CAPSULE SUPPORT ACCESS

Secure Connectivity & Monitoring that Works with Your IT Environment

This document describes the architecture and security features of Capsule Support Access. It is intended to help hospitals better understand how Capsule Support Access operates and how it meets your technical security requirements.

When one of your device interfaces is down or not functioning properly your facility is at risk of losing data, affecting patient care.

Capsule Support Access is a maintenance service for your medical device information system. It's designed to maintain performance and maximize uptime while reducing burden on your IT personnel or infrastructure. Capsule Support Access monitors operating parameters, and configuration of the SmartLinx server(s) in your facility. It does this through a software-based monitoring Agent that communicates securely with the Capsule Service Cloud.

THE SERVICE CLOUD EVALUATES THE PERFORMANCE OF YOUR SOLUTION AND PROVIDES A SECURE OPTION FOR REMOTE ACCESS IF HANDS ON DIAGNOSTIC TROUBLESHOOTING IS REQUIRED.

- Diagnostics identify issues to decrease unscheduled downtimes and eliminate trial and error troubleshooting via operator assistance through screen sharing and control
- Monitors the versions in use including Device Driver Interfaces (DDIs) and Data Management Modules (DMMs) to optimize utilization, effectiveness and awareness of product utilization

HOW IT WORKS

Capsule Support Access is comprised of two major components: the Remote Access Agent, which is software running on each SmartLinx server, and the Capsule Service Cloud hosted in ISO certified data centers.

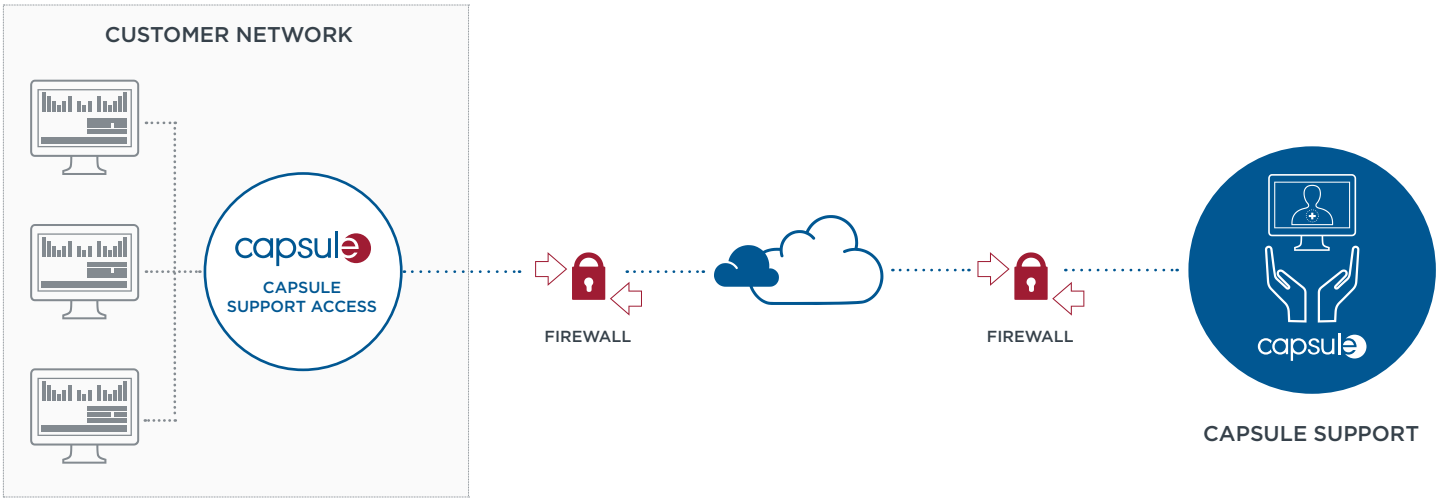
The Agent software monitors the SmartLinx server on a regular basis checking the status of key data elements that provide a picture of system setup and configuration and communicates this information with the Service Cloud environment.

Capsule Support Access leverages your existing network and security infrastructure. As long as the Agent can open an outbound connection to the Cloud Server using port 443, no changes are required in order for remote connectivity and monitoring to be established.

The secure communication method does not require the Agent server to have a fixed or publicly visible TCP/IP address. The Service Cloud will never initiate an inbound connection to the Agent. The Agent initiates all communications with the Service Cloud and Two-way communication will only occur after the connection has been initiated and authenticated. The Agent monitors a specific set of parameters and sends only data changes to the Service Cloud.

No patient, location or medical device results are sent.

Once a minute, the Agent sends a small message to the Service Cloud as a form of "heartbeat" to confirm the Agent is active. These messages enable Capsule support personnel to queue action requests, for instance to request an error log or initiate a remote session. The next time the agent "checks in," the request is delivered.



SYSTEM REQUIREMENTS & SECURITY

Capsule Support Access works within the SmartLinx MDIS infrastructure. No specific VPN or Public IP address is required. The technology provides two-way communication based on Hypertext Transfer Protocol (HTTP) with Secure Socket Layer (SSL) encryption. All communication is outbound on standard SSL port 443, requiring no other ports to be opened. Public or static IP addresses are not required. The communication is compatible with Proxy servers, Network Address Translation (NAT), and Virtual Local Area Networks (VLANs).

Any connectivity approach must provide layers of security to protect confidential information and access while at the same time not violating or changing existing security strategies of your IT policies or infrastructure.

CAPSULE SUPPORT ACCESS IS DESIGNED TO ADDRESS KEY INFORMATION SECURITY CONCERNS WITH FEATURES THAT

- **Protect data using strong encryption:** All communication between your SmartLinx server and the Capsule Service Cloud uses Secure Socket Layer/Transport Layer Security Protocol (SSL/TLS) with industry-standard, 2048-bit key encryption, using strong ciphers to protect confidentiality.
- **Protect against spoofing with connection validation:** The SSL/TLS protocol enables integrity and nonrepudiation of communications. The protocol requires the Agent to authenticate the server before posting data through the encrypted connection.
- **Ensure that system users are authenticated:** All access to the system is centrally controlled, requiring strong password authentication. All user actions are fully audited for traceability
- **Operate in a secure cloud infrastructure:** The Service Cloud is operated in ISO 27001:2005-certified data centers that undergo an annual SSAE-16 SOC 2 audit. Operational experts perform regular security tests and reviews to insure that data and access is protected.

Capsule Support Access is a free service available to all customers with an active Capsule Service Plan. It is compatible with Capsule DataCaptor v5, v6, SmartLinx v7 and greater.

FOR MORE INFORMATION, CONTACT US

NORTH AMERICA
+1 800-260-9537
support@capsuletech.com

INTERNATIONAL OFFICES
+33 1 84 17 12 50
international@capsuletech.com

CapsuleTech.com

→ Learn more at CapsuleTech.com