



Security quick reference guide

Thermo Fisher Connect Platform Individual edition | December 2025

Document valid through December 15, 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 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 various safeguards and procedures designed to help protect the Connect Platform Individual edition against intrusion and 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, security quick reference guides are updated annually to ensure we provide accurate information to our customers. This guide expires on **December 15, 2026**. Please contact your account representative to obtain the latest published version.

The information contained in this security quick reference 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" and/or "Thermo Fisher"). Additionally, this security quick reference 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 any customer that any of the methods or suggestions described in this security quick reference 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 security quick reference 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.

The 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 or reduce risk.



Product information

The Thermo Fisher™ Connect Platform Individual edition application delivers a suite of digital capabilities designed to enhance laboratory efficiency for managers and technicians. Connect Platform Individual edition is supported by Amazon Web Services™ (AWS™) and Amazon Virtual Private Cloud™ (Amazon VPC™) infrastructure

and provide cloud-based Internet of Things (IoT) device connectivity, data storage, scientific analysis applications and peer collaboration tools to simplify data analysis and enable greater data visibility.



Comprehensive security controls

Authentication & authorization

OpenID Connect (OIDC) manages authentication on Connect Platform Individual edition, supported by SAP™ Customer Data Cloud. Two login methods exist:

- **Direct login:** Users can establish their system identities directly within the Connect Platform Individual edition.
- **Federated login:** Federated login is available with Connect Platform Individual edition through customers' identity provider (IdP) and is supported on either OIDC or Security Assertion Markup Language (SAML) protocols. Thermo Fisher's Customer Identity Platform (CIP) team can configure a trust relationship with the customers' IdP upon request, providing two authentication options:
 - **Domain-based authentication:** All users from the customer's IdP can authenticate to the platform.
 - **Specific-user authentication:** This option restricts the authentication to a predefined list of users.

Please contact your Thermo Fisher business representative for more information on configuring your IdP with the Connect Platform Individual edition.

By default, the Connect Platform enforces multifactor authentication for either login method. Administrative access to Thermo Fisher application servers and infrastructure, including access to the AWS console used to manage the Connect Platform Individual edition, also requires multifactor authentication. Thermo Fisher limits access to application servers and supporting infrastructure to authorized personnel only.

Cloud security

Thermo Fisher has implemented a security control framework solution that monitors security controls implemented across various cloud accounts. Some examples of the controls it can enforce include network and firewall management, credential management, audit trail and log management and data protection configuration management.

Our Cloud Governance and Incident Detection and Response programs focus on the cloud security control framework. The Cloud Governance program implements procedures and utilizes automated tools designed to detect incorrectly configured cloud resources. The Incident Detection and Response program enforces the deployment of security tools to identify suspicious behavior at the cloud- and server-instance levels. Alerts from the security tools are directly sent to the appropriate response team for triage.

Network & endpoint security

Thermo Fisher manages Connect Platform Individual edition's network security using virtual private clouds (VPCs), network access control lists (NACLs) and security groups (SGs) to restrict network access, only allowing necessary traffic according to business requirements. Only externally facing services of Connect Platform Individual edition can be accessed via the internet.

The Connect Platform Individual edition utilizes AWS to host its infrastructure. AWS provides distributed denial-of-service (DDoS) protection called AWS Shield™ that safeguards all Thermo Fisher-hosted services, including the Connect Platform Individual edition. Additionally, the protection is further enhanced by scalability features such as elastic load balancers and auto-scaling groups to handle spikes in traffic.

Connect Platform Individual edition is supported by virtual machines (VMs) that leverage endpoint detection and response (EDR) tools. These tools are designed to detect, prevent and assist in response to sophisticated attacks that could bypass traditional antivirus solutions.

Thermo Fisher recommends that customers utilize our [Reporting Security Issues form](#) to report suspected or potential security issues.

Data encryption

Encryption at rest

Thermo Fisher stores device and customer-uploaded data to the Connect Platform Individual edition primarily in Amazon Simple Storage Service™ (Amazon S3™). The data stored in Amazon S3 is encrypted using Amazon S3 server-side encryption that utilizes 256-bit Advanced Encryption Standard (AES-256). Other database and storage services leverage native AWS encryption mechanisms. Backups that contain any customer data are also encrypted at rest.

Encryption in transit

Data uploaded from an instrument or a user to the Connect Platform Individual edition is encrypted in transit. Web and mobile access

to platform data communicates over Hypertext Transfer Protocol Secure (HTTPS) using Transport Layer Security (TLS) v 1.2 with 256-bit encryption to protect communications between the client and the platform via the internet.

For IoT-connected devices that integrate with the Connect Platform Individual edition, communications are secured using both Message Queuing Telemetry Transport (MQTT) over TLS and HTTPS protocols.



Secure product development lifecycle

Products, instruments, software and devices undergo 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, if applicable. The Connect Platform Product Development team reviews, evaluates and prioritizes security assessment findings for remediation, acting on them based on criticality and a business risk management process.

Additional security measures employed by the Connect Platform Product Development team as part of the product security assessment include storing source code in a Thermo Fisher-approved version control solution that contains built-in redundancy and maintaining software artifacts in an artifact management solution that provides visibility and control of

developed software builds. The version control solution also leverages static analysis and dynamic analysis tools to scan code repositories, web applications and application programming interfaces (APIs), where applicable, for potential security vulnerabilities.

Thermo Fisher follows a standardized change control process that requires various approvals based on logical segregation of duties prior to progression of tested and verified artifacts, such as source code, compiled code and generated images, to a higher environment. The Connect Platform Product Development team, in accordance with Thermo Fisher policies, follows documented standard operating procedures for application and infrastructure management. Thermo Fisher also monitors application and infrastructure health via health check tools, resource utilization and logging alarms.



 Questions? Please visit the **Thermo Fisher Connect Platform product website** for more information.

To request support for Connect Platform Individual edition, sign into **Connect Platform** and click the Feedback button located near the bottom-right corner.