Product security information guide

Thermo Scientific™ Ardia™ Platform | version 1.1 | May 2025

Document valid through June 1, 2026

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 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.

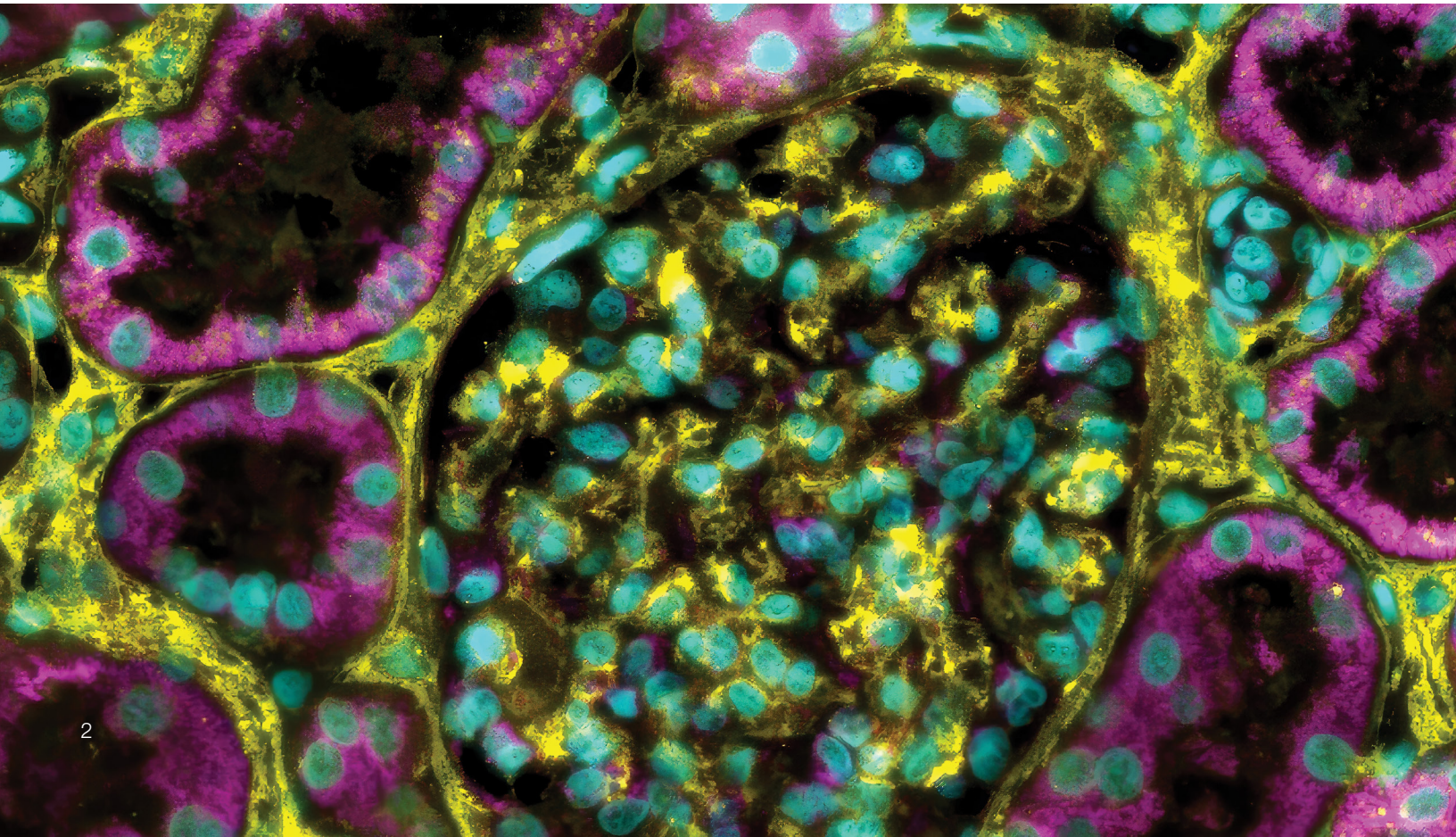
About this guide

Thermo Fisher Scientific has implemented safeguards and protections designed to help protect the Thermo Scientific™ Ardia™ Platform software version 1.1 against intrusion or data compromise. This document describes the various standards, controls and data security approaches and business practices that Thermo Fisher Scientific uses in this effort.

