Security Operations Guide

Connect Platform | IoT Connectivity

VERSION 4.3 | JUNE 9, 2020

ThermoFisher SCIENTIFIC

Introduction

Thermo Fisher Scientific safeguards the confidentiality, integrity, and availability of data and systems within the company's environment through our robust Cybersecurity Program led by a dedicated Chief Information Security Officer (CISO).

Thermo Fisher supports a continuously improving security program that reduces risk, responds to threats, and protects our company's intellectual property and the privacy of data while driving compliance with regulatory requirements and industry best practices. Committed to scientific advancement, we employ the latest security tools and offer solutions that enable our customers to push the boundaries of innovation.

As the world leader in serving science, our security professionals provide prevention, monitoring, detection, and response capabilities, so we can more quickly identify and act on ever-evolving global threats.

Thermo Fisher has implemented standards and policies to help protect data from unauthorized access in our Connect platform. This document describes the various standards, controls, data security approaches, business practices, and certifications used for the cloud-based storage that supports Connect.

By protecting our information and assets, we can achieve our mission of enabling our customers to make the world healthier, cleaner, and safer.

Mandating a Secure Foundation Fact Sheet

SECURITY CONTROL	STATUS	ADDITIONAL COMMENTS
Cybersecurity Program	Dedicated	
Chief Information Security Officer	Dedicated	
Data Privacy Officer	Dedicated	
Encryption In Transit	Enabled	
Encryption At Rest	Enabled	
Distributed Denial-of-Service Protection	Enabled	AWS and a third-party provider
Web Application Firewall	Enabled	Two independent solutions (cloud-based, host-based)
Network Intrusion Detection System	Enabled	
Cloud Compliance Enforcement	Enabled	
Anti-virus/Anti-malware	Enabled	Signature-based detection
Endpoint Detection & Response	Planned	Heuristic-based detection; Incident response capabilities
Host Intrusion Protection System	Enabled	
Integrity Monitoring	Enabled	
Multi-Factor Authentication	Enabled	AWS Management Console
Secure Coding Training	Yearly	
Static Analysis	Enabled	Source Code
Dynamic Analysis	Enabled	Web Applications
Bug Bounty Program	Enabled	
API Security	Enabled	
Product Security Assessment	Enabled	
Central Code Repository	Enabled	
Global Security Operation Centers	Enabled	Follow-the-sun model
Security Information and Event Management	Enabled	
Incident Management	Enabled	
Incident Response Plan	Defined	
Threat Intelligence	Enabled	
Digital Forensics Lab	Enabled	
Firewall/Access Control	Enabled	AWS Security Groups
Password Policy	Defined	
Security Awareness Training	Enabled	All Thermo Fisher Scientific employees
Personnel Background Checks	Enabled	
Physical Security Controls	Enabled	
Change Control	Enabled	
Patch Management	Enabled	
Health Monitoring	Enabled	
Scalability	Available	
Disaster Recovery Plan	Defined	
Disaster Recovery Testing	Enabled	Every six months
ISO 27001 Certification	Enabled	
ISO 9001 Certification	Enabled	
FedRAMP Authorization	Not Authorized	Connect platform is currently not FedRAMP authorized.

Connect Platform Architecture

Connect Instrument Software Agents

The specific software used on the instrument to handle connectivity may be specialized for various environments or use cases. The software must utilize the Internet of Things (IoT) Connectivity Software Development Kit (SDK) framework to communicate securely with the Connect platform. The software itself will be subject to the Secure Development

Connect Platform

The Connect platform is for secure, cloud-based data storage, scientific analysis applications, and peer collaboration tools. It provides asset management applications and web tools to allow a customer to schedule time on their lab's instruments via a mobile device. The solution also monitors real-time telemetry data and allows a remote analysis of instruments to facilitate prevention/resolution of issues with our service team. Connect is a foundational core of Thermo Fisher's full suite of digital capabilities creating new efficiencies in the lab.

