

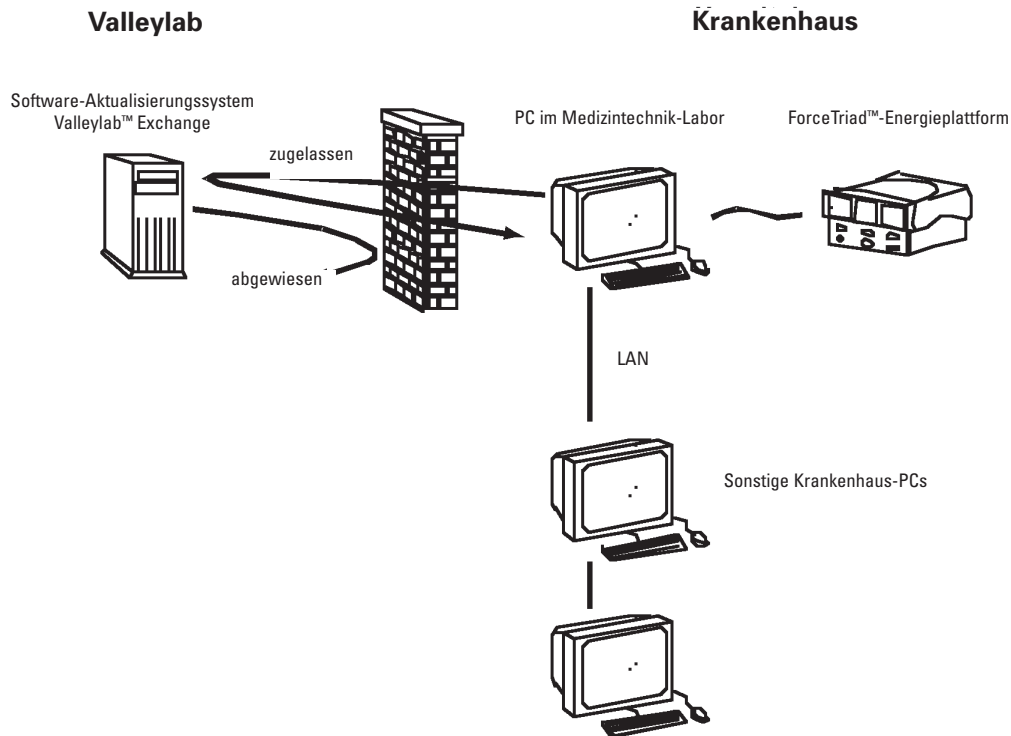
Funktionen des Valleylab™ Exchange Software-Aktualisierungssystems im Überblick

Valleylab, Boulder, CO

Das Software-Aktualisierungssystem Valleylab™ Exchange ermöglicht Valleylab die ferngesteuerte Aktualisierung der ForceTriad™-Energieplattform-Software, sobald neue Funktionen und neue Modi zur Energiabgabe zur Verfügung stehen. Die Möglichkeit der ferngesteuerten Aktualisierung macht es überflüssig, die ForceTriad™-Energieplattform zur Software-Aktualisierung an Valleylab zurückzusenden.

Das Software-Aktualisierungssystem Valleylab™ Exchange basiert auf intelligenter Gerätemanagement-Technologie (IDM; intelligent device management) der Questra Corporation. Die Technologie wurde für die Zusammenarbeit mit bestehenden Firewalls und Sicherheitsverfahren konstruiert. Damit Ihre Energieplattformen mit dem in unserem Support Center installierten Datenserver für das Software-Aktualisierungssystem Valleylab™ Exchange kommunizieren können, installieren die Techniker der medizintechnischen Abteilung einen sogenannten "Agenten" — eine kleine Software, die es der ForceTriad™-Energieplattform ermöglicht, durch den verwendeten PC zu kommunizieren. Die IT-Abteilung des Krankenhauses muss zur Nutzung des Agenten jedem für das Software-Aktualisierungssystem Valleylab™ Exchange aktivierten PC dieselben Standardmöglichkeiten zur Internetnutzung gewähren wie für sonstige PCs. Der Software-Agent stellt aus dem geschützten Bereich hinter Ihrer internen Firewall aus eine Verbindung mit Valleylab her, die den von Netzwerkadministrator und IT-Abteilung eingerichteten Sicherheitsrichtlinien voll entspricht. Mit dem Software-Aktualisierungssystem Valleylab™ Exchange lässt sich der PC des Medizintechnikers wie alle PCs des LAN betreiben.

