White Paper

RAPID Cybersecurity

Secure remote customer interactions and data protection

RAPID (Remote Access Program for Interactive Diagnostics) is a valuable service program for our customers to remotely interact with Thermo Fisher Scientific remote service engineers or application specialists to quickly and effectively troubleshoot instrument issues. Cybersecurity is a fundamental aspect of the systems Thermo Fisher uses for interaction with our customers. The purpose of this document is to provide Thermo Fisher customers with insights into the cybersecurity and data protection mechanisms we have built into our RAPID service.

What is remote support via RAPID?

RAPID allows instrument users to receive support from Thermo Fisher Scientific remote service engineers (RSEs) or application specialists through a VPN connection. With the consent of the user of the Customer Instrument, trained RSEs can perform the following actions using RAPID:

- Take over the Customer Instrument screen remotely to provide the required support
- Run service test software / diagnostics on Customer Instrument(s)
- Optimize Customer Instrument(s) performance
- Check and modify Customer Instrument(s) settings
- Patch and upgrade software
- View Customer Instrument images

At the request of the instrument user, a Thermo Fisher specialist from anywhere in the world can be invited to a RAPID support session, quickly troubleshooting problems and reducing the time to resolution.

How does RAPID work?

Each RAPID support session is initiated by the instrument user, who decides which RSE can participate in a RAPID support session. This ensures that the instrument user is always in control of the start and end of a RAPID support session. The instrument user and RSE agree upon a time slot during which the RSE delivers support.

Establishing a RAPID support session involves two main steps:

1. Setup of a secured network connection, based upon OpenVPN between the RSE remote laptop and the customer Support PC (SPC).
2. Setup of a secured remote desktop session between the RSE remote laptop and the Microscope PC (MPC or Microscope Controller) via the SPC.

Once these two main steps are executed, the RSE can remotely control the Customer Instrument and provide the necessary support actions. If needed, the RSE can use the TEM hand panels connected to their remote laptop to control the screen of the Customer Instrument.

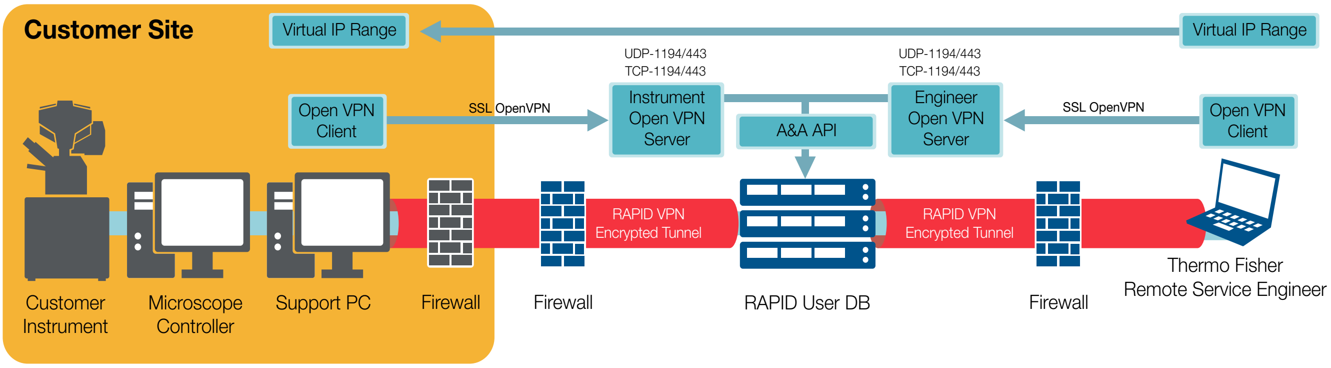

Figure 1. Secured network connection between RSE remote laptop and Support PC.

To set up a secured network connection, the following steps are executed (refer to Figure 1):

1. The instrument user launches the RAPID Connection Wizard (Customer version) on the SPC, selects the Customer Instrument RAPID Secure Server of their region, and provides the RAPID instrument credentials to make a secure OpenVPN connection to the Customer Instrument RAPID Secure Server.
2. The RSE launches the RAPID Connection Wizard (Engineer version) on the RSE remote laptop, selects the Engineer RAPID Secure Server in the same region as the customer, and provides their RAPID personal credentials to make a secure OpenVPN connection to the Engineer RAPID Secure Server.

Now that both the SPC and the RSE remote laptop are connected to RAPID Secure Servers in a specific region, a secured remote desktop session can be set up in the following way (refer to Figure 2):

1. The instrument user shares with the RSE the OpenVPN IP address that was assigned to the SPC and the credentials of the TeamViewer Host running on the MPC. Sharing is done “out of band,” e.g., by telephone.
2. The RSE launches TeamViewer on their RSE remote laptop and uses the SPC IP address and TeamViewer credentials received from the instrument user to connect to the MPC. The RAPID Connection Wizard running on the SPC contains a port-forwarder that proxies the TeamViewer session from the RSE remote laptop via the SPC to the MPC.