Note: The Connected Software components of the Ardia Platform are not in scope for this guide.

Due to the ever-changing cyber landscape, Thermo Fisher Scientific updates this Product Security Information Guide annually to maintain current and accurate information. This guide expires on **June 1, 2026.** 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 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 eliminate security risks, 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

Cybersecurity Program and leadership

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

Thermo Fisher Scientific's Cybersecurity Program maintains an International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2013 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 Scientific 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 Scientific employs a strategy using numerous technologies, processes and controls to manage or reduce risk.

Product overview

The Ardia Platform, an integrated application and data platform, enables chromatography and mass spectrometry instruments and applications to share and connect data seamlessly with each other and the larger laboratory operations ecosystem. This comprehensive software solution is designed to assist the transition to digital laboratory operations by connecting people, projects and instruments across an organization.

Key features include integration with various software tools for automated data transfer and direct access, centralized data storage with backup and archival capabilities and web-based access for data retrieval. Ardia Platform deployments include 4 core applications: Instruments, Data Viewer, Data Insights and Data Explorer. These applications have broad applicability, helping to increase productivity and connect analytical workflows, people and instruments.

System components and data

The Ardia Platform comprises these system components: Ardia Core software, Ardia Core applications and Connected Software.

The Ardia Core software is the underlying infrastructure that supports utility applications including, but not limited to, Client Registration and Management, License Management, Users and Roles and Core platform applications.

By default, the Core applications are bundled with the Ardia Core software and include Data Viewer, Instruments, Data Explorer and Data Insights. The Connected Software component refers to Ardia Platform's supporting connection to other software running on a standalone PC, including Ardia Data Sync, Ardia Platform Link and the following applications:

- Thermo Scientific BioPharma Finder™ software;
- Thermo Scientific Chromeleon™ Chromatography Data System (CDS) software;
- Thermo Scientific Compound Discoverer™ software;
- Thermo Scientific Proteome Discoverer™ software; and
- Thermo Scientific Xcalibur™ data acquisition and interpretation software.

Hardware specifications

Server name	Ardia Advanced Tower
Server model	Dell™ PowerEdge™ T550
Processor	(2x) Intel™ Xeon™ Platinum processor 8352M
Cores/Threads	64C/128T, 2.3 GHz
RAM	512GB
GPU	NVIDIA™ Ampere A30 2.3 GHz
Storage	HDD 128TB (96TB RAID6) SSD 960TB (480GB RAID1) NVMe™ 19.2TB (12TB RAID5)
Operating system	Ubuntu™ Linux™
Embedded management	iDRAC
Dimensions	459mm x 200mm x 680mm (H x W x D)
Operating temperature	10ºC to 35ºC (50ºF to 95ºF)
Storage temperature	-40ºC to 65ºC (-40ºF to 149ºF)
Humidity	Operating: 8% to 85% Storage: 5% to 95%
Power	Dual 2,400W (200V-240V)

Table 1: Ardia Advanced Tower hardware specifications

System specifications

The Ardia Platform software is preinstalled on the customer's selected Ardia Platform server using Ubuntu Linux as the default operating system. The Ardia Core applications use Kubernetes™ for containerization and orchestration on the Ardia Platform server. Customers can use the Microsoft™ Edge™ and Google™ Chrome™ supported web browsers to access the Ardia Platform. Ardia is compatible with the current offerings of liquid chromatographs, ion chromatographs, autosamplers and mass spectrometers. Please contact your dedicated support personnel for a complete list of instruments compatible with the Ardia Platform.

