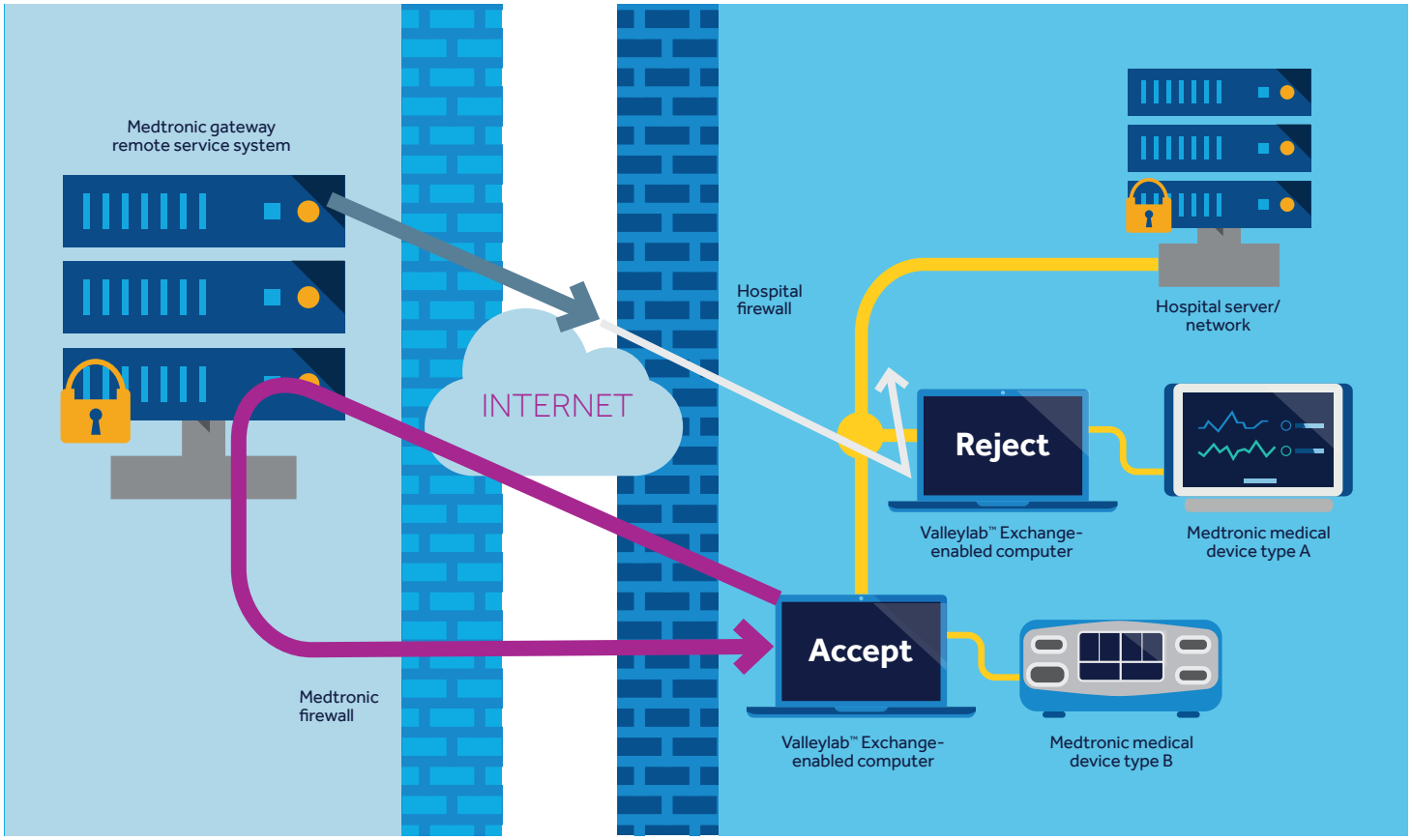

Figure 1: Valleylab™ Exchange connections originating internal to healthcare facility network are accepted

USERS

All users are trained or provided "Instructions for Use" in the appropriate use of Valleylab™ Exchange according to their role, and records of such training are maintained on the Server.

