

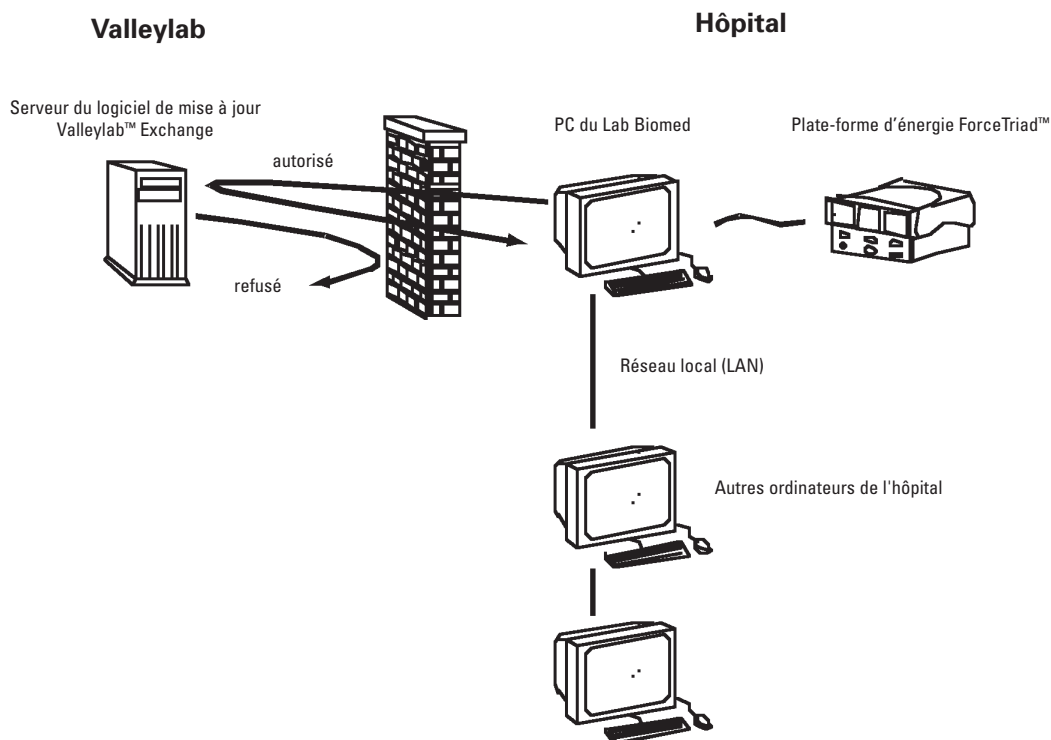
Un aperçu des fonctionnalités du système de mise à jour du logiciel Valleylab™ Exchange

Valleylab, Boulder, CO

Le système de mise à jour du logiciel Valleylab™ Exchange permet d'effectuer une mise à jour à distance de la plate-forme d'énergie ForceTriad™, au fur et à mesure de la disponibilité de nouvelles fonctionnalités et des de nouveaux paramétrages de délivrance du courant. La mise à jour à distance permet d'éliminer la nécessité de renvoyer la plate-forme d'énergie ForceTriad™ à Valleylab dans nos service techniques pour les mises à jour du logiciel.

Le système de mise à jour du logiciel Valleylab™ Exchange s'appuie sur la technologie de gestion intelligente du dispositif (IDM) de Questra Corporation. Cette technologie est conçue pour fonctionner avec les pare-feux et les procédures de sécurité. Pour permettre à votre équipement de communiquer avec le serveur d'entreprise du système de mise à jour du logiciel Valleylab™ depuis notre centre de support, les techniciens d'ingénierie biomédicale ont installé un « agent »— un petit logiciel capable de mettre en connexion la plate-forme d'énergie ForceTriad™ de Valleylab avec le PC utilisé pour la communication. Le département informatique de l'hôpital devra accorder à chaque PC prenant en charge le système de mise à jour du logiciel Valleylab™ Exchange les mêmes capacités d'accès internet standard que celles des autres ordinateurs. L'agent logiciel se connecte au serveur Valleylab derrière le pare-feu de votre entreprise, en adhérant aux stratégies de sécurité établies par l'administrateur du réseau de l'hôpital et le département informatique. Avec le système de mise à jour du logiciel Valleylab™ Exchange, le PC des techniciens d'ingénierie biomédicale fonctionne comme tout autre PC sur réseau local.

