Product Security Information Guide

Thermo Scientific™ Connect Edge | December 2024

Document valid through December 17, 2025

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 Connect Edge gateway against intrusion or data compromise. This document applies only to the Connect Edge gateway deployed within the customer's environment. It describes the various standards, controls, data security approaches and business practices that Thermo Fisher Scientific has employed for this configuration. This document does not apply to security features within the optional Thermo Fisher™ Connect Platform.

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 **December 17, 2025.** 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 Thermo Scientific Connect Edge solution lets you connect devices to a digital ecosystem to enable data communication between lab instruments and the Thermo Fisher Connect Platform. The Connect Edge Gateway currently supports devices, such as refrigerators, incubators and freezers, allowing for customers to connect their various devices to a central solution. Once connected, device sensor, scientific and operational health data may be shared in a standardized and traceable way, providing utilization and criticality data anytime, anywhere through the Thermo Fisher Connect Platform.

Hardware specifications

The Connect Edge Gateway and adapters have the following hardware specifications:

- Connect Edge gateway
  - Texas Instruments™ AM3352 Sitara™ processor 1GHz, 1 core
  - 1GB RAM
  - 8GB eMMC
  - 4G LTE cellular, Wi-Fi/Bluetooth (model-dependent)

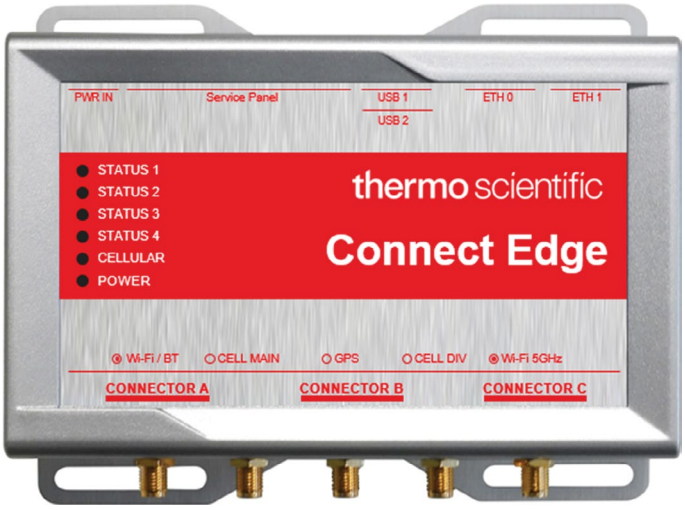


Figure 1: Connect Edge gateway

- Adapters (serial and sensor)
  - Serial port/sensors to network adapters
  - Both adapters contain the Expressif™ Systems ESP32™-Pico microcontroller
  - Ethernet available, Wi-Fi/Bluetooth (on demand)

System compatibility

The Connect Edge gateway is compatible with the following supported operating systems and software:

- Eurotech™ Everyware™ Linux™ operating system version 27.1.0 or newer
- Everyware Software Framework version 7.2.3 or newer
- Everyware Cloud Internet of Things (IoT) Platform version 5.10.2 or newer

Third-party assets

The Connect Edge gateway utilizes hardware manufactured by Eurotech, specifically the IoT Edge Gateway. The IoT Edge Gateway operates the Everyware Software Framework (ESF), which runs on a custom Linux operating system, Everyware Linux. The ESF provides provisioning, monitoring and diagnostic capabilities for the Connect Edge solution, allowing for gateway and imaging configurations and package installations

