Security quick reference guide

Remote Operations software
April 2026

Document valid through April 30, 2027

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 and TeamViewer™ established a strategic partnership to develop the Remote Operations software, a customized, LAN-only remote access application tailored for Thermo Scientific™ electron microscopes and associated computers. TeamViewer is an independent third-party provider and is not an affiliate of Thermo Fisher Scientific.

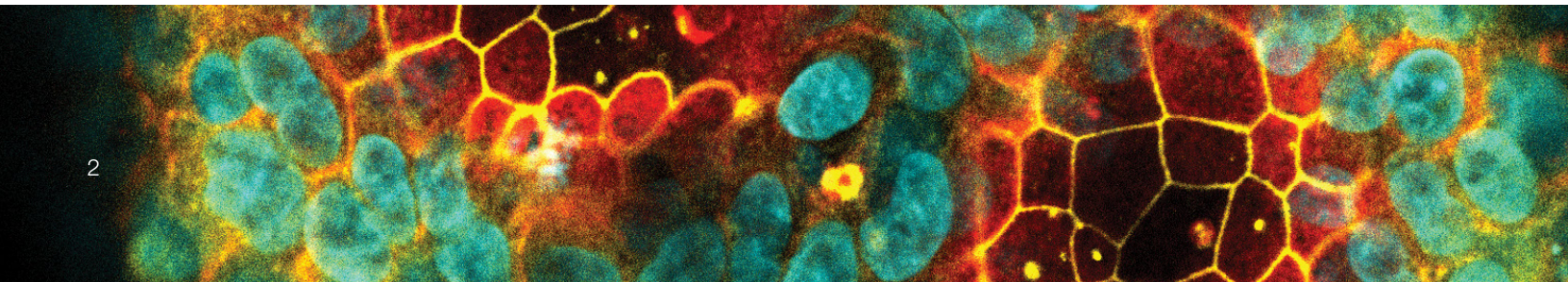
Thermo Fisher and TeamViewer have implemented safeguards and protections designed to help protect the Remote Operations software against intrusion or data compromise. This document describes the various standards, controls and data security approaches and business practices that Thermo Fisher and TeamViewer use in this effort.

TeamViewer provides the remote-connectivity technology and implements industry-standard security practices throughout design, development, testing and maintenance of the Remote Operations software components. This includes authentication mechanisms, end-to-end encrypted remote streaming and a secure software development lifecycle aligned with recognized frameworks. Please note that Thermo Fisher relies, in part, on information provided by TeamViewer regarding its security practices and does not independently verify all third-party controls. Responsibility for third-party components remains with the respective provider, subject to applicable agreements. Thermo Fisher integrates these components into the overall system, manages user accounts and access control, configures the appliance within customer networks and provides deployment and operational support. This shared-responsibility model ensures that TeamViewer delivers secure-by-design technology while Thermo Fisher governs its use within controlled laboratory environments. This model also allocates distinct responsibilities between the parties with TeamViewer responsible for the security of its technology components and Thermo Fisher responsible for configuration and deployment within the defined system scope. For more information on TeamViewer's security practices, please refer to the TeamViewer Security technical overview. Thermo Fisher is not responsible for the content, accuracy or updates of third-party documentation.

Due to the ever-changing cyber landscape, Thermo Fisher updates this security quick reference guide annually to maintain current and accurate information. This guide expires on **April 30, 2027.** Contact your account representative to get 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 subsidiaries or affiliates (collectively, "Thermo Fisher Scientific" 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 customers that any of the methods or suggestions described in this security quick reference guide will eliminate or reduce security risks, restore customer's systems, resolve issues related to any malicious code or achieve any other stated or intended results. Customers are solely responsible for evaluating and implementing appropriate security measures within their own environments and should not rely exclusively on this guide. The customer exclusively assumes all risks 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.

