Policy

Agilent
Trusted Answers

Security and Architecture Policy for Agilent SLIMS 7.2

Overview

Data security, privacy, and their various aspects, such as availability, integrity, and confidentiality, are of critical importance to our customers. Agilent commits to delivering the highest quality services to our customers, addressing security at all stages of the product development life cycle.

This document explains how Agilent SLIMS implements security measures that comply with assorted U.S., European and other regulations and standards. We have defined a set of policies, processes, and controls for security and privacy in accordance with the internationally accepted ISO 27001 and 27002 security standards, designed 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.

The document is divided into three sections:

1. The platform architecture and implementation that enable us to deliver the highest level of security and to comply with the regulations
2. The security measures we have deployed to ensure data availability, data integrity, and data confidentiality
3. The applicable data privacy regulations and how we comply

Platform Architecture

This section describes the hardware, software, and technologies used to support the SLIMS platform and our customers.

Agilent SLIMS offers flexible installation options:

- SLIMS Customer Hosted: hosted by customer, either on-premises or on their own cloud solution
- SLIMS Agilent Hosted: hosted by Agilent as Software-As-A-Service on a scalable, powerful, secure server.

Technology Architecture

SLIMS relies on tools that provide a scalable, web-oriented architecture. It is highly configurable and is extensible through various APIs. Plugins can be created and activated from several points within the system. A plugin is a unit of functionality implemented in Java, that is executed inside SLIMS Gate or SLIMS Gate Remote. Plugins implement additional functionality according to customer-specific needs, using SLIMS provided Application Programing Interfaces (APIs).

Other interfaces such as a REST API allow for other applications to integrate with SLIMS. The system is suitable for demanding and high-profile customers that appreciate the system's stability and flexibility.

SLIMS team operations are furthermore based on best practices and a commitment to excellence; see more details in the **Product Development Process** section of this document.

As documented in its corporate Quality Management Policy, the company promotes and supports a methodology that has achieved ISO 9001:2015 certification. Please visit Quality at Agilent for more details.

SLIMS Platform

The SLIMS architecture is layered in the following way:

The **data** is stored in a relational database and files are stored in a dedicated file store. The data is exposed to the rest of the framework by the Platform API. This layer provides low-level data access while guaranteeing business logic such as traceability and authorization.

SLIMS Server is the server side of the main UI (User Interface). It is hosted on an application server (Apache Tomcat) and presents the Web UI to the user. It provides the core functionality of SLIMS

Plugins can be useful for creating dedicated data entry forms or portals or to visualize sample-specific data using pluggable external web tools.

SLIMS GATE is an integration layer based on Apache Camel, an Enterprise Service Bus. This technology is built for integration with a wide variety of systems using a variety of protocols (e.g., direct database access, file exchange, HL7, ftp) and can be easily extended. SLIMS GATE furthermore includes XML configuration for defining small UI components that interact directly with the user from the SLIMS interface. Plugins can be installed and deployed from the user interface and there is a mechanism to pass parameters to the plugins. Another functionality plugins provide are file upload integration, enabling instrument uploads to file sharing. In addition to user-triggered actions, programmed actions such as nightly dumps or imports are also achieved.

The **REST API** is a language-agnostic API that provides read/write access to all system tables (location, content, result, etc.) and the file repository. This can be used to perform tasks such as submitting orders from a customer portal and requesting sample information or order statuses.

A **Python API** is also available. This API makes it possible to achieve complex tasks using concise scripts. An open cookbook with examples is available at python cookbook on GitHub and provides examples on data manipulation, defining a multi-step flow interacting with the user, a live report, an example portal for order submission, and an example of data plotting.

Connections

SLIMS connects to instruments and equipment in the laboratory through industry standard communications protocols and interfaces. The SLIMS connection library can be used with a valid SLIMS subscription license.

