

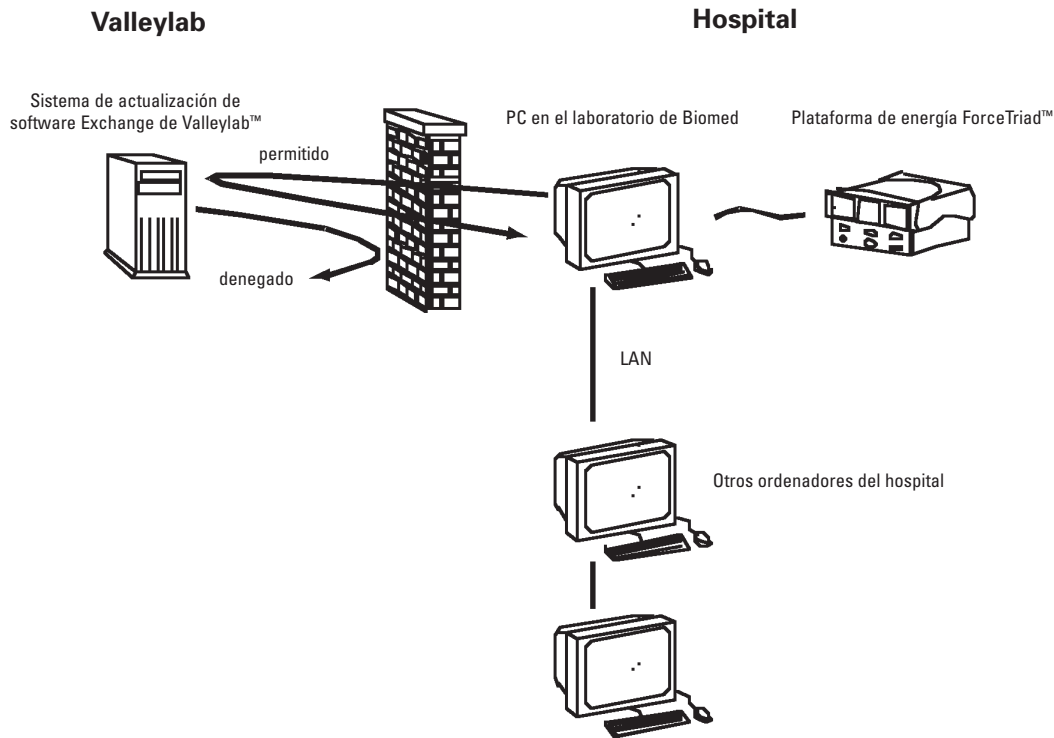
# Introducción a las características del Sistema de actualización de software Exchange de Valleylab™

Valleylab, Boulder, CO

El Sistema de actualización de software Exchange de Valleylab™ permite a Valleylab controlar remotamente el software de la plataforma de energía ForceTriad™ a medida que se disponga de las nuevas características y los perfiles de suministro de energía. La capacidad de actualización remota elimina la necesidad de devolver la plataforma de energía ForceTriad™ a Valleylab para incluir las actualizaciones de software.

El Sistema de actualización de software Exchange de Valleylab™ se basa en la tecnología de gestión inteligente de dispositivos (IDM) de Qestra Corporation. La tecnología está diseñada para funcionar con los procedimientos existentes de cortafuegos y de seguridad. Para que su equipo pueda comunicarse con el servidor de empresa del Sistema de actualización de software Exchange de Valleylab™ en nuestro centro de soporte, los técnicos de ingeniería clínica instalan un "agente"— un pequeño software que puede conectarse a la plataforma de energía ForceTriad™ de Valleylab en el PC que se está utilizando para la comunicación. El departamento de TI del hospital deberá conceder a cada PC con el Sistema de actualización de software Exchange de Valleylab™ las mismas capacidades estándares de acceso a Internet que otros PC. El agente del software se conecta a Valleylab desde detrás de la seguridad de su cortafuegos corporativo, cumpliendo todas las políticas de seguridad del administrador de red del hospital y del departamento de TI. Con el Sistema de actualización de software Exchange de Valleylab™, el PC del técnico de ingeniería clínica opera como cualquier otro PC de la red de área local.

