Thermo Fisher Scientific maintains a Cybersecurity Program, led by a dedicated Chief Information Security Officer (CISO), designed to safeguard the confidentiality, integrity, and availability of data and systems within the company’s environment.

Thermo Fisher supports a continuously improving security program model that is focused on reducing risk, defending against threats and protecting our company’s intellectual property and data privacy.

As the world leader in serving science, our security professionals provide prevention, monitoring, detection and response capabilities so we can more quickly identify and respond to ever-evolving global threats. By protecting our information and assets, we can achieve our mission of enabling our customers to make the world healthier, cleaner and safer.

Thermo Fisher has implemented safeguards and procedures designed to help protect Almanac against intrusion or data compromise. This document describes the various standards, controls, data security approaches and business practices that Thermo Fisher uses in this effort.
Stay connected to your science. Review and share instrument history, stay updated on current acquisition status, and prepare for what’s next all from one accessible productivity tool.

Almanac maintains both an instrument logbook and recent utilization statistics for your connected mass spectrometer. The logbook automatically records events such as calibration and software updates, allows the addition of custom entries and attachments, and offers an intuitive search to find past events of interest. Real-time acquisition status can be accessed anytime and anywhere by visiting the secure Almanac webpage or mobile app, or by configuring real-time notifications delivered through email or mobile app. As you plan upcoming experiments, reserving instrument time is easy using our shared instrument scheduler.

Supporting systems also utilize communication through the Almanac Agent to automatically and immediately notify you and/or the service team when a specific corrective action is recommended or required on your system. Updated instrument method templates can also be downloaded via the Agent.

Finally, if you have a problem on any of your configured instruments (MS, LC, IC or GC), request technical support with a single click through the Almanac Agent. By submitting the request this way, the basic instrument metadata your technical specialist will need to assist you is provided quickly, efficiently, and automatically.

The Almanac Agent Architecture, information flow, and security features are described in the following pages.
Almanac Agent Tray User Interface (UI)
The Almanac Agent Tray User Interface is the front end of the desktop-based Windows Almanac Agent Service and is built in vue.js, which is rendered into the desktop application using CEF-SHARP. The Tray UI is the bridge between instrument and cloud, allowing users to log in, link users, upload data, request support and generate service bundles.

Figure 1: Architecture
**Almanac Agent Service**
The Windows-based Almanac Agent Service is the back-end processing logic that is combined with the vue.js UI, and supports multiple functionalities, including creating a device digital twin, data transfer, remote execution of commands, requesting support and the generation of service bundles.

**Gateway API**
The Gateway application programming interface (API) is designed for the Almanac Agent Service to communicate to the external cloud platform. The API requires HTTPS connectivity and port 443 enabled. The API uses token-based authentication and authorization. Detailed logging identifies users who initiate application calls. These APIs are containerized and orchestrated using Amazon Elastic Container Service/Elastic Container Registry (ECS/ECR). Another certificate-based version of the Gateway API is used to stream data asynchronously between the Almanac Agent Service and cloud. API authentication and authorization occur on the server side.

**Detail API**
The Detail API is designed for the web and mobile application to invoke and process application data. This API requires HTTPS connectivity and port 443 to be enabled. API authentication and authorization are performed using SPROX exposed by the Thermo Fisher Connect platform. The user’s Thermo Fisher Connect username and password are being passed for authentication purposes. These APIs are containerized and orchestrated by Amazon ECS. The DECP platform facilitates deployments and maintenance of these APIs.

**MongoDB**
MongoDB is a NoSQL database that provides the flexibility to store data as a document. Almanac uses Mongo Atlas, a cloud version of the MongoDB, containing one or more cluster nodes providing high availability and durability. The data at rest is encrypted based on MongoDB’s native encryption. Performance monitoring is enabled, and includes details, such as dbstats (memory), size of collection, number of objects, average size of objects and replica info. Automated backup snapshot is enabled and maintained for 30 days.

**PostgresDB Relational Database Service**
PostgresDB RDS service is a distributed cloud relational database and a web service provided by Amazon that has built-in scalability and availability achieved through Multi-Availability Zones. The PostgresDB RDS instance offers automatic patching, backup, and recovery management. Scaling, storage and other compute resources can be performed in a single API call. Encryption has been established and performance metrics are enabled, including read query throughput, write query throughput, resource utilization and reliability. The PostgresDB RDS security group has been created to provide necessary access for the application/users. See Figure 2.