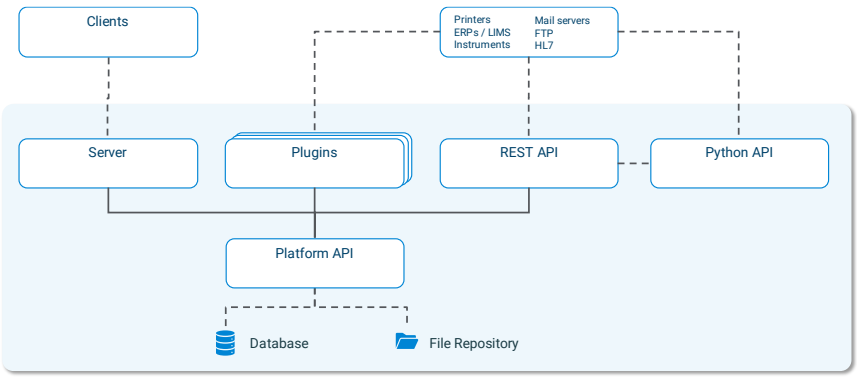

Figure 1. SLIMS General Architecture

Integrations

Integration with external systems such as EMR/EHR, environmental monitoring, billing, and CRM systems can be implemented via either file transfers (csv, xml, HL7) or APIs. Controlled vocabularies and industry standard ontologies are also supported. The SLIMS team have encountered and integrated many instruments and a plugin library is available for easier implementations.

Barcode use

SLIMS use is optimized with the use of barcode scanners and printers. Scanners can facilitate data entry and automate repetitive tasks when combined with Macros. Label Templates can be edited in SLIMS so print operations can be automatically run at specific steps of the workflow.

Manual files import

External documents can be added to SLIMS in a variety of ways. Digital media in common formats can be associated in the various phases of the process via drag and drop. Scanned laboratory information such as equipment certification or results can be uploaded independently of a sample or order.

Generic Excel import

SLIMS supports importing from and exporting to XLS(X) files out of the box. This approach is used when the integration is not frequent, or the third-party system is flexible in accepting or generating flat files.

Configuration of flows for CSV or XML files

Common formats are supported with predefined scripts available for importing from or exporting to files that can be configured by simple field mapping. Fields from the CSV/XML are mapped to fields in SLIMS and vice versa. This approach is used when the third-party software is less flexible or frequent interaction is needed and the customer wants to avoid manual manipulation of files.

Dedicated import/export flows

Dedicated scripts can be created in the case of more complex operations. An example is importing a sample taken from a subject; checking if the subject exists, and either adding the sample to the existing one or creating a new one.

Create dedicated API integrations

This type of interaction is used when deeper integration is needed (e.g., to query the live status of an instrument).

Platform Implementations Customer Hosted

This section applies to customers using the Customer hosted solution. The minimum server requirements for running SLIMS are listed in the *Agilent SLIMS 7.2 - Technical Requirements* document though the hardware specifications should be adjusted based on the actual usage patterns in the lab.

SLIMS runs on a web server that uses the HTTP(S) protocol and TCP/IP as its network transport. SLIMS needs to be installed within the same network range as the connected client computers, lab printers, instruments, and devices to connect with (either through physical network connections or via VPN bridges).

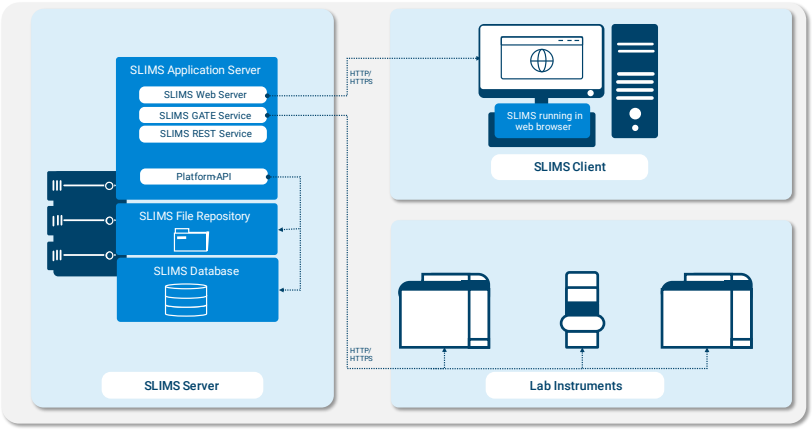

Figure 2. Customer Hosted SLIMS (One-Server Configuration)

