Keep connecting. We’ve got your back.

Count on leading services and instrument expertise to support your important work

Services and support

Thermo Fisher Connect Platform overview for technology professionals

Remote service and support technical information

Thermo Fisher Scientific is committed to innovation that drives scientific discovery and definitive clinical outcomes. The Thermo Fisher™ Connect Platform is designed to support maximum uptime of instruments by enabling secure remote service and support options.

This brochure is intended to provide our customers’ IT professionals with the technical information required for evaluating remote service and support functionality and network requirements of the Connect Platform.

Communication between the Connect Platform and customer's instrument

Figure 1 shows an example of a general network architecture where a Connect Platform–enabled instrument is installed.

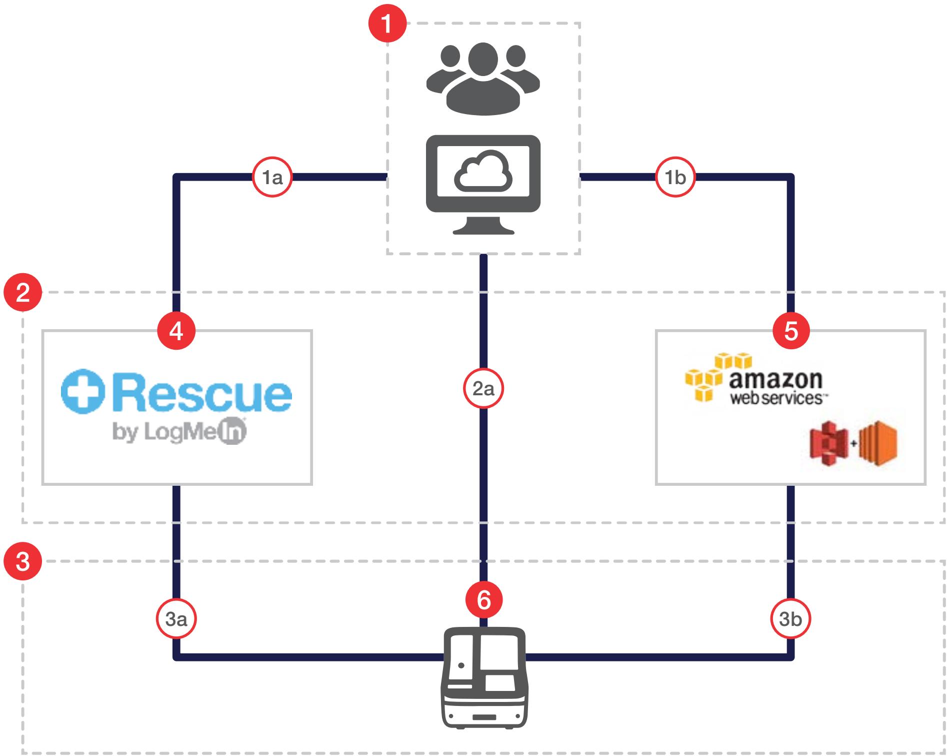


Figure 1. Remote support infrastructure.

1. **Thermo Fisher remote support teams**

   1a. HTTPS—authentication

   1a. TLS 1.2—media services

   1b. HTTPS—secure log file upload (non-PHI)

   1b. HTTPS—telemetry access (non-PHI)

2. **WAN: SAML/SSO cloud services**

   2a. HTTPS—instrument registration

   2a. HTTPS—instrument identity and certificate management

3. **Customer network**

   3a. HTTPS—authentication

   3a. TLS 1.2—media services

   3b. HTTPS—secure log file upload (non-PHI)

   3b. MQTT:443—telemetry collection (non-PHI)

