Agilent

Agilent CrossLab Connect

Technical Security Measures

Notices

Manual Part Number

5994-5168EN

Edition

First Edition, September 2024

Copyright

Printed in the USA

Agilent Technologies, Inc.
5301 Stevens Creek Blvd.
Santa Clara, CA 95051

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.

Contents

This page intentionally left blank.

About This Guide

The CrossLab Connect (CLC) Technical Security Measures guide describes configurations and the technical and organizational security measures that apply to CLC.

The Technical Security Measures have been designed so that information is reasonably available, secure, and usable when required adhering to the following key principles:

- **Least Privileged Access**: Access to information is provided only to those individuals who have a need to know within Agilent. The customer administrator is responsible for managing access within their organizations.
- **Data Quality**: Procedures are in place to support the completeness and accuracy of information and to protect against unauthorized modification, using, where appropriate, information access and modification tracking.
- **Data Integrity**: Provide secure data transfers to Agilent.

CrossLab Connect: Description

CLC is a suite of applications that collects information from connected laboratory assets through software and sensor technologies and displays asset operational data in a dashboard. Customers can view the data, report issues to Agilent, and schedule service calls through the platform. CLC provides a lab-wide view of the customer's connected laboratory assets.

Some applications may require hardware components, on-site activation, and installation. In some cases, additional services may need to be purchased separately.

CrossLab Service Manager

CrossLab Service Manager is a cloud-based application that provides controlled access to asset service information. Authorized users can digitally place and track requests for instrument repair, maintenance, and consumables replacement, and view service agreement status and service history.

Within CrossLab Service Manager, customer administrators have privileges to submit requests to update asset data, organize assets into groups that correlate to their organization's structure, and grant individual users access to view select assets and service data.

CrossLab Inventory Manager

CrossLab Inventory Manager is a cloud-based application that provides tools for authorized users to view and filter their assets, scan barcodes and QR codes, and export customized lists of assets to analyze and collaborate from a shared set of data.

Figure 1 CrossLab Inventory Manager.

CrossLab Asset Monitoring

CrossLab Asset Monitoring is an asset use monitoring service that collects and aggregates Asset Utilization Data, sends the Asset Utilization Data to a cloud-based software platform that performs analytics, and displays the data for the user on the CrossLab Dashboard. Asset Utilization Data is information concerning asset use activity that can be compiled to determine use patterns of the asset.

CrossLab Asset Monitoring consists of the following: File Monitoring, System Monitoring, and Power Monitoring.

- File Monitoring uses the File Monitor Utility (an on-premises software program installed on the customer's server) to collect and transmit Asset Utilization Data from operational files within the asset data collection software. This information is packaged into an XML extract and sent through the Lab Manager Gateway (an on-premises software program installed on a customer's PC or server) to Agilent servers to be displayed in the CrossLab Dashboard.
- System Monitoring collects Asset Utilization Data using software and hardware designed to communicate with Agilent (and some non-Agilent instruments) and securely sends the data through the Lab Manager Gateway to Agilent servers to be displayed in the CrossLab Dashboard.
- Power Monitoring uses Wi-Fi-enabled sensor hardware attached externally to assets to monitor power consumption variations. The power consumption data are transmitted to Agilent servers where the power data are interpreted and sent to be displayed in the CrossLab Dashboard.

The monitoring service engages multiple points to enhance the security of the data collected.

- All communication is one direction, initiated from inside the customer's firewall. No communication is initiated by the external servers. Asset monitoring data are sent to Agilent using HTTPS and SSL/TLS.
- File Monitor and System Monitor both leverage the CrossLab Lab Manager Gateway for outgoing communications. The gateway communicates to Agilent with a predefined set of URLs:
  - **https://raemanager.agilent.com**
  - **https://*.amazonaws.com**
  - Outbound Port: HTTPS Port 443

NOTE

Multiple URLs to amazonaws.com are used. Using the *.amazonaws.com wildcard filter has proved to be an effective and efficient approach.