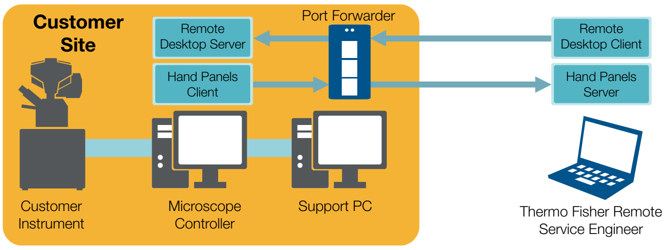

Figure 2. Remote desktop with TeamViewer and TEM hand panels connection between RSE remote laptop and Microscope PC.

Now that the RSE has set up a secured remote desktop session with the MPC using TeamViewer, they can provide the necessary support actions. The instrument user controls the RAPID session and can terminate the session if required.

What are the RAPID cybersecurity controls?

At Thermo Fisher Scientific, cybersecurity is a fundamental aspect of the systems we use for interaction with our customers. We have implemented several cybersecurity controls to reduce the risk of cyberattacks. These controls are described in the sections below.

RAPID user account management

Only authorized users can set up a connection to a RAPID Secure Server. The RSE and instrument user must use their RAPID user account and password. Every RSE and instrument user has a unique RAPID user account.

RAPID user accounts and passwords are managed in the following ways:

1. Dedicated Thermo Fisher RAPID administrators create, modify, enable, and disable RAPID user accounts on the RAPID admin portal. Access to the RAPID admin portal is only possible for authorized Thermo Fisher employees from Thermo Fisher trusted networks.
2. Users can change their passwords, reset forgotten passwords, and view user settings on the RAPID user portal. Users must use their RAPID user account to log in to the RAPID user portal.

Access control

To further restrict access to only authorized users, the following additional controls have been implemented:

1. An RSE and an instrument user can only connect via OpenVPN to the RAPID Secure Servers with a valid RAPID user account and password.
2. The OpenVPN client software launched by the RAPID Connection Wizard running on the RSE remote laptop must be equipped with the correct OpenVPN configuration files and dedicated RAPID Certificate Authority certificate to be able to connect successfully.

3. The OpenVPN client software launched by the RAPID Connection Wizard running on the SPC must be equipped with the correct OpenVPN configuration files and dedicated RAPID Certificate Authority certificate to be able to connect successfully.
4. User accounts will be disabled after three unsuccessful login attempts. User accounts can only be re-enabled by Thermo Fisher RAPID administrators.

Access by the RSE to the Customer Instrument via the MPC is controlled in the following ways:

1. The RSE can only connect to the Customer Instrument via TeamViewer if the RSE remote laptop and SPC are connected to the RAPID Secure Servers in the same region at the same time.
2. The RSE must use the correct TeamViewer credentials (dynamic OpenVPN IP address of the SPC and random, one-time password) of the customer MPC. These credentials are provided "out of band" by the instrument user to the RSE.

Audit logging of RAPID connections per customer

To detect suspicious login behavior and trace back user login activity, the RAPID Secure Servers log all connections in an audit log. The customer can view an audit log on the RAPID user portal of all RAPID connections initiated from the SPC by the instrument user account.

Application and data exchange restrictions

The RAPID Secure Servers infrastructure only facilitates one-on-one application connections and data exchange for the purpose of remote support on a Customer Instrument. Cybersecurity controls are implemented in the RAPID Secure Servers infrastructure to prevent improper use of RAPID. The following policy is enforced:

1. Only authorized applications, such as TeamViewer and TEM hand panel control, can be used by the RSE to remotely control the Customer Instrument.
2. An RSE remote laptop can connect only to the Engineer RAPID Secure Servers and not to the Instrument RAPID Secure Servers.
3. An SPC can connect only to the Instrument RAPID Secure Servers and not to the Engineer RAPID Secure Servers.
4. Data exchange between RSE remote laptops connected to the same Engineer RAPID Secure Server at the same time is not possible.
5. Data exchange between SPCs of different customers connected to the same Instrument RAPID Secure Server at the same time is not possible.

Data protection

Application data exchanged between the RSE remote laptop and the Customer Instrument is protected against eavesdropping and unauthorized alteration. Both the RSE remote laptop and the SPC connect to the RAPID Secure Servers by means of OpenVPN. For the control channel the OpenVPN connection uses TLSv1.2 with a cipher based on ECDHE-RSA-AES256-GCM-SHA384 and 2048-bit RSA key. For the data channel a cipher based on AES128-CBC is used with 128-bit key and a 160-bit message hash for HMAC authentication.

Connection initiation by the customer

Only the customer can initiate a RAPID connection (by starting the RAPID Connection Wizard). No inbound access is possible without customer interaction. As long as the customer does not initiate a RAPID connection, the RSE cannot access the Customer Instrument remotely. The customer is in full control and, therefore, always able to remove any sensitive material from the Customer Instrument before initiating the RAPID connection.