Plusieurs autres solutions d'accès à distance permettent également de fournir une connexion service distant pour divers types de communications de données ; elles nécessitent des réseaux privés virtuels (VPN), des lignes téléphoniques dédiées ou des connexions réseau spéciales. Le système de mise à jour du logiciel Valleylab™ Exchange ne nécessite aucune connexion spéciale. Il utilise l'infrastructure de sécurité de l'hôpital existante ; il fonctionne avec les pare-feux existants tout en adhérant aux stratégies de sécurité de l'hôpital.



Protection du monde extérieur

Au lieu d'accéder au réseau de l'hôpital, l'agent logiciel du système de mise à jour du logiciel Valleylab™ Exchange lui transmet toutes les données nécessaires — ainsi les adresses réseaux PC de l'hôpital ne sont jamais dévoilées au monde extérieur. Les communications étant toutes en sortie, le réseau d'entreprise de l'hôpital n'a besoin d'accepter aucune connexion de l'extérieur ni d'ouvrir de ports de communication pour que le système de mise à jour du logiciel Valleylab™ puisse faire son travail. Les ordinateurs prenant en charge le système de mise à jour du logiciel Valleylab™ Exchange n'accepteront de connexions d'aucun système ni d'utilisateurs hors du pare-feu de l'entreprise.

En outre, chaque fois que l'agent logiciel établit une connexion, celle-ci s'effectue via un canal basé sur des standards non visibles à des utilisateurs non autorisés capables « d'écouter » des ports réseaux standard. En fait, l'agent de service Valleylab™ Exchange ne peut communiquer qu'avec d'autres applications du système de mise à jour du logiciel Valleylab™ ou bien avec un technicien de Valleylab utilisant le logiciel de gestion du système de mise à jour du logiciel Valleylab™ Exchange. Ainsi, toute entité non autorisée ne pourra pas utiliser la connexion même si celle-ci est visible.

Toutes les communications sont **cryptées** grâce au protocole SSL (secure sockets layer) 256 bits.

Confidentialité des données sécurisée

L'équipe de service Valleylab ne s'intéresse qu'aux données de performance et de configuration de l'équipement, et ce uniquement pour optimiser la productivité de la plate-forme d'énergie ForceTriad™. Par conséquent, l'agent logiciel ne recueille que les informations de diagnostic pertinentes aux problèmes de service ainsi que les informations de configuration, afin de déterminer la compatibilité de la mise à jour du logiciel. Valleylab ne collecte aucune information propriétaire de l'entreprise ou sur les clients. Les données de performance de l'équipement sont stockées à des fins de diagnostic, dans une base de données accessibles uniquement à des ingénieurs de l'équipe de support technique Valleylab ayant reçu une autorisation spéciale.

Détails techniques

Le système de mise à jour du logiciel Valleylab™ Exchange ne nécessite aucune modification de la sécurité informatique existante.

L'agent logiciel prend en charge le protocole DHCP (Dynamic Host Configuration Protocol), de sorte qu'il n'est pas nécessaire d'attribuer des adresses IP fixes à chaque PC équipé du système de mise à jour du logiciel Valleylab™ Exchange. Chaque PC communique avec le pare-feu via l'agent, qui initie toutes les communications avec le serveur du système de mise à jour du logiciel Valleylab™ Exchange visible à l'agent via une adresse IP connue. Ainsi, le PC des techniciens d'ingénierie biomédicale communique en tant que client de la même manière qu'un navigateur Web accède à un site Web. Le système de mise à jour du logiciel Valleylab™ Exchange étant en conformité avec les normes des serveurs proxy, des pare-feux et de la sécurité réseau existants de l'hôpital, la mise à jour à distance du logiciel ne nécessitera aucune modification des procédures établies.

Réseaux privés virtuels non requis

L'échange des communications étant initié par l'agent au site du périphérique, en conformité avec un environnement informatique sécurisé, il n'est pas nécessaire d'avoir recours à un réseau privé virtuel. Il suffit seulement d'avoir une connexion internet.