After users have been trained, they are given login credentials, as is standard practice for any secure application. Each user is associated with unique login credentials including user name, password, location, facility ID/name, and customer ID. To gain access to Valleylab™ Exchange, users must log in whether they are using the Client or a Valleylab™ Exchange or management console.

Login credentials are associated with role-based permissions. This means that a user who has permission to access one supported Medtronic medical device type may not necessarily have access to another. Other role permissions include the ability to downgrade software, administer Valleylab™ Exchange itself, and upload software for deployment.

A user's training records are also used as a filter, because a user may not access certain role activities until the user has been appropriately trained.

All user activity is tracked in a permanent manner, and user activity records are never deleted.

SECURITY FOR DATA PRIVACY

Medtronic receives only data that helps to maximize the productivity and performance of Medtronic medical devices in the healthcare facility. The Client therefore collects only device related diagnostic information and configuration information where it can so that Valleylab™ Exchange can determine the compatibility of the software upgrade or licensed features.† Valleylab™ Exchange does not collect patient information or any proprietary customer information. The device related information collected by the Client is stored for analysis in a database that is accessible only by authorized Medtronic personnel with appropriate privileges.

AUDIT TRAIL

All activity on Valleylab™ Exchange is logged. The audit trail is secured by a signed industry standard checksum.

TECHNICAL DETAILS

Why Changes to Existing IT Security Are Not Required

Each computer communicates through the healthcare facility firewall via the Client, which initiates all communication with Valleylab™ Exchange. Valleylab™ Exchange is visible to the Client via DNS addressable URLs over standard TCP/IP ports 443 and 8443. This means the healthcare facility IT department does not need to manage IP addresses or ports. Thus the Client can communicate with Valleylab™ Exchange in the same way that a web browser accesses a web site. By complying with the existing healthcare facility network security, firewalls, and proxy servers, there is no need to make any changes to established procedures to support Valleylab™ Exchange.

Why VPNs Are Not Required

Because the Client 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 to implement a virtual private network (VPN). The only requirement is an internet connection. However, a VPN option is available should the customer require it.

Data Transmission Security

The Client communicates with Valleylab™ Exchange via transmissions that require password authentication to validate the identity of personnel using the system and provide authorization for use based on their role. Valleylab™ Exchange supports transmission via proxy servers, and all data transmissions are encrypted using 1024-bit Transport Layer Security (TLS)/Secure Socket Layer (SSL) protocol. Valleylab™ Exchange also supports bidirectional digital certificates for TLS/SSL.

Data Collection Security

The collected data are encrypted on disk, both at the Client and on the hosted cloud environment. Additionally, Valleylab™ Exchange is fully Part 11 compliant.

SUMMARY

Valleylab™ Exchange is designed with highly secure communications in mind for healthcare facility environments. As described in this document, all data communications are secure and initiated from behind customer firewalls. No changes to a healthcare facility's existing security procedures. Costly VPNs and their complicated deployment needs are also not required. For more related information, please do not hesitate to contact your Medtronic sales person.

TECHNICAL SPECIFICATIONS

Valleylab™ Exchange was specifically designed for secure, efficient RMDM communications. This includes a hardened software design for application and data security with support for widely used industry standards such as TCP/IP, HTTP, and XML for the broadest 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.

Application Layer

- Built as an application hardened for 24x7 operations in production environments, with automatic restart in event of system or software failure

†Not supported on all devices.

- Supports 128-bit (or higher) TLS/SSL encryption
  • Requires user and role authentication for all communication with the enterprise
- Supports bidirectional digital certificates for authentication and encryption
- Supports auditing of system events locally as well as on the enterprise, allowing local access to logs and audit files

Network Layer

- Supports 1024-bit SSL encryption
- Utilizes polled web services communications (to operate within the boundaries set by corporate firewalls)
- Supports load balancing of network traffic

Enterprise Layer

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

5920 Longbow Drive
Boulder, CO 80301 800.722.8772 **medtronic.com/covidien**

Medtronic