IoT Connectivity SDK

The IoT Connectivity SDK is a client-side software library that enables secure IoT connectivity for Thermo Fisher instruments into the Connect platform. The SDK, along with the device's firmware, runs a standalone service that establishes its Connect identity and acts as a connectivity protocol abstracter to communicate between the device and the Connect platform. This allows users to quickly and securely connect devices. The IoT Connectivity SDK is subject to the Secure Development Lifecycle security requirements.

Connectivity Process

Device Provisioning

Connect agent calls a custom authenticated REST API to get the device identity and x.509 credentials from the Connect platform.

AWS IoT Communication

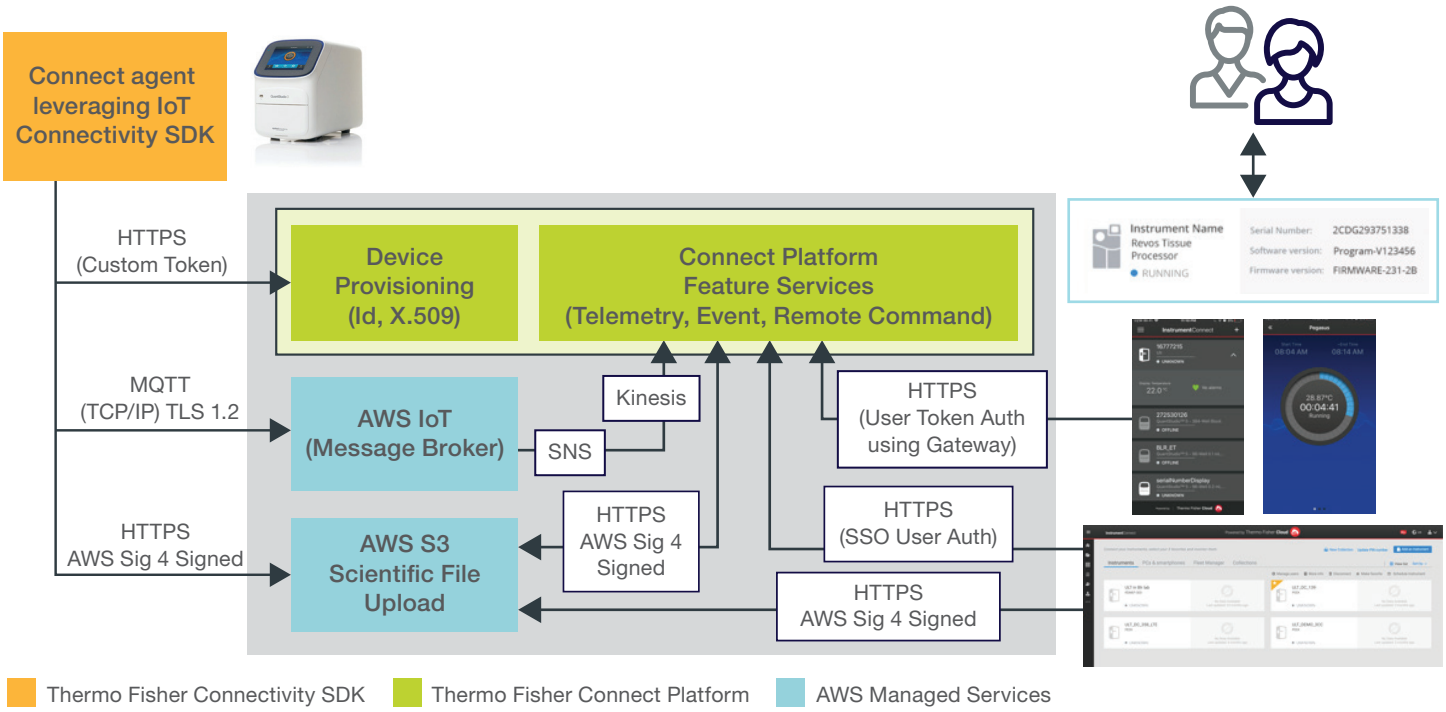
AWS IoT provides a scalable message broker with managed transport security end-to-end from the device to the Connect platform. AWS IoT acts as a gateway using the MQTT protocol for secure communication.