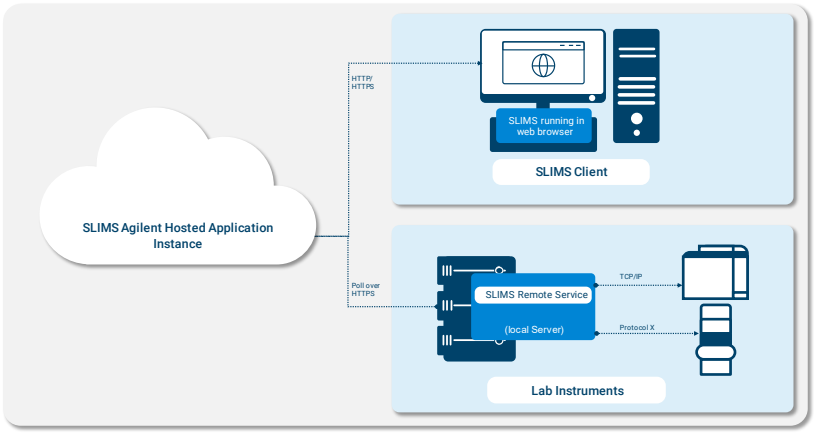

Figure 3. Agilent Hosted SLIMS (with Remote Service)

Agilent Hosted

This section applies to customers using SLIMS Agilent Hosted. Also, for customers that decide to use SLIMS Customer Hosted with SLIMS Remote, some aspects might be relevant.

Agilent Hosted SLIMS is deployed on Amazon Web Services (AWS), which are configured with the most stringent security provisions to limit access to hardware. Agilent applies AWS best practices for authentication and authorization, using TLS and multi-factor authentication by default, and only authorized personnel can access AWS accounts.

Agilent Hosted SLIMS instances use AWS Certificate Manager (ACM) for HTTPS certificates, which automatically renew each year. In addition, server responses always include an HTTP Strict Transport Security header, set to a lifetime of 1 year. These measures ensure that client traffic is always encrypted on its way to SLIMS.

Every customer is assigned a dedicated cloud environment in AWS, known as a Virtual Private Cloud, which encapsulates and isolates all customer-specific infrastructure necessary to run SLIMS.

Network traffic to-and-from SLIMS is handled within the VPC and is never mixed with any other customer's traffic. Firewall rules can be applied to implement customer-specific IP address and geographic filtering rules.

Inside the VPC, each customer is assigned a dedicated AWS RDS database and a dedicated AWS EFS instance for file storage. Both are configured with data replication to two availability zones to ensure redundancy. Both are also encrypted at rest with customer-specific encryption keys, meaning that the data stored on disk can only be read by processes with access to the encryption keys. Only the SLIMS application runtime is given access and is therefore the only process that can decrypt and use the customer's data. Encryption key material is stored in the AWS environment and can never be exported out.

SLIMS is hosted as a containerized application running in an AWS EC2 instance. Application containers are configured with reduced capabilities on the host system, minimizing the risk of any one container comprising the host. The use of containers provides a generic build for all customers which ensures they are replaceable and mobile across hardware with the previously stated advantages. Deployments are faster, environments are standardized and are easily accessed by SLIMS personnel for maintenance. Customers can rely on our DevOps experts for hosting and maintaining the system.

For connectivity to local instruments, a small service called SLIMS Remote can be installed on a customer computer. The remote service is available for downloading directly from SLIMS. This service can be installed on Windows or Linux. It runs as a Java service and the workstation or server it is installed on must remain connected constantly. The SLIMS Remote service acts as a proxy for SLIMS GATE, ensuring connectivity between SLIMS and the local equipment by initiating REST calls to the server. This eliminates firewall configuration issues.

SLIMS Remote uses a plugin system to download functionality from its server. This way, downloading new functionality or updating existing functionality does not require reinstalling the service. This reduces maintenance operations of the component.

Customers who require direct connectivity between the SLIMS cloud environment and the customer network, can opt to configure a private virtual network (VPN) connection. This can be set up in coordination between our DevOps and the customer's network and security staff, per contract terms.

Private and Encrypted Data

Every Agilent Hosted SLIMS instance connects to its own private database and file system. Customers never share these resources.

The database is only accessible from within the cloud environment's private network.

The application instance is configured to connect to the database endpoint over a secure TLS connection.

The database and file systems use AWS backup options:

- An instance-specific encryption key is used for backups.
- Backups are set with a window of 30 days. Database backups are continuous, while file system backups occur every hour. This means the customer can revert for any reason, to any previous point in time within this window, with a granularity of one hour.

Access to customer information is governed by the following policies and conditions:

- Access user-generated content for user support.
- Only trained employees can access the environment.
- Administrative access to the hosting environment is only allowed from known Agilent networks (office IP and VPN IP).

Role-Based Access Control

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: can choose between four levels of complexity. 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.

For more details about our infrastructure, security, and software development policies, please visit: agilent.com/chem/agilentslims-policies.

