

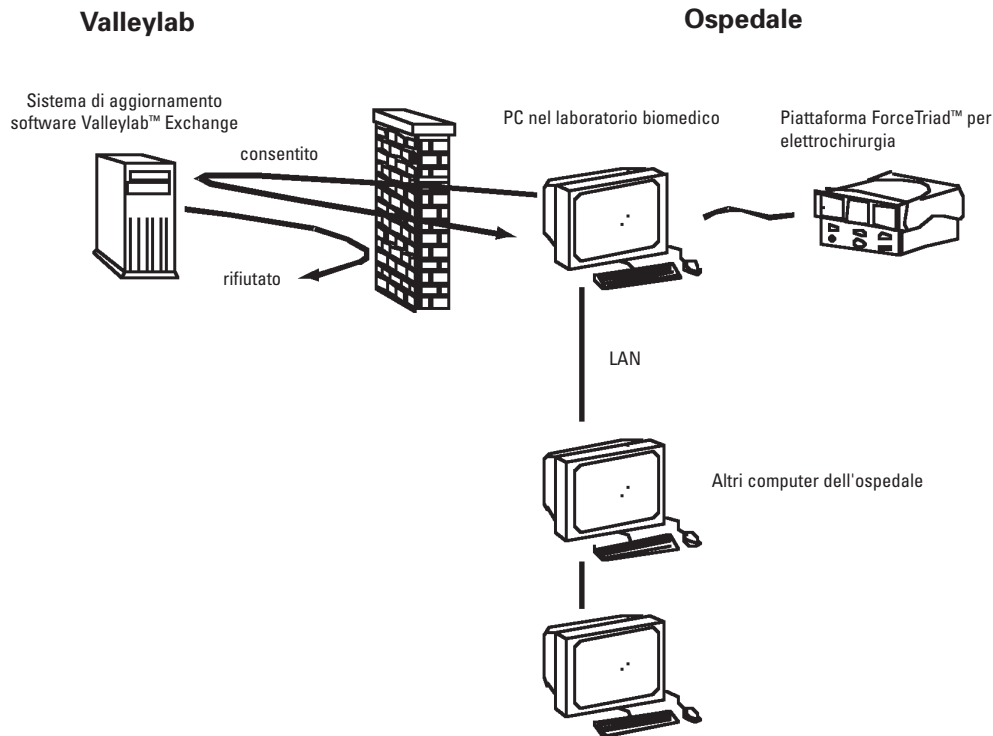
Panoramica sulle caratteristiche del sistema di aggiornamento del software Valleylab™ Exchange

Valleylab, Boulder, CO

Il sistema di aggiornamento del software Valleylab™ Exchange consente a Valleylab di aggiornare a distanza il software della piattaforma per elettrochirurgia ForceTriad™ quando si rendono disponibili nuove caratteristiche e nuovi profili di erogazione di energia. La capacità di aggiornamento a distanza elimina la necessità di restituire la piattaforma ForceTriad™ per elettrochirurgia a Valleylab per gli aggiornamenti di software.

Il sistema di aggiornamento del software Valleylab™ Exchange si basa sulla tecnologia di gestione intelligente dei dispositivi (IDM) di Questra Corporation. Questa tecnologia è stata progettata per funzionare con firewall e procedure di sicurezza già esistenti. Per consentire alle proprie apparecchiature di comunicare con il server aziendale del sistema di aggiornamento del software Valleylab™ Exchange al nostro centro di assistenza, i tecnici di ingegneria clinica installano un "agente"— un piccolo software in grado di collegarsi con la piattaforma per elettrochirurgia ForceTriad™ Valleylab nel PC utilizzato per la comunicazione. Il reparto informatico della struttura sanitaria dovrà garantire a ciascun PC abilitato per il sistema di aggiornamento del software Valleylab™ Exchange le stesse capacità di accesso standard ad Internet degli altri PC. L'agente software si collega a Valleylab al riparo della sicurezza del proprio firewall aziendale, aderendo alle politiche di sicurezza impostate dall'amministratore di rete dell'ospedale e dal reparto informatico. Con il sistema di aggiornamento del software Valleylab™ Exchange il PC del tecnico di ingegneria clinica opera come qualunque altro PC della LAN.