Large File Transfer (Optional)

Due to MQTT payload size limits, HTTPS, utilizing a pre-signed Sig 4 AWS certificate, is used to transfer scientific and protocol files into the Connect platform.

User Access

A user uses the single-sign-on (SSO) authenticated Instrument Connect dashboard hosted on the Connect platform and/or Instrument Connect native mobile application to monitor devices and data.



Encryption

At Rest

User-uploaded data for Connect is stored in the AWS S3. The data is encrypted using AWS S3 server-side encryption that utilizes 256-bit Advanced Encryption Standard (AES-256). All backup data containing customer data encrypts at rest.

Metadata in databases, such as references to data in S3 and metadata, is not encrypted at rest due to performance considerations.

Certificates

Connect uses AWS certificates, which is a Trusted Certificate Authority.

Device Certificate:

After being provisioned, this certificate will be used by the device to establish an MQTT communication from the device to the Connect Platform.

Device Provisioning Certificate:

This certificate is used to generate a secure token. The secure token is exchanged with the Connect Platform to get the device identity and credentials (X.509 device certificate for MQTT communication).

HyperText Transfer Protocol Secure (HTTPS)

For HTTPS communications, TLS v1.2 encrypts the connection between the device and the broker. Authentication delegates to AWS Signature Version 4.

Devices leverage HTTPS to send device data to S3 and for device initialization. The device initialization process also handles end-to-end provisioning, which includes device identity creation and x.509 certificates for MQTT communication.

In Transit

Data in transit to the Connect platform is encrypted using Transport Layer Security (TLS) v1.2 encryption. Web and mobile client access to Connect data uses HTTP over TLS, otherwise known as HTTPS, utilizing 256-bit encryption. The HTTPS connections are terminated at the cloud web tier, API gateways, and the Amazon Web Services (AWS) S3 service.

For IoT connected devices integrated with Connect, both MQTT over TLS and HTTPS are used to secure communications.

Message Queue Telemetry Transport (MQTT)

IBM introduced MQTT in 1999, and OASIS standardized it by 2013 (Amazon based IoT on MQTT). MQTT is advantageous for device connectivity due to its low bandwidth requirements and publish/subscribe architecture. It is designed to provide embedded connectivity between applications and middleware on one side and networks and communications on the other side.

The IoT Connectivity SDK uses a TCP/IP connection from the device to perform simple device data streaming (telemetry, events, status) and remote command communication through the MQTT protocol (TCP/IP/TLS v1.2) over port 443. The X.509 certificate generated on device provisioning is used to authenticate the MQTT connection.

TLS client authentication is used by AWS IoT to identify devices, and all traffic to and from AWS IoT encrypts over TLS v1.2.

Cloud Protection

Cloud Compliance Enforcement

Thermo Fisher has implemented a security control framework that allows for simple and automated adoption of the cloud while maintaining security compliance.

The solution monitors and enforces thousands of controls in hundreds of cloud accounts simultaneously. Some examples of the controls it can enforce include network and firewall management, credential management, audit trail and log management, data protection, configuration management, and more. The solution is a highly available application that is hosted by Thermo Fisher and automatically scales both the web application and the worker nodes to handle dynamic loads.

Distributed Denial-of-Service (DDOS) Protection

Connect leverages AWS to host its infrastructure. AWS provides DDoS protection using scalability features and elastic load balancers. Also, Thermo Fisher leverages a third-party solution that deflects network-layer DDoS traffic and absorbs application-layer DDoS traffic at the network edge. Mitigation capabilities are implemented natively in-path, protecting against attacks in the cloud before they reach the Connect platform.

Network Intrusion Detection System (IDS)

A network-based IDS continuously monitors for malicious activity and unauthorized behavior to protect the Connect platform. The solution uses machine learning, heuristic detection, and integrated threat intelligence to detect and categorize threats.