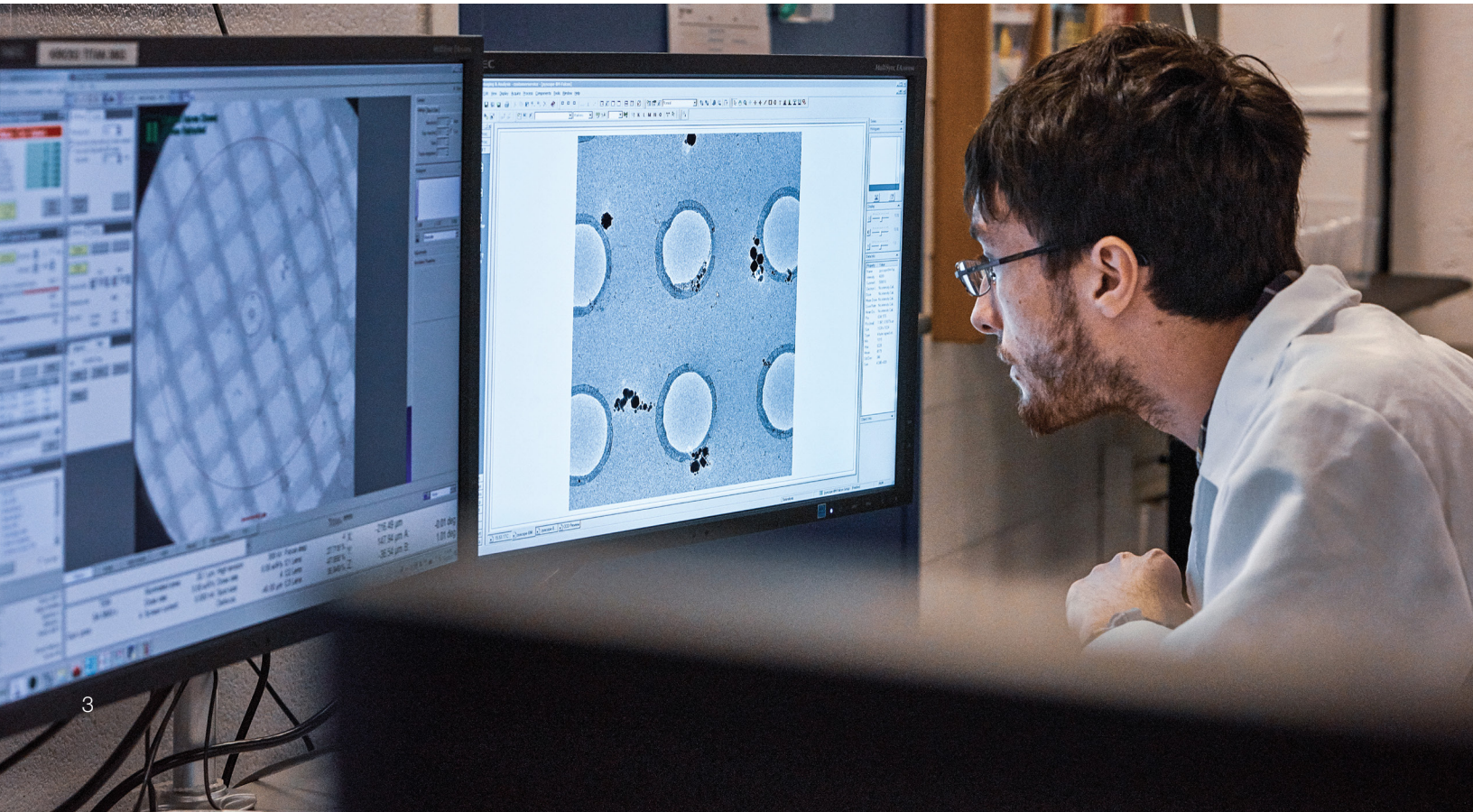
Thermo Fisher's Cybersecurity Program maintains an International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2022 certification for the management of the following areas:

- 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 cybersecurity risk.



Product overview

The Remote Operations software is an on-premises application designed to enable remote access to Thermo Fisher electron microscopes and their associated control PCs. It allows authorized users to view instrument status and control the microscope graphical user interface (GUI) from a remote workstation within the customer's internal network.

Remote Operations software is designed to support multiple workflows including:

- Remote operation of scanning electron microscope (SEM) and transmission electron microscope (TEM) instruments;
- Unattended or attended control with explicit operator approval;
- Session monitoring and termination by local personnel; and
- Remote viewing and collaboration scenarios.

The Remote Operations software is composed of lightweight software components installed on designated Microsoft™ Windows™ PCs and a secured Linux™-based appliance, referred to as the Remote Operations appliance. The Remote Operations software does not require cloud connectivity. When deployed as designed, all communication occurs within the customer's internal environment, supporting compliance with customer IT policies and restricted lab networks.

Comprehensive security controls

Authentication & authorization

The Remote Operations software is designed to require user authentication before any system interaction or remote session initiation. Only authenticated users may request access to registered microscopes where user accounts for remote operators are created by Thermo Fisher service engineers. TeamViewer does not manage customer operator accounts or have access to customer credentials. The Remote Operations Connector guides users through the login sequence with detailed instructions included in the User Manual.