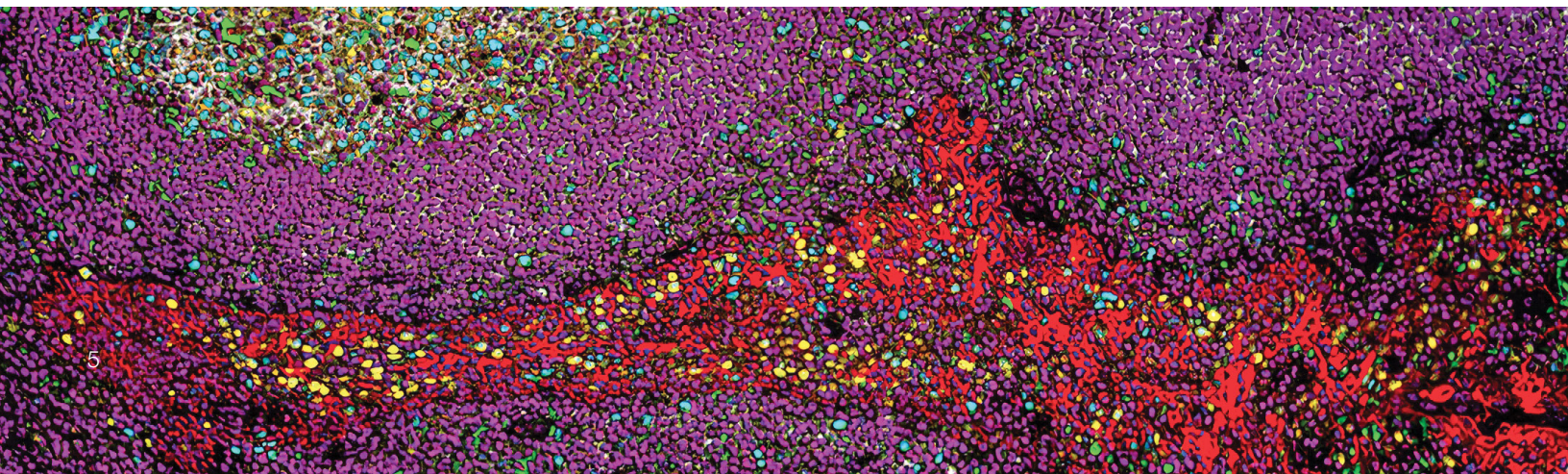
Thermo Fisher Scientific recommends that customers use the default configuration of the Ardia Platform.

Third-party assets

The Ardia Platform uses various third-party software components to operate the Core platform and applications. The names, version numbers and license links for each component are listed in a table under the Infrastructure section of the release notes for each part of the platform. Access the release notes in the Chromatography and Mass Spectrometry Help Portal.

Security certifications or regulatory standards

The Ardia Platform Software Development team utilizes a Quality Management System (QMS) aligned with ISO 9001 standards that encompasses policies and procedures including, but not limited to, disaster recovery, data backup and recovery, business continuity, data security and change management procedures.



