Applied Biosystems Diomni software version 4.3 | March 2026

Thermo Fisher SCIENTIFIC

Product security information guide

Applied Biosystems Diomni software version 4.3 | March 2026

Document valid through March 31, 2027

Introduction

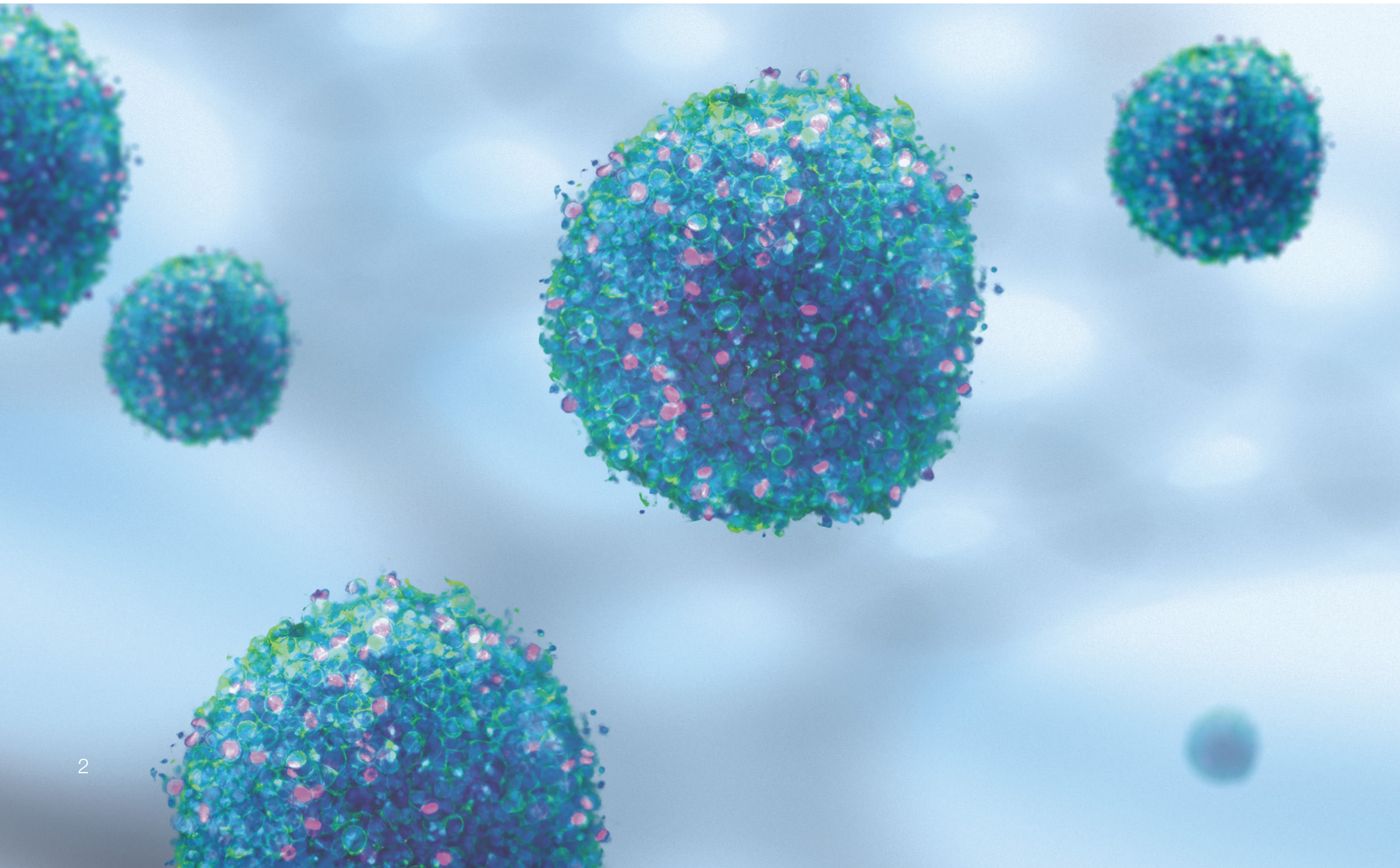
Thermo Fisher Scientific maintains a Cybersecurity Program which is designed to safeguard the confidentiality, integrity and availability of data and systems within our environment. Thermo Fisher supports a continuously improving security program model that has measures designed to focus on reducing 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 has implemented safeguards and protections designed to help protect the Applied Biosystems™ Diomni™ software version 4.3 against intrusion or data compromise. This document describes the various standards, controls and data security approaches and business practices that Thermo Fisher uses in this effort.