Power Monitor connects to the customer Wi-Fi network using 802.11 b/g/n protocols or 802.1x in the 2.4 GHz ISM Band and uses DHCP. The following Wi-Fi network security options are supported:

- Broadcasted and unbroadcasted SSID
- WEP

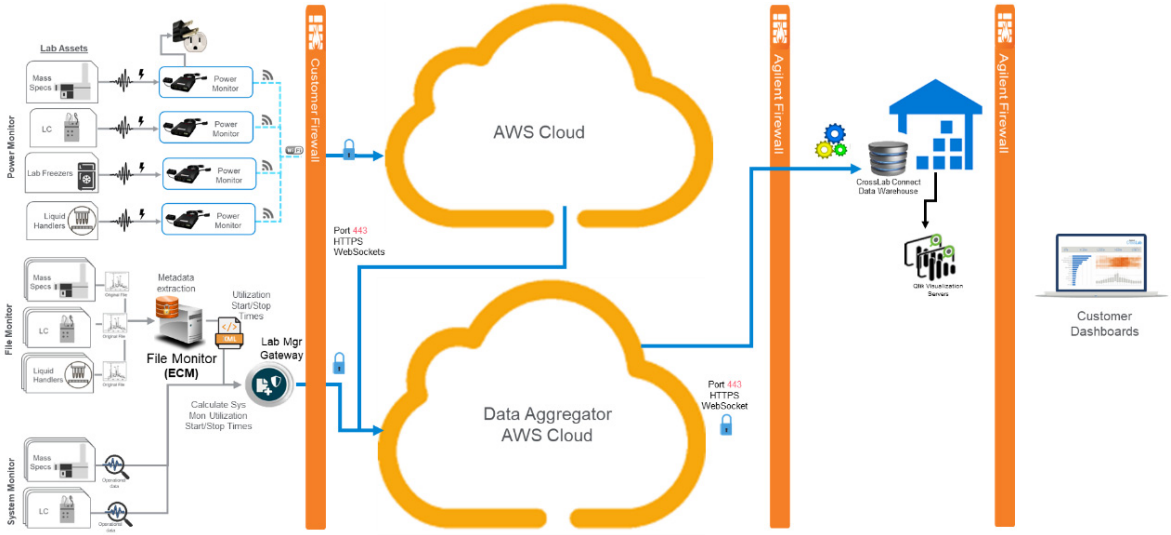

Figure 2 Asset monitoring infrastructure.

CrossLab Smart Alerts

CrossLab Smart Alerts is a PC-based software application that monitors Early Maintenance Feedback (EMF) data from Agilent instruments and alerts users by email when maintenance and/or consumables replacement are recommended, based on predefined templates. The emails are sent to the address(es) added by the customer's designated administrator and will consolidate alerts from assets across the lab. A copy of preventive maintenance alert emails, but not consumables alerts, will also be sent to Agilent unless the customer opts out of this option in the CrossLab Smart Alerts Admin Configuration menu. Maintenance notification emails provide links to order Agilent parts and consumables and request service for the instrument.

When EMF counters are reset on the instrument, the results are captured in the CrossLab Smart Alerts EMF Reset History table, providing a record of the instrument's maintenance history.

Smart Alerts operates independently of the chromatography data system (CDS) and communicates directly with the instrument. It does not change any instrument settings. For instruments isolated from the laboratory, network communication can also be achieved using the Smart Alerts relay service software.

Smart Alerts software is installed on a PC in the lab. If enabled, the Remote Assist feature allows end users to immediately send a service request to Agilent.

1. Choose to use Smart Alerts with a standalone instrument.
2. Connect instruments or workstations to a local area network for lab-wide monitoring.
3. Connect Smart Alerts to an email server.
4. Connect to the Internet to enable direct ordering of replacement consumables and other capabilities.

Smart Alerts basic installation

Smart Alerts communicates to Agilent instruments over the same local area network (LAN) used by the CDS. Users can access the Smart Alerts user interface through a web browser on the Smart Alerts PC.

