Secure Implementation of Agilent OpenLAB Electronic Lab Notebook (ELN)

INCREASING YOUR LABORATORY PRODUCTIVITY

Whitepaper

Introduction

As demand for more efficient scientific discovery increases, laboratories are seeking to improve the way their results are captured, analyzed, and shared. Many are considering transitioning from paper-based to fully electronic laboratory notebooks.

OpenLAB ELN is a flexible laboratory notebook solution that simplifies and accelerates the capture, analysis, and sharing of all types of laboratory information. A high-productivity alternative to traditional paper notebooks, OpenLAB ELN safeguards intellectual property and supports 21 CFR Part 11 requirements through advanced security features, a comprehensive audit trail and robust IP protection capabilities.

Because OpenLAB ELN is web-based, multidisciplinary software, security is a key component of its successful implementation. OpenLAB ELN provides a robust security strategy that adds controls at multiple levels of data storage, access, and transfer.

This whitepaper explains how OpenLAB ELN is designed to protect an organization’s data. It also explains the steps that must be taken to ensure that OpenLAB ELN is implemented securely within the customer’s IT environment.
The OpenLAB ELN security strategy has six components:

- Access control: OpenLAB ELN provides a range of options for authentication and access control, which customers can implement in accordance with their organization’s needs.
- Software development: Agilent has a robust software development process, with built-in review and traceability to avoid implementation-level security vulnerabilities.
- Java client security: because OpenLAB ELN is a web-based application, which uses a Java applications server and an Oracle database, no experimental data resides on client hard drives. OpenLAB ELN works with a signed applet with a trusted certificate, compatible with the highest security level of the Java Runtime Environment (JRE). Agilent monitors and reacts quickly to the latest Oracle developments and security updates for the JRE.
- Server operating system security: OpenLAB ELN uses a Java application server in an approach widely known for its reliability and robustness.
- Database security and disaster recovery: regular backups enable the system and data to be reinstalled in the event of disaster.
- Regulatory compliance and electronic records security: OpenLAB ELN supports the compliance requirements mandated by US FDA 21 CFR Part 11.

OpenLAB ELN Architecture

OpenLAB ELN is a multi-tier, web-based Java application. It is composed of a thin and rich client, a web and application server, and a database server.

Users access OpenLAB ELN from their web browser, where they can record, browse and search experiments, and view PDF reports.

The software uses an embedded Java applet, running inside the JRE, to perform tasks such as creating, editing and witnessing experiments, and administering the system. The web and application server handle HTTP or HTTPS requests from clients, and the internal business logic associated with these requests.

The Oracle database server is a persistent layer used to store OpenLAB ELN data.
**Access Controls**

OpenLAB ELN access controls include authentication, authorization controls, and system logs, which can be configured to meet customer-specific security requirements.

**Authentication controls**

The OpenLAB ELN administration module is used to control access to experiments. Control of user access can be configured in two ways: users can be built-in, or the implementation can use an external authentication mechanism.

Users authenticated by OpenLAB ELN must have a unique ID, and may, depending on the configuration, use one or two passwords to log in and to sign experiments. Password management rules, for example password length, expiration, non-reusability over a number of updates, or blocking after a number of unsuccessful login attempts, are available. These rules are set using the administration module. Agilent recommends using the OpenLAB ELN default values.

If a customer chooses to authenticate externally, OpenLAB ELN can be used with an Active Directory or Lightweight Directory Access Protocol (LDAP) system. Once OpenLAB ELN is configured for one of these options, login and experiment signing are checked by the external authentication system.

When authenticating users across a multi-site OpenLAB ELN implementation, adequate network connectivity between sites must be verified.

**Authorization controls**

Beyond authentication, it is also important to control user access to the various OpenLAB ELN functions. With OpenLAB ELN, access rights are based on user-specific and company-wide privileges that are defined using the administration module. OpenLAB ELN includes a wide range of user roles to choose from:

- System administrator
- Local administrator
- Template/forms administrator
- EHS Manager
- Analysis request manager
- Author
- Browser
- Signer
- Super user

These roles determine which actions users will be allowed to perform. For more information, consult the online help manual available in OpenLAB ELN.