Due to the ever-changing cyber landscape, Thermo Fisher updates this product security information guide annually to maintain current and accurate information. This guide expires on **March 31, 2027.** Contact your account representative to get 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 subsidiaries or affiliates (collectively, "Thermo Fisher Scientific" and/or "Thermo Fisher"). Additionally, this product security information guide does not create an independent contract or agreement between any customer and Thermo Fisher. Thermo Fisher does not make any promises or guarantees to customers that any of the methods or suggestions described in this product security information guide will eliminate security risks, restore customer's systems, resolve issues related to any malicious code or achieve any other stated or intended results. Customers exclusively assume all risks of utilizing or not utilizing any guidance described in this product security information guide.



Corporate Cybersecurity Program

Cybersecurity Program and leadership

Thermo Fisher's Cybersecurity Program employs technical, administrative and physical safeguards designed to detect vulnerabilities and address potential threats.

Thermo Fisher's Cybersecurity Program maintains an International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2022 certification for the management of the following areas:

- Cybersecurity program management and governance including risk management;
- Cybersecurity operations including security operation centers;
- Product security;
- Cybersecurity architecture and engineering; and
- Security awareness and training.

Cybersecurity governance and risk management

Thermo Fisher remains vigilant against potential threats for cyberattacks and other cybersecurity incidents and, therefore, we incorporate cybersecurity into our overall risk management process. We accomplish this through various corporate mechanisms, including quarterly business reviews, annual budget planning and targeted risk-based engagements.

Our commitment to cybersecurity emphasizes using a risk-based, "defense in depth" approach to assess, educate, block, identify, respond to and recover from cybersecurity threats. Recognizing that no single technology, process or control can effectively prevent or mitigate all risks, Thermo Fisher employs a strategy using numerous technologies, processes and controls to manage cybersecurity risk.

Product overview

Applied Biosystems™ Diomni™ software version 4.3 for *in vitro* diagnostic (IVD) and research use only (RUO) purposes is an on-premises, browser-based solution that unifies all steps of real-time polymerase chain reaction (qPCR) workflows into a single digital ecosystem. Designed to optimize the use of Applied Biosystems QuantStudio™ instruments, it enables integration of instruments, assays and consumables while offering multimode workspaces through a consistent, intuitive interface for both assay development and routine testing.

Using standardized assay definition files (ADFs), Diomni software is designed to streamline setup, reduce manual errors and enable labs to easily expand test menus. The platform integrates sample preparation, assay selection, testing, analysis, automated quality control and interpretive reporting, providing results in approximately 3 hours.

The Diomni software includes configurable security, audit and e-signature (SAE) features designed to support customers' compliance with regulatory requirements such as the U.S. Food and Drug Administration (FDA) 21 CFR Part 11. Scalable and collaborative, Diomni software allows centralized access for multiple users, integrates with laboratory information management systems (LIMS)/laboratory information systems (LIS) and supports automation, helping laboratories enhance efficiency, reduce turnaround time and maintain data integrity in both research and diagnostic environments.

System compatibility

The Diomni software is compatible with the following operating systems, web browsers and instruments:

- Operating systems
  - Microsoft™ Windows™ 10 (64-bit) or Windows 11
- Supported browsers
  - Google Chrome™
  - Microsoft Edge™
  - Mozilla™ Firefox™
  - Apple™ Safari™
- Instruments
  - Applied Biosystems QuantStudio 7 Pro Real-Time PCR System
  - Applied Biosystems QuantStudio 5 Real-Time PCR System
  - Thermo Scientific™ KingFisher™ Apex™ Purification System

Security certifications or regulatory standards

The Diomni software is developed in accordance with the following design control and general quality system requirements:

- ISO 9001:2015: Quality management systems – Requirements;
- ISO 13485:2016: Medical devices – Quality management systems – Requirements for regulatory purposes;
- IEC 62304:2006+A1:2015: Medical device software – Software life-cycle processes; and;
- 21 CFR Part 820: Quality System Regulation.