**Device Registration**
Device registration refers to creating a digital twin in Amazon Web Services (AWS) Internet of Things (IoT). Thermo Fisher Device Connect Service provides the interface for AWS IoT. The Almanac Agent Tray UI accepts three input parameters: device serial number, device type and device model. These are communicated to the
Device Connect Service for device registration. Once the device registration is completed, an X509 certificate is downloaded as the unique identity for that Almanac Agent installation/device.

**Service Bundle Generation**
A service bundle is a zipped folder containing instrument logs and reports that can be used for troubleshooting purposes by the Service Team. Data collected here is described in the "Actively, Voluntarily Shared Data" section. Service bundles can be generated independently for the Service Team already working on an issue or can be generated as part of the primary request for support.

**Request Support**
A user with appropriate permissions as defined by an administrator can open a formal request for instrument technical support through the Support tab on the Almanac Agent Tray UI. Basic call-back information, symptom information and system information, including a linked service bundle, are shared as part of this request.

**Control Flow to Instrument via Thermo Fisher Connect (Almanac Cloud UI)**
Remote control of the instrument acquisition queue is achieved in control flow. The following functionalities can be invoked remotely from the Almanac web application:

- Pause the acquisition
- Resume the acquisition
- Stop the acquisition

**Almanac Web Application**
The Almanac web application allows users to interact with their instrument logbook, view instrument status, and generate utilization reports. The web application is hosted under Amazon’s Simple Storage Service (S3) and the dynamic content is retrieved through the detail API.

**Almanac Mobile Application**
The Almanac mobile application allows users to view instrument status, receive real-time notifications and schedule instrument time from a linked mobile device.

**Actively, Voluntarily Shared Data**
End users can choose to share with Thermo Fisher the following data when requesting technical support:

- Instrument identifier
- Instrument configuration (hardware and software)
- Symptom category and description
- Call-back contact information — This information is deleted from the Almanac database once it has been passed to the Service Team and the issue has been resolved.
- Service bundle
  - PC status information
  - Instrument configuration
  - Installed Thermo Fisher software
  - SW log files
  - Instrument log files
  - Calibration reports
  - Diagnostic reports
  - Instrument bootup reports
  - Calibration file
  - Windows error/event logs
  - IQ reports
  - Cache files
  - Add-in registry/cache files

**RDS Configuration**

<table>
<thead>
<tr>
<th>DB version</th>
<th>DB instance</th>
<th>Multi-AZ/Autoscaling enabled</th>
<th>Storage type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>PostgreSQL 11.5</td>
<td>db.t3. small—2vCPU, 2GIB RAM</td>
<td>YES</td>
<td>General purpose (SSD)</td>
<td>100 GB scalable up to 1,000 GB</td>
</tr>
</tbody>
</table>

*Figure 2: PostgresDB*
– Data fault service configuration file
– Windows firewall logs
– Services status snapshot file
– Microsoft SQL Server error logs
– Setup log files

• Method files
• Raw data files
• Screen shots

Passively Shared Data
The following data is shared automatically with Thermo Fisher for the purpose of remote monitoring, notification, logging and analysis following Almanac Agent registration:

• Instrument identifier
• Instrument configuration
  – Hardware
  – Software
• Instrument readbacks
  – Status
  – Settings
  – Calibration/evaluation results
  – Errors
  – Usage data/injection counts
• Experimental sequence status information

Personal, Sample, and Project Identifiers
Personal/user identifiers, sample/patient identifiers, project identifiers, method identifiers and experimental raw data are not shared with the Service Team unless requested by an active end-user. Following intended use, Thermo Fisher’s process involves the deletion of end-user-supplied information from Thermo Fisher Connect.

Thermo Fisher does not collect or request, and a user shall not share, any Personal Data with Thermo Fisher, except their user identifiers, when a user requests instrument technical support through the Support tab on the Almanac Agent Tray UI, as such information is not necessary for the provision of the services through Almanac.

Personal Data means any information relating to an identified or identifiable natural person (for example, not a company). Such natural person is also referred to as “data subject” and one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sample names, sequence names and method names display on the Almanac Cloud UI web application status tab while a sequence is active. Only the sequence name will persist on the Events tab once a sequence is complete. The Almanac Cloud UI web application can be disabled to prevent this information from being shared to the cloud, if necessary.

