Rotor-Gene AssayManager 2.1 Security and Privacy Guide

Introduction

Organizations have individual requirements for the safe and secure usage of systems on their premises and within the networks to which the devices are connected. Additional privacy requirements apply to the data that these devices generate, receive, transmit and store. Many organizations must also augment the technical measures implemented in QIAGEN® devices with organizational measures, such as regulating access to export folders and properly securing networks that carry sensitive data.

To help users of the system fulfill their privacy and security responsibilities, we provide in this document information about the technical implementation of security and privacy measures. We also describe the known limitations of these as well as details for potential additional options for situations where our technical measures cannot fully mitigate potential issues.

This privacy and security guide will help you install, configure, operate and maintain your devices safely and securely and in compliance with your data protection regulations.

Although we aim to provide all important aspects in this guide, some necessary information might be omitted.

About this guide

As a manufacturer of medical devices, we design, implement and verify our products within the context of cybersecurity. To take advantage of these security features, it is important that our products are installed, configured and maintained securely at your site. This guide is intended for the people that are responsible for ensuring secure operation of their QIAGEN device. We also aim to provide all security information necessary for selecting and purchasing the medical device.

In particular, this guide will help you ensure the following:

- Confidentiality of users of the system and patient data
- Integrity of the product and produced data
- Availability of the intended functionality

The following are required to ensure secure operation:

- Control of user access to the system
- Information about data in transfer and at rest
- Backup and recovery capabilities
- Responsibility disclosure for users of the system and service personnel

Contacting us regarding product security

If you require any additional information or would like to report any security or privacy issues in conjunction with our products, please contact QIAGEN Technical Support. You can find contact information at www.qiagen.com/service-and-support/contact/technical-support/.

▷

Purpose of this document

This security and privacy guide presents the technical aspects that are relevant for IT security and data privacy of the Rotor-Gene AssayManager® (RGAM) system consisting of the Rotor-Gene® Q MDx cycler used with the RGAM 2.1 software. This information is intended to support secure installation, configuration, maintenance and operation. This document can also be used by QIAGEN personnel to support the procurement process.

Security program

Security and privacy requirements of the users of the system are important input for our product development. Our security program covers the entire process, including the secure product development lifecycle — from design with security testing to secure integration and operation in the user's environment.

The secure product development lifecycle includes the following:

- Threat assessment and cybersecurity risk management
- Automated code analysis
- Test activities based on the results of these assessments
- System hardening and secure configuration
- Update planning

We are dedicated to continually improving our security efforts.

System information

System overview

The RGAM system consists of the RGAM 2.1 software, a database server and one or more Rotor-Gene Q MDx cyclers. These cyclers are delivered with a QIAGEN notebook. Each instance of the RGAM software can control up to four Rotor-Gene Q MDx cyclers connected to the notebook. Database server software is part of the installation process and can optionally be installed to support any of the setup variants described below.

The RGAM system is designed for the detection and identification of pathogen nucleic acids. The system is only for use in a laboratory environment where proper physical access to the involved systems is ensured.

Within the laboratory environment, samples are prepared and processed using a Rotor-Gene Q MDx cycler, which is controlled by the RGAM software. The gathered data are then analyzed by the software. The software produces analytic results and generates PDF reports about these results.

The system can be set up in a number of ways. A single QIAGEN notebook can connect to up to four cyclers and the database server can be installed locally on the notebook. In network variants, all QIAGEN notebooks and the database server are connected to the same isolated laboratory network.

In these network variants, multiple notebooks (each up to four cyclers per notebook) use the same database server running on a separate PC. The QIAGEN notebooks can also be used without connection to a cycler for run approval and report generation only.

The network in which the RGAM installations operate should be isolated from outside access (e.g., the Internet or other public networks) to reduce the risk of cybersecurity attacks.

Hardware specifications

A computer with the required specifications for operating the Rotor-Gene Q MDx instrument and RGAM v2.1 is supplied as part of the Rotor-Gene Q MDx instrument which is referred to as "QIAGEN notebook" in this document. In general, the minimum requirements defined in the *Rotor-Gene AssayManager Core Application User Manual* must be fulfilled to run RGAM.