Web Application Firewall (WAF)

Two separate, comprehensive WAF technologies provide a strong defense-in-depth strategy against web-based attacks. The first layer of defense is a cloud-based WAF solution that guards against the web-based attacks before they ever reach the Connect platform. A host-based WAF is used to provide an additional layer of protection as it analyzes traffic at the web server level and provides visibility and incident response capabilities to identify quickly and mitigate threats.

Endpoint Protection

Anti-virus/Anti-malware

Connect leverages a modern anti-virus solution that detects and prevents the execution of malicious software using signature-based indicators of compromise through its comprehensive threat database. The solution provides both real-time and on-demand protection against file-based threats.

Endpoint Detection & Response (EDR)

In addition to an anti-virus solution, Connect leverages an EDR platform to detect, prevent, and assist in responding to the sophisticated attacks that bypass traditional antivirus solutions.

Behavioral and heuristic-based detection methods are leveraged to proactively seek and prevent indicators of attack that are indicative of malicious activity. Whereby, traditional antivirus primarily uses known indicators of compromise from a reactive perspective. Also, the EDR platform provides security analysts the ability to perform rapid forensic examinations and deploy countermeasures like host containment to mitigate threats.

Host-based Intrusion Prevention System (HIPS)

The HIPS solution provides additional protection against network-based attacks at the host level. It inspects incoming and outgoing traffic to detect and block malicious activity. Additionally, it can be used to “virtually” patch systems from network-based attacks until a patch deploys.

Integrity Monitoring

The Connect platform infrastructure utilizes an integrity monitor to detect changes to critical system files and folders, like the Windows registry, that could indicate malicious activity. The integrity monitor takes a configuration baseline of all systems and constantly compares changes to that the baseline against common tactics of malicious software such as persistence methods.

Secure Development Life Cycle

API Security

As part of Thermo Fisher's ongoing efforts to advance the way the world does science, we are invested in leveraging the benefits of cloud computing to enhance data analytics and collaborate on shared research. To do this safely and effectively, we employ regular API scans of all internal and externally exposed APIs to ensure these functions are not vulnerable to outside influence. Likewise, as part of our ongoing efforts to re-affirm the security of our externally exposed APIs, we perform regular security checks manually with highly skilled, certified individuals who have years of experience in Web Application Security testing.

Bug Bounty Program

Thermo Fisher participates in a bug bounty service that rewards vetted white-hat hackers for discovering vulnerabilities in our software and infrastructure. Crowdsourced vulnerability management is key to maintaining a secure Connect platform and can help detect complex vulnerabilities that traditional scanners can't find.

Dynamic Analysis

Thermo Fisher regularly performs Dynamic Analysis of all web applications developed by the company. These scans are performed automatically via API requests as part of software engineering's continuous integration pipelines during the development process and again on a regularly scheduled cadence for all publicly accessible web applications. Dynamic Analysis scans provide feedback to development teams as quickly as the scans finish and aggregate into reports for visibility and prioritization.

Product Security Assessments

Products, instruments, and devices undergo different levels of security assessments during the product development lifecycle. A product security assessment typically includes a mixture of technical assessments of various components of the overall solution, such as a security architecture overview, software testing, and hardware testing. Development teams receive security assessment findings for prompt remediation.

Secure Software Development Training

At Thermo Fisher, we certify our Software Development teams with training in 25 attack vector categories—including SQL Injection, Broken Access Control, File Upload Vulnerabilities, and Toxic Dependencies. Training module completion is tracked per developer, with all 25 attack vector categories required in order to receive certification. Development teams are re-certified annually to ensure they maintain fresh knowledge of both new and existing attack vectors.

Source Code Management

Innovation is at the heart of the work we do at Thermo Fisher, and to do that at scale we employ a centralized version control system across the company to enable software development teams to collaborate on common software projects. Some of the benefits for having a centralized version control system include the ability to perform Static Analysis at scale for each project—as well as protect our source code from malicious dependencies. Likewise, by utilizing a centralized source code management tool, we can ensure we maintain data loss prevention by syncing this system with other security tools employed throughout Thermo Fisher.