Molti altri tipi di soluzioni di accesso remoto offrono connessione di assistenza a distanza su una varietà di comunicazioni dati, e possono rendere necessarie reti virtuali private (VPN), linee telefoniche dedicate o connessioni a reti speciali. Il sistema di aggiornamento del software Valleylab™ Exchange non richiede collegamenti speciali. Esso utilizza l'infrastruttura di sicurezza della struttura sanitaria e funziona con firewall e procedure di sicurezza già esistenti.



Protezione dal mondo esterno

Il sistema di aggiornamento del software Valleylab™ Exchange non entra nella rete della struttura sanitaria, è invece l'agente software a far uscire eventuali dati necessari — gli indirizzi della rete di PC della struttura non vengono mai rivelati al mondo esterno. Dal momento che tutte le comunicazioni sono dirette all'esterno, la rete aziendale della struttura sanitaria non ha la necessità di accettare collegamenti dall'esterno o aprire porte perché il sistema di aggiornamento del software Valleylab™ Exchange faccia il suo lavoro. I computer abilitati per il sistema di aggiornamento del software Valleylab™ Exchange non accettano semplicemente collegamenti da nessun sistema o utente al di fuori del firewall aziendale.

Inoltre, ogni qualvolta l'agente software stabilisce una connessione, questo avviene attraverso un tunnel basato su standard, non visibile a utenti non autorizzati "in ascolto" alle porte standard di rete. Infatti, le sole applicazioni che possono comunicare con l'agente di servizio del Valleylab™ Exchange sono altre applicazioni del sistema di aggiornamento del software Valleylab™ Exchange o un tecnico dell'assistenza Valleylab che usa il software di gestione del sistema di aggiornamento del software Valleylab™ Exchange. Questo significa che la connessione non può essere utilizzata da utenti non autorizzati, anche se riescono a "vederla".

Tutte le comunicazioni sono **criptate** utilizzando il protocollo secure socket layer (SSL) a 256 bit.

Sicurezza per la riservatezza dei dati

Il team di assistenza di Valleylab è interessato unicamente a ricevere dati sulla performance e sulla configurazione delle apparecchiature per contribuire all'ottimizzazione della produttività della piattaforma ForceTriad™ per elettrochirurgia. L'agente software raccoglie quindi solo informazioni diagnostiche pertinenti ai problemi di assistenza, oltre a informazioni di configurazione, per stabilire la compatibilità dell'aggiornamento del software. Valleylab non raccoglie alcuna informazione di clienti o nessun dato proprietario dell'azienda. I dati sulla performance delle apparecchiature vengono memorizzati per uso diagnostico in un database accessibile, unicamente a tecnici del team di assistenza Valleylab in possesso di autorizzazioni e permessi speciali.

Dettagli tecnici

Il sistema di aggiornamento del software Valleylab™ Exchange non richiede modifiche ai dispositivi di sicurezza informatica

L'agente software supporta il protocollo dynamic host configuration protocol (DHCP), quindi non è necessario assegnare indirizzi fissi IP a ciascun PC abilitato per il sistema di aggiornamento del software Valleylab™ Exchange. Ciascun PC comunica attraverso il firewall mediante l'agente, che avvia la comunicazione con il server del sistema di aggiornamento del software Valleylab™ Exchange visibile all'agente stesso mediante ad un indirizzo IP conosciuto. Per questo motivo, il PC del tecnico di ingegneria clinica è il grado di comunicare in qualità di client con le stesse modalità con cui un browser web accede ad un sito web. Poiché si conforma al sistema di sicurezza della rete ospedaliera esistente, ai firewall e ai server proxy, non sono necessarie alcune modifiche alle procedure stabilite per supportare l'aggiornamento remoto del software per il sistema di aggiornamento del software Valleylab™ Exchange.

VPN non necessarie

Poiché l'agente ha il compito di avviare la comunicazione bi-direzionale in una modalità compatibile con la sicurezza dell'ambiente informatico del sito del dispositivo, non c'è neppure la necessità di una virtual private network (VPN). Il solo requisito è una connessione ad Internet.

