

# Product Security Information Guide

SampleManager LIMS™ Software | Version 21.2 | September 2023

Document valid through September 15, 2024

## Introduction

Thermo Fisher Scientific maintains a Cybersecurity Program, led by a dedicated Chief Information Security Officer (CISO), designed to safeguard the confidentiality, integrity, and availability of data and systems within our environment. Thermo Fisher Scientific supports a continuously improving security program model that is focused on reducing risk, defending against threats, maintaining data privacy, and protecting our company's confidential information, including trade secrets and intellectual property.

# About this guide

Thermo Fisher Scientific has implemented safeguards and procedures designed to help protect the Thermo Scientific™ SampleManager Laboratory Information Management Software (LIMS) Version 21.2 against intrusion or data compromise. This document applies only to SampleManager LIMS Version 21.2 deployed within the customer's environment. It describes the various standards, controls, data security approaches, and business practices that Thermo Fisher Scientific has employed for this configuration.

Due to the ever-changing cyber landscape, Product Security Information Guides are updated annually to ensure accurate information is being provided to our customers. This guide expires on **September 15, 2024**. Please reach out to your account representative to obtain the latest published version.

The information contained in this Product Security Information Guide is for reference purposes only. Nothing contained in this

document or relayed verbally to any customer will be deemed to amend, modify, or supersede the terms and conditions of any written agreement between such customer and Thermo Fisher Scientific, or Thermo Fisher Scientific subsidiaries or affiliates (collectively, "Thermo Fisher Scientific"). Additionally, this Product Security Information Guide does not create an independent contract or agreement between any customer and Thermo Fisher Scientific. Thermo Fisher Scientific does not make any promises or guarantees to customers that any of the methods or suggestions described in this Product Security Information Guide will restore customer's systems, resolve issues related to any malicious code, or achieve any other stated or intended results. The customer exclusively assumes all risk of utilizing or not utilizing any guidance described in this Product Security Information Guide.



# Corporate Cybersecurity Program

Thermo Fisher Scientific maintains a Cybersecurity Program that includes technical, administrative, and physical safeguards designed to detect vulnerabilities and mitigate against potential threats. Controls include web application firewalls (WAFs), intrusion detection systems (IDSs), multiple-endpoint detection

and response solutions, multifactor authentication (MFA), and email protection. Thermo Fisher Scientific's Cybersecurity Program maintains International Organization for Standards (ISO) 27001:2013 certification.



# Product overview

SampleManager LIMS Software delivers laboratory management, scientific data management, and process execution/procedural electronic laboratory notebook (ELN) capabilities in a single solution. Laboratories across many industries, including pharmaceutical, food and beverage, oil and gas, petrochemical, water and environmental, manufacturing, and contract testing rely on SampleManager LIMS Software to unlock the power of their laboratory data.

SampleManager software can be deployed on premises or in the Amazon Web Services™ (AWS) cloud. On-premises server deployments or deployments to a customer's own cloud hosting service are managed by the customer based on their infrastructure standards.

Note: This Product Security Information Guide refers only to on-premises deployments and not the SampleManager LIMS cloud subscription service.

## System compatibility

SampleManager LIMS Software Version 21.2 is supported on the following operating systems, databases, and browsers:

- Database server
  - Oracle™ 19c
  - Microsoft SQL Server™ 2019
  - PostgreSQL™
- Application and web server operating systems
  - Microsoft Windows Server™ 2022
  - Microsoft Windows Server 2019
- Web portal server operating system
  - Microsoft Windows Server 2022
  - Microsoft Windows Server 2019

- Client operating systems
  - Microsoft Windows™ 11 x64 Professional
  - Microsoft Windows 11 x64 Enterprise
  - Microsoft Windows 10 x64 Professional
  - Microsoft Windows 10 x64 Enterprise
  - + Citrix XenApp Server™ 7.15, connecting using Citrix Receiver™ for Web
- Web application and web portal browsers
  - Microsoft Edge™
  - Google Chrome™

Any combination of server and client operating system can be used. If the database is installed on the same machine as the SampleManager LIMS Software application server, the database version must be compatible with the server operating system.