Note: Please refer to the ISO and IEC websites for additional information on these specific certifications.

Cybersecurity controls for the Diomni software are designed with reference to applicable industry standards and regulatory guidance, including:

- Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, U.S. FDA, September 27, 2023;
- MDCG 2019-16 Guidance on Cybersecurity for Medical Devices, European Commission, July 2020 (Rev. 1); and
- NIST SP 800-218 Secure Software Development Framework (SSDF), Version 1.1, February 2022.

The Diomni software uses a Security, Audit and Electronic Signature (SAE) system to help support compliance with FDA 21 CFR Part 11 requirements for electronic records and electronic signatures. The SAE system is designed to help customers ensure that electronic data is securely managed and protected from unauthorized access. Additional information about the SAE system is provided below in the System access controls section.

Architecture diagram

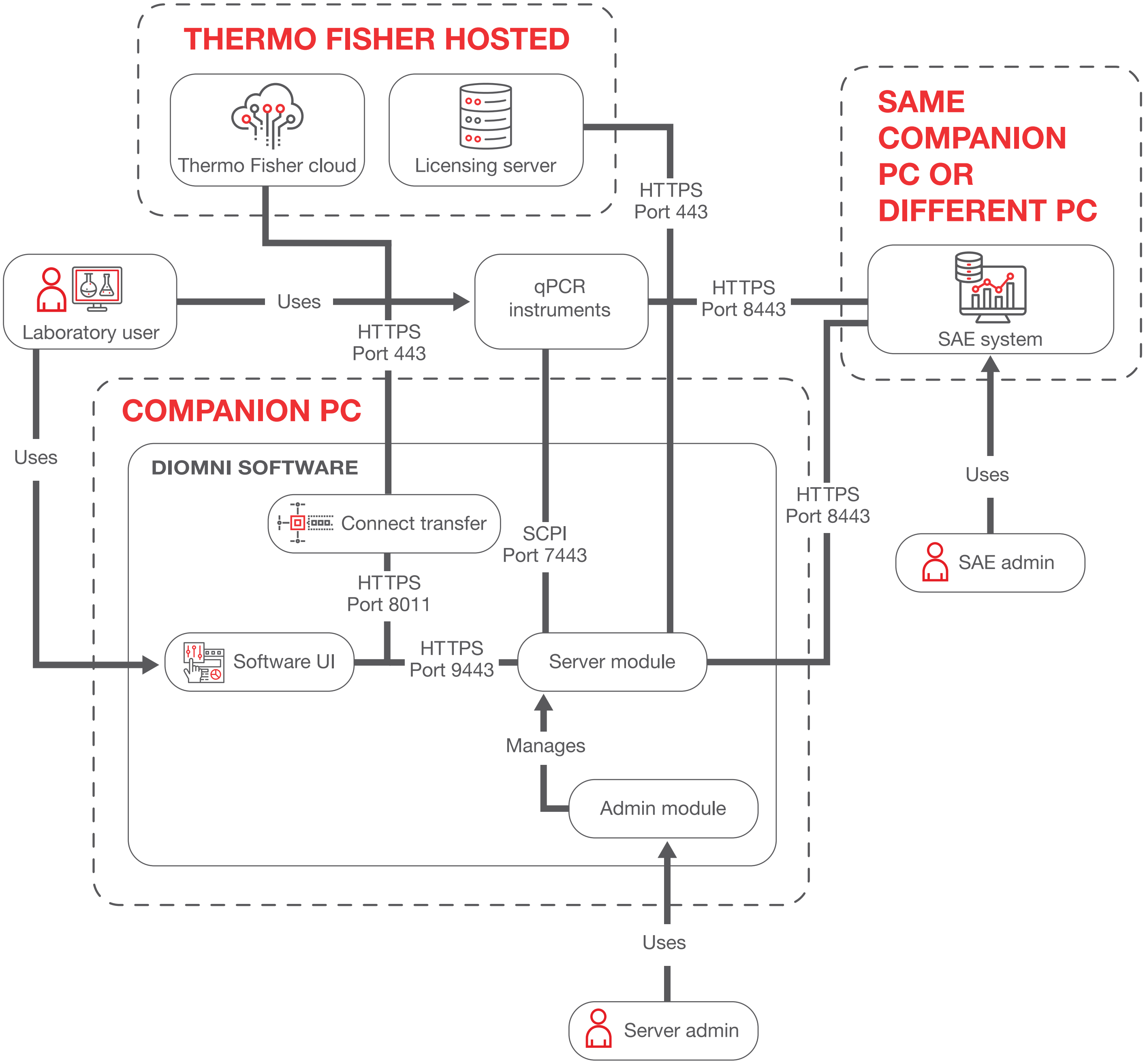


Figure 1: Diomni version 4.3 software architecture diagram

Component glossary

Component	Description
Server module	The core component of the Diomni software ecosystem, developed in Oracle™ Java™ Development Kit (JDK™) 21 and running on the Amazon Corretto™ Java runtime environment, which is supported by Amazon™ until 2030. To see more information on the support by Amazon please refer to Amazon Corretto FAQs.
Administrator module	A thick client that runs alongside the server module to provide admin functionality such as start, stop and restart, configure language, LIS and network share locations, and the SAE server location. It also manages backups of the encryption key stored in Windows credentials.
User interface (UI) module	A JavaScript™-based application that runs within a web browser. It visualizes the data obtained from the server module and handles user interaction.
SQLite™ database	The primary Diomni software database that stores configuration and experiment files.
Licensing server	Manages the licensing of Diomni software and is designed to validate that only authorized users can access its full functionality.
SAE system	A shared security component used for authentication, authorization, auditing and e-signatures.
Thermo Fisher™ Connect Platform	Stores data generated by Diomni (such as ADFs) software and provides catalog application programming interfaces (APIs) to capture product information from the Thermo Fisher eCommerce store.
Connect Transfer	A background service designed for securely transferring select Diomni software data such as ADFs and system metrics from the on-premises Diomni environment to the Connect Platform. The service includes a web server that exposes integration endpoints used by the Diomni software to submit data files. Connect Transfer uses an embedded H2 database for local queuing and state management, communicates with the Diomni server module via internal APIs and transmits data to Thermo Fisher cloud services over authenticated and encrypted Hypertext Transfer Protocol Secure (HTTPS) connections.