To extend the standard user roles, custom groups can be defined. Privileges (rules) can be built using any combination of the following parameters:

- User location (site, department, or laboratory)
- User roles and groups
- Project
- Project confidentiality
- Experiment status

The experiment access window can be used to control specific user access.
Using the privileging capabilities in the administration module, OpenLAB ELN implementations can range from very “open” to very tightly controlled. Organizations can configure the rules to match their desired level of security. User privileges (actions) that can be configured include:

- Log to administration module
- Always open experiment
- Open experiment
- Create experiment
- Set experiment access permissions
- Override experiment access permissions
- Print or preview experiment
- Search molecule source
- Collaborate to experiment

By default, OpenLAB ELN is open; all users have all of these privileges. After the system is installed, Agilent experts are available to train customers how to use the rules and privileges to implement restrictions.

System logs

Monitoring system access is an important component of security. OpenLAB ELN logs every instance of administrative and user access in the administrative and application logs. These logs can be viewed in the administration module. System logs are protected on the server and can be accessed by authorized personnel when needed.

Administrative and applications logs are stored in and backed up with the OpenLAB ELN database. System logs reside on the server and are backed up based on customer-defined rules.

Key Points:

- OpenLAB ELN provides a range of options for authentication and access control.
- Customers implement these options to meet the requirements of their organization.
- Agilent experts are available to provide guidance and further information.
Security in Agilent Software Development

Software coding errors can be a security risk. For this reason, Agilent adheres to a stringent software development lifecycle with security as a core component. This lifecycle ensures full traceability and completeness, from specifications to tests, including tests for performance and reliability. This approach is essential because many, if not most, types of implementation-level security vulnerabilities are caused by oversights by the software developer. Agilent’s software development and code review teams are aware of and work together to avoid these vulnerabilities to create secure code.

Key Point:
Agilent has a robust software development process, with built-in peer review and traceability, to avoid implementation-level security vulnerabilities.

Java Client Security

OpenLAB ELN uses a client applet to perform tasks such as creating, editing and witnessing experiments. While there have been many warnings related to Java applet security, these warnings concern executing an applet containing malicious code that would give client access to unauthorized users. This risk has been eliminated in OpenLAB ELN.

Because OpenLAB ELN is a web-based application, no experimental data reside on client hard disks. Even in the case of a security breach by another application or website, OpenLAB ELN data cannot be accessed and stolen.

In addition, OpenLAB ELN uses a signed applet with a trusted certificate, compatible with the highest security level (“very high”)1 of the JRE. This security level dramatically reduces the probability of running malicious code.

Oracle addresses security concerns with frequent security updates. The Agilent software engineering team reacts very quickly to every new JRE release to ensure OpenLAB ELN is compatible with the latest JRE. According to Oracle, a “whitelist” will eventually become available to determine which applets are authorized to run. This will further ensure that only content provided by trusted providers would run on client machines.

Customer network settings must be configured to regard the OpenLAB ELN server as a trusted site. If OpenLAB ELN is operated outside a VPN, communication must be configured with a secure HTTPS protocol.

Key Points:
• OpenLAB ELN is a web-based application, so no experimental data reside on client or user hard drives.
• OpenLAB ELN works with a signed applet with a trusted certificate that is compatible with the highest JRE security level.
• Agilent monitors and reacts quickly to Oracle’s security updates.
• Customers must ensure their company network settings are configured to recognize the OpenLAB ELN server as a trusted site.
• If OpenLAB ELN is operated outside a VPN, communication must be via HTTPS.
Server Operating System Security

OpenLAB ELN’s web-based architecture uses a Java application server. The default configuration uses the Apache Tomcat software implementation of the Java Servlet and Java Server Pages technologies, which are widely known for their reliability and robustness.

Access to the application server relies on operating system security. Provided the server is configured following industry best practices, access to the application log files is well protected. To ensure secure communications, Apache can be configured to the server pages in the HTTPS mode.

Key Points:
• OpenLAB ELN uses a Java application server, in an approach widely known for reliability and robustness.
• Customers need to ensure their servers are configured according to industry best practices.

Database Security and Disaster Recovery

Database security

OpenLAB ELN uses an Oracle database. With the industry’s most advanced technology for safeguarding data, Oracle is the de facto leader in database security. The company provides a comprehensive portfolio of security solutions to ensure data privacy and to protect against insider threats. With powerful database activity monitoring and blocking, privileged user and multifactor access control, consolidated auditing and reporting, and secure configuration management, customers can deploy reliable data security solutions that do not require changes to existing applications.