Static Analysis

It is Thermo Fisher's policy to perform Static Analysis on every application, microservice, and function. We achieve this at scale by connecting our Next Generation Static Analysis tool to the version control system our software development teams are using to track code changes—whereby each new commit and pull request into the Master branch is then scanned for both software vulnerabilities as well as good coding practices. Feedback for software developers is rapidly aggregated and provided back through various mechanisms such as their Integrated Development Environment, an internally facing Web UI, and via an internally accessible API.

Security Monitoring & Incident Response

Digital Forensics and Incident Response (DFIR)

The DFIR program is a multidisciplinary profession that focuses on identifying, investigating, and remediating security threats. Thermo Fisher has a dedicated DFIR program that leverages threat intelligence and internal data, along with digital forensics techniques, to investigate potential cyber intrusions. The DFIR also has responsibility for investigating potential insider threats which are persons that may pose a threat to our company, assets, intellectual property, or employees.

Global Security Operation Centers (SOC)

While a defense-in-depth strategy is used to prevent threats, Connect also has the support of a 24-hour SOC that provides continuous monitoring, detection, and response capabilities to anomalous traffic. This team follows-the-sun to provide regionally nuanced support with global visibility and impact. We structure response efforts through a risk-based approach designed to leverage threat intelligence and automation to efficiently mitigate threats at scale.

Incident Management

Thermo Fisher maintains a rigorous process for managing cybersecurity incidents based on our Incident Response Plan (IRP). Thermo Fisher documents all incidents into an Incident Management System (IMS), and all incidents assigned a severity of critical are assigned an Incident Response Coordinator to ensure the immediate mitigation and remediation of the threat. Once the threat has been mitigated, the teams turn to root cause analysis and begin the process of continuous improvement and reducing the opportunity for reoccurrence.

Customers are informed in the event of a security incident that impacts their information as outlined by applicable laws and regulations in addition to contractual requirements.

Security Information and Event Management (SIEM)

Comprehensive security logs are retained and managed by the SIEM for a period of time as determined by applicable policies, regulations, and contracts. Audit logs are not made available to end users or customers, and our internal data privacy assessment program has approved the data collection process.

Threat Intelligence

Thermo Fisher maintains relationships with various threat intelligence partnerships, both premium sources as well as community based or “crowdsourced” intel. This helps us to develop a deep understanding of existing and emerging security hazards to better respond to threats in real-time. Threat Intelligence also makes security analysts more efficient and can reduce false positive alerts. Finally, with actionable intelligence, we can empower senior decision makers.

Access Control

Authentication

Administrative access to the AWS console requires multi-factor authentication (MFA). Thermo Fisher limits access to application servers and infrastructure to only authorized personnel. For administrative use, Thermo Fisher maintains authentication mechanisms utilizing both generated SSH (secure shell) keys and individual user credentials. These keys are retired and changed as necessary. Encryption keys for encryption of data are provided as a service by AWS and not maintained directly by Thermo Fisher.

Firewall

AWS facilitates secure network configuration through security groups for host-level virtual firewalls, network access control lists (NACLs) for controlling traffic in and out of subnets, and virtual private clouds (VPCs) to isolate virtual networks from one another. Only external services are hosted in public subnets, while private subnets host internal services and infrastructure, such as databases that are not publicly accessible. Network access is locked down via NACLs and security groups so only necessary communication is allowed per business requirements.

Identity and Access Management (IDAM)

Access permissions assigned to individuals and applications are based on their need to manage and support applications and are configured with the principle of least privilege.

As a security practice, a list of access owners is regularly audited by assigned managers. Authorized mobile access to Thermo Fisher information assets is provided only via SSL connection.

Password Policy

The proper creation, structure, and renewal of passwords is essential to preventing unauthorized access and/or exploitation. Thermo Fisher's Information Security Password Policy mandates password requirements based on industry best practices that are enforced by internal controls managed by the Cybersecurity Program.