Table 1: Component glossary

System access controls

Authentication

The SAE system manages user access to the Diomni software using the SAE Administrator console. During installation, a default user account with Administrator privileges is created. Upon first sign-in, the administrator is prompted to change the default password in accordance with defined password complexity requirements. Administrators can subsequently create and assign additional user accounts and permissions based on operational needs and associate users with the appropriate applications managed by the SAE server.

The SAE system operates as a client-server configuration consisting of 3 components:

- **SAE Administrator console** – A tool used by administrators to configure security, audit and e-signature settings. The console runs in a web browser although it is installed locally on the computer. Google Chrome is the recommended browser; however, Mozilla Firefox and Microsoft Edge are also supported.
- **SAE server** – A background service that implements the core security business logic for authentication, authorization, auditing and electronic signatures, and stores associated system settings, user accounts, audit records and e-signature records. By default, the server is installed on the same computer as the console. Communication between the console and server is protected using encrypted HTTPS protocols. The server starts automatically when the host computer is powered on.
- **SAE user interface** (application interface) – A set of screens integrated into the Diomni software. These screens prompt users to sign in, provide audit reasons and apply e-signatures. A single instance of the console can manage multiple connected applications.

Authentication for access to the Diomni software is administered via the SAE Administrator console, which allows users to configure SAE functions.

The SAE system can be installed either on the same computer as the Diomni software or on a separate computer. Customers can use the installer provided with the Diomni software to install the SAE system in either configuration. For detailed instructions, refer to the Diomni Software v4.3 Installation Guide provided with purchase of the software.

Note: Customers receive documentation for the Diomni software, including the Installation Guide and User Guide, upon purchase of the software. External links to this documentation are not available.

Authorization

The Diomni software leverages role-based access control (RBAC) through the SAE Administrator console to grant permissions and access to authorized users, where roles are configurable to meet business requirements. Thermo Fisher recommends that role assignments follow the principle of least privilege, providing only the required system access needed to manage or use the Diomni software. Customers are responsible for defining, implementing and periodically reviewing role assignments consistent with their internal security policies and applicable regulatory requirements.

