BD Assurity Linc™ Software Security

White Paper

Contents

Overview

This white paper provides information about the security features of BD Assurity Linc™ remote systems management software, which is installed on a BD workstation and connected to a BD instrument. The BD Assurity Linc connection enables BD to monitor your instruments and, as a result, provide you with fast and efficient service and support.

BD Assurity Linc software is powered by the Axeda® platform, a leading technology for remote service connections for highly secure environments such as government, banking, healthcare, data centers, and manufacturing.

System Architecture

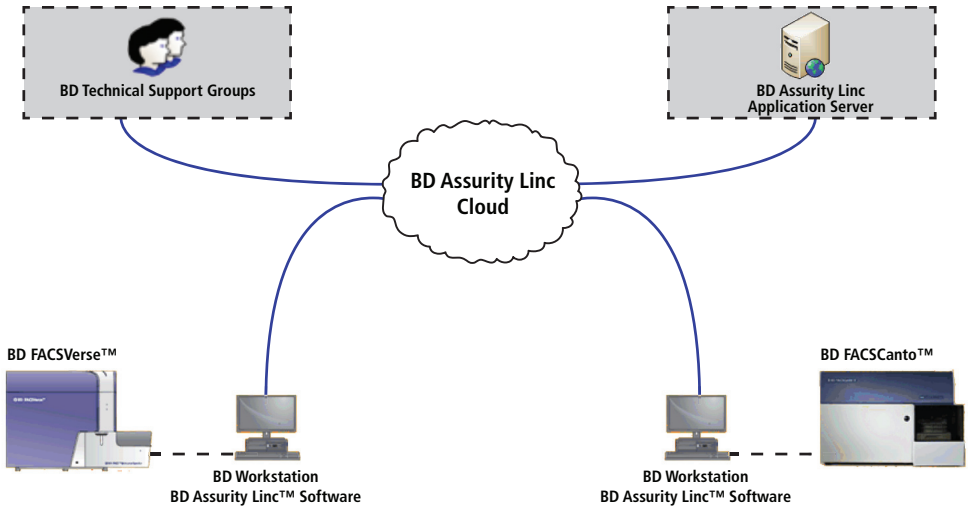

Figure 1. BD Assurity Linc communication structure

Each component of the BD Assurity Linc system is designed to provide security while keeping implementation as simple as possible.

BD Assurity Linc Software

BD Assurity Linc software runs as a service on a BD workstation and collects diagnostic and performance data from an instrument. The software monitors the health of the instrument and sends small amounts of status information to BD Customer Support. When you contact BD to report a problem or ask a question, BD support staff can view this data and, with your permission, open a secure, firewall-friendly connection to your system. BD uses this connection to diagnose the problem or assist you with system operation.

- **Supports secure encrypted data transmission.** All communications between the BD workstation and BD Assurity Linc™ Cloud server are encrypted using 128-bit Secure Socket Layer (SSL) and Advanced Encryption Standard (AES) for secure transmission of data. SSL provides a protocol for transmitting private data using the internet and encryption, and provides authentication to ensure that both the sender and receiver of data are known to each other. This protects data from unauthorized access during transit. All outbound communications are initiated using the HTTPS protocol exclusively on port 443. The software initiates all communication and transmits only to a BD Assurity Linc Cloud server having an appropriate SSL certificate.
- **Leverages existing security infrastructure.** The BD workstation resides inside your network and receives the same network security protection as all other computers within your organization. No public IP address is required.
- **Integrates easily into the existing network environment.** BD Assurity Linc software supports Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT), which facilitates setup within your environment. Your local IT staff does not need to change the existing network settings or security configuration. Once connected to the local network, the BD workstation is ready to communicate.

BD Assurity Linc Cloud Server

The BD Assurity Linc Cloud server provides a secure, scalable infrastructure for maintaining connection with BD Assurity Linc software. This server maintains extensive audit logs of all user-access requests and all application functions performed on BD instruments. Audit logs provide comprehensive reporting capabilities and allow BD to ensure complete accountability for activities performed by BD personnel. Examples of audited functions include user logins, file transfers, and remote desktop sharing sessions. BD Assurity Linc Cloud operations are certified to meet the ISO Standard 27001 Information Security Management System (ISMS) framework.

BD Assurity Linc Application Server

The BD Assurity Linc™ Application server hosts tools that BD service and support personnel use to monitor and maintain your instruments for maximum uptime and operational availability. It resides in a highly secure environment and is accessible only by BD employees. BD follows industry standard security measures. Access to the BD Assurity Linc Application server requires username and password authentication, and user-access security is addressed in the following two ways:

- Activity-based access control. Limits BD personnel's access to only the application functions that are required to perform their specific roles.
- Device-based access control. Limits BD personnel's access to only the customer's instruments to which they have been granted access.