## Relevant security certifications and regulatory standards

SampleManager is developed under a Quality Management System, which is certified to the International Organization for Standardization (ISO) 9001:2015. Through continual improvement and regular assessment, this certification helps ensure clear, repeatable processes for software development activities. Our ISO 9001:2015 certificate can be accessed at the [Thermo Fisher Scientific Digital Science Support Resource Center website](#).

**Note:** User authentication is required to access the Thermo Fisher Scientific Digital Science Support Resource Center website. A customer must have a valid support agreement to access the website. If you have questions, please contact a Thermo Fisher Scientific technical support resource for more information.

# SampleManager LIMS Software architecture diagram

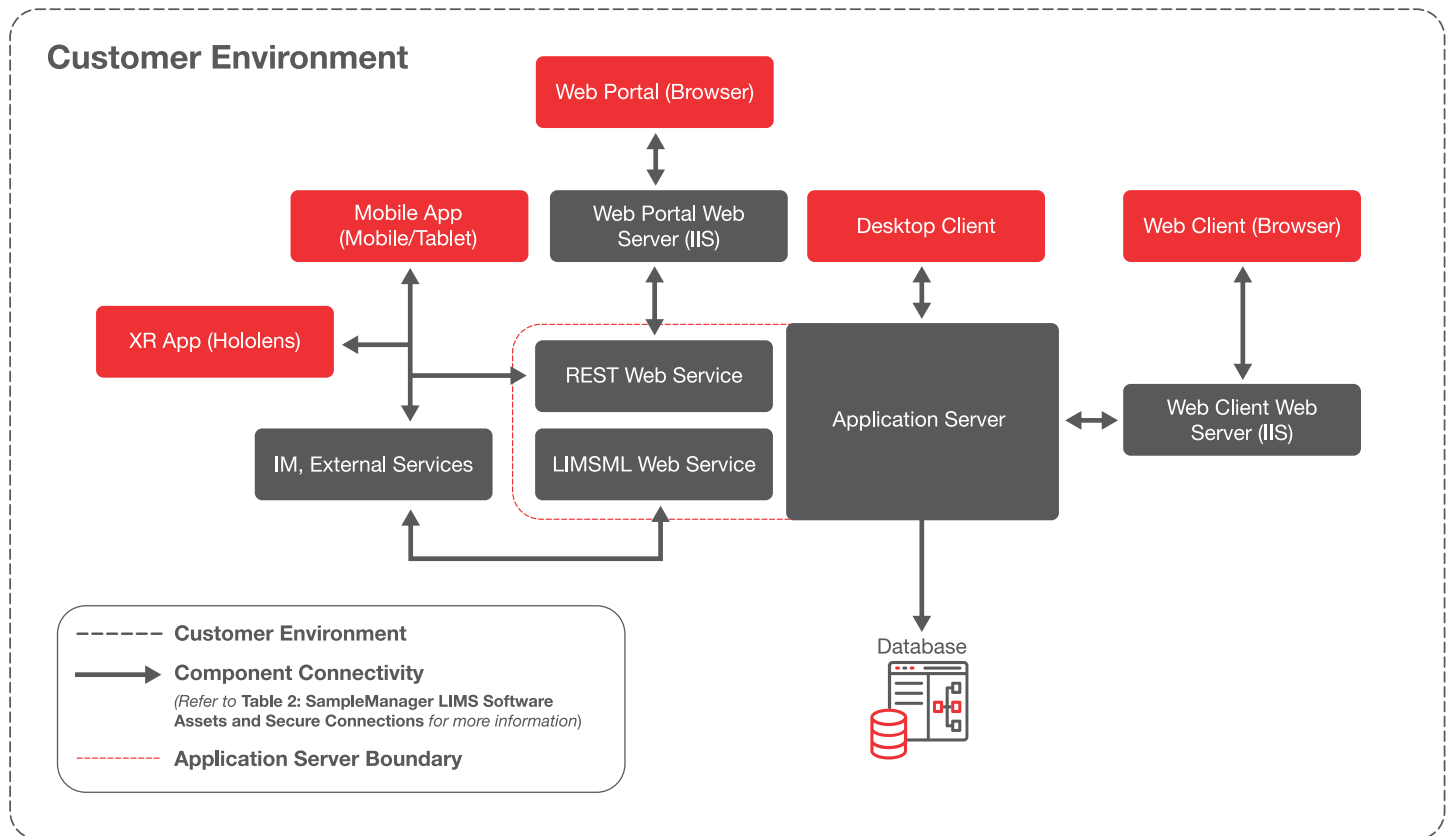


Figure 1: SampleManager LIMS Software architecture diagram

## Architecture component terms and definitions

Component term	Definition
Application server	The main service for SampleManager LIMS Software application connections. A client (desktop, web portal web server or web client web server) makes a request to a connection service through a TCP/IP port which will run a dedicated process to serve the client.
Database server	Stores all the data about the laboratory and the samples it processes. Customers have multiple database options: Oracle, SQL Server or PostgreSQL, where the application server uses Microsoft ActiveX™ Data Objects (ADO) to allow the application code to be agnostic of database vendor. The database features used are simple and limited to tables, fields, views, indexes, and sequences. No stored procedures or triggers are used.
Web application server (IIS)	The web server for web clients which is managed by Microsoft Internet Information Services™ (IIS).
Web portal server (IIS)	Web server for the web portal managed by IIS.
REST Application Programming Interface (API) web service	The REST application programming interface (REST API) allows external agents to connect with SampleManager LIMS Software using the JavaScript Object Notation (JSON) open standard file format. This is internally used by the mobile app, XR App (defined below in this table), and the web portal.
LIMSML web service	The Simple Object Access Protocol (SOAP) used to exchange XML data with external agents. The LIMSML web service is still supported but not actively developed.
Desktop client	Windows Forms client that runs on either Windows 10 or 11.
Web application client	The main web browser client; it provides most of the functionality offered on the desktop client.
Web portal client	The web browser client for the web portal. It offers limited functionality and is intended primarily for the customers of contract labs to submit work.
Mobile app (mobile/tablet)	A downloadable app available for Apple iOS™, Google Android™ and Microsoft Windows Universal Windows Platform™ (UWP), available from each company's respective app store. It connects to SampleManager LIMS Software application server through REST APIs.
