

## Healthcare Re-imagined

GE is dedicated to helping you transform healthcare delivery by driving critical breakthroughs in biology and technology. Our expertise in medical imaging and information technologies, medical diagnostics, patient monitoring systems, drug discovery, and biopharmaceutical manufacturing technologies is enabling healthcare professionals around the world discover new ways to predict, diagnose and treat disease earlier. We call this model of care "Early Health." The goal: to help clinicians detect disease earlier, access more information and intervene earlier with more targeted treatments, so they can help their patients live their lives to the fullest. Re-think, Re-discover, Re-invent, Re-imagine.

GE Healthcare  
800 Centennial Avenue  
Piscataway, NJ 08855-1327  
U.S.A.

[www.gehealthcare.com](http://www.gehealthcare.com)  
[www.labcrew.com](http://www.labcrew.com)



## GE Healthcare Life Sciences

# Bio InSite

## Technical Infrastructure and Security Features

### Overview

This document describes the security features of the Bio InSite™ digital services delivery platform from GE Healthcare Life Sciences. Bio InSite software enables GE to diagnose and manage device performance in real-time over a secure Internet connection.

Bio InSite is based on intelligent device management (IDM) software developed by Qestra Corporation, a leading provider of IDM software for the healthcare industry. As part of an intellectual property agreement, Qestra licenses its intelligent device management software to GE Healthcare for use in the development of its digital services solutions. The Qestra software "backbone" enables GE Healthcare to ensure that service on its devices is delivered in a safe and secure manner.

Recognizing that network and data security are major concerns for the life sciences industry, GE Healthcare has designed Bio InSite to meet your exacting security and regulatory compliance requirements. With Bio InSite, you can have confidence in your data security because:

**Your control is absolute.** The end user initiates/ends all connections. There is no threat of unauthorized changes or access to the system because you are always in control.

**Your data is protected.** Bio InSite supports robust audit trail functionality and 128-bit SSL encryption.

**Your IT infrastructure is uncompromised.** With Bio InSite there's no need to open non-standard ports on your firewall, modify your networks, establish a VPN, or add IP addresses. Bio InSite uses the standard https port 443 to establish only outbound connectivity.

### Bio InSite Security Features

Bio InSite is the easy-to-implement, secure digital services solution, with features optimized for the life sciences:

- Firewall transparent
- No changes needed to your existing IT and security infrastructures
- Highly secure and efficient 128-bit SSL data transmission and password authentication
- Customer-controlled access

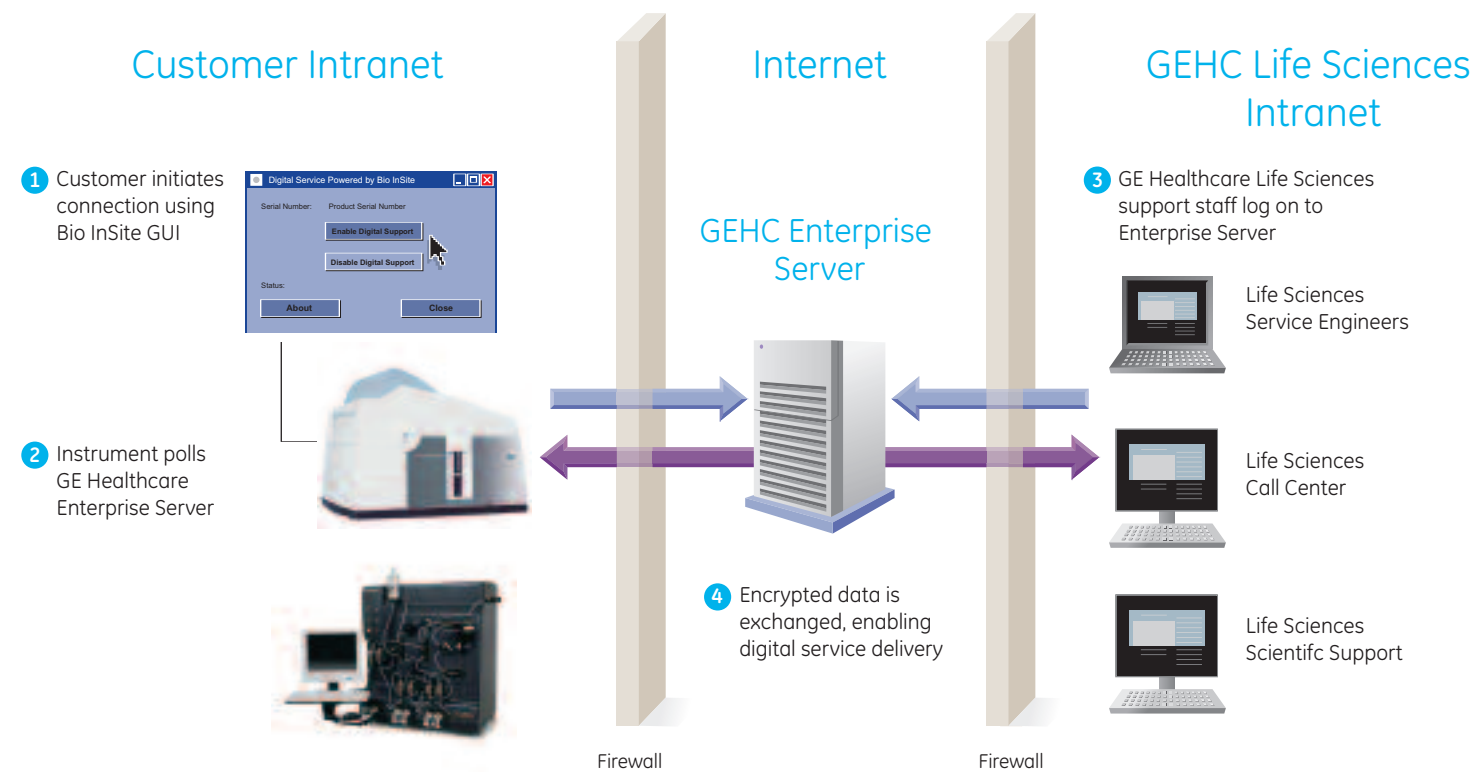
### Comprehensive security at every level

GE Healthcare understands that comprehensive security means looking at security from all aspects of system integrity. Bio InSite is designed to integrate into an existing IT environment without breaching existing safeguards. IT departments have invested money and time creating a safe corporate environment and Bio InSite software does not undermine these efforts. The software is firewall compatible and specifically designed to not compromise expensive security measures. Instead, it works within your environment and limits itself to specific pre-defined interactions with the device.

