Technology and Security Overview:
CARESTREAM Smart Link Remote Management Services

Carestream Health has adopted an innovative technology to provide the most effective remote service offering in the industry. This document is intended for Carestream customers, particularly IT managers and administrators, and describes the configuration, security, and technology of Smart Link Remote Management Services (Smart Link RMS).

Smart Link RMS allows Carestream to deploy remote services securely over the Internet to equipment installed behind customer firewalls. The solution is designed for high performance and security at every level of its architecture.

Using Web services to establish secure outbound communication over the Internet, Smart Link RMS links Carestream equipment to CARESTREAM Smart Link Enterprise Servers. Your equipment can provide performance data, alerts, and alarms to our support team, resulting in proactive, rapid service and support with advanced remote troubleshooting capabilities. No patient and user information is collected by Smart Link RMS.

Feature	Benefit
Device monitoring	Automatic alert notifications to the service team. No customer action required.
Consolidated device data history stored for each device	Advanced troubleshooting through comprehensive device performance history.
Remote management and desktop control	Ease of training. Rapid troubleshooting and fixes.
Remote diagnostics	Rapid troubleshooting and fixes.
Software management	Convenient, timely, and secure software updates.
Centralized remote service and support	Rapid responses and after-hours support capabilities.

Table 1: Features and Benefits

Solution Components

The two major technical components of Smart Link RMS are the Agent and the Server.

Agent	Server
Is installed at customer sites; embedded software is installed directly on the medical device.	Resides within Carestream authorized remote data centers.
Handles Smart Link RMS functions at the customer site.	Communicates with the Agent using secure Web services.
• Establishes secure communications to the Server through the Internet. • Sends machine data and log files to the Server. • Monitors device performance and sends alarm to the Server. • Supports remote download and deployment of software updates from the Smart Link Enterprise Server.	• Processes the data files and alarms from the Agent. • Is the management console for Smart Link Remote Services.

Table 2: Technical Components

The Server allows the Carestream support team to:

- Consolidate and analyze data.
- Run diagnostics remotely.
- Set automated rules for taking action when specific events occur.
- Specify security and access to customer devices.
- Set up software updates for distribution.

Solution Configuration

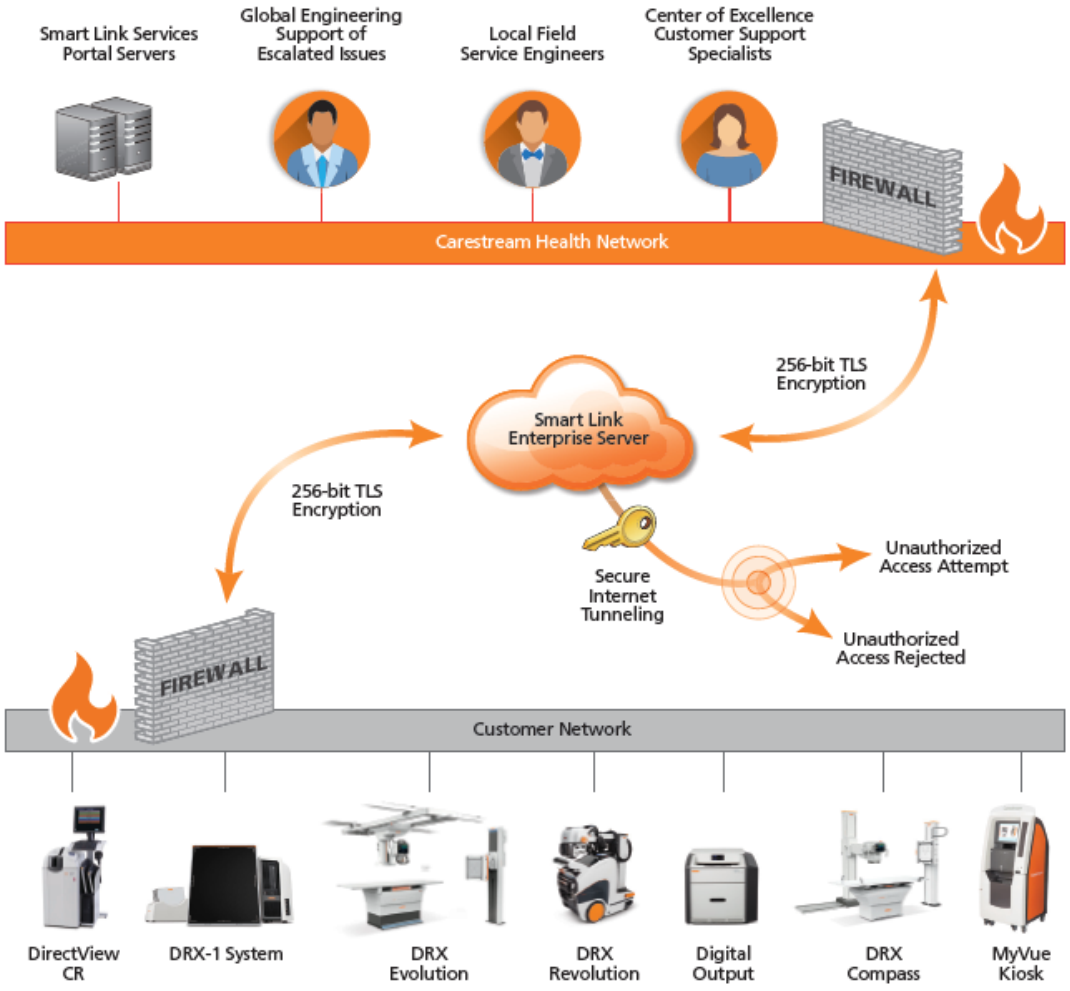
The Agent makes a connection to the Smart Link Enterprise Server from within the safety of your corporate firewall, adhering to your security policies. There is no need for any special changes to a proxy Server.