XR App	A dedicated Microsoft HoloLens™ device app providing a new interface to SampleManager LIMS Software features. The app can be downloaded from the Microsoft Store™.
External services	External services can interface with SampleManager LIMS Software using REST APIs.

**Table 1:** Architecture component terms and definitions



# Access controls

## Authentication

SampleManager LIMS Software provides three authentication mechanisms to suit environment-specific needs:

- **SampleManager LIMS Software native authentication:** This is the default configuration for authentication. SampleManager LIMS Software creates a unique record for each user in the SampleManager LIMS Software database. Users will be required to authenticate using their SampleManager LIMS Software credentials (username and password), which are stored on the customer system hosting the SampleManager LIMS Software.
- **Domain authentication:** Users authenticate using their network domain credentials. SampleManager LIMS Software validates the user-supplied credentials on domain controllers on the customer's network. Once the user authenticates, the roles assigned are those defined within SampleManager LIMS Software.
- **Single sign-on (SSO) authentication:** Customers can utilize their organization's Identity Provider (IdP) to verify user access to SampleManager LIMS Software. Authentication via SSO allow users to launch the SampleManager LIMS Software desktop client or web client and log into a specific application server without having to enter their credentials at login. Once the user authenticates, the roles assigned are those defined within SampleManager LIMS Software.

To learn more about each authentication method, please refer to the [SampleManager LIMS Documentation section "Accessing SampleManager" \(System Administration > Security > Accessing SampleManager\)](#).

**Note:** User authentication is required to access SampleManager LIMS Documentation. A customer must have a valid support agreement to access the website. If you have questions, please contact a Thermo Fisher Scientific technical support resource for more information.

Thermo Fisher Scientific recommends that customers configure reauthentication prior to performing critical operations using e-signatures. Thermo Fisher Scientific also recommends that customers configure user notifications on critical operations

such as password resets. Please refer to the [SampleManager LIMS Documentation Messaging section \(Getting Started > User Interface > SampleManager Messaging\)](#) for more information.

## Authorization

SampleManager LIMS Software leverages role-based access control (RBAC) to grant permissions and access to users. Roles are configurable to meet necessary business requirements. Thermo Fisher Scientific recommends that role assignments be configured using the principle of least privilege based on the user's need to manage and support the SampleManager LIMS Software.