4. **LogMeIn Rescue™ platform (isolated tenant)**

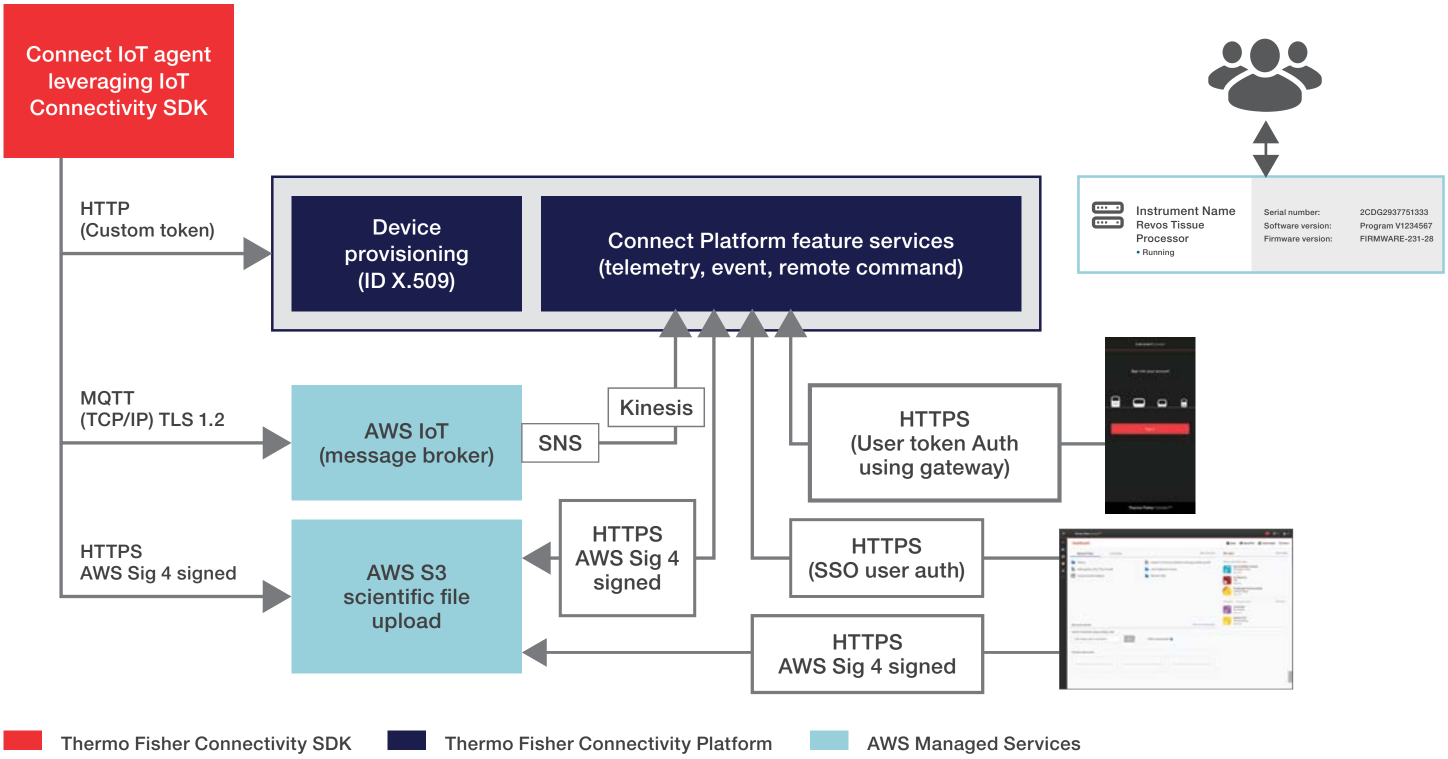
5. **AWS™ Simple Storage Service (S3) and EC2™ platform (isolated tenant)**

6. **Connected instrument**

Connectivity process

Figure 2 shows an example of the connectivity process and communication flow between the instrument and the Connect Platform.

Device provisioning	AWS IoT communication	Large file transfer (optional)	User access
Connect IoT agent calls a custom authenticated REST API to get the device identity and x.509 credentials from the Connect Platform.	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.	Due to MQTT payload size limits, HTTPS, utilizing a pre-signed AWS™ Signature Version 4 (Sig 4) certificate, is used to transfer scientific and protocol files to the Connect Platform.	A customer 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.


Connect IoT agent leveraging IoT Connectivity SDK
HTTP (Custom token)
Device provisioning (ID X.509)
Connect Platform feature services (telemetry, event, remote command)
MQTT (TCP/IP) TLS 1.2
AWS IoT (message broker)
SNS
Kinesis
HTTPS (User token Auth using gateway)
HTTPS AWS Sig 4 signed
AWS S3 scientific file upload
HTTPS AWS Sig 4 signed
HTTPS (SSO user auth)
HTTPS AWS Sig 4 signed
🟥 Thermo Fisher Connectivity SDK
■ Thermo Fisher Connectivity Platform
🟦 AWS Managed Services

Instrument Name
Revos Tissue Processor
• Running

Serial number:	2CDG2937751333
Software version:	Program V1234567
Firmware version:	FIRMWARE-231-28

Figure 2. Example of the connectivity process.

Connect Platform remote service and support

The Connect Platform ecosystem includes remote services and support to ensure maximum uptime for our customers' laboratory investments. Communication with supported instruments is facilitated though secure channels brokered by embedded partner software solutions, meeting and exceeding industry-standard best practices for regulated environments. The purpose of the following sections is to advise customer technology professionals and business partners on the components used in facilitating secure connectivity between the Connect Platform and the instruments residing at customer sites.

Device provisioning

Thermo Fisher service and support uses certificates issued by an AWS™ Certificate Authority. After being provisioned, this certificate will be used by the device to establish an MQTT communication from the device to the remote service platform.

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).