Viele andere von Lösungen für den Remote-Zugriff bieten Remote-Service-Verbindungen über eine Reihe von Datenkommunikationen. Sie können Virtuelle Private Netzwerke (VPN), spezielle Datenleitungen, Telefonleitungen oder spezielle Netzwerkverbindungen erfordern. Das Software-Aktualisierungssystem Valleylab™ Exchange erfordert aber keine speziellen Verbindungen. Es greift auf die bestehende Sicherheitsinfrastruktur des Krankenhauses zurück und arbeitet mit Ihren bestehenden Firewalls und Sicherheitsrichtlinien.



Schutz vor der Außenwelt

Das Software-Aktualisierungssystem Valleylab™ Exchange dringt nicht in das lokale Netzwerk ein, sondern vielmehr sendet der Software-Agent die erforderlichen Daten hinaus — die Netzwerkadressen der lokalen PCs werden also der Außenwelt gegenüber keinesfalls sichtbar gemacht. Da alle Kommunikationsvorgänge nach außen gerichtet sind, muss das interne Netzwerk keine von der Außenwelt ausgehenden Verbindungen akzeptieren oder Ports öffnen, damit das Software-Aktualisierungssystem Valleylab™ Exchange seine Arbeit machen kann. Für das Software-Aktualisierungssystem Valleylab™ Exchange aktivierte PCs werden keine Verbindung von irgendeinem System oder Benutzer außerhalb der internen Firewall akzeptieren.

Zusätzlich verlaufen alle vom Software-Agenten hergestellten Verbindungen durch einen auf Standards basierenden Tunnel, der für nicht-autorisierte Benutzer Standard Ports "abhören" nicht sichtbar ist. Genaugenommen sind die einzigen Anwendungen, die mit dem Valleylab™ Exchange Service-Agenten kommunizieren können, andere Applikationen des Software-Aktualisierungssystems Valleylab™ Exchange oder ein Valleylab-Supportmitarbeiter, der die Management-Software des Software-Aktualisierungssystems Valleylab™ Exchange verwendet. Also können unautorisierte Ressourcen die Verbindung nicht nutzen, selbst wenn sie sie "sehen" könnten.

Alle Kommunikationsvorgänge werden über ein SSL-Protokoll mit 256 bit **verschlüsselt**.

Datenschutz

Das Valleylab-Serviceteam ist nur an Daten über die Leistung und Konfiguration der Ausstattung interessiert, um die Produktivität der ForceTriad™-Energieplattform zu maximieren. Daher sammelt der Software-Agent nur diagnostische Informationen, die für die Wartung relevant sind, sowie Konfigurationsinformationen, um die Kompatibilität der Software-Aktualisierung zu bestimmen. Valleylab sammelt keinerlei kundenbezogene oder firmeninterne Informationen. Leistungsbezogene Daten werden für den diagnostischen Gebrauch in einer Datenbank gespeichert, auf die nur zertifizierte Supporttechniker von Valleylab mit besonderen Befugnissen zugreifen können.

Technische Details

Das Software-Aktualisierungssystem Valleylab™ Exchange erfordert keine Änderung an den bestehenden IT-Sicherheitseinstellungen

Der Software-Agent unterstützt DHCP (dynamic host configuration protocol), sodass kein Bedarf an einer Zuweisung fester IP-Adressen an für das Software-Aktualisierungssystem Valleylab™ Exchange aktivierten PCs besteht. Jeder PC kommuniziert durch die Firewall über den Agenten, der die gesamte Kommunikation mit dem Server des Software-Aktualisierungssystems Valleylab™ Exchange initiiert. Dieser wird dem Agenten durch eine bekannte IP-Adresse angezeigt. Dadurch kann der PC eines Technikers der medizintechnischen Abteilung genau so als Client kommunizieren, wie ein Webbrowser auf eine Website zugreift. Durch die Kompatibilität mit den bestehenden Netzwerksicherheitseinstellungen, Firewalls und Proxy-Servern sind keine Änderungen an den üblichen Verfahren erforderlich, um die ferngesteuerte Aktualisierung durch das Software-Aktualisierungssystem Valleylab™ Exchange zu ermöglichen.

VPNs nicht erforderlich

Da der Agent mit der geräteseitigen sicheren Rechenumgebung kompatibel ist, besteht auch kein Bedarf an einem VPN. Es ist lediglich ein Internetzugang erforderlich.