## Firewall and network controls

The application server firewall must be configured to allow SampleManager LIMS Software clients (desktop application, web application, and web portal) to communicate with the SampleManager LIMS Software servers (application server, web application server, and web portal server). The default SampleManager LIMS Software application server port is 56100. For the web application server and web portal server, the customer must configure the ports used for these connections with the SampleManager client. Please refer to the [SampleManager LIMS Documentation section "Setting the Port Number for the SMDaemon Service" \(System Administration > Operating Environment > Windows Services > Setting the Port Number for the SMDaemon Service\)](#) for more information.

Thermo Fisher Scientific recommends that customers configure firewall rules to only allow necessary traffic to and from the SampleManager LIMS Software servers (application server, web application server, and web portal server).

## Password management

Strong password creation, structure, and renewal policies can help prevent unauthorized system access. For customers leveraging the SampleManager LIMS Software default authentication, the software prompts customers to change the initial password upon first login. It also provides functionality

to enable customers to configure passwords that adhere to their business requirements. The passwords stored in SampleManager LIMS Software are “hashed,” or converted by algorithm into a fixed-length string of letters and numbers adhering to industry standards.

For customers delegating authentication to the domain controller or to the IdP, the password policy requirements are those set by their domain controller or IdP.

Thermo Fisher Scientific recommends that all password requirements be based on industry best practices and standards, such as compliance with the National Institute of Standards and Technology (NIST) standards and guidelines.

### Logging and auditing functions

Auditing and recording system user activities and processes are critical security functions. Auditor functionality provides customers with the ability to record any changes made to any data stored in SampleManager LIMS Software. Auditing can be applied to an individual table or an individual field within a table. There are three types of audit attributes that determine how the audit interacts with a user: No Audit, Silent Audit, and Prompt Audit.

- **No Audit:** Records of changes to data stored on the table will not be tracked.
- **Silent Audit:** Changes to the table are recorded, but the user is not informed or required to enter an explanation for the changes made.

- **Prompt Audit:** Changes to the table are recorded and the user must enter a reason for the changes made.

Thermo Fisher Scientific recommends that only the system administrator role be granted permission to view audit log functionality to protect confidentiality of the data stored in audit logs. Refer to the [SampleManager LIMS Documentation section “Audit Configuration” \(System Administration > Audits > Audit Configuration\)](#) to learn about tracking table and field changes.

### Event logging

SampleManager LIMS Software utilizes the Apache log4net™ utility to generate log files for monitoring system health and performance. Each SampleManager LIMS Software application server and desktop client creates entries in the system application event log. The default setting is “Off.”

When logging is enabled, the default configuration is to log unhandled exceptions (fatal errors). Other items that can be logged include user authentication activities and/or server-side actions for application server, web application/web portal server, and desktop clients.

Customers should enable logging within the application and web servers to continually monitor system performance and health. Further information on logging capabilities as well as how to change the default storage location can be found in the [SampleManager LIMS Documentation Configuration Files section referencing log4net](#).





# Secure component connectivity

## SampleManager LIMS Software assets and secure connections

Asset	Secure connection
Application server to database server	The connection between the application and database server is configured via ADO. The communication between the application server and the database should leverage encryption mechanisms offered by the database. Instructions for configuring encryption in transit on the database can be found in the vendor-specific documentation for the selected database.
Desktop/web application/web portal clients to application/web application/web portal servers	Traffic should be configured to Hypertext Transfer Protocol Secure (HTTPS) with Transport Layer Security (TLS) 1.2 as a minimum.
Web application/web portal servers to application server	Traffic should be configured to HTTPS with TLS 1.2 as a minimum.
SampleManager LIMS mobile app to application server	Communication between the SampleManager LIMS mobile app and application server uses the REST web service. The REST web service should be configured to HTTPS with TLS 1.2 as a minimum.
XR App to application server	Communication between the XR App and the application server uses the REST web service. The REST web service should be configured to HTTPS with TLS 1.2 as a minimum.
External components to LIMSML	LIMSML should be configured to deliver the traffic over HTTPS with TLS 1.2 as a minimum, when possible.

**Table 2:** SampleManager LIMS Software assets and secure connections

### Ports and protocols

Multiple services are used to run and manage SampleManager LIMS Software. A few key services can be customer-configured. Thermo Fisher Scientific recommends encrypting network traffic through customer-configured ports. Unused ports should be closed to limit unnecessary connections and in line with industry standards and best practices.