Within your network, the Agent is like another personal computer on the LAN. Setting up the Agent at your site requires:

- A physical or wireless connection to an existing LAN (TCP/IP)
- Outbound Internet access for the device (or through a proxy)

A Carestream Field Service Engineer (FE) will set up the Agent on the device(s) and configure network connections according to your IT requirements.

Figure 1: Devices with the Smart Link RMS Agent are configured in the same way as any other network-enabled computing device on your LAN.



Carestream

Technology and Security

The Agent is efficient and will not affect the optimal performance of your equipment, due to three main design features:

- The Agent polls the device at manageable intervals of 60 seconds.
- The Agent can transmit data to the Server at scheduled times or when an error code indicates that immediate notification is needed.
- The messaging protocol delivers small, efficient (0.5-3 KB) messages; Smart Link RMS communications will not affect the network bandwidth.

Network Security

The goal of Smart Link RMS is to support your existing network standards and security practices, while maintaining a high level of secure communications and data confidentiality. Smart Link RMS only requires an outbound connection over port 443 (https). Carestream does not require your IT department to make exceptions to established IT policies that would compromise your firewall. Smart Link RMS applies security to three layers: device, network, and enterprise. The layers are built using technology designed for secure, efficient Smart Link communications.

The technology includes:

- A hardened software design for application and data security
- Support for industry standards such as TCP/IP, HTTPS, SOAP, and XML

Device Layer	Network Layer	Enterprise Layer
• Is hardened for 24x7 operations in production environments; automatically restarts in the event of a system or software failure • Runs as a system service rather than as an application • Supports 256-bit TLS encryption • Supports digital certificates for end-point authentication • Supports auditing of medical device system events locally as well as on the Smart Link Enterprise Server, allowing local access to logs and audit files	• Supports 256-bit TLS encryption • Utilizes polling Server-based communications to operate within corporate firewalls • Supports load balancing of network traffic	• Provides TLS encryption as a default for all communications • Requires username and password authentication • Supports digital certificates for increased security • Supports user-level authorization for application functionality, limiting access to devices, data views, and interactions • Supports robust auditing of device access, user interactions and system events

Table 3: Technical Specifications for Security at Each Layer

No Special Ports

Other manufacturers' remote access solutions may mandate the use of a specific port number. The network administrator must then configure the firewall so that connections to a specific TCP port, such as 5631, on the public side of the firewall are mapped to port 5631 at the device, requiring a static IP address assigned to the device. If there are multiple devices on the enterprise LAN, additional devices must be assigned different, static, nonstandard ports on the firewall.