Datenübertragung

Der Service-Agent kommuniziert mit dem Softwareaktualisierungssystem Valleylab™ Exchange durch Übertragungen, die zur Authentifizierung ein Passwort erfordern, um die Identität von Geräten zu validieren, die Informationen mit dem Unternehmen austauschen. Der Server des Software-Aktualisierungssystems Valleylab™ Exchange unterstützt die Übertragung via Proxy Server, wobei alle Datenübertragungen anhand eines SSL-Protokolls mit 128 Bit oder mehr verschlüsselt werden.

Datenerhebung

Die sichere Datenübertragung bereits an der Quelle mit der Kontrolle der für die Übertragung erhobener Daten. Der Software-Agent wird so eingerichtet, dass er nur auf die Leistungs- und Konfigurationsdaten der ForceTriad™-Energieplattform Zugriff hat.

Fernzugriff

Bei Anwendungen wie etwa Remote Desktop haben Gerätebediener und Systemadministratoren hinter der internen Firewall den Schutz einer vollständigen Kontrolle über den Zugriff auf den Desktop ihrer Geräte. Benutzer können Fernzugriffs-Sitzungen den Zugang gewähren oder verweigern. Wenn ein Problem auftritt, kann der Techniker der medizintechnischen Abteilung vom Valleylab-Wartungspersonal eine Fernzugriffs-Sitzung anfordern. Das Softwareaktualisierungssystem Valleylab™ Exchange gibt nur autorisierten Benutzern bei Valleylab die Möglichkeit, sich mit Benutzername und Kennwort anzumelden. Als weitere Sicherheitsmaßnahme entscheiden Login-Profile darüber, welche Informationen zu Kunden und Geräten der Support-Techniker einsehen kann und welche Zugriffsebene zugelassen wird. Alle Interaktionen zwischen Valleylab-Benutzer und Valleylab-System werden zu Prüfungszwecken protokolliert.

Zusammenfassung

Die Remote-Service-Lösung von Valleylab ist für den bei Krankenhäusern vorherrschenden Bedarf an hochgradig sicherer Kommunikation konstruiert. Wie bereits beschrieben, sind alle Kommunikationsvorgänge sicher und werden aus dem sicheren Bereich hinter der Firewall des Kunden generiert. Es sind keine Änderungen an bestehenden Sicherheitseinstellungen oder kostspielige VPNs erforderlich. Weitere Informationen bitten wir Sie von Ihrem Valleylab-Serviceteam zu erfragen.

Technische Daten

Das Software-Aktualisierungssystem Valleylab™ Exchange wurde anhand von Questras SecureLink -Technologie speziell für die entwickelt. Zu den Merkmalen gehört ein robusteres Software-Design für die Sicherheit von Anwendungen und Daten mit dem Support weit verbreiteter Industrienormen wie TCP/IP, HTTP, SOAP und XML. Browser-Schnittstellen basieren ebenfalls auf standardmäßigem Java und HTML, während die Enterprise-Software zur Erhöhung der Portabilität und Erweiterbarkeit mit J2EE konstruiert wird.

Folgende Komponenten werden von der Questra-Technologie unterstützt:

Device Layer

- Eine Anwendung für den pausenlosen Betrieb in Produktionsumgebungen mit automatischer Wiedereinschaltung im Falle eines System- oder Softwarefehlers.
- Unterstützt SSL-Verschlüsselung mit 128 Bit oder mehr
- Erfordert bei allen Kommunikationsvorgängen mit dem Unternehmen eine Passwort-Authentifizierung
- Unterstützt Bestandsaufnahmen von Software-Aktualisierungen, die lokal sowie im Unternehmen durchgeführt werden und den lokalen Zugriff auf Protokolle und Bestandsaufnahme-dateien

Network Layer

- Unterstützt SSL-Verschlüsselung mit 128 Bit
- Verwendet serverbasierte Kommunikationsvorgänge (innerhalb der von internen Firewalls gesetzten Grenzen)
- Unterstützt den Lastenausgleich beim Network-Traffic

Enterprise Layer

- Bietet SSL-Verschlüsselung als Standardeinstellung für alle Kommunikationsvorgänge
- Erfordert Anmeldung mit Benutzername und Kennwort
- Unterstützt digitale Zertifikate zur Non-Repudiation von Benutzer und Gerät
- Unterstützt die Autorisierung für die Funktionalität aus Benutzerebene (und schränkt damit den Zugriff und Geräte- und andere Daten und Interaktionen ein)
- Unterstützt robuste Bestandsaufnahmen von Interaktionen zwischen Benutzer und Gerät und von Systemereignissen