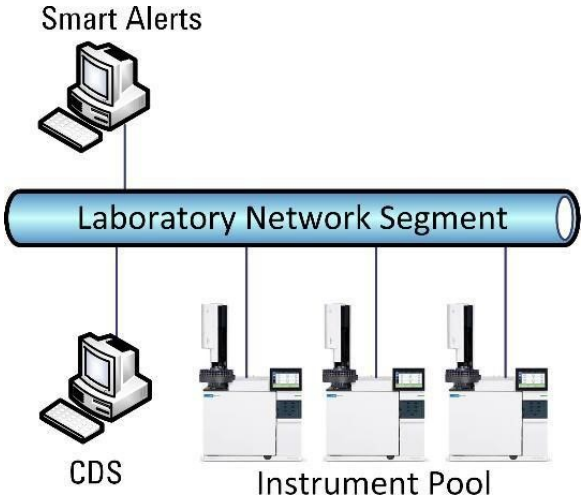

Figure 3 **Smart Alerts basic installation.**

Smart Alerts LAN installation

Users can access Smart Alerts from other PCs connected to the network. Users can connect to Smart Alerts by entering the IP address or hostname of the Smart Alerts PC followed by :1337 into the address field of Microsoft Edge, Google Chrome, or Firefox web browsers. Examples are: http://192.168.10.10:1337 or http://CN321:1337. Port 1337 is the listening port for Smart Alerts incoming user connection requests. The default installation of Smart Alerts is HTTP as all data are contained behind the customer firewall. During installation configuration, the customer is presented an option to install using HTTPS.

Windows Defender and antivirus software firewalls will block unsolicited inbound communications to the computer on many TCP ports. Create an inbound rule in Windows Defender or the antivirus software firewall to enable TCP ports 1337 and 9705.

Not all instruments connect to laboratory networks. In many OpenLab, Empower, and Chromeleon configurations, instruments connect to a small, isolated network on a second network interface of the CDS or acquisition PC.

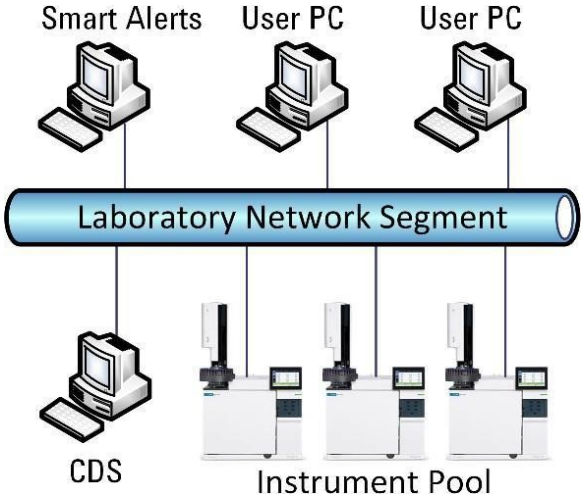

Figure 4 Smart Alerts LAN installation using small, isolated network, second network interface of the CDS or an acquisition PC.

Installation of Smart Alerts on the CDS or acquisition PC may not be allowed. It is also not practical to install Smart Alerts on CDS PCs when multiple configurations (**Figure 5**) exist in the laboratory.

A Smart Alerts connection to the instruments in the configuration (**Figure 5**) appears to be impossible, because the CDS PC isolates the instruments from the Laboratory Network Segment.

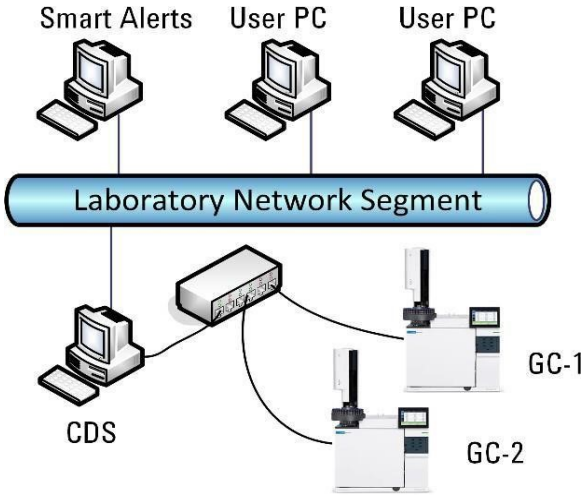

Figure 5 Smart Alerts LAN installation on CDS PCs with multiple configurations in the laboratory.

The Agilent TCP relay service is a port forwarding service that listens for commands from Smart Alerts on the LAN network interface, then forwards the commands to the instrument on the isolated instrument network (Figures **6** and **7**).

Configuration of the relay service is executed from the Smart Alerts PC.

Windows Defender and antivirus software firewalls will, by default, block unsolicited inbound communications to the computer on many TCP ports.