Architecture diagram

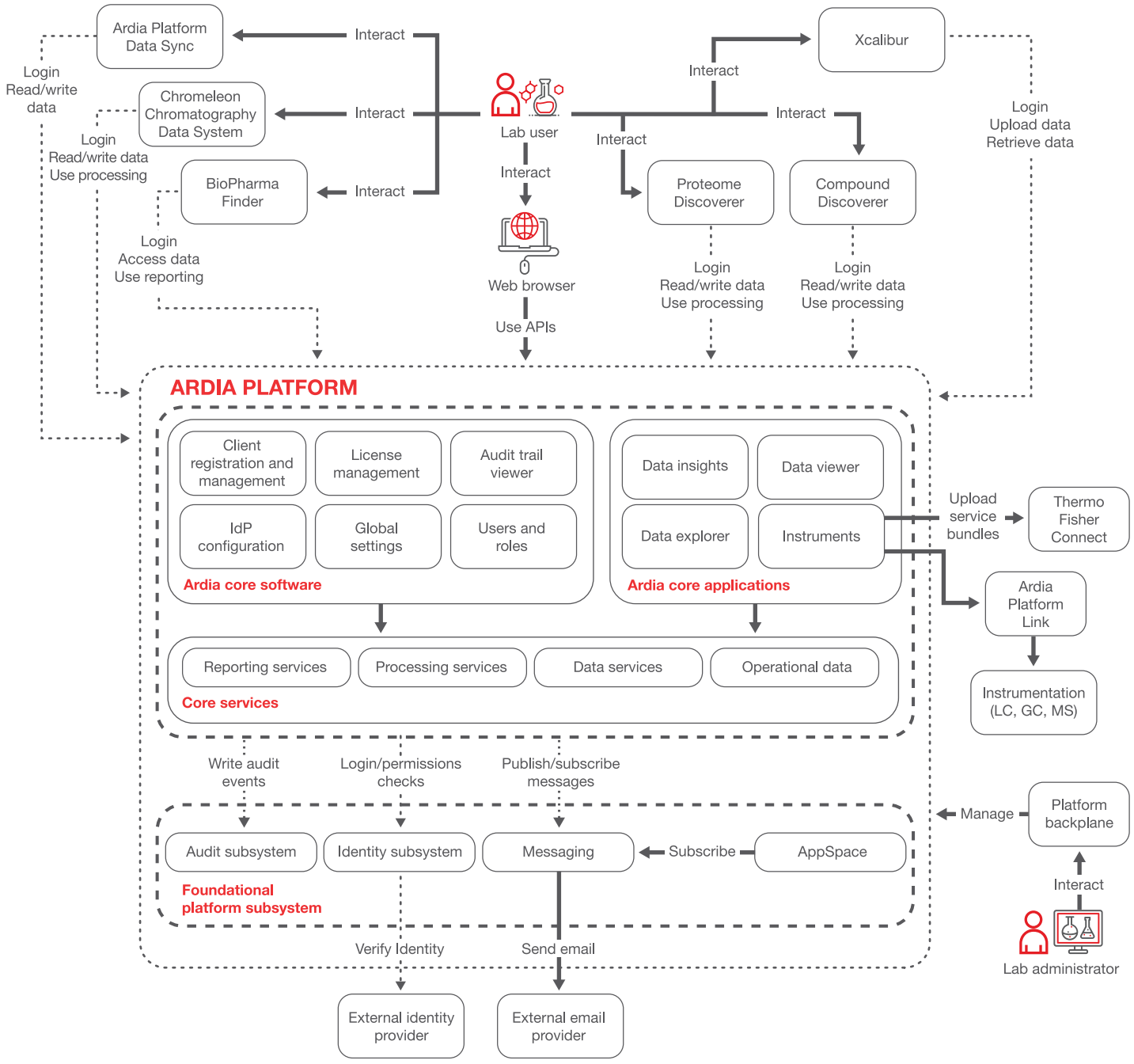


Figure 1: Ardia Platform architecture

Component glossary

Component	Description
Audit trail viewer	Displays audited events, such as user access and data operations. Audit records include versioning and timestamps.
Client registration and management	Creates and manages application registration codes utilized to connect Thermo Scientific desktop applications to the Ardia Platform.
Global settings	Defines administrative settings that are applied to the entire Ardia Platform.
IdP configuration	Configures, edits and removes the identity providers (IdPs) used by the Ardia Platform.
User and roles	Adds new users and manages existing users in the Ardia Platform; it also defines roles, users and attributes and configures permissions.
License management	Adds and manages licenses for applications across the Ardia Platform.
Ardia repository	The digital storage space accessible from Ardia applications, such as Data Explorer and Data Viewer and connected external software like Chromeleon CDS and BioPharma Finder, to facilitate seamless access, sharing and management of data objects.
Data explorer	Browses and manages folders, files and data objects stored in the Ardia Platform.
Data viewer	Visualizes and qualitatively analyzes chromatography and mass spectrometry data.
Data insights	Provides dashboards that offer key laboratory insights on resource availability, instrument status and performance, allowing users to track and monitor various system metrics with customizable filters.
Instruments	Manages, schedules and monitors data acquisition on all instruments connected to the Ardia platform.
Ardia Platform Data Sync	Allows users to automatically download data from the Ardia Platform to a local computer and upload data from a local computer to the Ardia Platform, enabling them to leverage the Ardia Platform while maintaining the flexibility to process data in non-integrated software.
Ardia Platform Link	Required to use the Ardia Instruments application; the Ardia Platform Link enables communication between instruments and the Ardia Platform and is also used to monitor and manage all Ardia instrument services running on the instrument PC.
External connected software	Software like BioPharma Finder, Proteome Discoverer, Xcalibur, Chromeleon CDS, Skyline and other third-party applications can connect to the Ardia Platform to facilitate data storage, management and sharing between chromatography and mass spectrometry instruments.
Thermo Fisher™ Connect Platform	Customers can send instrument service data to the Thermo Fisher Connect Platform software to analyze data anytime, anywhere. Security features within the Thermo Fisher Connect Platform are not in scope for this document. Please refer to the Thermo Fisher Connect Platform product security information guide.
Audit subsystem	The Ardia Platform uses this subsystem in conjunction with the Audit Trail Viewer to view, write and store audit events.