Data transmission

There are three main forms of communication:

- **Telemetry/machine data:** Continuous "HTTPS POST" (ALPN over SSL) sends messages to the Connect Platform web service hosted in an isolated AWS tenant. These messages contain instrument identity and status and machine monitoring data, such as temperature, voltage, current, and pressure. All data and file transmissions are secured utilizing 256-bit encryption.
- **Instrument-initiated log file transfer:** Nonpersistent outbound "HTTPS" connection to the AWS cloud tenant of Thermo Fisher is used for sharing of instrument performance log files, and the contact information of the lab operator requesting assistance. Connections are initiated by users authenticated on the instrument and terminated at the end of the file upload.
- **Remote desktop sharing instrument access:** Authentication "HTTPS" and media services "TLS 1.2" through our technology partner cloud, the LogMeIn Rescue platform, is used for on-demand remote assistance between the instrument or workstation and a Thermo Fisher service representative. Once the user is validated by Thermo Fisher support personnel, the instrument user is required to approve the connection via a one-time six-digit PIN to create the connection. Once the session is terminated at either end, the connection is closed. All interactions are recorded in an audit log and can be provided upon request.

Typical bandwidth usage includes:

- Telemetry data packet payload is roughly 2 KB or less at intervals of approximately 5–30 seconds.
- Log file transfers will vary in size, typically 5 MB or greater depending on the instrument information being compressed and sent.
- 400 kbps bandwidth is required for desktop sharing and software updates.

All communication between the instrument and the Connect Platform leverages commonly used ports to securely broker traffic, relieving additional requirements to modify common firewall port assignments. The device initialization process handles end-to-end provisioning, which includes device identity creation and x.509 certificates for MQTT communication. All telemetry data and log file transmissions are encrypted with industry-standard 256-bit AES encryption over SSL.

The Connect Platform enterprise system

Thermo Fisher assumes that a customer's business partners and IT professionals maintain a safe and secure network and have a firewall and sophisticated security protection for its Local Area Network (LAN). The following sections describe the infrastructure components of the Connect Platform as related to data security.

Data center

The Connect Platform servers are housed on the state-of-the-art data centers of Amazon Web Services, located in the continental United States. User-uploaded log and run file data are stored in AWS S3. The data are encrypted using AWS S3 server-side encryption that utilizes 256-bit Advanced Encryption Standard (AES-256). All backup data containing customer log and run files, and lab operator contact information, are encrypted at rest. For HTTPS communications, TLS v1.2 encrypts the connection between the device and the broker. Authentication delegates to AWS Signature Version 4. Metadata in databases, such as references to data in AWS S3 and metadata, are not encrypted at rest due to performance considerations.

Antivirus protection

Monitoring and intrusion protection

The Connect Platform has many logging and monitoring features built into the system, throughout the ecosystem:

- **Antivirus/anti-malware protection:** The Connect Platform leverages a modern antivirus 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 and response (EDR):** In addition to an antivirus solution, the Connect Platform 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. Traditional antivirus solutions primarily use 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 against 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 Microsoft™ Windows™ registry, that could indicate malicious activity. The integrity monitor takes a configuration baseline of all systems and constantly compares changes to that baseline against common tactics of malicious software, such as persistence methods.

Access control management

Only Thermo Fisher technical support, field service engineers (FSEs), field application scientists (FASs), other support-related agents, and other authorized representatives have access to the Connect Platform infrastructure.

- Three levels of access controls are in place to authenticate a Thermo Fisher representative's access to the Connect Platform infrastructure.
- Access control management for Thermo Fisher representatives is defined by the user's product training, support role, geographic location, and corporate SSO status.
- Access of Thermo Fisher representatives to connected instruments and data is restricted by role-based security and is governed by the applicable security, privacy, and confidentiality regulations.

Privacy and confidentiality

A diverse set of technical and administrative safeguards is incorporated into the Connect Platform's infrastructure to help ensure privacy and confidentiality.

- Connected instruments transmit system performance data for immediate review by the Thermo Fisher service and support organization. Most of this information is pertinent to mechanical function (e.g., temperature, pressure, voltage, motion, status, lamp/laser hours) and in some cases analytical function (e.g., calibration and QC information).
- Other than during remote desktop sharing sessions, the Connect Platform neither transmits nor stores any patient-identifying information other than sample ID. Thermo Fisher therefore recommends you do not include patient names or other medical information in the sample ID field.
- While in the customer-approved remote desktop sharing mode, everything that appears on the screen in the lab appears on the screen of the remote desktop.
- All Thermo Fisher service and support personnel, including those authorized to use the Connect Platform, stay current with annual training requirements of the Health Insurance Portability and Accountability Act (HIPAA) and good distribution practice (GDP) regulations that govern the handling of protected health information.

Installation

Installation of the instrument and connection to the Connect Platform is performed by a Thermo Fisher FSE and requires minimal effort by the customer and IT support staff. In order to enable network connectivity, the customer must provide the following:

- A completed Thermo Fisher service and support installation checklist
- A physical RJ-45 network drop, or for selected instrument families, wireless network credentials to connect to the internet
- A dynamically or statically assigned IP address, subnet mask, and gateway for the instrument. The instrument MAC address can be provided to IT staff prior to or at time of installation, as required.
- Outbound proxy server IP address, as required
- Enable whitelisting of Connect Platform URL/IP endpoints and open outbound ports in the customer firewall to Connect Platform servers

For additional support, email us at **TFC.Device.Connectivity.Support@thermofisher.com**