Customers can configure the following services to leverage any port they choose:

- SampleManager Connection Service
- SampleManager Lock Service

- SampleManager Windows Communication Foundation™ (WCF) Service
- SampleManager WCF REST Service

For more information on the services used to run SampleManager LIMS Software, please refer to the [SampleManager LIMS Documentation section “Windows Services”](#).

Typically, SampleManager LIMS Software service port numbers are in the dynamic port range with default base port number 56100. Upon initial installation, SampleManager LIMS Software prompts to enter the first port number and then allocates adjacent port numbers for the remaining services.

# Data encryption methods

## Encryption at rest

SampleManager LIMS Software data can be stored in two primary locations: In the file system on the application server or web server, or on the database. To encrypt configuration files stored on the application server or web server file system, Thermo Fisher Scientific recommends that customers enable operating system-level encryption (such as Microsoft BitLocker™) or other industry-standard encryption mechanisms.

To encrypt data generated by SampleManager LIMS Software, Thermo Fisher Scientific recommends that customers utilize encryption mechanisms offered within the selected database to encrypt data at rest. Refer to instructions for configuring encryption mechanisms in vendor-specific documentation for the selected database

## Encryption in transit

Thermo Fisher Scientific recommends configuring data being sent to the application server (including the REST and LIMSML web services), web application server, and web portal server to deliver traffic over Secure Sockets Layer (SSL)/TLS. This configuration should encrypt and secure the traffic from a SampleManager client (including desktop client, web application, web portal, mobile app, and XR App) to a SampleManager server.

Additionally, Thermo Fisher Scientific recommends that the communication between the application server and the database leverages encryption mechanisms offered by the specific database. Refer to instructions in the vendor-specific documentation for database encryption mechanisms.



# Secure product development lifecycle

## Secure software development training

SampleManager LIMS Software Product Development teams complete secure software development training to further reinforce their knowledge of secure coding principles and review the latest development standards and guidelines. Additionally, Thermo Fisher Scientific colleagues receive regular updates about the latest cybersecurity trends through the corporate Cybersecurity Program. These training activities help sustain and strengthen a “security first” mindset.

## Product security assessments

Products, instruments, software, and devices are subject to custom security assessments as part of the product development lifecycle. Customization is based upon the components included with the solution and the complexity of these component interactions. The assessment may include technical review, focused testing of identified components, and regulatory review. A product security assessment includes multiple technical assessments of various components, such as a security architecture review, and software and hardware testing. The Product Development team reviews, evaluates, and prioritizes security assessment findings for remediation and acts upon them based on criticality.

## Source code management

The SampleManager LIMS Software Product Development team stores source code in a Thermo Fisher Scientific-approved version control solution that has no public exposure or access and contains built-in redundancy to support data loss prevention.

## Artifact management

The SampleManager LIMS Software Product Development team stores and maintains software artifacts including, but not limited to, executables, images, and libraries in a Thermo Fisher Scientific-approved artifact management solution that provides visibility and control on developed software builds. This allows for dependencies with known vulnerabilities to be identified and acted upon.

## Static analysis

The SampleManager LIMS Software Product Development team uses a Thermo Fisher Scientific-approved and managed static analysis tool that scans code repositories each time code is committed to the system to identify potential security defects. Conducting a static analysis scan benefits our customers by evaluating code quality and integrity through the increased efficiency of code reviews. The Product Development team reviews and prioritizes security alerts for remediation based on criticality.

## Peer code reviews

The SampleManager LIMS Software Product Development team conducts manual peer reviews of code before testing and deployment into a product. Manual code reviews provide benefit by accounting for the overall context and business logic in which the code was developed, which supplements findings from the static analysis tool.

## Web application scanning/dynamic analysis

The SampleManager LIMS Product Development team uses a Thermo Fisher Scientific-approved dynamic analysis tool to scan web applications and APIs upon execution for potential code defects and/or vulnerabilities. Unlike static analysis where the code is reviewed prior to execution, dynamic analysis identifies defects during software runtime. The SampleManager LIMS Product Development team reviews and prioritizes findings from the scans for remediation based on criticality.

## Secure APIs

Within SampleManager LIMS Software, there are two primary APIs that are available for use: REST and LIMSML web services. The SampleManager LIMS Product Development team scans APIs security vulnerabilities and resilience to outside influence prior to product release.