Architecture diagram

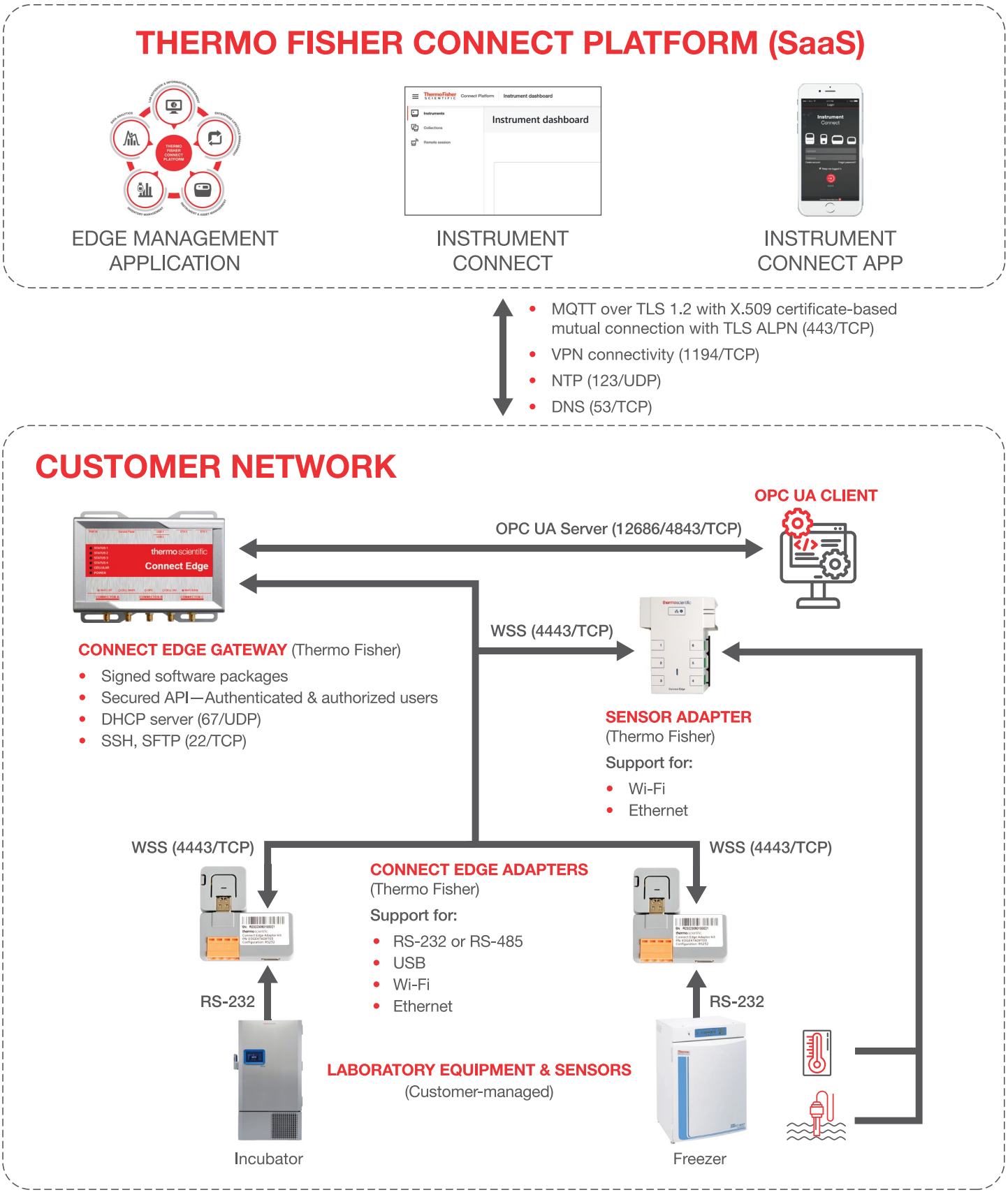
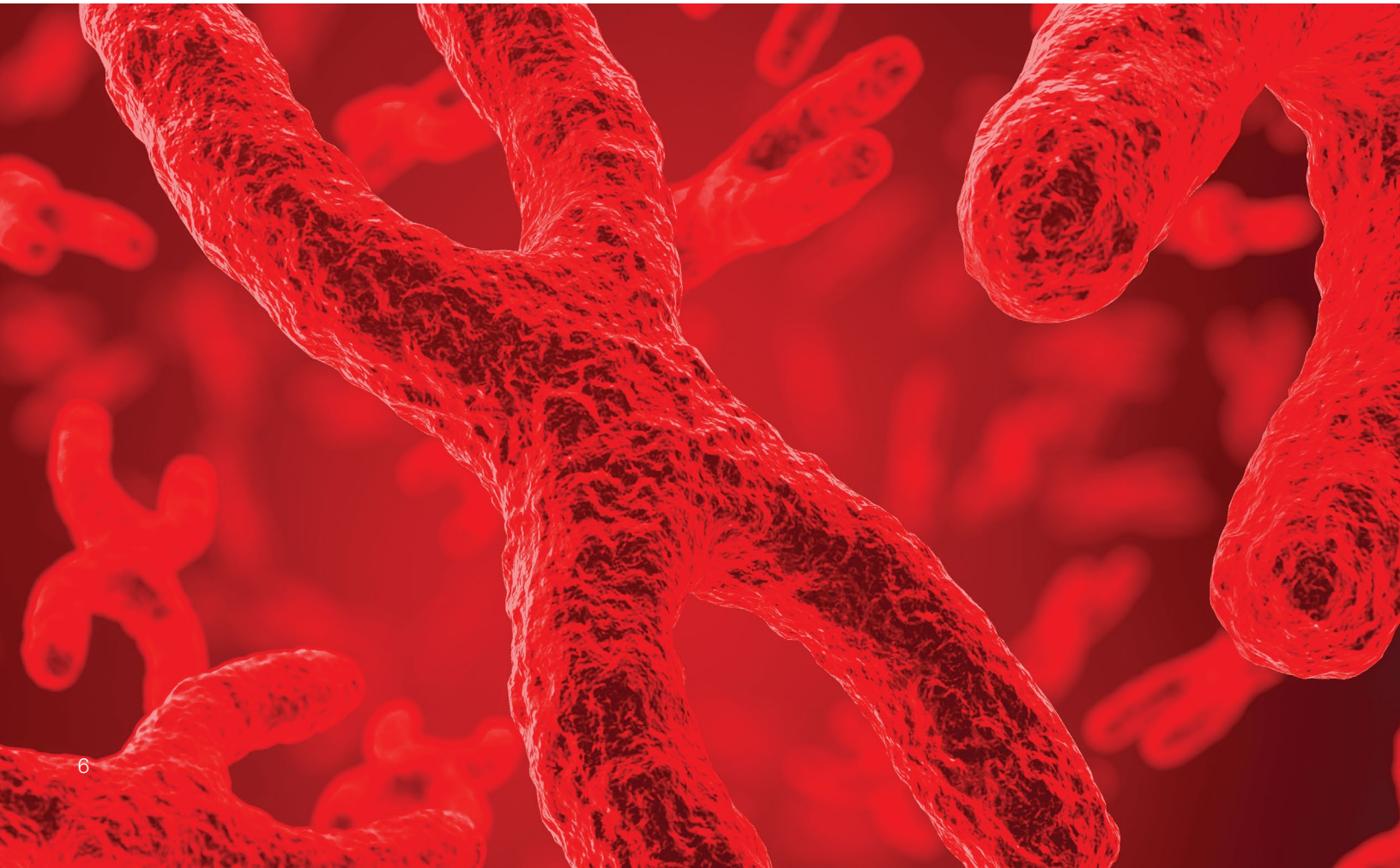