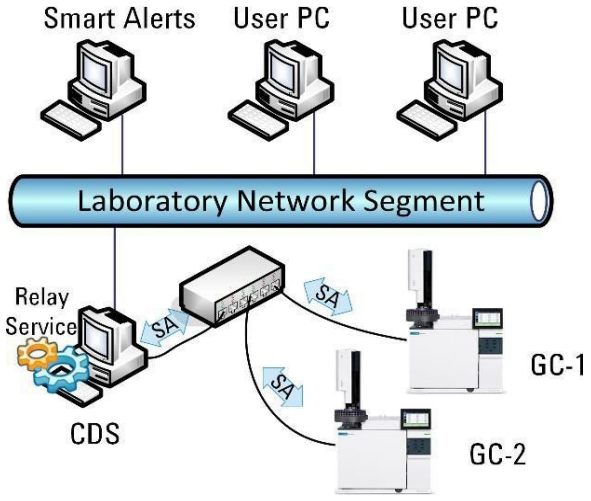

Figure 6 Smart Alerts LAN installation using Agilent TCP relay service.

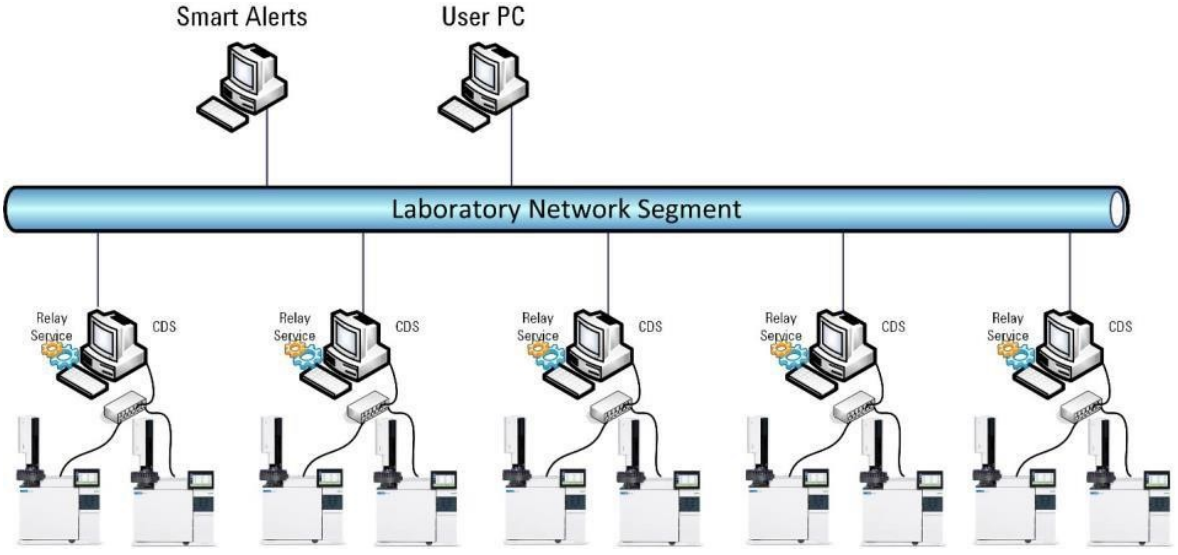

Figure 7 Networked example with multiple CDS using Agilent TCP relay service.

Firewall filters

Alerting communications require that firewall filters be enabled to allow communications to the TCP ports, as outlined in **Table 1**.

Table 1 Communications requirements.

Application	Inbound or outbound filters	TCP port numbers
Smart Alerts application for access from other PCs on the network	Inbound ports on Smart Alerts PC	1337 9705 9703 (used when migrating Smart Alerts to a new PC)
Agilent email server	Outbound Internet to Amazon Web Services (AWS)	443 URL: **https://*.amazonaws.com**
Smart Alerts desktop notification	Inbound ports on Desktop notifications PC	1337 9705
Smart Alerts connection to Agilent Licensing Portal	Outbound Internet to **Agilent.com** and **Flexnet.com**	443 URL: **https://flex1613-fno.flexnetoperations.com**
Agilent TCP relay service	Inbound ports Relay service (CDS) PC	9068 9100-9103

HTTP or HTTPS installation option

Alerting can be installed for the user web interface to use either HTTP or HTTPS. HTTPS encrypts all communications between Smart Alerts and the user's PC. A security certificate warning message will display when first accessing the Alerting app if it was installed as HTTPS.