Notifications
Users may configure status and/or corrective action notifications via the Almanac mobile app or email. Additionally, when configured by the instrument administrator, notifications can be sent from the instrument directly to the Service Team when an unrecoverable error has occurred. The user receives notification of these types of errors and will be contacted by the Service Team for resolution.
Security Activities

Security Assessment Process

Secure Code Training
The Development Team participated in a developer-focused Security Vulnerability Training course as recently as April 2020. Additional training to developers is provided on an ongoing basis about recent developments in the vulnerability mitigation space.

Secure Code Repository
Source code is stored in Azure DevOps Git repositories. User groups, managed by Thermo Fisher Active Directory, provide granular-level access permissions to the source code. Thermo Fisher’s policies call for access to source code to be limited to Thermo Fisher developers contributing to the project.

Static Analysis
It is Thermo Fisher Scientific’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 is scanned for both software vulnerabilities as well as acceptable coding practices. Feedback for software developers is rapidly aggregated and provided back through various mechanisms such as the Integrated Development Environment, an internally facing Web UI, and via an internally accessible API.

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.

Penetration Testing
All components of Almanac have been tested by Thermo Fisher’s Penetration Testing team against the Open Web Application Security Project’s (OWASP) Top 10 IoT list, a document that represents a broad consensus about the most critical security risks to web applications.

The testing is intended to identify potential vulnerabilities from an attacker’s perspective and to provide guidance for remediation. Almanac will be retested as appropriate, such as after changes to functionality or the back end.

Remediation
All components of Almanac that have been tested receive remediation guidance from the Penetration Testing team. This allows the Almanac Development team to focus on potential issues and reduce the product’s risk profile.

User Access Control

Identity Service
Identity service authorizes communication between instrument drivers (instruments). It uses the HTTPS protocol to receive an authorization token.

Login /Logout
Any Thermo Fisher Connect registered user can log into Almanac Cloud UI or Almanac Agent Tray UI provided they
have appropriate credentials and been given access by the Almanac Agent administrator. The Almanac Agent validates the user with Thermo Fisher Connect.

Audit Logging
Currently, the desktop Almanac Agent has no audit logging related to user management. For the Almanac Cloud UI web application, PostgresDB RDS pgaudit is enabled to track operations such as READ, WRITE, ROLE and FUNCTIONS.

Encryption and Protocols

Encryption at Rest
Storage and encryption are handled two ways:
- **Edge** – The Almanac Agent receives data from the instrument and stores the data on a SQLite database. The database is encrypted with the AES-256 algorithm and requires both a password and a private key for access.
- **Server-side** – Once the instrument data has been received server-side, the data will be stored in a PostgresDB RDS instance with native encryption enabled. The automatic snapshot with encryption is enabled as well. After a 30-day retention period, the snapshot is deleted.

Encryption in Transit
HTTPS is the primary secure communication protocol for data transfer to the cloud. Almanac Agent also uses the MQTT protocol for device registration and data transfer to the cloud. MQTT uses the AWS IoT device certificate for establishing a secure channel. In addition to HTTPS, another security layer provides an authorization mechanism designed to avoid man-in-the-middle attacks.

Certificates
X.509 based certificates are used to authenticate a device. X.509 certificates authenticate client and device connections to AWS IoT and enable asymmetric keys to be used with devices.

Hypertext Transfer Protocol Secure (HTTPS)
External communication between the Almanac Agent and cloud is established through HTTPS. The Thermo Fisher Connect Platform team rotates the server certificate. HTTPS requires network port 443 to be enabled for the client to communicate.

Message Queue Telemetry Transport (MQTT)
MQTT is an open OASIS and ISO standard (ISO/IEC 20922) protocol. It is a lightweight, publish-subscribe network protocol that transports messages between devices. The protocol usually runs over TCP/IP; however, any network protocol that provides ordered, lossless, bidirectional connections can support MQTT. It is designed for connections with remote locations where a “small code footprint” is required or the network bandwidth is limited.

MQTT protocol communication is used for creating a digital device twin in AWS IoT and for operations such as propagating device status and user-linking.

Security Lifecycle

System Support
On end-user systems, operating system-level support and security updates, network security, and malware protection are managed by IT departments in compliance with their standard operating procedures.