Figure 2: Connect Edge gateway architecture diagram

Component glossary

Term	Definition
Thermo Fisher Connect Platform	Data (instrument telemetry and/or sensor) from the Connect Edge gateway is transmitted to the Thermo Fisher Connect Platform to analyze data anytime, anywhere. Security features within the Thermo Fisher Connect Platform are not in scope for this document.
Connect Edge gateway	The Connect Edge gateway enables data communication from instruments, such as incubators, ultra-low temperature freezers and independent sensors to the Thermo Fisher Connect Platform or OPC Unified Architecture (OPC UA) for data viewing and analysis.
OPC UA client	The Connect Edge gateway includes an embedded OPC UA server, allowing customers to connect their existing software, including Delta V, SCADA and LIMS, to the gateway. Where feasible, customers are encouraged to use port 4843 for encrypted communication.
Connect Edge device adapters	The device adapters transfer data between Instruments and the Connect Edge gateway. Use of Connect Edge adapters is required for Instruments that use serial port communication.
Connect Edge sensor adapter	Sensor data, such as temperature and carbon dioxide (CO2) levels, are monitored by the sensor adapter and transmitted to the Connect Edge gateway. Both sensor adapters and device adapters can connect to the same gateway.
Laboratory equipment and sensors	Examples of the instruments supported by the Connect Edge gateway are ultra-low temperature freezers and incubators. Examples of sensors supported are PT100 temperature sensors, CO2 sensors and door open/close sensors. Sensor adapters are required to monitor sensors.