Security certificates can only be created after the installation of the Alerting app. Security certificates must be created and installed by the IT department to eliminate security error messages when accessing Alerting.

Technical and Organizational Measures

The CLC team within Agilent works with researchers, lab managers, and administrators to support customer information security needs, but the customer is responsible for identifying their own needs. Security is a company-wide priority at Agilent, and we continuously invest in our people, processes, and tools to strengthen our security posture to protect both Agilent and our customer's data.

Technical security measures are in place to guard against security threats. Agilent takes measures across the multiple layers of the application framework to maximize security precautions.

Hardware protection

Agilent hosts services in our ISO 27001 data center and our AWS environment, providing protection from unauthorized access; there are disaster recovery plans and best practices in place to maximize uptime.

Application protection

CLC is built upon an application stack which integrates best-in-class operating systems, database-servers, and application servers. Agilent has technical and organizational security measures in place to prevent and monitor unauthorized attempts to gain access or control of the service. Service applications deployed within the customer environment residing on a customer-maintained server or personal computer need to adhere to operating system, security software, and security patches and releases that are consistent with the customer policies and controls.

Authentication

Authorized individuals who have registered accounts on Agilent.com are provided access to CLC through Agilent's identity management system in accordance with the following security principles.

- **Authenticated system access**

  Accessing the service requires authentication with a login identifier and password. Login identifiers are unique, and all passwords are always encrypted. 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 strong passwords that include a combination of alphabetic and numeric characters. Agilent salts and encrypts stored passwords.

- **Two-factor authentication**

  Agilent uses email-based, two-factor authentication to validate customer authorization. Asset Monitoring users are required to enter their corporate email account when creating their account. At login, a verification code is sent to their corporate email account. This verification code is required to complete their login.

- **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. Server access attempts are audited by Agilent.

- **Authorization**

  The 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 segregation**

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

- **Data privacy**

  To provide the service and access to CLC, Agilent collects and processes non-sensitive personal data including customer usernames and contact details. Such data are processed in accordance with Agilent's Privacy Policy available at **https://www.agilent.com/home/privacy-policy**.

  User accounts and information (username, password, and email) can be deleted 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.

- **Access to CLC data**

  Agilent may access data in CLC for the following purposes:

  - To provide user support and review
  - To provide maintenance, improvement, and development

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

Auditing

Agilent has measures in place aimed at tracking access and modification of information in the service.

Auditing user activity

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 (e.g., SQL injection)
- Cross-site request forgeries (CSRF)
- Improper error handling
- Logical data separation to ensure that one customer's data are not visible to others even in the case of programmer error
- Protection of customer data from corruption even in case of programmer error

Network protection

CrossLab Connect engages multiple points of security to ensure the security of the data collected and to ensure compliance with customers' security policies.

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 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 are encrypted in transfer with strong encryption standards such as AES-256 to prevent sniffing/eavesdropping attacks.
- Web-based applications that collect or display customer 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 alert the service team of suspicious activity to enable appropriate response and action to be taken.

The enterprise monitoring application on host machines is configured to alert Agilent support staff when predefined system thresholds are exceeded that include:

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

Disaster recovery

Agilent's disaster recovery plan is designed to protect your information stored in CLC and ensure business continuity.

The CLC disaster recovery plan ensures the safety and integrity of your data in a catastrophe. A multi-tiered data security approach includes regular data backups that are replicated to geographically remote facilities to ensure data availability and prevent data loss. The disaster recovery plan includes efficient data restoration processes to minimize downtime due to a disaster event. Disaster recovery drills are executed to ensure the plan is effective and up to date.

Data security

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

Site status

Site status and disruptions can be accessed through: **https://status.agilent.com/**

Application support

Customer support for this application is managed through the email address: **crosslab.support@agilent.com**.

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**

Digital Services to Accelerate Laboratory Excellence

CrossLab Connect leverages transformative digital technologies to increase operational efficiency. Agilent CrossLab Digital Solutions amplify the performance of 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**.

This page intentionally left blank.

www.agilent.com

DE-000570

First Edition, September 2024

5994-5168EN