Rescue Remote Support built by GoTo™

August 2024

Document valid through August 15, 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.

Overview

At Thermo Fisher Scientific, our technical support representatives leverage Rescue Remote Support built by GoTo (formerly known as LogMeIn™ Rescue™) software to assist customers who request secure remote support sessions for Thermo Fisher Scientific products and services. Customers initiate the remote support process by contacting our technical support in their region.

Thermo Fisher Scientific has implemented safeguards and procedures designed to help protect company users and platforms while using Rescue Remote Support. This document describes the business practices and security controls that Thermo Fisher Scientific uses in this effort and provides vendor resources for learning more about the product. The Thermo Fisher Scientific Product Security team reviews this document annually to ensure it contains current, accurate information. Contact Thermo Fisher Scientific at **product.security@thermofisher.com** to request the latest published version. This version expires **August 15, 2025.**

How we secure system access

Authentication

Thermo Fisher Scientific technical support representatives sign into Rescue Remote Support accounts using a Thermo Fisher Scientific-controlled enterprise single sign-on solution that utilizes password complexity requirements and multifactor authentication to help guard against unauthorized access.

Access controls

Thermo Fisher Scientific reviews and approves application access requests for account activations or deactivations and assigns appropriate user roles and permissions for remote support technicians. Account privileges are restricted by default to limit access to remote customer support sessions. Thermo Fisher Scientific maintains a policy to encourage the principle of least privilege by which permissions for user accounts and/or processes are restricted to only those system resources that are required to support or manage specific products or services.

Thermo Fisher Scientific conducts regular security settings reviews with the application vendor. These include a review of system settings and account permissions to help ensure ongoing adherence to security best practices.

How we handle remote session reports

Thermo Fisher Scientific restricts access to Rescue Remote Support data. We can produce specific reports from Rescue Remote Support about session times and durations, customer consent, chat logs and transferred sessions if, for example, a technician transfers a call or session for troubleshooting or collaboration. However, Thermo Fisher Scientific cannot access remote session data about users or their workstations and PCs.

Reports are saved to a secured location on the Thermo Fisher Scientific corporate network with data exported to a reporting dashboard accessible only to administrators. The dashboard is updated weekly and retains no prior data.

About Rescue Remote Support

Visit the **Rescue Remote Support website** to learn more about the product. For detailed information about product compliance and security measures, refer to GoTo's **Technical and Organizational Measures for GoTo Digital Engagement.**

If you have further comments and questions, please email the Thermo Fisher Scientific Product Security team at **product.security@thermofisher.com.**