Security Measures

SLIMS Deployment Types and Responsibilities

Table 1. SLIMS Agilent Hosted and SLIMS Customer Hosted each have different security responsibilities and implications

Responsibility	SLIMS Agilent Hosted	SLIMS Customer Hosted
Infrastructure provider	Agilent managed AWS infrastructure	Customer's responsibility
Infrastructure managed by	Shared responsibility model between Agilent & AWS	Customer's responsibility
Infrastructure security measures managed by	Shared responsibility model between Agilent & AWS	Customer's responsibility
Secure SLIMS configuration & customization	Shared responsibility model between Agilent & Customer	
SLIMS customizations	Shared responsibility model between Agilent & Customer	

Security Measures 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

Table 2. Availability

Feature	SLIMS Agilent Hosted	SLIMS Customer Hosted
Facilities	AWS data centers demonstrate a strong physical security process, as acknowledged by their ISO 27001, ISO 27018, SOC1, SOC2, and SOC3 certifications.	Customer's responsibility
Backup / restore	All AWS features used to store data (S3, EC2, EBS, RDS) are backed up and replicated in different physical availability zones; restore tests are performed at least once a year. The application instance specific encryption key is used for these backups. Database backups are set to client SLA specifications. The SLIMS file uploads are backed up to a separate storage service every hour and are kept for 30 days.	Customer's responsibility
High Availability & Disaster Recovery	Agilent can configure the instance so that in case of a major incident in one of the physical availability zones (AZ) the SLIMS cloud instance starts in one of the other 2 physical AZs in the region. Application instance data is available in all physical AZs. (Available for purchase separately)	Customer's responsibility

Table 3. Integrity

Feature	SLIMS Agilent Hosted	SLIMS Customer Hosted
Public Key Infrastructure	All communications between client and application are protected by encryption provided by certificates issued by AWS CA. AWS PKI is used for encryption at rest of the customer data.	Customer's responsibility
Data durability	Replicated and fault tolerant storage of database volume and backups in 3 separate physical availability zones (within one geographical region).	Customer's responsibility
Hardware checks	All hardware underlying AWS services are permanently checked for failures and proactive migrations are performed.	Customer's responsibility
Intrusion detection	Continuous scanning of incoming and outgoing traffic is performed with AWS Guard Duty, which triggers alarms in case of suspicious events.	Customer's responsibility

Table 4. Confidentiality

Feature	SLIMS Agilent Hosted	SLIMS Customer Hosted
Authentication	SLIMS authentication options • Local authentication • Single Sign-On (SSO) with OpenID Connect (Okta, Google, Identity providers supporting OpenID Connect Discovery) • SAML • OAuth 2.0 for API Clients SLIMS security options • Configurable password complexity and lifetime • Configurable failed login attempts before user lockout and session time-out	
		LDAP integration
Authorization	SLIMS Role Based Access Control (RBAC)	
Isolation	Dedicated SLIMS File Storage and SLIMS database instance. The database is only accessible from within the cloud environment's private network, and it is not publicly accessible from the internet.	Customer's responsibility
Encryption	• Data at rest encrypted with AES-256 (database, file storage, backups) • Encrypted database connection (TLS) • Encrypted application endpoint (TLS), terminated at Application Load Balancer	Customer's responsibility
Firewall	Packet filtering firewall for ingress HTTP(S) traffic. Network best practices (data storage on private network segments).	Customer's responsibility
Intrusion detection	Automated anomaly detection is performed on infrastructure logs for suspicious events.	Customer's responsibility

Table 5. Auditability

Feature	SLIMS Agilent Hosted	SLIMS Customer Hosted
Application data traceability	SLIMS keeps a detailed history of records on both data and configuration tables. 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. The behavior of electronic signatures can be configured to regulate record changes.	
Logging	• Application logging • Access logging • Infrastructure and security logging	• Application logging • Access logging • Infrastructure and security logging are customer's responsibility
Change management	SLIMS development uses a Secure SDLC (Software Development Life Cycle).	
	Infrastructure changes are thoroughly tested, reviewed and version controlled.	Customer's responsibility
Incident management	SLIMS customer support and incidents managed in online Agilent Service Desk portal.	
	SLIMS infrastructure incidents are managed by Agilent and logged and managed in an internal and central system. An RCA (root cause analysis) is performed when the cause of the incident is unknown, to guarantee continuous improvement.	Customer's responsibility

Table 6. Monitoring

Feature	SLIMS Agilent Hosted	SLIMS Customer Hosted
Update Management	Available software updates are continually monitored for the components used in the environment and maintenance for updates is scheduled when necessary.	Customer's responsibility
Monitoring Resources	All critical monitoring resources are maintained and run outside the AWS production environments. This ensures that monitoring is not compromised in case of any AWS-specific service disruption	Customer's responsibility
Application Availability	The important customer application endpoints are monitored for availability and Agilent is alerted when there is a problem.	Customer's responsibility

Product Development Process

SLIMS is developed based on industry best practices and incorporate information security throughout the development lifecycle.