Table 1: Component glossary

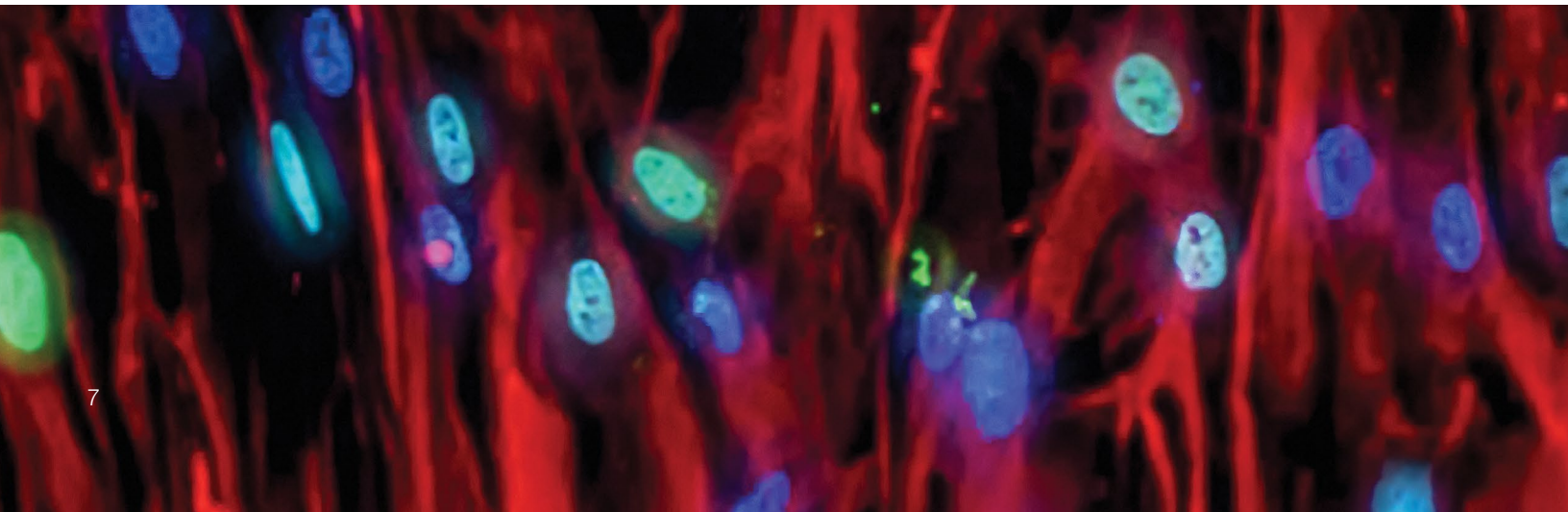


Secure connectivity

Component connectivity

Hardware	Supported instruments	Connectivity offerings	Security considerations
Connect Edge gateway	The Connect Edge gateway supports refrigerators, incubators, freezers and ultra-low temperature freezers. Support for additional instrument types is planned in future releases.	Serial	The connection from laboratory equipment to the Connect Edge adapters supports RS-232, the standard protocol for serial connectivity, in addition to RS-485, TTL RS-232 and USB. Wi-Fi and Ethernet are also supported within the Connect Edge adapter.
		Wi-Fi	The Connect Edge gateway supports the following Wi-Fi authentication schemes: WEP, WPA, WPA2 and WPA2 Enterprise (802.1X). For customers who configure Wi-Fi authentication based on WPA2 Enterprise (802.1X), the supported protocols include EAP-TLS and PEAP MSCHAPv2. Thermo Fisher Scientific recommends that customers configure a supported Wi-Fi authentication scheme based on their business and IT requirements.
		Ethernet (TCP/IP)	The connection from the instrument to the Connect Edge gateway can also leverage a direct Ethernet connection using the Connect Edge adapter. Thermo Fisher Scientific recommends that customers restrict physical access to the instrument and the Connect Edge gateway to ensure a stable and secure connection.

Table 2: Connect Edge component connectivity



Services, ports and protocols

Services	Ports	Network context
Hypertext Transfer Protocol Secure (HTTPS)/virtual private network (VPN)/Message Queue Telemetry Transport (MQTT)	443/TCP	Internet
Secure Shell (SSH) protocol, SSH File Transfer Protocol (SFTP)	22/TCP	Customer
Dynamic Host Configuration Protocol (DHCP) server	67/UDP	Customer
Domain Name System (DNS)	53/TCP	Internet or customer
Network Time Protocol (NTP)	123/UDP	Internet
HTTPS, HTTPS over Secure Web Socket (WSS)	443, 4443/TCP	Customer
OPC UA	4843/TCP 12686/TCP	Internet or customer

Table 3: Connect Edge assets and secure connections

Various system services are used to run and manage the Connect Edge gateway. Key services that can be configured by the customer are listed in Table 3. For the OPC UA client, customers are encouraged to use HTTPS (port 4843) for encrypted communication where feasible.

Thermo Fisher Scientific recommends maintaining the native encryption mechanisms in use and encrypting network traffic wherever feasible. Thermo Fisher Scientific also recommends closing any unused ports to limit connections and to follow industry standards and best practices.