Firewall and network controls

In alignment with cybersecurity best practices, Thermo Fisher recommends implementing firewalls consistent with customer IT security policies. Customers are responsible for configuring firewall rules to allow only necessary traffic to and from the Diomni software, aligning with business and IT requirements.

Specific ports must be open to allow for communication to and from the Diomni software. The Diomni software installer includes a script that automatically creates a firewall rule for TCP traffic on port 9443. This rule enables inbound traffic to the Diomni software, allowing other authorized computers on the same network to access the software without requiring manual firewall configuration. The script is compatible with the default Windows firewall but may not function with third-party firewall solutions. Please refer to the Diomni software v4.3 Installation Guide for more information about the required ports to open.

Thermo Fisher recommends closing any unused ports to limit connections and follow industry standards and best practices.

Password management

Customers are responsible for managing computer access passwords for user accounts in accordance with their internal policies and applicable regulatory requirements.

An SAE system administrator can configure and manage passwords for user accounts that access the Diomni software.

Thermo Fisher recommends that customers' password requirements follow industry standard practices and their internal IT security policies.

Remote support

Customers initiate remote support for the Diomni software by contacting technical support in their region. If the technical support representative recommends that troubleshooting can be provided remotely, the representative will establish a remote session with customers using a Thermo Fisher-managed and -approved third-party remote support solution.

Thermo Fisher maintains internal policies and procedures that govern the storage, retention and disposal of any customer data obtained through a remote support session.

Logging

The Diomni software integrates with the SAE system to audit and track actions performed by users within the Diomni application.

The SAE system also records and maintains its own audit logs for authentication, authorization, auditing and electronic signature events, including changes made within the SAE system itself.

Customers can perform the following auditing tasks:

- Specify the audit mode; and
- Generate reports for audited user actions and SAE system changes and software actions.

By default, log files produced from the SAE system are stored locally on the customer-managed system with access controlled in accordance with customer's internal policies and procedures.

To generate and export an audit report for a run, the SAE user account must have the Generate Run Audit Report permission. In the RUO workspace, open a run, select **More actions > Audit report** and export the audit report in PDF format. Audit reports for individual samples can also be generated by selecting the **Samples tab,** choosing a sample and clicking **Export audit.** The report will download as a PDF file.

For additional details regarding the available audit reports and export options, refer to the Diomni software v4.3 User Guide.

Data storage and encryption

By default the data generated from the Diomni software is stored in a SQLite database. Customers also have the option to configure network file shares to read from and write to external storage locations as part of run workflows and data management activities. Customers can configure up to 10 network folder locations per run workspace, enabling integration with laboratory file systems for data export, archival or downstream processing in accordance with customer IT policies.

Data stored within the Diomni software is encrypted utilizing Advanced Encryption Standard (AES)-128 encryption. Transmitted data being sent to and from the Diomni software communicates using HTTPS over Secure Socket Layer (SSL)/ Transport Layer Security (TLS) v1.2 and later.

Secure product development lifecycle

Secure software development training

Software development training is available to the Diomni Software Development team, which reinforces their knowledge of secure coding principles and allows them to review the latest development standards and guidelines.

Company-wide cybersecurity training

We believe cybersecurity is the responsibility of every Thermo Fisher employee, and Thermo Fisher regularly has educational programs to share best practices and to raise awareness of cybersecurity threats. Thermo Fisher accomplishes this through a security awareness training program, including regular exercises and periodic cyber-event simulations.

Product security assessments

Products, instruments, software and devices undergo custom security assessments as part of the product development lifecycle. Customization is based on the components included in the solution and their complexity. The assessment may include technical review, focused testing of identified components and regulatory review, if applicable. The Diomni Software Development team reviews, evaluates and prioritizes security assessment findings for remediation and acts on them based on criticality and a business risk management process.

Source code management

The Diomni software source code is stored in a Thermo Fisher-approved version control solution that contains built-in redundancy to support data loss prevention. Continuous Integration/Continuous Deployment (CI/CD) is in use, automating the implementation and delivery of changes made to the code.