Trasmissione dati

L'agente di servizio comunica con il sistema di aggiornamento del software Valleylab™ Exchange mediante trasmissioni che richiedono l'autenticazione della password per convalidare l'identità dei dispositivi che scambiano informazioni con l'azienda. Il server del sistema di aggiornamento del software Valleylab™ Exchange supporta la trasmissione via server proxy e tutte le trasmissioni dei dati sono criptate mediante il protocollo secure socket layer (SSL) a 128 bit (o maggiore).

Raccolta dati

La trasmissione sicura dei dati inizia alla fonte con il controllo sui tipi di dati che vengono raccolti per la trasmissione. L'agente software viene configurato per avere accesso unicamente ai dati di performance e di configurazione della piattaforma per elettrochirurgia ForceTriad™ e non è in grado di accedere a nessun altro dato.

Accesso remoto

Per applicazioni quali un desktop remoto, gli operatori delle apparecchiature e gli amministratori di sistema al di là del firewall aziendale hanno la protezione totale sull'accesso remoto da desktop ai loro dispositivi. Gli operatori possono concedere o negare l'accesso alle sessioni di accesso remoto. Se sorgono problemi, il tecnico di ingegneria clinica può richiedere una sessione di accesso remoto da parte del personale di assistenza Valleylab. Il sistema di aggiornamento del software Valleylab™ Exchange consente unicamente il log on con nome utente e password ad utenti autorizzati presso Valleylab. Come ulteriore sicurezza, i profili con login utente controllano quali clienti e apparecchiature può visualizzare il tecnico di supporto, oltre al livello di accesso consentito. Tutti gli utenti Valleylab e le interazioni di sistema effettuano l'accesso a scopi di revisione.

Riepilogo

La soluzione di assistenza a distanza di Valleylab è stata ideata per rispondere alla necessità di comunicazioni altamente sicure delle aziende sanitarie. Come precedentemente descritto, tutte le comunicazioni dati sono sicure e generate al di là dei firewall di clienti. Non sono necessari cambiamenti a procedure di sicurezza esistenti né costose VPN. Per maggiori informazioni, non esitare a contattare il proprio team di assistenza tecnica Valleylab.

Specifiche tecniche

Il sistema di aggiornamento del software Valleylab™ Exchange è stato creato utilizzando la tecnologia SecureLink di Questra, ideata in modo specifico per comunicazioni sicure ed efficienti di gestione intelligente dei dispositivi (IDM). Tra le caratteristiche vi è un modello di software 'hardened' per la sicurezza delle applicazioni e dei dati con il supporto di standard ampiamente utilizzati nel settore, quali TCP/IP, HTTP, SOAP e XML, per offrire il massimo delle opzioni di integrazione. Inoltre le interfacce dei browser sono basate su Java e HTML, standard del settore, mentre il software aziendale viene creato utilizzando J2EE per garantire la portabilità e l'estensibilità.

La tecnologia Questra supporta:

Device Layer

- Creato come applicazione indicata per le operazioni 24 ore su 24 7 giorni su 7 in ambienti produttivi con riavvio automatico in caso di interruzione del sistema o del software
- Supporta il criptaggio SSL a 128 bit (o maggiore)
- Richiede l'autenticazione della password per qualunque comunicazione con l'azienda
- Supporta la revisione degli aggiornamenti del software eseguiti localmente oltre che sull'azienda, consentendo l'accesso locale a file di registro e audit

Network Layer (strato di rete)

- Supporta il criptaggio SSL a 128 bit (o maggiore)
- Utilizza comunicazioni di polling (interrogazione) basate su server (per operare con i limiti impostati dai firewall aziendali)
- Supporta bilanciamenti di carichi di traffico di rete

Enterprise Layer

- Offre criptaggio SSL di default per tutte le comunicazioni
- Richiede autenticazione di nome utente e password
- Supporta certificati digitali di non ripudio nei confronti di utenti umani e dispositivi
- Supporta l'autorizzazione di livelli di utenti per la funzionalità applicativa (limitando l'accesso alla visualizzazione di dati e di dispositivi e per l'interazione)
- Supporta una energica revisione di interazione di dispositivi, utenti e eventi sistema