- All system and software changes are tested before deployment.
- 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

Agilent Access to information

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

- With customer permission, user-generated content may be used for the purpose of user support and troubleshooting.
- Only trained employees can access the hosting environment and the support portal.
- Administrative access to the hosting environment is only allowed from within Agilent networks.

Applicable security & data privacy regulations

Agilent security team works with security experts to ensure that our platform is compliant with international regulations, and that it helps our customers comply with international standards.

GDPR

In May 2018, the European Union (EU) General Data Protection Regulation (GDPR) replaced the 1995 EU Data Protection Directive (European Directive 95/46/EC). GDPR at Agilent is managed at the corporate level. Agilent has a comprehensive GDPR compliance program and provides a processing solution that incorporates the relevant GDPR requirements and that allows a customer to be assured that in choosing Agilent they are making a GDPR compliant choice. To facilitate our global business, we adhere to the requirements for safeguarding transfers of personal data internationally, including using Standard Contractual Clauses. Agilent personnel receive training on the GDPR and Agilent's obligations as both a data controller and a data processor to our customers.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, established requirements for the protection and security of patient health information held by Covered Entities and Business Associates in the United States. HIPAA was expanded by the Health Information Technology for Economic and Clinical Health (HITECH) Act, as incorporated in the American Recovery and Reinvestment Act of 2009, to address increasing reliance on electronic maintenance and storage of patient health information. The requirements of HIPAA/HITECH are contained in rules that include the:

- Privacy Rule: Protects the privacy of Protected Health Information (PHI) in any form (that is, written, recorded, spoken orally, or electronic).
- Security Rule: Sets forth standards for the security—that is, the confidentiality, integrity, and availability—of PHI maintained in electronic form (known as ePHI) only.
- Breach Notification Rule: Requires Covered Entities and Business Associates to provide certain notifications following breaches of unsecured PHI.

Where Agilent is a Business Associate, we partner with our Covered Entity customers to ensure that appropriate HIPAA-compliant agreements and controls are in place.

ISO 27001

ISO/IEC 27001:2022 is an information-security standard that controls the following aspects of the security-management system of a company:

- Information-security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development, and maintenance
- Supplier relationships
- Information-security incident management
- Information-security aspects of business continuity management
- Compliance with internal requirements such as policies, and with external requirements such as laws

The SLIMS platform has been ISO 27001 certified by an independent auditor for its development, management, and support for its cloud deployment.

21 CFR Part 11

US FDA Part 11 in Title 21 of the Code of Federal Regulations (CFR), and its EU analog, Eudralex Chapter 4, Annex 11, describe the requirements for electronic records and electronic signatures for regulated pharmaceutical organizations. Released in 1997, 21 CFR Part 11 has been enforced since 1999. The intent of these guidelines is to ensure that all appropriate electronic records are attributable, legible, contemporaneous, original, accurate, and maintained with integrity. A White Paper provides a detailed description of how Agilent supports users and their organizations in achieving the requirements of each section of those regulations. The descriptions assume that system access, including instrument hardware and software, is controlled by the staff responsible for the electronic records contained on the system. Thus, the system is designed as a "closed system" as defined in 21 CFR Part 11.3(b)(4) For more details, please refer to the resource *Support for Title 21 CFR Part 11 and Annex 11 compliance: Agilent SLIMS 7.2*.

Conclusion

As described in this document, an extensive set of security measures are put in place by Agilent during development, implementation, deployment, and support of SLIMS. These measures ensure that confidentiality and privacy of customer data is at the top of our considerations in providing customers with a robust, powerful, and highly secure digital solution for the laboratory.

www.agilent.com/chem/agilentslims

DE-003734

5994-8075EN
Revision 1.0

Printed in the USA, Jan 14, 2025

Agilent
Trusted Answers