Artifact management

Software artifacts including, but not limited to, executables, images and libraries for the Diomni software are stored and maintained in a Thermo Fisher-approved artifact management solution. This provides visibility and control on developed software builds, enabling the Diomni Software Development team to identify dependencies with known vulnerabilities that are prioritized for remediation based on criticality and a business risk management process.

Static analysis

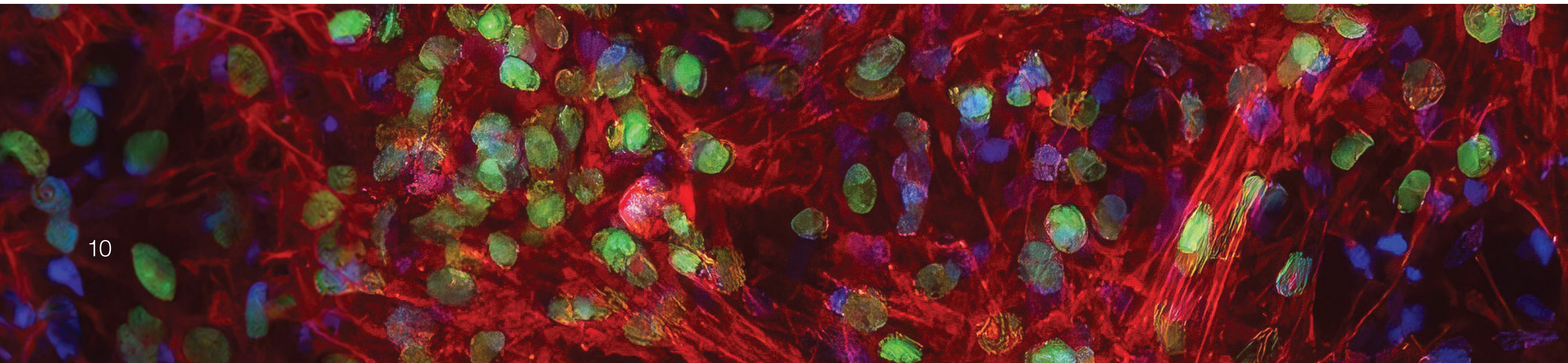
The Diomni Software Development team utilizes a Thermo Fisher-approved static analysis tool to scan code repositories. This tool helps identify potential security defects, maintain code quality and integrity and allow for the prompt review and prioritization of security alerts for remediation based on criticality and a business risk management process.

Peer code reviews

The Diomni Software Development team conducts manual peer reviews of code before testing and deployment to help assess adherence to coding standards and design requirements. These reviews provide additional insight into the overall context and business logic of the code, complementing the information gathered from the static analysis tool.

Web application scanning/dynamic analysis

The Diomni Software Development team uses a Thermo Fisher-approved dynamic analysis tool to evaluate web applications and application programming interfaces (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. APIs are scanned for security vulnerabilities and resilience to outside influence. The Diomni Software Development team reviews and prioritizes findings from the scans for remediation based on criticality and a business risk management process.

Penetration tests

Thermo Fisher's Penetration Testing team tests core components of the Diomni software against the Open Worldwide Application Security Project (OWASP) Top 10 Internet-of-Things (IoT) list. The team, comprised of trained penetration testers, uses technical approaches to identify vulnerabilities during product development.

Vendor assessments

To evaluate risks from cybersecurity threats associated with the company's use of certain third-party technology providers, we have incorporated a risk-based assessment into the corporate information technology procurement process designed to assess the security risk of certain third parties providing new technology solutions to our environment. This process does not extend to all suppliers or situations but reflects a balanced approach to reduce risk and effectively manage resources.

Product security maintenance

Antivirus/anti-malware

Thermo Fisher recommends the use of antivirus software on computers running the SAE system and the Diomni software. Please refer to the Diomni User Guide for more information on using antivirus software with the Diomni application.

Thermo Fisher recommends that customers follow their organization's IT policies and procedures for antivirus management and maintain up-to-date virus definitions to ensure continued protection against emerging threats.

Vulnerability and patch management

The Diomni Software Development team assesses security updates and system patches throughout the lifecycle of the product and makes them available to customers based on criticality and a business risk management process.