Access controls

Authentication

The Connect Edge gateway authentication leverages username and password, prompting users to change the initial password at the first login. Please refer to the Connect Edge gateway User Manual for instructions on how to initially configure the device and network settings.

Note: A customer must have a valid support agreement to access the Connect Edge gateway User Manual. If you have questions, please contact Connect Edge Support for more information.

Authorization

The Connect Edge gateway leverages role-based access control (RBAC) to grant permissions and access to required users, where roles are configurable to meet necessary business requirements. Thermo Fisher Scientific configures role assignments to use the principle of least privilege based on the need to manage and support the Connect Edge gateway.

Firewall and network controls

The Connect Edge gateway uses the Linux-native utility iptables to block and allow traffic. Ethernet is available as the default network configuration for the Connect Edge gateway. The gateway also has Wi-Fi capabilities, which are disabled by default. If the Connect Edge gateway is unable to establish a connection with the gateway management endpoint during bootup, then Wi-Fi will be temporarily enabled.

For Connect Edge gateway IP assignment, Thermo Fisher Scientific recommends that customers reserve a dedicated IP address within their network configuration for consistent communication with the gateway adapters. For IP assignment of the devices connected to the Connect Edge gateway, Thermo Fisher Scientific recommends that customers utilize the gateway's DHCP client mode as this is the default configuration. In addition, Thermo Fisher Scientific recommends that customers reserve IP addresses to be used by the gateway's DHCP client mode within their own network. Please contact Connect Edge Support for questions about supporting advanced network configurations.

Password management

The Connect Edge gateway user interface (UI) requires passwords for user authentication. Upon initial authentication, a password change is required. User account passwords must meet the following requirements:

- 12 to 80 characters in length
- At least 1 uppercase letter
- At least 1 lowercase letter
- At least 1 numeral
- At least 1 special character

All local web UI passwords are stored on the Linux file system and encrypted.

Logging

The Connect Edge gateway logs multiple types of activities, capturing specific user actions and system performance anomalies. A combination of Linux-native tools and utilities are used for system logging and auditing, such as security enhanced (SE) Linux as well as the auditd (writes audit records to storage) and systemd-journald (collects and stores logging data) services.

By default, log files produced from the Connect Edge gateway are stored locally and will be transmitted to Thermo Fisher Connect Platform using MQTT over TLS v1.2.

Encryption

Hypertext Transfer Protocol Secure (HTTPS)

For HTTPS communications, TLS v1.2 encrypts the connection between the Connect Edge gateway and the MQTT broker, and the WSS connection between the Connect Edge gateway and the gateway adapters.

Message Queue Telemetry Transport (MQTT)

The Connect Edge gateway IoT Connectivity Software Development Kit (SDK) uses TCP/IP (IP port 443) to establish an MQTT connection, allowing simple device data streaming (such as telemetry, status or event data) and remote command communication. MQTT provides advantages for device connectivity because of 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.

Certificates

The Connect Edge gateway utilizes an X.509 device certificate to establish and authenticate the MQTT communication from the gateway to Thermo Fisher Connect Platform. This certificate generates a token that is exchanged with the Thermo Fisher Connect Platform to obtain device identity and credentials.

Secure product development lifecycle

Secure software development training

Software development training is available to the Connect Edge gateway Product 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 best 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 Connect Edge gateway Product 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 Connect Edge gateway 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 used, 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 Connect Edge gateway are stored and maintained in a Thermo Fisher Scientific-approved artifact management solution. This provides visibility and control on developed software builds, enabling the Connect Edge gateway Product 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 Connect Edge gateway Product 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 Connect Edge gateway Product 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 Connect Edge gateway Product 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 Product Development team reviews and prioritizes findings from the scans for remediation based on criticality and a business risk management process.

Architecture review

Thermo Fisher Scientific conducts a security architecture review on the Connect Edge gateway to assess its security measures. Led by product security architects, this assessment involves understanding the components, interactions and connections within the product and evaluating potential security implications. The feedback and

findings from the review are then prioritized by the Connect Edge gateway Product Development team for remediation based on criticality and a business risk management process.

Penetration testing

Thermo Fisher Scientific's Penetration Testing team tests core components of the Connect Edge gateway against the Open Web Application Security Project (OWASP) Top 10 IoTs and Top 10 API lists. The team, comprised of trained penetration testers, use technical and non-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

Vulnerability and patch management

The Connect Edge gateway Product Development team tests and validates security updates and system patches throughout the lifecycle of the product and deploys them to the impacted environments based on criticality. Security patches are released as a software update to the Connect Edge gateway. Upon receiving customer approval, the Connect Edge gateway software updates can be applied remotely from the Thermo Fisher Connect Platform.