Table 2: Component glossary

Component	Description
Messaging	Send communications from the Ardia Core software and applications to the external email provider.
External email provider	Dedicated service for email communications.
Identity subsystem	Used to verify the identity of a user authenticating into the Ardia Platform by confirming that there is a valid user record within the external identity provider.
External identity provider	A trusted entity that verifies user identities and issues authentication tokens or credentials for accessing various Ardia applications and utilities through single sign-on (SSO).
AppSpace	AppSpace provides a common UI shell and UI components used by most other applications. Most other applications surface as AppSpace applications' respective widgets.
Platform backplane	Allows for access to the Ardia Platform server configuration settings, including but not limited to Ardia URL, backup and archive.

Table 2: Component glossary, continued

System access controls

Authentication

Authentication to the Ardia Platform is managed via an IdP. All IdPs used in the Ardia Platform are industry standard OAuth 2.0-compliant and offer a scalable, simplified solution for authenticating Ardia Platform users.

The default identity provider for the Ardia Platform is Ardia IdP, which comes preconfigured with the Ardia Core software. However, users also can choose from a range of other tested identity providers offered by the Ardia Platform including, but not limited to, generic Open ID Connect (OIDC), such as Chromeleon CDS, Facebook™ and Google, as well as Microsoft Entra™ ID.

Authorization

The Ardia Platform leverages role-based access control (RBAC) to grant permissions and access to authorized users, where roles are configurable to meet necessary business requirements. Thermo Fisher Scientific recommends that role assignments follow the principle of least privilege, providing only the required system access needed to manage the administration of the Ardia Platform. Roles available to customers are fully configurable in the Users and Roles section. Users with administrator-level privileges can configure roles and permissions for other users.

Firewall and network controls

Ardia Platform server firewall configuration is optional based on customer requirements. If customers want to deploy a firewall solution, they must configure ports 22, 80 and 443 to allow inbound communication from their network to the Ardia Platform server's static IP address. Customers must provide their own firewall solution as Thermo Fisher Scientific does not provide a firewall as part of the Ardia Platform.

Thermo Fisher Scientific recommends configuring firewall rules to allow only necessary traffic to and from the Ardia Platform server according to industry standard practices and business requirements.

Password management

For customers leveraging the default Ardia IdP, administrators can configure user passwords requirements within Global Settings and assign different levels of password complexity, including the use of uppercase letters, lowercase letters, numeric characters and non-alphanumeric symbols. In addition to password complexity, administrators can enforce password expiration, account lockout and/or prohibiting the reuse of passwords.

For customers delegating authentication to an external IdP, the customer's IdP sets the password policy requirements.

Thermo Fisher Scientific recommends that password requirements follow industry standard practices.

Auditing and logging

Auditing

The Ardia Platform logs various activities, including user access, data operations and configuration changes. Audit records capture user information, timestamps, user-added comments and entry details to evaluate system performance and document specific tasks.

The built-in Audit Trail Viewer allows authorized users to view these automatically generated audit entries. Users can create queries to filter specific time periods, view precise events, compare versions and revert objects to previous versions within the application. Audit trail entries can be exported using the export function after performing a query search. The Audit Trail Viewer does not record entries for Data Viewer, Data Insights and Ardia Platform Link.

Logging

By default, log files produced from the Ardia Platform are stored locally on the server with access managed by the customer. These log files are used as part of the troubleshooting process by service personnel when providing customer support.

