smiths medical
bringing technology to life

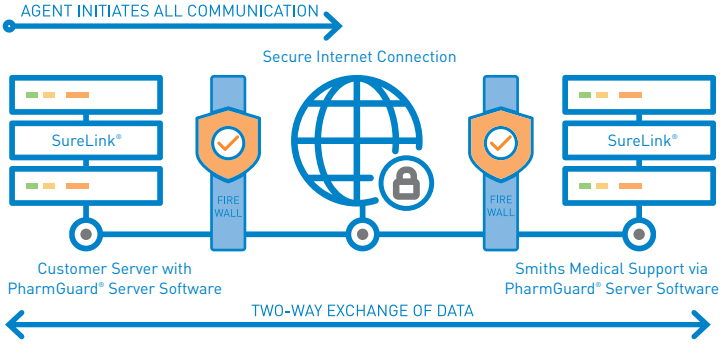
WHITE PAPER

PharmGuard® SureLink® Remote Support Software System Security

Connecting any computer to the internet raises security concerns, and connecting intelligent devices is no different. Whether hackers are trying to harm a device with corrupt data or viruses, steal data traveling between the device and manufacturer, or gain unauthorized access to critical information, software systems must guard against these and other security threats.

PharmGuard® SureLink® remote support software includes a suite of software products that allows remote devices to exchange information with people and enterprise business systems. The transportation and handling of this information must be done in a secure manner to protect trade secrets and potentially sensitive end-user information. PharmGuard® SureLink® software is designed to address key information security concerns with features that:

- Maintain network security integrity
- Conceal data from unauthorized parties
- Confirm that system users are authenticated
- Limit each user to specific data, views, and actions



MAINTAINING NETWORK SECURITY INTEGRITY

To avoid security breaches, most devices connected to the internet are not directly addressable from outside the company. That is because most of the computers connected to the internet are located within a corporate information technology environment or call into an internet service provider (ISP) and are therefore assigned local, often temporary, IP addresses unique only within the company or ISP network. This IP address may belong to the device only while it is connected. When that device leaves the network, the address is assigned to the next computer that connects. As a result, the only computers typically connected directly to the internet are a company's main web site, and only these computers are given globally unique and publicly visible IP addresses.

Network administrators also prefer that their computers and devices are hidden from the outside world behind secure firewalls, routers, and proxy servers. This enables users within the facility to have full access to the internet while proactively helping to prevent any outside people or applications from gaining visibility or access to the computers within the facility.

PharmGuard® SureLink® software overcomes these constraints with patented Firewall-Friendly™ communication technology that lets remote devices exchange information securely with PharmGuard® SureLink® software Enterprise servers – even when devices are hidden behind corporate firewalls. PharmGuard® SureLink® software's technology for device-initiated communications is based on standard Hypertext Transfer Protocol (HTTPS) and Extensible Markup Language (XML) standards. With PharmGuard® SureLink® software, the remote devices initiate all communications with a PharmGuard® SureLink® software enterprise server located at a globally visible address. This enables devices to be deployed in many different locations without requiring modification of security settings within the local network environment.

In simpler terms, if a web browser can access the internet using a network connection, the PharmGuard® SureLink® software-enabled device can perform two-way communications with the PharmGuard® SureLink® software enterprise server using that same network connection.

This method of communication:

- Leverages existing security infrastructure at the device location. The device receives the same network security coverage as all other computers within the facility.
- Simplifies device deployment. The local IT staff does not need to change their existing security configuration. Once connected to the local network, the device is ready to communicate.
- Secures the device from attack. Since the device initiates all communication only to a specified server, and does not have a public IP address, there is little opportunity for an attacker to exploit the communication to access the device.

FACILITATING DATA CONFIDENTIALITY

Much of the information that travels across the public internet uses plain text encapsulated within standard HTTP messages. Hackers can gain network access at a point close to the source or destination of the message and then capture and view the text of these HTTP messages with readily available tools.

Similarly, the operational data from deployed devices is susceptible to unauthorized access while it is in transit. Taken out of context, this information has little or no value. However, if captured in quantity, the information may expose private customer data or sensitive business details.

PharmGuard® SureLink® software helps solve this problem by encrypting the message contents sent between the device and the enterprise, so that only the applications at each end can decode them. PharmGuard® SureLink® software uses Secure Sockets Layer (SSL) to provide secure transmission of data. SSL provides a protocol for transmitting private data via the internet. In addition to encrypting data, the SSL standard also provides authentication to verify that both the sender and receiver of data are known to each other. SSL supports key length up to 168 bits and mutual authentication using certificates. PharmGuard® SureLink® software can also enable secret key AES 256-bit message encryption, which may be used with SSL to encrypt data beyond the Demilitarized Zone (DMZ).

PharmGuard® Software to PharmGuard® SureLink® Software Enterprise Server

PharmGuard® SureLink® software initiates all communication with the PharmGuard® SureLink® software enterprise server. This intelligent agent enables the software to act as a web client, and initiates messages to the PharmGuard® SureLink® software enterprise server that are sent as HTTP POST commands. Each message contains data encoded in XML format and may be encrypted through a SSL connection from the PharmGuard® SureLink® software agent to the PharmGuard® SureLink® software enterprise server. The encryption method is selected during system install and the same encryption method is used for all agents. For applications that require device authentication and data encryption, Smiths Medical recommends using SSL.

ADDRESSING OTHER SECURITY ISSUES

Automatic Logoff

Data is at risk whenever a computer is left on and unattended with an open application. Anybody can sit down at that computer and access data, regardless of whether or not permission was granted. To help prevent this situation, PharmGuard® SureLink® software applications require a user to log in again after ten minutes of inactivity. The inactivity period is adjustable in the configuration of the PharmGuard® SureLink® software enterprise server.

Audit Log

The PharmGuard® SureLink® software enterprise server maintains an audit log of significant user actions that occur in the system. Examples of audited functions include user logins, trigger creation or modification, and PharmGuard® SureLink® software access application sessions. The audit log provides a method for the system administrator to analyze the user actions when tracing an event.

SUMMARY

PharmGuard® SureLink® software has been designed to leverage the power of the internet while verifying that the data handled by the system is protected. Smiths Medical maintains an active involvement in internet security matters.

SureLink Remote Support Software

PharmGuard® SureLink® Software from Smiths Medical is powered by Axeda. **www.axeda.com**

PRODUCT(S) DESCRIBED MAY NOT BE LICENSED OR AVAILABLE FOR SALE IN CANADA AND OTHER COUNTRIES

Smiths Medical ASD, Inc.
6000 Nathan Lane North
Minneapolis, MN 55442, USA
Tel: 1-614-210-7300
Toll-Free USA: 1-800-258-5361

MPAUCA-1690

Rx ONLY

smiths medical

Find your local contact information at: www.smiths-medical.com/customer-support /contact-us