Defects related to customer-facing functionality are addressed through a regular release cadence of the software and are continually reviewed for resolution in upcoming releases corresponding to the development roadmap.

Depending on severity, and especially in the case of issues related to any discovered security vulnerabilities, hotfixes and patches may be released outside of the scope of the standard release roadmap to minimize risk.
Qualification/Validation
Thermo Fisher Connect applications follow a documented software development plan and operating procedures. These include monitoring application health, security scanning and vulnerability checks. Applications must have documented and maintained test procedures and executed results in the Test and Production environments. Additional validation of the Almanac desktop application may be conducted by customers based upon their SOP definitions. For example, a customer may need to turn off automatic upgrades of the desktop application to fulfill their security requirements.

System Compatibility

OS/Browsers
Almanac software is supported on the Microsoft Windows 10 Enterprise Long Term Service Branch (LTSB) 2016. Google Chrome (Version 66 or above) is the recommended browser for accessing the Almanac web application.
<table>
<thead>
<tr>
<th>Instrument</th>
<th>Click for Support</th>
<th>Remote Monitoring***</th>
<th>Utilization Reporting</th>
<th>Logbook (Auto Entry)</th>
<th>Method Template Download</th>
<th>Corrective Action Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thermo Scientifc™ Orbitrap Tribrid™ MS Series</td>
<td>≥ 3.1</td>
<td>≥ 3.1</td>
<td>≥ 3.1</td>
<td>≥ 3.1</td>
<td>≥ 3.4</td>
<td>≥ 3.4</td>
</tr>
<tr>
<td>Thermo Scientifc™ TSQ™ Triple Quadrupole MS Series</td>
<td>≥ 3.1</td>
<td>≥ 3.1</td>
<td>≥ 3.1</td>
<td>≥ 3.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thermo Scientifc™ Orbitrap Exploris™ MS</td>
<td>OES 1.1</td>
<td>OES 1.1</td>
<td>OES 1.1</td>
<td>OES 1.1</td>
<td>OES 2.0</td>
<td></td>
</tr>
<tr>
<td>Thermo Scientifc™ Q Exactive™ MS Series</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thermo Scientifc™ Q Exactive™ GC Orbitrap</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thermo Scientifc™ TSQ™ 9000 Triple Quad GC-MS/MS System</td>
<td>All* or CM&gt;7.2.10</td>
<td>All* or CM&gt;7.2.10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thermo Scientifc™ TSQ™ 7000 Single Quad GC-MS System</td>
<td>All* or CM&gt;7.2.10</td>
<td>All* or CM&gt;7.2.10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thermo Scientifc™ TRACE™ 1300/1310 Series GC System</td>
<td>All* or CM&gt;7.2.10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thermo Scientifc™ TriPlus™ 500 Headspace Autosampler</td>
<td>All* or CM&gt;7.2.10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thermo Scientifc™ TriPlus™ RSH Autosampler</td>
<td>All* or CM&gt;7.2.10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thermo Scientifc™ Al/AS 1310 Series Autosampler</td>
<td>All* or CM&gt;7.2.10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thermo Scientifc™ Vanquish™ UHPLC Systems</td>
<td>CM&gt;7.2.10; SII&gt; 1.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thermo Scientifc™ UtiliMate™ UHPLC Systems</td>
<td>CM&gt;7.2.10; SII&gt; 1.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thermo Scientifc™ EASY-nLC™ System</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thermo Scientifc™ Dionex™ Integrion™ HPIC™ System</td>
<td>CM&gt;7.2.10; SII&gt; 1.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thermo Scientifc™ Dionex™ ICS-6000 and ICS-4000</td>
<td>CM&gt;7.2.10; SII&gt; 1.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thermo Scientifc™ Dionex™ Aquion™ IC System</td>
<td>CM&gt;7.2.10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thermo Scientifc™ Dionex™ ASE™ 350 Accelerated Solvent Extractor</td>
<td>CM&gt;7.2.10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* When running on Xcalibur or Foundation, all GC Devices drivers supported; when on CM, 7.2.10 or above required

** GC devices do not currently generate Service Bundles, ticket will be automatically generated, but without a service bundle

*** Remote monitoring is only supported when instruments are acquiring data in Xcalibur or Trace Finder ≥ 5.0

Figure 3: Instruments and Control Software
Questions? To reach a member of our team and discuss this product, please contact us at AlmanacSupport@thermofisher.com