Data encryption

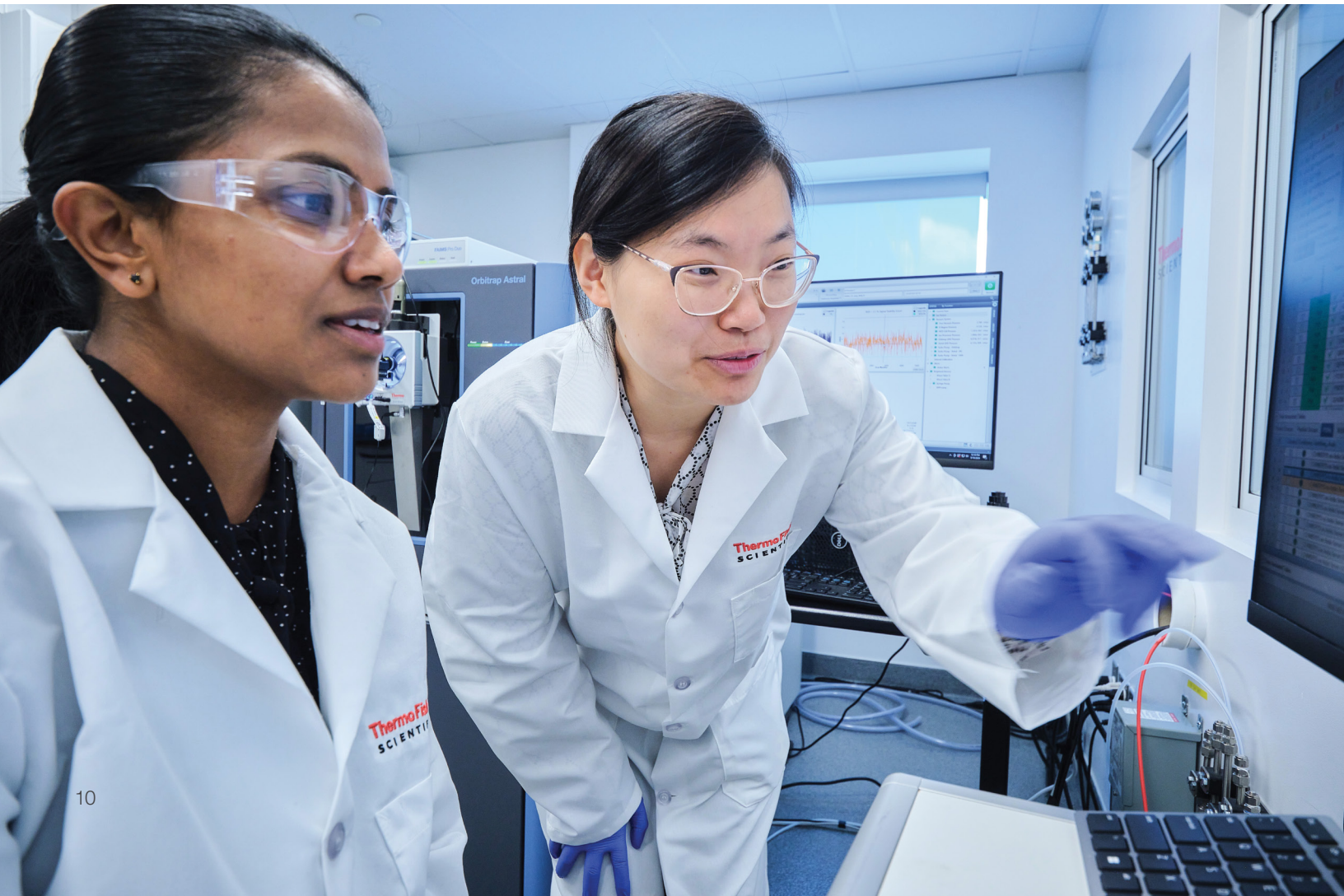
Transmitted data being sent to and from the Ardia Platform server is communicated over a Secure Sockets Layer (SSL) connection using Transport Layer Security (TLS) v1.2 and greater. Web and mobile client access to platform data employs HTTPS, which requires the use of port 443, to protect external communications between the client and the platform.

Certificates

The Ardia Platform uses two security certificates to support the encryption of data in transit: one for the Kubernetes cluster and another for the ingress controller. The Kubernetes certificate is configured to automatically renew prior to expiration. The certificate for the ingress controller is used to establish the encrypted connection between the customer's clients and the Ardia Platform server.

As part of the Ardia installation process, customers are required to use a certificate provider of their choice to issue a certificate for the domains used to access the Ardia Platform server. An expired certificate may result in issues that prevent customer clients from accessing and operating the Ardia platform.

Thermo Fisher Scientific recommends that customers use the default configuration of the Ardia Platform.



