Agilent SLIMS

Technical Security Policy

Scope

The purpose of this document is to outline the strategies and control mechanisms that form the Security Management practices of the SLIMS software service. Additionally, it provides a description of the information security safeguards provided by third-party tools and vendors used by SLIMS.

Purpose

The purpose of the Security Management practices is to ensure that information stored and accessed through SLIMS is managed such that:

- All information is available and usable when required.
- All information is observed by/disclosed to only those individuals who have a right to know it.
- All information is complete, accurate, and protected against unauthorized modification.
- All information exchanges can be trusted.
- Where appropriate, information access and modifications are tracked for audit purposes

Approach

Genohm is now officially Agilent Technologies. Agilent works continuously with researchers, lab-managers, and administrators to identify information-security needs, and with experts in the hardware security, application security, and network security to update the service to meet those needs.

Overview

Technical security measures are in place to guard against security threats including:

- Damage or unauthorized access to hardware
- Low level vulnerabilities such as Buffer overflow attacks
- Application or OS vulnerability and misconfiguration
- Data malformation attacks, including SQL injection, and XSS
- Session fixation attacks
- Sniffing/eavesdropping
- Network attacks

Agilent takes measures across the three layers of the application framework in order to maximize security precautions:

- System level protection
- Application protection
- Network protection and monitoring

System Level Protection

Hardware Protection

Agilent does not host hardware internally but uses an external cloud service that has the most stringent security provisions to limit access to hardware.

Hosting Provider Security

Agilent applies the cloud provider's best practices for authentication and authorization. This is by default over TLS and using multi factor authentication.

Application Protection

SLIMS is built on a state-of-the-art application stack, integrating best-in-class operating systems, database servers and application servers. We frequently update our application stack with security patches.

Secure Channels

Certificates

SLIMS uses AWS Certificate Manager (ACM) for HTTPS certificates, which automatically renew each year.

HSTS Header

SLIMS includes an HTTP Strict Transport Security header in the server response with a lifetime of 1 year.

Authentication

Measures aimed at ensuring that only authorized individuals can access the SLIMS Service.

Authenticated System Access

The SLIMS application is only accessible by authenticating against a known set of users in the database using role-based access control (RBAC) for authorization. No anonymous access is possible by default.

The SLIMS application provides a variety of administrative controls to control authorization for the client instance:

- Define password restrictions: Four levels of complexity available to choose from. Simple, Basic, Standard, and CLIA Compliant.
- Failed password attempts: Configure the number of failed login attempts allowed before user account is locked.
- Inactive session termination: The length of time before the user is logged out after no activity is configurable per SLIMS instance. There is a separate server timeout and local client timeout, though only the latter is visible to the end user.
- Password expiration: The number of days before passwords expire and need to be reset or changed.
- SLIMS Share server and user password must be defined to control access.

Authorization

Measures aimed at ensuring that only authorized users can access specific pieces of information in the SLIMS Service.

Intra-Cluster Traffic

While the applications are running on shared compute resources in the same cluster, they are separated on the host by containerization of the application components.

Containerization

The application containers do not run under a privileged user, so it has reduced capabilities on the host system.

Agilent Access to information

All Agilent access to user-generated content is controlled by the following policies and conditions:

- Access user generated content for the purpose of user support.
- Only trained employees can access the environment.

- Administrative access to the hosting environment is only allowed from known networks (office IP and VPN IP).

Auditing

Measures aimed at ensuring that only authorized users can access specific pieces of information in the SLIMS Service.

Auditing User Activity

SLIMS maintains detailed logs of access to and modification of all information in the Service (history records). Audit entries capture:

- Username
- Date and time of modification
- A description of the action taken
- Identity or name of affected data, system or resource
- Old value/new value information for changed data, where appropriate

Audit trails are protected from unauthorized modifications.

Database

Private Database Instance

Every SLIMS application instance connects to its own private database instance. Customers are not allowed to connect to the same database.

The database is only accessible from within the cloud environment's private network and it is not publicly accessible from the internet.

Encryption at REST

The application instance specific encryption key is used to encrypt the database disk at rest.

Secure SSL Database Connection

The application instance is configured to connect to its database endpoint over a secure SSL connection.

Backups

- The database instance uses the available automatic backup option of AWS.
- The application instance specific encryption key is used for these backups.
- Database backups are set to client SLA specifications.

Product Development Process

All software applications are developed based on industry best practices and incorporate information security throughout the development lifecycle.

- All system and software changes are tested before deployment.
- Separate development, staging, and production environments are maintained.
- Production data is never used for testing or development.
- All test data and accounts are rendered inaccessible or inactivated before production systems become active.
- All temporary accounts, usernames, and passwords are removed or inactivated before an application is released to customers.

- Source code is reviewed, and applications are tested (pen testing) periodically for security vulnerabilities, especially those related to:
    - Invalid login and authentication
    - Cross-site scripting (XSS) attacks
    - Injection vulnerabilities (for example, SQL injection)
    - Cross-site request forgeries (CSRF)
    - Improper error handling
- Logical data separation to ensure that one customer's data is not visible to others even in the case of programmer error.
- Customer data is protected from corruption even in case of programmer error.

Data Protection and Encryption

A new encryption key is generated per SLIMS instance which is used to encrypt the application data at rest (database disk encryption and encryption of the file system for SLIMS uploads).

The backing key, which manages data encryption and other encryption key rotation, is rotated every year.

SLIMS File Repository (Upload Storage)

Encryption at REST

The application instance specific encryption key is used to encrypt the SLIMS upload storage at rest.

Backups

The SLIMS file uploads are backed up to a separate storage service every hour and are kept for 30 days.

Encryption of Backups

While the database backups use a unique encryption key for their backups, SLIMS uploads and instance configuration backups use a shared encryption key managed by Agilent.

Only trained Agilent employees can access the backup repository.

Disaster Recovery

The SLIMS file repository backup and the instance configuration are exported and saved in another backup repository.

This configuration allows the application instance to be recreated in the cluster in case of a disaster.

Network and Monitoring

Network Policies

Network Policy rules are defined per application instance so only components of the same application can talk to each other in the cluster network.

SSL Termination

Incoming HTTPS traffic is terminated at the load balancer before entering the compute cluster.

HTTP traffic from end-users' travels unencrypted to its destination container within the cluster network. Only traffic that is required for that application container is forwarded.

Monitoring

Update Management

Available software updates are continually monitored for the components used in the environment and maintenance for updates is scheduled when necessary.

Server Resources

All critical server resources are monitored and stored outside the production environment, so they are always available in case of emergency.

Application Availability

The important customer application endpoints are monitored for availability and Agilent is alerted when there is a problem.

This Policy was last updated on July 27, 2020.

Published in the USA, July 27, 2020
DE.2964699074

Agilent
Trusted Answers