### Architecture review

Thermo Fisher Scientific performs a security architecture review on SampleManager LIMS Software as part of the product security assessment. Led by product security architects, the assessment consists of understanding the major components involved in SampleManager LIMS Software, their interactions and connections, and determining how security can be impacted based on the technology and configurations in use. The SampleManager LIMS Product Development team considers and prioritizes feedback and findings for remediation based on their criticality.

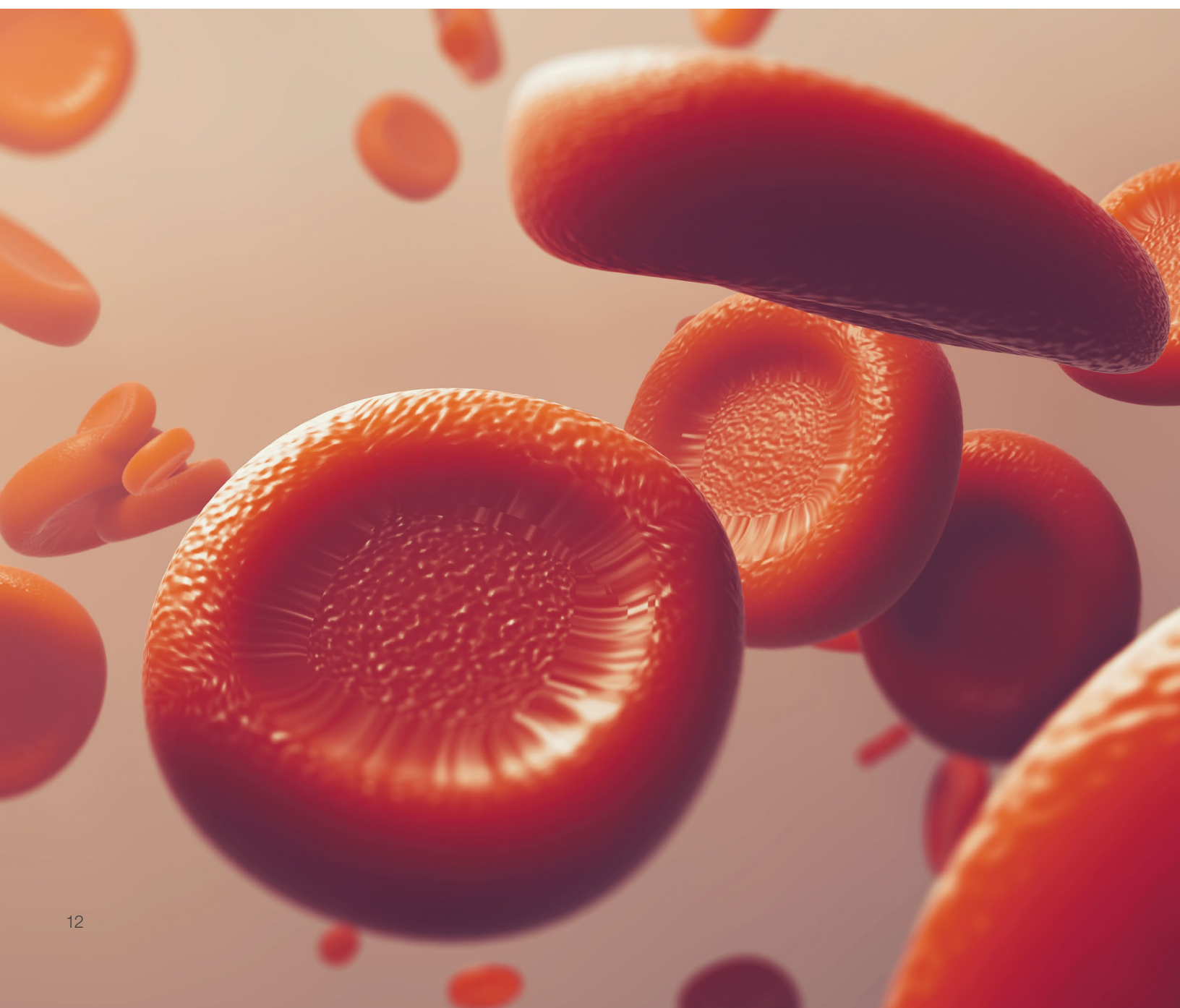
### Penetration testing

Thermo Fisher Scientific's Penetration Testing team tests core components of SampleManager LIMS Software against the Open Web Application Security Project's (OWASP) Top 10 list, a

document that represents a broad consensus about the most critical security risks to web applications. The team is comprised of trained penetration testers who use various techniques to identify potential vulnerabilities during product development.