Muchos otros tipos de soluciones de acceso remoto ofrecen conexión de servicio remoto a varias comunicaciones de datos y pueden requerir redes privadas virtuales (VPN), líneas de teléfono dedicadas o conexiones de red especiales. El Sistema de actualización de software Exchange de Valleylab™ no requiere conexiones especiales. Usa la infraestructura de seguridad existente en el hospital y funciona con sus cortafuegos y políticas de seguridad del hospital.



### Protección del mundo exterior

***El Sistema de actualización de software Exchange de Valleylab™ no se incluye en la red del hospital, sino que el agente del software envía los datos necesarios (las direcciones de red del PC del hospital nunca se revelan al mundo exterior). Como toda la comunicación es saliente, la red corporativa del hospital no necesita aceptar las conexiones del exterior ni abrir puertos para que el Sistema de actualización de software Exchange de Valleylab™ haga su trabajo. Los ordenadores habilitados para el Sistema de actualización de software Exchange de Valleylab™ simplemente no aceptarán conexiones desde cualquier sistema o usuario fuera del cortafuegos corporativo.***

Además, cuando el agente del software establezca una conexión, será mediante un túnel basado en estándares invisible a los usuarios no autorizados que "escuchen" en puertos de red estándares. De hecho, las únicas aplicaciones que pueden comunicarse con el agente de servicios Exchange de Valleylab™ son las otras aplicaciones del Sistema de actualización de software Exchange de Valleylab™ o un técnico de soporte de Valleylab que utilice el software de gestión del Sistema de actualización de software Exchange de Valleylab™. Esto significa que las entidades no autorizadas no pueden usar la conexión aunque la "vean".

Todas las comunicaciones están **encriptadas** con un protocolo de capas de zócalos seguros (SSL) de 256 bits.

## **Seguridad para la privacidad de datos**

El equipo de servicio de Valleylab sólo está interesado en recibir datos sobre rendimiento y configuración de equipos para ayudar a maximizar la productividad de la plataforma de energía ForceTriad™. Por lo tanto, el agente del software recopila sólo información de diagnóstico relevante para cuestiones de servicio e información de configuración para determinar la compatibilidad de la actualización del software. Valleylab no recopila información corporativa propietaria o de clientes. Los datos de rendimiento del equipo se almacenan para uso de diagnósticos en una base de datos a la que sólo pueden acceder ingenieros certificados del equipo de soporte de Valleylab con autorización y permiso especiales.

## **Detalles técnicos**

*El Sistema de actualización de software Exchange de Valleylab™ no requiere cambios en la seguridad de TI existente.*

El agente del software admite el protocolo de configuración de host dinámico (DHCP), por lo que no es preciso asignar direcciones IP fijas a cada PC habilitado con el Sistema de actualización de software Exchange de Valleylab™. Cada PC se comunica mediante el cortafuegos a través del agente, que inicia toda comunicación con el servidor del Sistema de actualización de software Exchange de Valleylab™ que ve el agente mediante una dirección IP desconocida. Por lo tanto, el PC del técnico de ingeniería clínica puede comunicarse como cliente del mismo modo que un explorador de Web accede a un sitio Web. Al cumplir con la seguridad de red, cortafuegos y servidores proxy existentes del hospital, no se necesitan cambios en procedimientos establecidos para admitir la actualización remota del software para el Sistema de actualización de software Exchange de Valleylab™.

### *VPN no necesarias*

Como el agente es responsable de iniciar la comunicación bidireccional de modo compatible con el entorno informático seguro del sitio del dispositivo, tampoco hay necesidad de una red privada virtual. El único requisito es una conexión de Internet.