Bio InSite consists of four components:

- The graphical user interface (GUI) that gives the user control of digital services
- The Service Agent that provides intelligent monitoring and secure bi-directional communications
- GE Healthcare's back-office Enterprise Servers that communicate with the Service Agent
- The remote desktop application that works through the Service Agent to provide remote desktop functionality





### GUI

To establish connectivity, the user starts up the Bio InSite GUI and requests connection by clicking the appropriate button. The GUI becomes visible on the screen whenever a remote session is initiated and remains visible until the session is ended. At the conclusion of the remote session, both the Bio InSite agent and VNC server are stopped and unloaded from memory. The customer has full control of the system at all times. Once the Bio InSite Agent is disconnected via the GUI, connectivity to the instrument computer hosting Bio InSite is no longer possible.

### Service Agent

The Bio InSite Service Agent is a compact, network-independent application that enables devices to access and provide Web services across any wired or wireless network. Security has been designed into every level of the Service Agent solution to ensure that there is no need to set up virtual private networks (VPNs), open up firewalls, or make any changes to IT security procedures in order to deliver the benefits of digital services.

When a connection is initiated using the GUI, the Bio InSite Service Agent component starts up and begins to periodically poll the enterprise back office server at GE Healthcare by means of https-based Web services. When a VNC-based remote desktop session or a file transfer is requested, the Bio InSite Service Agent acts as a tunnel for the resulting network traffic.

All communication between the instrument/instrument computers and GE's enterprise servers is encrypted via 128-bit SSL and tunneled by the Bio InSite agent through https port 443. At the enterprise end, access is limited via GE's single sign on (SSO), which prevents unauthorized access. In addition, audit features at the Enterprise Server end track user access through log file generation.

The Bio InSite Service Agent initiates all communication with GE's enterprise servers on customer request only. GE personnel cannot start the Bio InSite service agent remotely and cannot access a customer computer on which the service agent is not running. GE's enterprise servers are visible to the Service Agent via a known Web URL using the https protocol.

Client devices communicate with GE Healthcare in the same way that a Web browser accesses a secure Web site with 128-bit SSL encryption. The Service Agent communicates with the GE Healthcare service enterprise servers via transmissions that require password authentication. The passwords can be set and changed at the customer's request.

The Bio InSite Service Agent supports DHCP, so there is no need for fixed IP addresses. The Service Agent supports transmission via proxy servers and also supports password authentication to validate the identity of devices exchanging information with the enterprise.

The Service Agent is written in hardened C++ and is compatible with Windows® 2000 or Windows XP operating systems, independent of instrument devices.

### Enterprise Server

The back office enterprise servers process information provided by the Bio InSite Service Agent and host the secure Web Services that facilitate communication with the Agent. The servers function as the management console for Bio InSite, allowing only authorized GE Healthcare personnel to initiate remote desktop sessions, transfer files, and specify security and access to customer devices. These enterprise servers run the Questra Control Center, which provides an open, scalable application platform for the deployment of enterprise solutions geared towards digitally delivered service and support.

In addition to ensuring smooth interoperability with your existing IT infrastructure, GE Healthcare has implemented security features at the Enterprise Server to control user access to the system and provide application and data security. The Enterprise Server Control Center provides administration for devices enabled with the Bio InSite Service Agent. The control center sets up profiles for users, devices, or groups that meet security management needs. Only authorized users can log in with username and password authentication to access Control Center functions. Their profiles dictate which devices or device groups they can access, as well as the level of access (including the allowed data views) for each device and application. All user and system interactions are supported by robust audit trails.

### Remote Desktop Functionality

Bio InSite establishes remote desktop connectivity through the Service Agent via the Ultra-VNC server. This server is available as an open-source application and is unmodified by GE Healthcare Life Sciences. The VNC default configuration is "Loopback Only" mode to prohibit any VNC connectivity to the instrument computer, even from the customer's own network. The Ultra-VNC server application can be password-configured by the customer. Running GE Healthcare digital services network traffic on the Bio InSite Agent eliminates the need to open up non-standard ports on the customer's firewall, thus maintaining the customer's network security.

Authorized GE service and support personnel can transfer data (run files, error logs, software updates, etc.) to and from the customer equipment for troubleshooting purposes. Using remote desktop (VNC tunneled through Bio InSite), these personnel can view and control the customer screen in real time.

### Commitment to an Evolving Solution

Bio InSite from GE Healthcare is a leading-edge remote diagnostics software solution optimized for the life sciences industry. Instrument lines deployed with Bio InSite are fully tested for both hardware/software compatibility and digital support capabilities before being deployed in the field.

The software has been designed with security features at every level to fit a wide variety of end-user environments and firewall configurations. The hardened software design ensures application and data security, with adherence to standards that will provide a smooth transition as your security requirements evolve in the future.

For additional information on how Bio InSite can bring you the productivity and performance benefits of digital service while protecting your data and application security, contact GE Healthcare Life Sciences.