### Vendor assessments

Our Cybersecurity Program includes security assessments of third-party vendors and service providers to evaluate and approve the solution for use within Thermo Fisher Scientific's environment. Assessments of third-party vendors and service providers are critical to help ensure that new and existing vulnerabilities and attack vectors are not introduced into Thermo Fisher Scientific's environment.



# Product security maintenance

## Vulnerability and patch management

The SampleManager LIMS Product Development team tests and validates security updates and system patches throughout the lifecycle of the product and deploys them to the impacted environments based on criticality. The SampleManager LIMS Product Development team works closely with the Cybersecurity Program to identify and remediate vulnerabilities and bundles resulting updates and security patches into a service pack release. For critical issues, the SampleManager LIMS Product Development team creates an emergency update for the affected versions and communicates the availability of the patch to customers.

Thermo Fisher Scientific recommends validating and applying patches to affected SampleManager LIMS Software versions upon notification, keeping applicable systems up to date and minimizing risk associated with vulnerabilities. Thermo Fisher Scientific also encourages customers [to report all potential security issues](#) to our Cybersecurity Program.

## Disaster recovery and business continuity

The SampleManager LIMS Software has data backup capabilities and tools based on the customer's selected database to prevent data loss and aid in restoring normal functionality. Thermo Fisher Scientific suggests that these backup capabilities and tools are leveraged and included in Disaster Recovery plans and testing in accordance with customer policy. Thermo Fisher Scientific also suggests performing regular database backups with the relevant stakeholders in accordance with policy.

Further information on the data backup capabilities and tools within the SampleManager LIMS Software can be found in the [SampleManager LIMS Documentation section "System Administration"](#) for each supported database:

- [Oracle \(System Administration > Data Storage and Handling in Oracle\)](#)
- [SQL Server \(System Administration > Data Storage and Handling in SQL Server\)](#)
- [PostgreSQL \(System Administration > Data Storage and Handling in PostgreSQL\)](#)

## System hardening


System hardening, a critical security function, can mitigate the potential exploitation of system vulnerabilities and can prevent potential threats. SampleManager LIMS Software supports various application hardening practices, including the use of antivirus software and implementing access restrictions through role-based authentication. Thermo Fisher Scientific recommends maintaining operating systems and network hardening practices on the relevant infrastructure supporting SampleManager LIMS Software.

## Service handling

Application-specific support and global training serve as critical components to deploying and successfully supporting laboratory informatics solutions. Thermo Fisher Scientific's experienced team of professionals use a global, follow-the-sun support approach for technical assistance and rapid escalation if critical issues should arise.

Please contact your Thermo Fisher Scientific Sales Representative for more information about how to purchase a Critical Maintenance and Support plan.



 Questions? To reach a member of our team and discuss this product, please contact us at [product.security@thermofisher.com](mailto:product.security@thermofisher.com)

**For Research Use Only. Not for use in diagnostic procedures.** © 2023 Thermo Fisher Scientific Inc. All rights reserved. All trademarks are the property of Thermo Fisher Scientific and its subsidiaries unless otherwise specified.

Amazon Web Services (AWS) is a trademark of Amazon Technologies, Inc. Android and Google Chrome are trademarks of Google LLC. Apache log4net is a trademark of Apache Software Foundation. IOS (iOS) is a trademark of Cisco Systems, Inc.+ Citrix XenApp Server and Citrix Receiver for Web are trademarks of Citrix Systems, Inc. Microsoft Windows, Microsoft Windows Server, Microsoft SQL Server, Microsoft Edge, Microsoft Windows Communication Foundation (WCF), Microsoft ActiveX, Microsoft Internet Information Services (IIS), Microsoft Windows Forms, Microsoft Universal Windows Platform (UWP), Microsoft HoloLens, Microsoft Store and Microsoft BitLocker are trademarks of Microsoft Corporation. Oracle is a trademark of Oracle Corporation. PostgreSQL is a trademark of PostgreSQL Community Association of Canada.