Patches are distributed to customers through the Thermo Fisher Connect Platform. Patches are not released on a routine basis but are incorporated into the next annual software release. High-risk or critical security issues can be addressed outside of the annual software cadence. Customers receive a secure URL to download the updated software.

Customers may independently install software updates; however, Thermo Fisher does not recommend installing any third-party software on the computer running the Diomni software or the SAE system. The only exception is antivirus software recommended in the Antivirus/anti-malware section of this guide.

Thermo Fisher recommends that customers utilize our Reporting Security Issues form to report suspected or potential security issues.

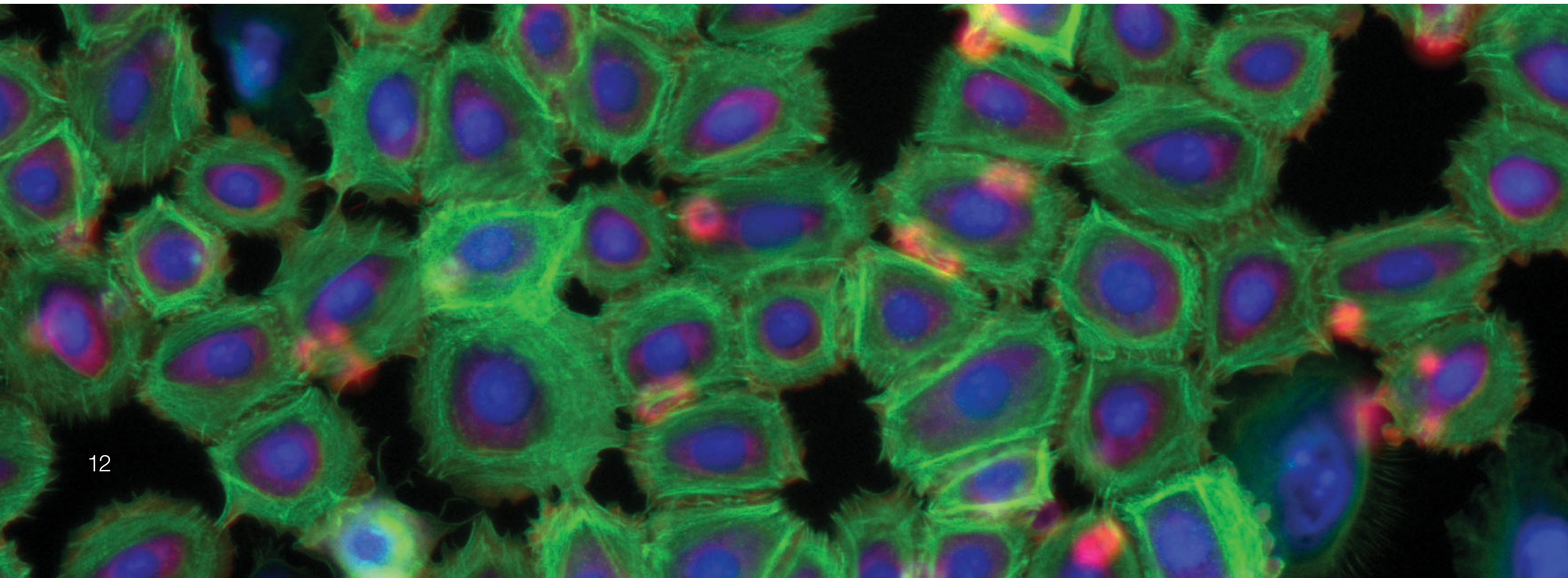
Disaster recovery and business continuity

The Diomni software has data backup capabilities designed to support the recovery of data and aid in restoring normal functionality in the event of disruption. Thermo Fisher suggests that customers leverage these backup capabilities and include them in disaster recovery plans and testing in accordance with their policies. Thermo Fisher also suggests that customers perform regular file system and database backups with laboratory managers and IT administrators in accordance with their policy.

Service handling

Application-specific support and global training serve as critical components to maintaining and supporting the Diomni software. Thermo Fisher'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 our Technical Support team to initiate a support request for any issues that may arise.



Questions? To reach a member of our team to discuss the security of this product, please contact us at **product.security@thermofisher.com**