Transmission des données

L'agent de service communique avec le serveur du système de mise à jour du logiciel Valleylab™ Exchange en transmettant des données qui nécessitent une authentification par mot de passe pour valider l'identité des périphériques échangeant les informations avec l'entreprise. Le serveur du système de mise à jour du logiciel Valleylab™ Exchange prend en charge la transmission via un serveur proxy ; toutes les données transmises sont cryptées grâce au protocole SSL (secure sockets layer) 128 bits (ou supérieur).

Collecte des données

La transmission sécurisée des données commence en premier par le contrôle des types de données à collecter pour la transmission. L'agent logiciel n'est configuré que pour avoir accès aux données de configuration et de performance de la plate-forme d'énergie ForceTriad™, à l'exclusion de tout autre type de données.

Accès à distance

Pour les applications telles que Bureau à distance, les opérateurs du matériel et les administrateurs système peuvent travailler sous la protection de pare-feu d'entreprise et disposent d'un contrôle total de l'accès à distance du bureau de leurs périphériques. Les opérateurs peuvent accorder ou refuser l'accès aux sessions d'accès à distance. En cas de problème, le technicien d'ingénierie biomédicale a la possibilité de saisir directement le personnel de service Valleylab pour effectuer une session d'accès à distance. Seuls les utilisateurs autorisés par Valleylab peuvent se connecter, par authentification du nom d'utilisateur et du mot de passe, au système de mise à jour du logiciel Valleylab™ Exchange. Par mesure de sécurité supplémentaire, des profils de connexion utilisateur sont utilisés pour contrôler ce que le technicien est autorisé à visualiser : client, matériel et niveau d'accès. Toutes les interactions utilisateur et système sont enregistrées à des fins d'audit.

Récapitulatif

La solution service à distance de Valleylab est conçue pour satisfaire aux besoins de communication hautement sécurisés des hôpitaux. Comme décrit plus haut, toutes les communications de données sont sécurisée et générées derrière les pare-feux du client. Le service ne nécessite aucune modification des procédures de sécurité existantes ni de réseaux privés virtuels. Pour plus d'informations, n'hésitez pas à contacter votre équipe de service technique Valleylab.

Caractéristiques techniques

Le système de mise à jour du logiciel Valleylab™ Exchange est construit avec la technologie efficace et sécurisée SecureLink de Qestra, spécialement conçue pour les communications IDM (gestion intelligente des périphériques). Il comporte les fonctionnalités suivantes : conception logicielle durcie pour la sécurité des données et des applications avec prise en charge des normes industrielles telles que TCP/IP, HTTP, SOAP et XML pour intégrer la plus vaste gammes d'options. En outre, les interfaces navigateur sont conformes aux normes industrielles Java et HTML, tandis que le logiciel d'entreprise est extensible et portable car il est construit sur la plate-forme J2EE.

La technologie Qestra prend en charge :

Couche physique

- Application conçue pour fonctionner 24 h sur 24 en environnement de production avec redémarrage automatique en cas de défaillance du système ou du logiciel
- Prise en charge du cryptage SSL 128 bits (ou supérieur)
- Nécessite l'authentification par mot de passe pour toutes les communications avec l'entreprise
- Prise en charge de l'audit des mises à jour du logiciel réalisées localement et en entreprise, autorisant l'accès local aux enregistrements et fichiers d'audit

Couche réseau

- Prise en charge du cryptage SSL 128 bits
- Utilisation de communications serveur par interrogation (pour un fonctionnement dans les limites fixées par les pare-feux)
- Prise en charge de l'équilibrage de charges du trafic réseau

Couche entreprise

- Cryptage SSL par défaut pour toutes les communications
- Nécessite l'authentification du nom d'utilisateur et du mot de passe
- Prise en charge de certificats numériques pour le non-rejet d'utilisateurs physiques et de périphériques
- Prise en charge de l'autorisation niveau utilisateur pour la fonctionnalité de l'application (limitation de l'accès à la visualisation du périphérique et des données et à l'interaction)
- Prise en charge d'un audit robuste des interactions périphérique utilisateur et des événements du système