Secure software development lifecycle

Secure software development training

Software development training is available to the Ardia Platform 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 Scientific employee and regularly educate and share industry-leading practices with them to raise awareness of cybersecurity threats. Thermo Fisher Scientific accomplishes this through a security awareness training program, including regular exercises, periodic cyber-event simulations and annual attestation to our Technology Acceptable Use Policy.

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 with the solution and their complexity. The assessment may include technical review, focused testing of identified components and regulatory review, if applicable. The Ardia Platform 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 Ardia Platform source code is stored in a Thermo Fisher Scientific-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 Ardia Platform are stored and maintained in a Thermo Fisher Scientific-approved artifact management solution. This provides visibility and control on developed software builds, enabling the Ardia Platform 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 Ardia Platform Software Development team utilizes a Thermo Fisher Scientific-approved static analysis tool to scan code repositories during each code commit. 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 Ardia Platform 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 Ardia Platform Software Development team uses a Thermo Fisher Scientific-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 Software Development team reviews and prioritizes findings from the scans for remediation based on criticality and a business risk management process.

Architecture guidance and penetration testing

Thermo Fisher Scientific's Product Security Architecture team provided early architecture and design consultations for components of the Ardia Platform. This assessment involves

understanding the components, interactions and connections within the product to evaluate potential security implications and provide feedback on security controls.

Thermo Fisher Scientific's Testing and Research team tested the Ardia Platform version 1.1 against industry standards, including the Open Worldwide Application Security Project (OWASP) Top 10 and the OWASP Internet-of-Things (IoT) Top 10 list. The team, comprised of trained penetration testers, use various approaches to identify vulnerabilities during product development. The team followed internal methodologies developed from guidance and resources established by OWASP, the National Institute of Standards and Technology (NIST), the Open Source Security Testing Methodology Manual (OSSTMM) and the Penetration Testing Execution Standard (PTES).

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

Vulnerability and patch management

The Ardia Platform Software Development team tests and validates security updates and system patches throughout the lifecycle of the product and incorporates them into product updates based on criticality and a business risk management process.

Thermo Fisher Scientific recommends that customers stay informed of and apply available product updates per guidance from service personnel and in alignment with the Master Service Agreement (MSA). Please contact your dedicated service personnel for assistance with deploying patches to the Ardia Platform server.

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

Disaster recovery and business continuity

The Ardia Platform server has data backup capabilities to prevent data loss and aid in restoring normal functionality. Thermo Fisher Scientific suggests that customers leverage these backup capabilities and include them in disaster recovery plans and testing in accordance with their policies. Thermo Fisher Scientific also suggests performing regular file system and database backups with laboratory managers and IT administrators in accordance with policy.

System hardening

System hardening, a critical security function, can mitigate potential system vulnerabilities and prevent potential threats. The Ardia Platform Software Development team ran Linux hardening scripts derived from the Center for Internet Security (CIS) Benchmark Level 1 profile on the Ardia Platform server. The Level 1 profile helps organizations reduce their attack surface (the potential entry points an attacker can use to gain unauthorized access to a system) by providing security recommendations while minimizing potential performance impacts to the targeted systems.

Some examples of the security measures implemented on the Ardia Platform server include but are not limited to disabling unnecessary services and ports, enforcing strong password policies, the principle of least privilege and enabling logging and monitoring.

Thermo Fisher Scientific recommends that customers install and regularly update antivirus software on their PCs that have access to the Ardia Platform. Thermo Fisher Scientific also recommends maintaining operating systems and network hardening practices on relevant infrastructure supporting the use of the Ardia Platform.

Technical support

Application-specific support and global resources serve as critical components to maintaining and supporting the Ardia Platform. Thermo Fisher Scientific's experienced team of professionals use a global, follow-the-sun support approach for technical assistance and escalation if critical issues should arise.

Customers initiate remote support for the Ardia Platform by contacting technical support in their region. Please contact digital.support@thermofisher.com per the terms of your support contract for assistance with general issues and inquiries. Additional support references include the Thermo Fisher Scientific's Digital Science Support Resource Center website for software downloads, knowledge articles, product defect information and customer forums. Video tutorials are also available for customers to reference.

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 any questions, please contact digital.support@thermofisher.com for more information.

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

BRE0066580