Thermo Fisher Scientific does not recommend that customers independently install security patches to the Connect Edge device as this will cause the device to fall out of vendor support per the guidelines in the Master Service Agreement (MSA). Please contact Connect Edge Support for assistance with deploying a patch to the Connect Edge gateway.

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

System hardening

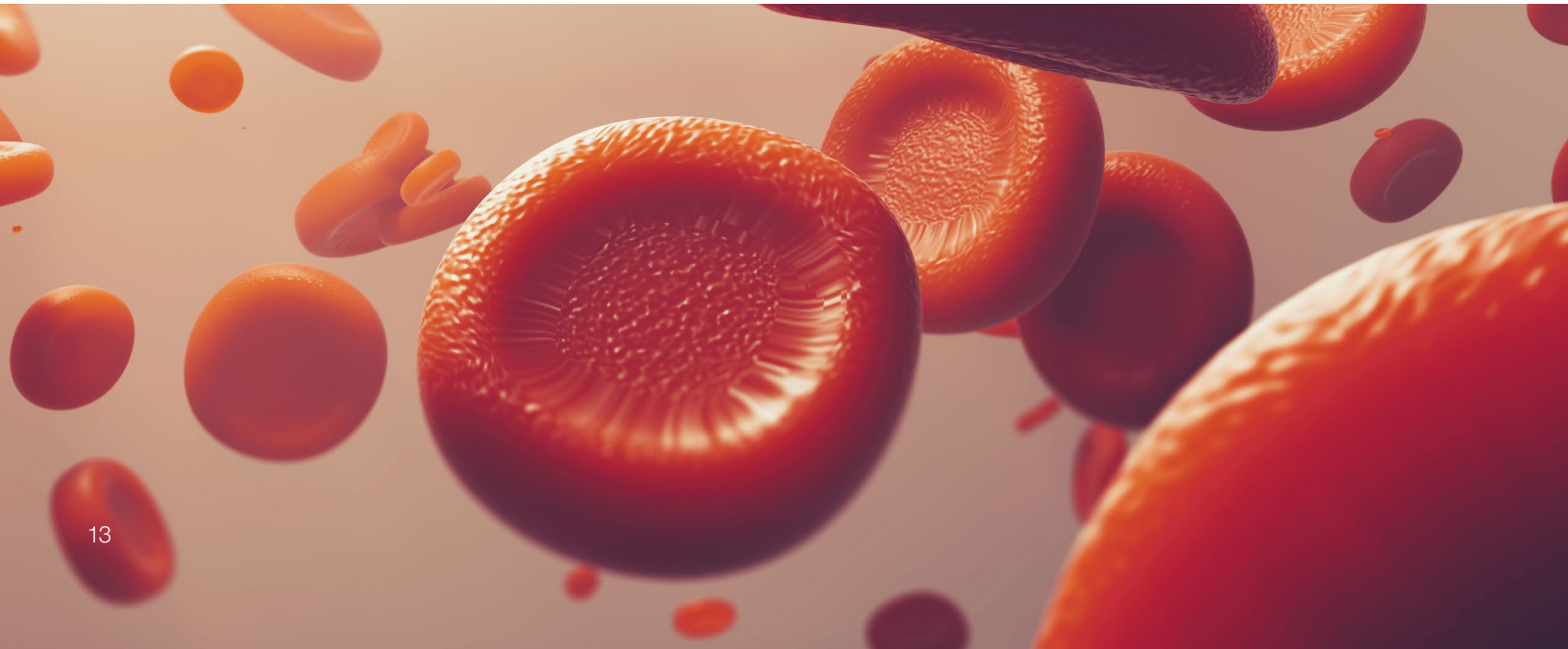
System hardening, a critical security function, can mitigate the potential exploitation of system vulnerabilities and prevent potential threats. The Connect Edge gateway Product Development team uses system hardening practices prior to deployment, which includes disabling the Connect Edge gateway SD slot. Thermo Fisher Scientific recommends that antivirus and anti-malware agents are not installed on the Connect Edge gateway.

Thermo Fisher Scientific recommends maintaining network hardening practices on relevant infrastructure supporting the use of Connect Edge gateway.

Service handling

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

Please contact Connect Edge Support with questions or concerns pertaining to the Connect Edge gateway. For standard service inquiries, please refer to the Connect Edge gateway User Manual for the service number.



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

XX80982-EN1224