Full visibility to the customer of actions by RSEs

All remote actions performed on the Customer Instrument by the RSE are executed via TeamViewer on the desktop interface, which is fully viewable by the customer. All data that the RSE can see will appear on-screen on the Customer Instrument.

TeamViewer preconfigured security settings

The TeamViewer screen sharing application comes with a set of preconfigured security settings that cannot be changed. The settings ensure that a TeamViewer connection is only possible via a RAPID connection.

TeamViewer logs all actions in a local log file on the MPC or SPC. The RSE can manually collect these log files so that Thermo Fisher can investigate operation and functioning of TeamViewer.

Automatic configuration updates

When the RAPID Connection Wizard is launched on the RSE remote laptop or SPC, and the user has provided their RAPID credentials, the RAPID Connection Wizard first connects to the Update API running on the RAPID user portal to check for configuration updates. The Update API verifies the user credentials and presents a configuration update file to the RAPID Connection Wizard when applicable. The RAPID Connection Wizard downloads the file and automatically installs the configuration updates. This mechanism ensures the integrity of the RAPID Connection Wizard configuration files and provides a centralized way of enforcing on-demand configuration changes to the RAPID Connection Wizard running on the RSE remote laptop or SPC when needed.

Only dedicated and authorized Thermo Fisher RAPID administrators have access to the file storage area of the Update API via the RAPID admin portal and can store configuration update files. Configuration update files are thoroughly tested before being released to the Update API.

Automatic software updates

RAPID Connection Wizard comes with automatic updates that allow users to keep the software updated without having to check for and install available updates manually. When automatic updates are enabled, the RAPID Connection Wizard automatically checks for updates at startup and will download and install with user consent. Enabling or disabling of auto-updates can be configured via Windows registry. The updates go through a process to digitally sign binaries and installers as a way for end-users to verify the code they receive has not been altered or compromised by a third party. The updates are stored in a secure environment managed by authorized Thermo Fisher Administrators.

SPC recommendations

To have the best RAPID support experience and to reduce the risk of cyberattacks on the SPC and Customer Instrument, we recommend our customers use an SPC with the specification noted below (see Table 1). Note that customers are responsible for the security and management of the SPC.

Protection of RAPID Secure Server infrastructure

In the table below are the specifications of the RAPID Secure Server infrastructure, which is located in several AWS regions. (see Table 2).

Recommended SPC specifications	
Operating system	Windows 10 Pro
Processor	1 GHz or higher
RAM	4GB or more
Hard Drive	10 GB or larger
LAN Adapters	2
Recommended Security Settings	• Ensure Windows software patches are installed on a regular basis (automatic updates are preferred) • Use anti-malware/anti-virus software with automatic updates • Enable Windows defender or other host-firewall software

Table 1. Recommended SPC specifications.

RAPID VPN Server (DNS name)	Connection ports	Location
vpn-use1.rapid.thermofisher.com	**TCP** 1194 or 443 / **UDP** 1194 or 443	US East 1 (Northern Virginia)
vpn-usw1.rapid.thermofisher.com	**TCP** 1194 or 443 / **UDP** 1194 or 443	US West 1 (Los Angeles)
vpn-apne1.rapid.thermofisher.com	**TCP** 1194 or 443 / **UDP** 1194 or 443	APAC Northeast 1 (Tokyo)
vpn-euw1.rapid.thermofisher.com	**TCP** 1194 or 443 / **UDP** 1194 or 443	Europe West 1 (Dublin)
rapidvpn.thermofisher.cn	**TCP** 1194 or 443 / **UDP** 1194 or 443	China (Shanghai)

Table 2. RAPID Secure Server DNS Names, connection ports, and locations.

The infrastructure is developed, built, tested, deployed, and managed by Thermo Fisher.

We apply the following best practices to protect the RAPID Secure Server infrastructure:

1. Use of AWS Network Firewalls to block unallowed network traffic
2. Use of AWS high-availability solutions like Availability Zones, Elastic Kubernetes clusters, and Load Balancers to optimize availability
3. Use of secured containerized applications running on a security-oriented, lightweight Linux distribution to minimize the risk of software vulnerabilities
4. Use of separated development (DEV), quality assurance (QA), staging (STG), and production (PROD) environments for development, testing, and deployment of new software
5. Use of change approval process and automated CI/CD pipeline to minimize the risk of human implementation errors
6. Regular security audits, penetration testing, and static code analysis by Thermo Fisher Corporate Information Security to guarantee compliance with corporate security policy
7. Monitoring of the systems in the PROD environment to have 24x7 visibility into systems health

For further technical questions about RAPID, contact us at MSD.rapidsupport@thermofisher.com.

Learn more at **thermofisher.com/remote-service**

For research use only. Not for use in diagnostic procedures. For current certifications, visit thermofisher.com/certifications