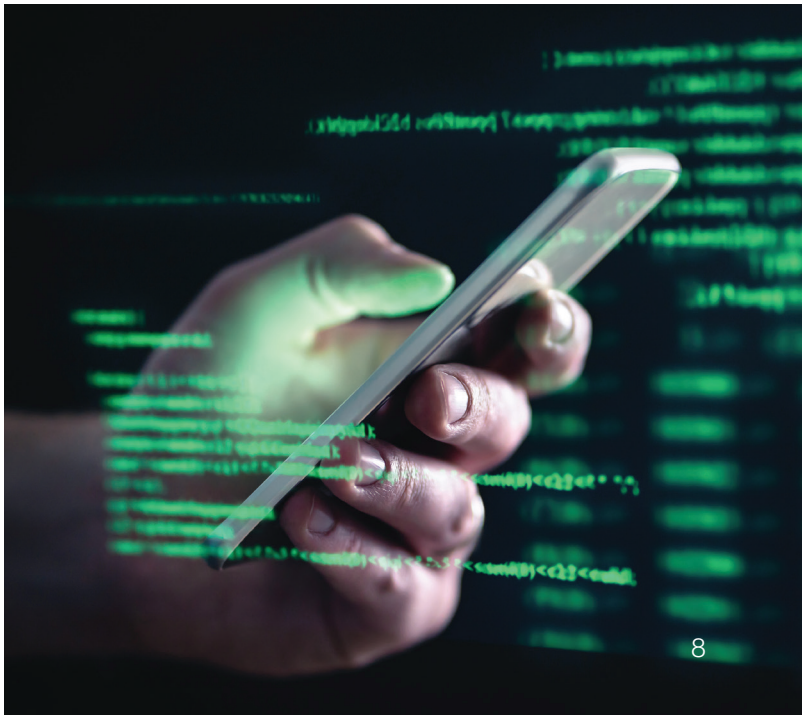
Remote Access

Secure VPN Connections control remote access on authorized devices from Thermo Fisher and access is terminated in the event of employee separation.

Secure Areas

Thermo Fisher uses physical access controls as well as globally controlled card keys and security cameras to maintain information security when accessing cloud-based third-party services. Card keys are managed globally by the physical security team, and access can be added or revoked within minutes by 24/7 physical security representatives.

All externally audited security plans in each Connect facility received an ISO 27001 Information Security Management System Certification. Each Connect facility has a site lead who ensures that only appropriate persons have access to the facility and that access is appropriate for controlled access areas within the facility.



Resiliency

Change Control

Thermo Fisher follows a standardized change control process that requires supervisor, configuration item owner, and QA governance approval. All releases are security scanned for application and infrastructure vulnerabilities, and all application teams maintain test procedures that are executed in test, stage, and production environments.

Compliance

The Thermo Fisher Connect platform is ISO 27001:2013 certified, which is a global standard focused on information security management systems (ISMS). The ISMS is a framework of policies and procedures that includes legal, physical, and technical controls involved in an organization's information risk management processes. ISO/IEC 27001:2013 certification helps ensure that the quality, safety, service, and product reliability of the Connect platform. has been safeguarded.

The Connect team is ISO 9001:2015 certified, which establishes quality management principles with a strong customer focus on the process approach and continuous improvement. The ISO 9001 certification process maintains assessments and registers of risk.

The Connect platform and applications are not currently validated for Good Laboratory Practices (GLP)/Good Manufacturing Practices (GMP) compliance for PaaS or SaaS.

Patch Management

Thermo Fisher's patch management policy is to apply security patches to all systems on a monthly basis. The security team will work with respective groups to identify and update/remediate vulnerabilities accordingly.

Personnel security

Human resource personnel from Thermo Fisher perform background checks on all potential employees and contractors to the extent permitted under applicable law.