With OpenLAB ELN, typically only the database administrator may access the database. This is OpenLAB ELN’s default setting. No one else is allowed to explore experiment data outside of the OpenLAB ELN application, enforcing company-wide data access security rules. Agilent recommends giving a limited number of individuals access to the database.

Disaster recovery

Depending on the allowable downtime, there are several disaster recovery options available with OpenLAB ELN. Minimally, database backups are performed on a regular basis. In the event of a disaster, the application server can simply be reinstalled, and the database backup is reloaded into a fresh database. OpenLAB ELN backups are performed daily with hourly options for large systems. Customers need to periodically verify that the backup works and can be restored.

More sophisticated OpenLAB ELN setups allow more rapid recovery. A mirror system on standby can replace a production system in minutes once the IP addresses are correctly rerouted to the standby system. The choice of approach should be based on the balance between business requirements, acceptable downtime and cost.

Key Points:
• Oracle provides a comprehensive portfolio of security solutions to ensure data privacy and protect against insider threats.
• Database backups enable the system to be reinstalled in the event of disaster.
• Customers need to verify periodically that the backups work and can be restored.
Electronic Records Security and Regulatory Compliance

Compliance

Compliance requirements for electronic records are covered by the FDA’s part 11 Title 21 of the Code of Federal Regulations; Electronic Records; Electronic Signatures (21 CFR Part 11) for a closed system. OpenLAB ELN includes features to support the requirements set forth 21 CFR Part 11. In particular it ensures:

- Accurate and complete copies of records
- Versioning of all relevant records for traceability
- Controlled copies of the data
- Records of changes captured in user-independent time-stamped audit trails

These features can be configured during, or after installation to meet customer-specific standard operating procedures (SOPs) and security requirements. Configurable settings include very granular specification of user roles and privileges to restrict access to functionality to particular users. The system administrator can make changes to these settings at any time.

Electronic signatures

OpenLAB ELN offers several options for electronic or digital signatures. Electronic signatures can be applied to every experiment version using server signatures or individual certificates. The digital time stamping service provides an unforgeable seal on each electronic record.

Using the administration module, these records can be exported in an independent, standard format for review for audits or court cases.

To use OpenLAB ELN electronic record and security features appropriately, customers need to define and follow a password management procedure.

Key Points:

- OpenLAB ELN supports the compliance requirements set forth in FDA 21 CFR Part 11.
- Customers can configure the OpenLAB ELN settings to meet their SOPs and security needs.
- Customers need to define and follow an appropriate password management procedure.

Conclusion

OpenLAB ELN is built around robust security strategy with a comprehensive set of security features. To ensure a secure OpenLAB ELN implementation, customers must:

- Configure their network settings to recognize OpenLAB ELN as a trusted server
- Setup their servers according to industry best practices
- Select appropriate authentication and access settings for users
- Define and follow an appropriate password management procedure
- Verify periodically that backups work and can be restored

Such measures, along with the Agilent’s rigorous approach to software development and implementation, will ensure that experimental data and information are stored securely and can be accessed quickly.
Notes:

1) Oracle defines three levels of security in the JRE:

Medium
You are prompted to accept all types of Java applications. The JRE version should be at or above the latest security update release of Java from Oracle, otherwise, you are prompted to upgrade your JRE.

High (Default)
If the JRE is at or above the security baseline, you are prompted to accept apps that are signed with a trusted certificate, self-signed, or unsigned. Local applets are not allowed to run. If the JRE is below the security baseline, you are prompted to accept apps that are signed with a trusted certificate, all other apps are not allowed to run. If the JRE is below the security baseline, you are given an option to update.

Very High
You are prompted to accept apps that are signed with a trusted certificate. All other apps are not allowed to run. If the JRE is below the security baseline, you are given an option to update.

For more information

Learn more:
www.agilent.com/chem/openlab

Find an Agilent customer center
www.agilent.com/chem/contactus

U.S. and Canada
1-800-227-9770
agilent_inquiries@agilent.com

Europe
info_agilent@agilent.com

Asia Pacific
inquiry_lsca@agilent.com

This information is subject to change without notice.

© Agilent Technologies, Inc. 2014
Printed in the USA. March 28, 2014
5991-3793EN