Note: Customers receive the User Manual as a PDF upon purchase of the software. Each operator is assigned a unique 16-digit system-generated password which may be reset or regenerated by service engineers at any time. The Remote Operations software is designed not to support persistent shared credentials or unmanaged accounts. Passwords are intended to be unique per user, should never be reused and do not grant administrative system rights. The Remote Operations software does not utilize persistent remote desktop passwords for session establishment. Instead, sessions use appliance-validated session credentials that are single-use and designed to expire immediately after the session ends.

The Remote Operations software supports 2 modes of operation: Attended or Unattended. Attended mode is preconfigured by default with an auto-reject feature designed to prevent unapproved connections. When Attended Mode is enabled, the local operator physically present at the microscope must approve each remote access request before the session begins. The local operator may:

- Approve or deny session requests;
- Observe active sessions; or
- Terminate sessions at any time.

In Unattended mode, a local operator is not required to be present. This setting must be enabled by the customer at their discretion and customers are responsible for assessing the associated security risks of enabling this mode.

The Remote Operations software leverages role-based access control (RBAC) to grant permissions and access levels to authorized users, where roles are configurable to meet necessary business requirements. Authorization is enforced by the Remote Operations appliance based on configured roles and system settings. Permissions for the Remote Operator and Administrator roles are:

- Remote Operator role:
  - Authenticates to the Remote Operations Connector;
  - Can view available microscopes assigned to their organization; and
  - Can initiate remote access sessions.

Note: This role **cannot** modify device data, load licenses or manage configuration.

- Administrator role (Thermo Fisher service engineers):
  - Creates or deletes Remote Operator user accounts as part of service and support activities;
  - Generates and resets operator passwords;
  - Registers or update devices;
  - Applies product licenses; and
  - Adjusts general system configurations during service operations.

Network security

The Remote Operations appliance leverages the Linux-native utility iptables to manage and restrict network traffic. Only necessary ports required for system operation are configured for use. Additional network security controls include configuration settings designed to disable outbound internet communication and publicly facing interfaces, automatically closing network ports once the remote session ends and terminating persistent listeners on the microscope PC.

Customers may further restrict communication using their own firewall or network segmentation provided that required ports remain accessible. Customers are solely responsible for the configuration, security and monitoring of their network infrastructure.

