Agilent CrossLab Service Management

Technical Security Measures

Notices

Manual Part Number

5994-5168EN

Edition

August 2022

Copyright

Printed in the USA

Agilent Technologies, Inc.
2850 Centerville Road
Wilmington, DE 19808

Warranty

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Agilent disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Agilent shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Agilent and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

Restricted Rights Legend

U.S. Government Restricted Rights. Software and technical data rights granted to the federal government include only those rights customarily provided to end user customers. Agilent provides this customary commercial license in Software and technical data pursuant to FAR 12.211 (Technical Data) and 12.212 (Computer Software) and, for the Department of Defense, DFARS 252.227-7015 (Technical Data - Commercial Items) and DFARS 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation).

Safety Notices

CAUTION

A CAUTION notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a CAUTION notice until the indicated conditions are fully understood and met.

WARNING

A WARNING notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

About This Guide

The CrossLab Service Management Technical Security Measures guide describes various types of configurations and the security associated with these configurations.

Scope

The purpose of this document is to outline the strategies, control mechanisms, and 3rd audit & verification measures for the security management practices of the CrossLab Service Management (the "Service"), one of Agilent's Enterprise SaaS products.

Purpose

The purpose of the security management practices is to ensure information stored and accessed through the service 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.
- 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.

This page intentionally left blank.

Contents

This page intentionally left blank.

Introduction to CrossLab Service Management

CrossLab Connect is Agilent's software application suite of digital services that provides a lab-wide instrument and lab management application that lets you focus on the science and business results. Through CrossLab Service Management, your permissioned users can request instrument service, receive real-time updates to service status, and view service history and pending services across assets and labs when and where needed. With views to see all assets and service levels, and the ability to request edits to asset information, group assets, and instruments to match your organization, you can take proactive steps to manage your instruments and plan your service strategy.

The system is designed to provide secure and real-time updates to service information and asset data. Users can request services for instruments, see service history, and view upcoming service events. The software is browser-based and users and instruments can be grouped to limit features, views and privileges. All users and user groups are identified and authenticated upon login prior to accessing any asset or service details.

Approach to Security

Agilent works continuously with researchers, lab managers, and administrators to identify information security needs, and teams up with experts in 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 cross-sites injection
- Viruses hidden in email attachments
- 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 two layers of the application framework to maximize security precautions:

- Application protection
- Network protection and monitoring

Application protection

CrossLab Service Management is built upon an application stack which integrates best-in-class operating systems, database-servers, and application servers. Agilent continuously updates all components of the stack with the latest security patches and releases to prevent unauthorized attempts to gain access or control of the service. Any service application deployed within the customer environment residing on a customer-maintained server or personal computer needs to adhere to operating system, security software, and security patches and releases that are consistent with the customer policies and controls.

Authentication

Only authorized individuals who are registered via Agilent's enterprise single sign-on solution (Okta) are provided access to CrossLab Service Management.

Authenticated system access

Accessing the service requires authentication with a login identifier and password. All login identifiers are unique and all passwords are always encrypted. All successful and failed service login attempts are logged to identify suspicious activity trends.

Customer Identity

The identity of the customer and their association with a specific institution, as well as other entitlements, are passed through a JSON Web Token (JWT), secured and signed by the enterprise Okta solution according to accepted best practices.

Strong passwords

The service requires all passwords be at least six characters, and include a combination of alphabetic and numeric characters. Agilent salts and encrypts all stored passwords.

Inactive session termination

To mitigate the risk of unauthorized access from a user forgetting to log out of the service, sessions will be automatically terminated after 30 minutes.

Server access

Only registered administrators have access to the service server infrastructure. Secure, unique passwords are required for each administrator. All server access attempts are audited by Agilent.

Authorization

Application security rules engine allows application, object, and row level security leveraging Active Directory Federation Services (ADFS). This security is controlled at the individual user level through assigned roles.

Data partitioning

Data is partitioned at a company level. Users can read asset information for the company to which they have access.