Annual Security Awareness Training is provided to all employees in addition to phishing simulation as well as in person training sessions focused on functional roles which help our employees cultivate a "security first" mindset.

Standard Images

Thermo Fisher maintains standard images that are updated regularly or when vulnerabilities are detected, and applications are deployed using these standard images.

Backups and Disaster Recovery

Daily data backups are maintained for at least seven days. In the event of a large-scale recovery, there is a standard order of restoration. Data backup and disaster recovery plans are tested every six months.

AWS services maintain data within a specific region. Connect retains high availability within an AWS region. Connect utilizes multiple availability zones and appropriate networking and load-balancing services. In the event of a wide-scale service interruption within the deployed AWS region, Thermo Fisher will only restore service once AWS has restored service to the region.

Multiple copies of the data are maintained for backups, utilizing AWS S3 that maintains object durability service- level agreement (SLA) of 99.999999999%.

Thermo Fisher maintains requirements for recovery point objective (RPO) and recovery time objective (RTO). Infrastructure is maintained as "Infrastructure-as-Code" utilizing scripts, including standard Amazon Machine Images (AMIs), and AWS CloudFormation configuration for AWS services. Databases are backed up daily, using AWS and third party–provided services.

Health Monitoring

Management of the Connect platform infrastructure and applications follow documented, standard operating procedures.

Application and infrastructure health are also monitored using health check tools, resource utilization alarms, logging alarms, and synthetic transactions.

Scalability

Connect is a multi-tenant SaaS application and is scaled to meet necessary demand, not specific to an individual customer. SLAs are not guaranteed; however, scalability is "practically unlimited" as AWS services are utilized to achieve scalability. Monitoring capabilities are leveraged to identify scaling needs.

AWS storage services maintain all data, such as the Relational Database Service (RDS), DynamoDB, and S3 in the deployed AWS Region. AWS automatically handles the scalability of services, with the exception of RDS where Thermo Fisher manages storage levels and proactively provisions storage as necessary through configuration of the service.

Addendum I

TSX Series Ultra-low Freezers

Connected Lab Functionality

The TSX series achieves customer specific monitoring requirements by saving all events and system temperatures for maintenance and record keeping. The connected lab functionality allows secure connections into the Connect platform to enable real-time monitoring of telemetry and alarm data for better insights into equipment health and availability. Customers can now receive critical alerts to any mobile device that provides both peace of mind and real-time alerts to take action to protect their most valuable assets.

Platform Architecture (diagram below)

The TSX Series control platform consists of an embedded controller and an operating system-based user interface controller. The design includes a high degree of separation between each controller to ensure cargo temperature is maintained. The user interface records unit health telemetry both on-board and, if configured, to Connect utilizing its device provisioning and IoT Connectivity SDK.

Network/Wireless Architecture

The connected TSX Series platform relies on Connect to allow monitoring of real-time telemetry data, and as such needs to be connected as a client to a wireless network. Network connectivity is managed through the user interface directly on the ULT. The wireless supplicant supports modern authentication and encryption schemes to allow for secure connectivity to the network. The only required outbound ports are HTTPS (TCP 443), and NTP (UDP 123).

Data Transmitted

The TSX Series sends the following data to the Connect platform:

- Unit metadata including the production identifier and software version;
- Unit telemetry data including temperatures, voltages and other control state information; and
- Event data including door open/close events and alarms. If applicable, the logged in username will accompany some of the event information.

Encryption

TSX Devicelink embedded connectivity uses a TCP/IP connection from the device to perform device data streaming through the MQTT protocol (TCP/IP / TLS v1.2) over port 443.

Data Use and Access

Terms of Use can be found directly through an account with Connect or here:

https://apps.thermofisher.com/apps/amp/#/printeula.

Authentication

There are two stages of authentication. The first involves signing into the TSX Series platform using credentials created on the Connect platform. The second stage leverages an X.509 certificate which was generated upon device provisioning to authenticate the MQTT connection.