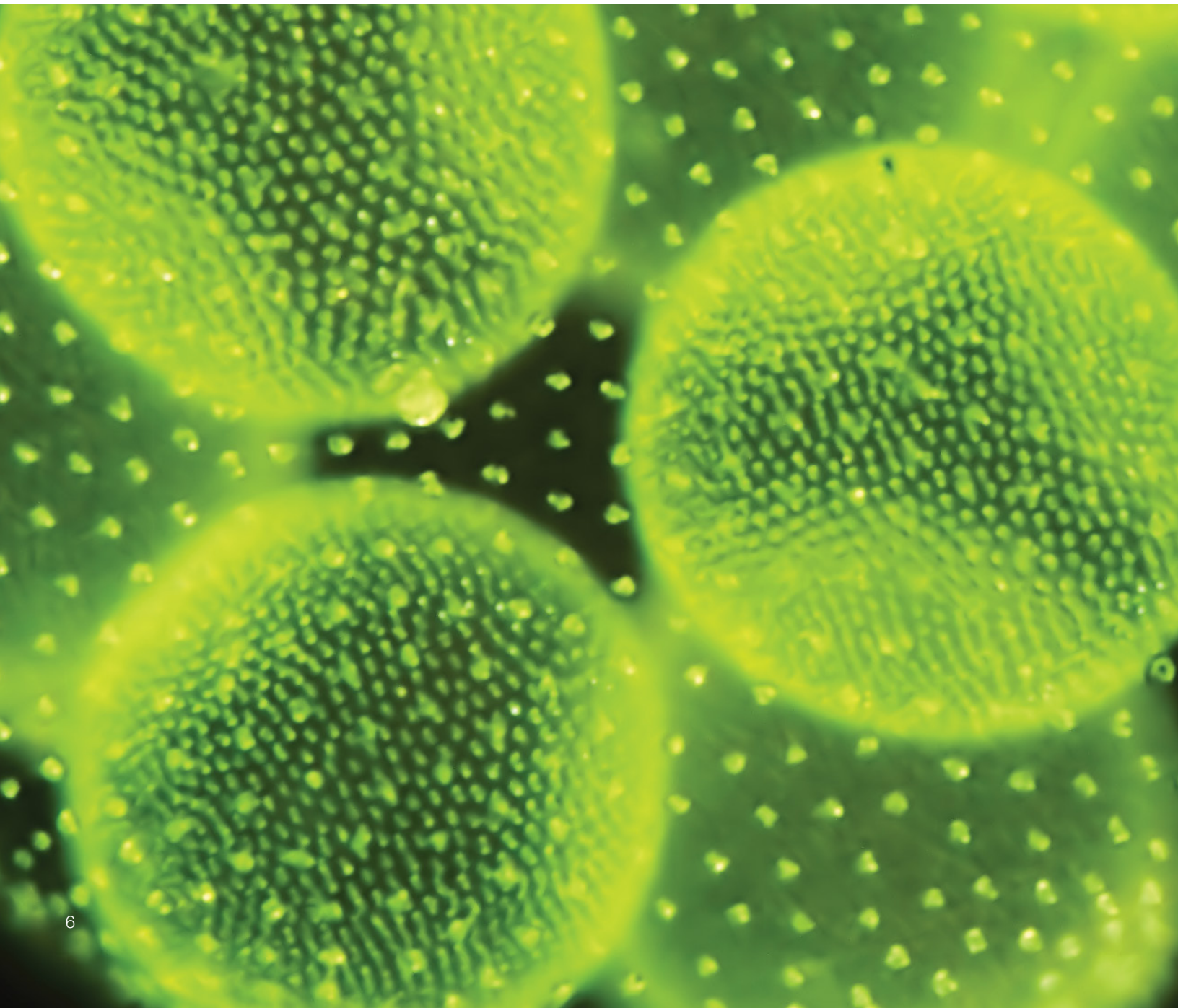
Logging

The Remote Operations software is designed to record certain security-relevant events to support customers with their own compliance and incident review activities. Logged events include, depending on configuration:

- User authentication success and failure;
- Session requests, approvals, denials;
- Session start and end timestamps;
- Device identities involved in each session;
- Hand panel connection activity (if applicable); and
- Local operator actions during attended sessions.

System logs are generated and maintained using a combination of Linux-native logging services, including systemd-journald and application-level logging. Log files produced by the Remote Operations software are stored locally with customer-managed access. By default, the logs are not transmitted outside the customer network.

TeamViewer does not receive logs as part of the standard operation of the Remote Operations software. Customers may export or aggregate logs into their Security Information and Event Management (SIEM) application or monitoring tools, if desired.



Data storage and encryption

Session metadata, configurations, audit logs and internal operational data stored by the Remote Operations appliance are located entirely within the customer environment when the system is deployed as designed. By blocking inbound traffic with firewall rules and restricting database ports to the internal Docker™ network, access to the appliance database is limited to internal appliance services. External access to the database is blocked by iptables firewall rules and direct database queries from outside the appliance are not supported in standard configurations.

Customers may additionally apply full-disk or volume encryption to the Remote Operations appliance according to their internal IT policies.

The effectiveness of data protection measures depends on proper system configuration, deployment and maintenance, including controls implemented by the customer.

Encryption in transit

The Remote Operations software is designed to encrypt communication between system components using industry standard practices. All Hypertext Transfer Protocol Secure (HTTPS) communication uses Transport Layer Security (TLS) v1.2 or higher to help protect confidentiality and integrity while data moves between the Remote Operator workstation, Remote Operations appliance, support PC and microscope PC. Actual encryption behavior may depend on system configuration and environment.

The Remote Operations appliance is designed to present a unique server certificate generated specifically for each customer's deployment. This certificate is intended to help support authentication of the appliance to internal components and to help reduce the risk of unauthorized connections by enabling operators to connect only to an authorized system instance.

The remote desktop streaming channel is protected using end-to-end encryption (E2EE). The operator's inputs and device frames are intended to be encrypted before transmission and decrypted only on the intended endpoint for that session. The effectiveness of this encryption depends on correct system configuration and the security of endpoint devices.

Secure product development lifecycle

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 the complexity of these component interactions. The assessment may include technical review, focused testing of identified components and regulatory review, if applicable. The Remote Operations Product Development team reviews and evaluates security assessment findings and may communicate them to TeamViewer for prioritization and remediation based on criticality and a business risk management process.

TeamViewer follows a secure software development lifecycle that includes controlled source code management, artifact integrity validation and automated static code analysis to identify potential security issues early in the development process. Additionally, Remote Operations software components undergo security testing before release.

While TeamViewer develops and provides security updates and system patches throughout the lifecycle of the product, Thermo Fisher deploys them to the impacted environments based on factors such as criticality and a business risk management process. Thermo Fisher does not guarantee the availability, timing or completeness of any security updates or patches. Security patches are typically released as a software update to the Remote Operations components. Upon receiving customer approval, the Remote Operations software updates can be applied by Thermo Fisher service personnel. Customers are responsible for timely approval and implementation decisions within their environment. If customers encounter technical issues, they are encouraged to initiate a request through their standard support channels.

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

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

FL0305-EN-04-2026