Data privacy

No Personally Identifiable Information (PII) is maintained. All customer username and passwords are managed in accordance with established company and government guidelines. User accounts and information (username, password, and email) can be deleted at any time upon customer request. If a user leaves the company and must be deprovisioned, it is the responsibility of the company using the service to notify Agilent.

Agilent access to information

All Agilent access to asset usage information is controlled by the following policies and conditions:

- Access for the purpose of user support and review
- Access for the purpose of maintenance and development: this access is restricted to the Agilent Cloud Site Reliability team and necessary members of the Agilent CrossLab R&D Software Engineering and Marketing groups; all other Agilent staff must work through these groups for access.

Customer usage of the product may be monitored through services such as Google Analytics for product support and development purposes.

Auditing

Agilent maintains detailed logs of access to and modification of all information in the service. Audit trails are protected from unauthorized modifications. Audit entries capture:

- Username
- Date and time of login
- 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, test, staging, and production environments are maintained.
- All temporary accounts, usernames, and passwords are removed before an application is released to customers.

- Source code is reviewed, and applications are tested 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.

Network protection

Network security

CrossLab Service Management engages multiple points of security to ensure the privacy of the data collected and to ensure compliance with customers' security policies. All communication is one direction, initiated from inside the customer firewall. No communication is initiated by the external servers. Service request data sent to Agilent uses HTTP and SSL. The Amazon Web Services (AWS) cloud computing environment leverages the AWS Virtual Private Cloud (VPC), subnet, and security group services to isolate the application from the Internet and other networks.

The service deploys multi-level security products from leading security vendors and proven security practices ensure network security.

- To prevent malicious attacks through unmonitored ports, external firewalls allow only SSH, HTTP, and HTTPS traffic on specific ports.
- All data is encrypted in transfer with strong encryption standards such as AES-256 to prevent sniffing/eavesdropping attacks.
- Web based applications that collect or display customers' data do not allow access through unsecured HTTP and redirect all HTTP connections to HTTPS (SSL/TLS).
- Remote administration protocols such as SSH are tunneled through the Agilent secured Virtual Private Network (VPN). Telnet, FTP, or VNC are never used for remote administration.

- Router Access Control Lists (ACLs) are configured to refuse any type of network connection that is not explicitly allowed by the ACL rules.
- The ability to make changes to the router ACLs is limited to one single user account. - High availability routers are in place and configured to provide failover services in the event of primary router failure.

Monitoring

Agilent has implemented systems to monitor security and immediately alert the service team of suspicious activity to allow a response before the first level of defense is breached.

The enterprise monitoring application on host machines is configured to alert support staff personnel when predefined system thresholds are exceeded that include, but are not limited to, the following:

- Disk space
- CPU load
- Memory usage
- Backup success and failure
- Connectivity and availability

Data security

All customer data is stored on the enterprise cloud owned by Agilent in AWS and is Agilent secured. In accordance with Agilent Data Security policies, all Agilent users, including support and maintenance functions, who access data must have current training as per company policy on customer data security.

Information Security Management

Compliance

Agilent is ISO 27001 information security management certified.

Physical security

All physically stored data are stored in SOC 2 accredited data centers.

Site status

Site status and disruptions can be accessed through:

https://status.agilent.com/

Application Support

Customer support communication for this application is managed through a third party application. For more information, please visit:

https://www.teamsupport.com/customer-support-software-security

Data Privacy

Agilent Technologies, Inc. and its subsidiaries are committed to protecting and maintaining privacy. To view the entire Customer Privacy Statement, please visit:

https://www.agilent.com/home/privacy-policy

CrossLab Connect Digital Services Accelerate Laboratory Excellence

CrossLab Connect leverages transformative digital technologies to increase operational efficiency. The Agilent CrossLab Digital Solutions amplify the performance of the lab operations through enhanced lab-wide visibility, access to previously unavailable instrument diagnostic data, and expert guided advanced analytics designed for the lab. CrossLab Connect helps show all the benefits of a smart, connected lab.

Learn more at **www.agilent.com/crosslab**.

www.agilent.com

DE54636771

August 2022

5994-5168EN

Agilent