Secure Software Development Training

All developers working on the TSX series complete yearly assigned secure code training. Thermo Fisher certifies our Software Development teams with training in 25 attack vector categories – including SQL Injection, Broken Access Control, File Upload Vulnerabilities, and Toxic Dependencies.

Source Code Management

All source code is stored within a managed code repository at the product level, ensuring the integrity of the code and allowing access to only authorized developer staff.

Penetration Test & Remediation

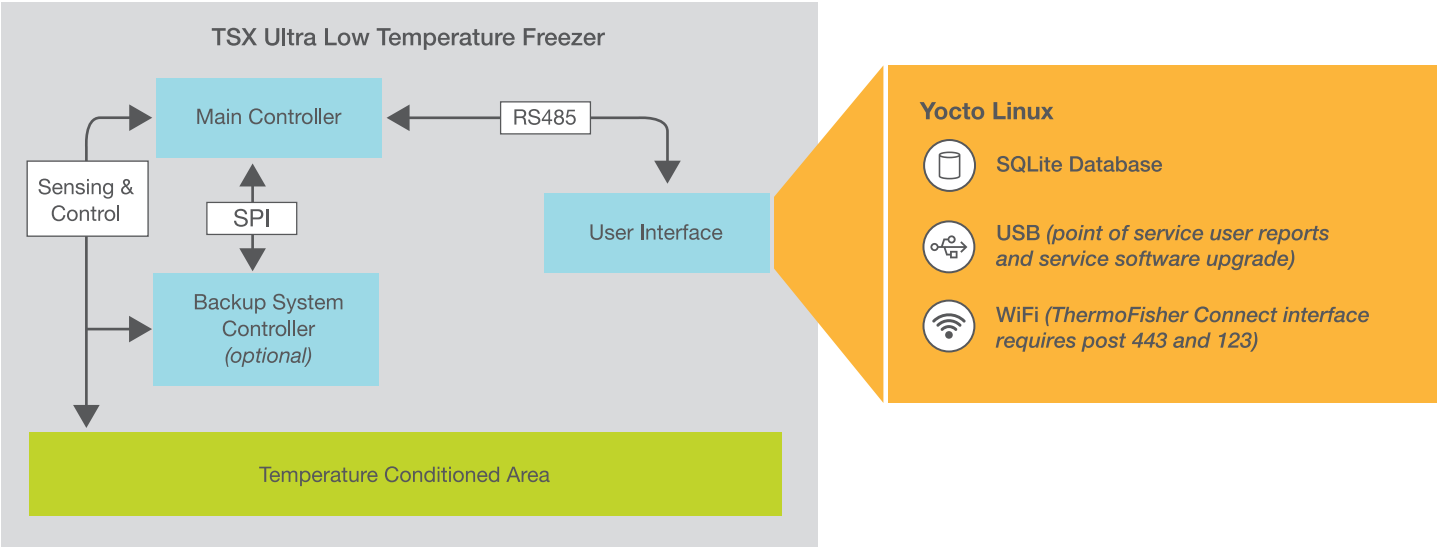
A product security assessment typically includes a mixture of technical assessments of various components of the overall solution, such as a security architecture overview, software testing, and hardware testing. DeviceLink Embedded Connected Lab Functionality for TSX Ultra-Low Temperature (ULT) Freezer has undergone a complete security penetration test of the hardware, software, and communications. Test findings are evaluated for risk and remediation of these findings take place in a prioritized order. Ongoing penetration testing and vulnerability scanning will be conducted in accordance with Thermo Fisher policy and security recommendations.

Remote Access

The TSX Series does not offer any remote connection for intentional use by either Thermo Fisher or the unit owner whereby the product configuration or settings may be changed. The only network capability outbound involves the transmission of data to the Connect platform using HTTPS.

Patch Management

Patch management standards include the application of security patches to all products on a routine basis. The security team will work with respective groups to identify and update/remediate vulnerabilities accordingly. Patches and updates will be applied by Field Service Engineers.



For Research Use Only. Not for use in diagnostic procedures.

ThermoFisher SCIENTIFIC