### *Transmisión de datos*

El agente de servicio se comunica con el Sistema de actualización de software Exchange de Valleylab™ mediante transmisiones que requieren autenticación con contraseña para validar la identidad de dispositivos que intercambian información con la empresa. El servidor del Sistema de actualización de software Exchange de Valleylab™ admite la transmisión mediante servidores proxy, y todas las transmisiones de datos se encriptan con el protocolo de capa de zócalos seguros (SSL) de 128 bits (o más).

### *Recopilación de datos*

La transmisión de datos segura empieza en el origen controlando los tipos de datos que se recopilan para la transmisión. El software del agente se configura para tener acceso sólo a los datos de configuración y de rendimiento de la plataforma de energía ForceTriad™ y no puede acceder a otros datos.

### *Acceso remoto*

Para aplicaciones como el escritorio remoto, los operadores de equipos y los administradores de sistemas detrás del cortafuegos corporativo tienen la protección de control total en el acceso del escritorio remoto a sus dispositivos. Los operadores pueden conceder o denegar el acceso a sesiones de acceso remoto. Si surge un problema, el técnico de ingeniería clínica puede solicitar una sesión de acceso remoto desde el personal de servicio de Valleylab. El Sistema de actualización de software Exchange de Valleylab™ permite que sólo los usuarios autorizados de Valleylab inicien la sesión con la autenticación de nombre de usuario y contraseña. Para mayor seguridad, los perfiles de inicio de sesión de usuario controlan qué clientes y equipos puede ver el técnico de soporte, así como el nivel de acceso permitido. Todas las interacciones del sistema y de los usuarios de Valleylab se registran a efectos de auditorías.

## Resumen

La solución de servicio remoto de Valleylab está diseñada para satisfacer la necesidad de los hospitales de realizar comunicaciones muy seguras. Como se describió anteriormente, todas las comunicaciones de datos son seguras y se generan desde detrás de los cortafuegos del cliente. No se requieren cambios en los procedimientos de seguridad existentes ni VPN costosas. Para más información no dude en contactar con su equipo de servicio técnico de Valleylab.

## Especificaciones técnicas

El Sistema de actualización de software Exchange de Valleylab™ se creó utilizando la tecnología SecureLink de Questra diseñada para las comunicaciones seguras y eficientes de gestión inteligente de dispositivos (IDM). Las características son un diseño de software más robusto para la seguridad de aplicaciones y de datos con soporte de estándares muy usados en el sector como TCP/IP, HTTP, SOAP y XML para la gama más amplia de opciones de integración. Las interfaces del explorador también se basan en Java y HTML estándares del sector, mientras que el software de empresa se creó utilizando J2EE para la portabilidad y extensibilidad.

### La tecnología Questra admite:

#### Capa del dispositivo

- Creado como una aplicación para operaciones las 24 horas en entornos de producción con reinicio automático en caso de fallo del sistema o del software
- Admite encriptación SSL de 128 bits (o más)
- Requiere autenticación con contraseña para toda comunicación con la empresa
- Admite auditoría de actualizaciones de software realizada localmente y en la empresa, lo que permite el acceso local a registros y archivos de auditoría

#### Capa de red

- Admite encriptación SSL de 128 bits
- Utiliza comunicaciones basadas en servidor de consulta (para operar en los límites que establezcan los cortafuegos corporativos)
- Admite el equilibrio de carga del tráfico de red

#### Capa de empresa

- Ofrece encriptación SSL de forma predeterminada para todas las comunicaciones
- Requiere autenticación con nombre de usuario y contraseña
- Admite certificados digitales para el no repudio con usuarios humanos y dispositivos
- Admite la autorización a nivel de usuario para la funcionalidad de la aplicación (limitando el acceso a la interacción y vistas de datos y de dispositivos)
- Admite una auditoría robusta de interacciones de usuarios y dispositivos y eventos del sistema