Network Settings for BD Assurity Linc Communication

For BD Assurity Linc software to communicate with the BD Assurity Linc Cloud server, standard HTTPS traffic from the workstation to the internet should be permitted on port 443. Communication to the BD Assurity Linc Cloud server and at least two of the Global Access servers must be enabled. If your network uses an Access Control List (ACL) or hosts file to restrict outbound internet communications, please include the following entries:

IP Address	URL	Description
209.202.167.31	bd.axeda.com	Assurity Linc Cloud
89.234.8.217	ghuk1.axeda.com	Global Access Server UK
209.202.157.179	ghsom1.axeda.com	Global Access Server Boston, MA USA
198.66.245.39	ghsj1.axeda.com	Global Access Server San Jose, CA USA
124.40.23.210	ghjap1.axeda.com	Global Access Server Japan
122.202.65.179	gas-aus.axeda.com	Global Access Server Australia

Security Configuration of BD Workstations

Users need to configure BD workstations to ensure a reasonable level of security for systems connected to their network.

Note: *Before you begin this process, read the Information Security Guidelines document (23-14533-01), which can be downloaded from bdbiosciences.com. This document provides recommendations on how to manage antivirus software, Microsoft® updates, Microsoft® Windows® user account permissions, software firewalls, and removable storage media security.*

BD's responsibility

BD is responsible for configuring the BD workstation with a default system image.

Note: *BD workstations run on the Microsoft Windows XP operating system (OS) with Service Pack 3 or the Microsoft Windows 7 Professional OS with Service Pack 1 or later.*

Customer's responsibility

Customers must ensure that the guidelines in the *Information Security Guidelines* document are implemented so that antivirus and Windows updates are installed and maintained on the BD workstation, and that if enabled, a software firewall is configured correctly.

Customers may choose to enable individual Windows user accounts with limited access to the workstation. Windows Administrator accounts should be restricted to Lab managers, IT administrator(s), and BD service personnel.

User accounts

The Windows 7 Professional OS is preconfigured with three Windows user accounts:

- **Admin.** Administrator account for local IT administrator(s)
- **BDFSE.** Administrator account for BD field service personnel.
- **Operator.** Limited account for local instrument operators.

Refer to the *Information Security Guidelines* document for information about user account permissions, if additional limited Windows accounts for operators are required.

Firewall

The Windows firewall is enabled by default. If you prefer to install and configure your own software firewall, refer to the *Information Security Guidelines* document.

BD Data Privacy and Organizational Security Measures

BD has implemented systems to ensure reasonable data privacy and security while operating BD Assurity Linc software. Internal Data Privacy Policies implemented by BD to comply with applicable privacy laws also help ensure that:

- Remote access to a customer's network and instrumentation will be implemented only upon agreement with the customer.
- Training is provided for all BD support personnel so that they understand and comply with BD's internal data privacy policy.
- All BD personnel who might inadvertently be exposed to Protected Health Information (PHI) as a consequence of supporting our customers understand their responsibility to maintain such information in confidence.
- Auditable records are kept of each customer with whom remote desktop sharing is enabled.

We also have implemented a range of measures to ensure that information access and control can be managed in a secure fashion. These measures include, but are not limited to:

- A comprehensive security management system to ensure that users are given access only to information and information systems as required by their role in the organization.
- User training and awareness on data privacy and confidentiality.
- Physical security measures to ensure that non-authorized users cannot enter BD premises. This includes physical access restrictions to data servers and data hosting environments for non-authorized personnel.
- Access to and permissions on BD business desktops, laptops, and data and application servers are controlled by a combination of two-factor authentication and Microsoft Group policies. Additionally, Virtual Private Network (VPN) authentication is required for BD users accessing BD systems from outside the BD network.
- Password complexity and expiration policies are in place to ensure that passwords cannot easily be compromised.
- Systems connected to the BD network are protected from external security risks with a combination of hardware firewalls, antivirus software, intrusion prevention systems, and regular updating with Microsoft security updates.
- Hard disks of decommissioned computers are erased using the US Department of Defense compliant software. This software erases the contents of the hard disk multiple times to ensure that no data remains on the hard disk.
- Access and use of BD information systems are auditable.
- BD personnel are trained in and expected to comply with the Acceptable Use policy of BD business systems and information systems. Random checks are carried out by BD to ensure that all personnel act according to this policy.
- BD conducts random audits to ensure that the internal data privacy policy is respected and that any deviations from the policy are addressed in a timely manner.

BD Recommendations for Practical Security Measures

Customers can take additional measures to improve the overall security of BD workstations connected to the customer's network and the internet. The following measures are acceptable to safeguard the data on workstations provided they do not involve installation of third-party hardware or software:

- Information security management system/privacy and data protection management system
- Physical security
- Access controls
- Security and privacy technologies
- Awareness, training, and security checks in relation to personnel
- Incident/response management/business continuity
- Audit controls/due diligence

23-15755-01

BD Biosciences
bdbiosciences.com