In that scenario, the firewall must be configured so that only authorized devices establish connections on those specific ports, placing more burden on the network administrator. Unauthorized users could also scan for the specific port and use protocols to discover what is on that connection. **The Smart Link RMS Agent does not require a special port.**

No Fixed IP Address Is Required for Communication

The Agent's ability to communicate with the Enterprise Server is independent of the supported device's IP address. Typical firewall configurations allow outbound connections to initiate securely from behind the firewall, over port 443 (https). The Agent communicates through the firewall using port 443 and initiates outbound communication to the Smart Link RMS Enterprise Server. Since all communication is outbound, your corporate network does not need to accept connections from the outside or open additional ports. Equipment enabled for Smart Link RMS will not accept connections from any system outside the customer's corporate firewall.

Only Connects to the Smart Link Enterprise Server

An important issue for IT managers is whether a connection is with Smart Link Enterprise Server or with an unknown entity. If the Agent listens on a TCP port while waiting for a connection, the device could become a potential target for unauthorized access. With Smart Link RMS, Carestream can guarantee the identity of the Smart Link Enterprise Server for the connecting Smart Link Agent using digital certificates. Therefore, identity is never an issue. The Agent sends an encrypted request for new instructions to the trusted Smart Link Enterprise Server and then only acts upon responses received from the trusted Smart Link Enterprise Server.

Flexibility

The Service Agent is not dependent on a static IP address or subnets and supports corporate network infrastructures that require Internet proxy servers (auto-configuration proxy,HTTP proxy). The Agent's flexibility and compatibility can accommodate changing network infrastructures.

Secure Tunnel Exclusive to Users of Smart Link Remote Services

Once the Agent establishes a secure point-to-point tunnel with Smart Link Enterprise Server, the connection is visible only to Smart Link RMS clients and services (users and applications). Unauthorized clients and services that attempt to occupy a free TCP port and protocol cannot use the connection or establish a new connection. Therefore, unauthorized entities cannot use the connection, even if they can see it.

VPN-Free Security

The Agent initiates a bi-directional communication tunnel that is compliant with the secure computing environment at the customer site, removing the need for a hardware-supported virtual private network (VPN). The Agent requires only an Internet connection. This is less complicated and less costly than supplying, configuring, and maintaining VPN hardware.

Carestream service personnel and Carestream equipment are in the different network, while VPN personnel are in the same network.

In addition, Carestream service personnel can only access Carestream equipment through Smart Link RMS servers. All other equipment on the same network is NOT visible to Carestream. While through VPN, the entire network and all resources are open to users.

Secure Data Transmission

All data transmissions are encrypted using 256-bit TLS protocol, the same technology that banks use for secure, online, financial transactions. The Smart Link RMS device agents validate digital certificates with the Smart Link Enterprise Server before accepting requests or sending data.

Secure Data Collection

The Agent only collects device data relevant to the performance and usage of your equipment. Carestream does not collect or store your confidential or proprietary information. Carestream monitors data such as error codes, log files, and other device properties that assist with equipment troubleshooting, performance trending, and problem resolution. Remote desktop access to equipment using Smart Link RMS requires strict adherence to Carestream's policy (as outlined in the service training), which is GDPR compliant as it does NOT collect, transmit, or store any personal information.

Secure Server Access

At the enterprise level, Smart Link Enterprise Server only allows users authorized by Carestream to log in with username and password authentication. User login profiles control which customers, equipment, and files the user can access as well as the level of access allowed. All remote access sessions are logged for audit purposes. Customers can also enable remote desktop notification. Once enabled, customers will be notified when a remote desktop request is initiated. If the customer does not respond, the remote desktop request will be rejected automatically.

Conclusion

Carestream is committed to continually improving your service experience by investing in and implementing new support methods. Smart Link RMS uses current technology to provide an optimized and simplified service approach for your Carestream product, while complying with critical regulations around security and privacy. For more information, contact your local Carestream representative, or visit www.carestream.com/smart-link-services.

Carestream