Network diagram

Network diagram of the solution

Figures 1 and 2 show an overview of the RGAM communication network. They contain the following common components:

- QIAGEN notebook with Windows® operating system
- RGAM software running on the notebook
- Rotor-Gene Q MDx cycler (up to four cyclers can be controlled by one RGAM software); communication uses a RS232 protocol via USB
- Optional: USB drive for temporary data transfer between other systems
- Optional: Handheld bar code reader to read information of assay kits
- Optional: LIMS terminal; information is exchanged only via a USB pen drive

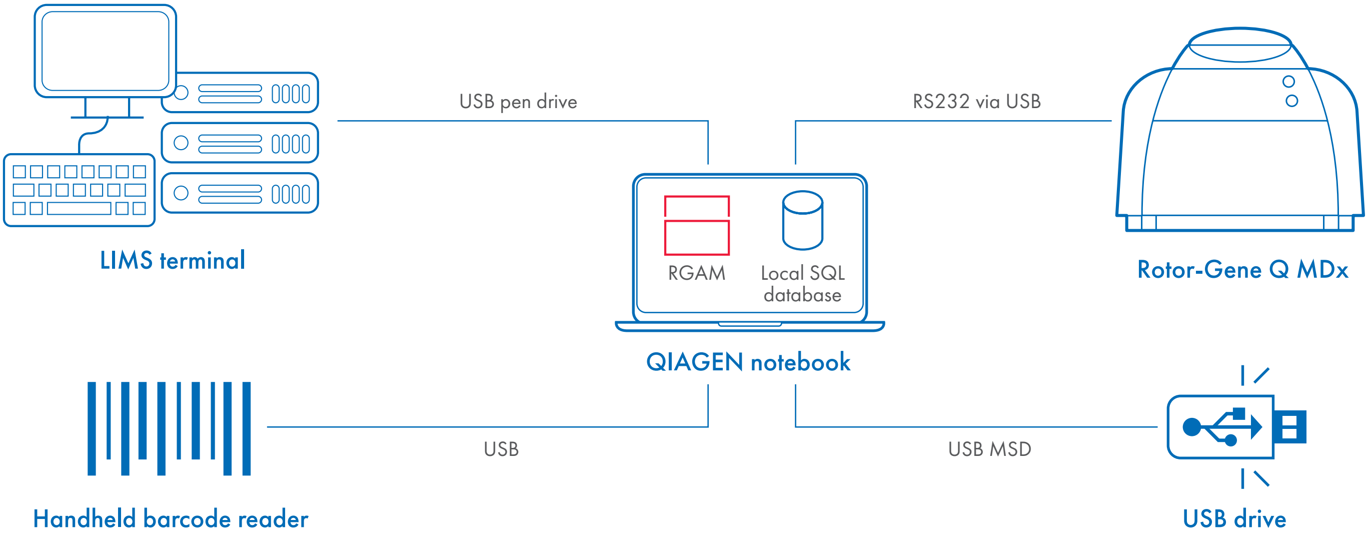

Figure 1. General network diagram of RGAM system with local database.
The specific component depicted is the local SQL Express database running on the notebook (default option).

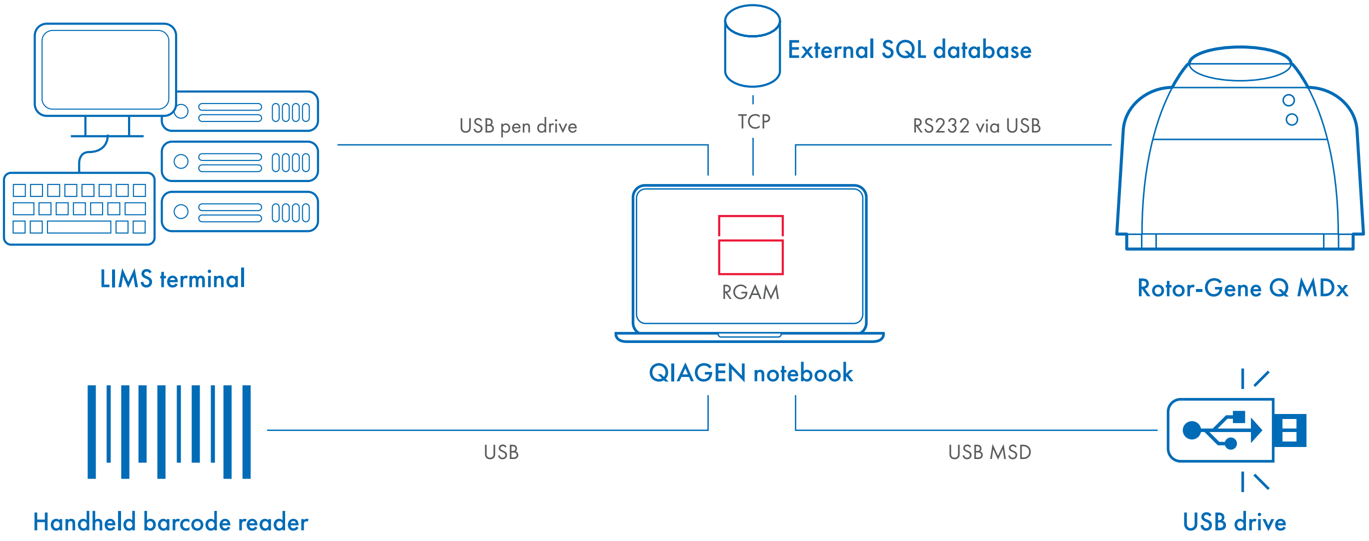

Figure 2. General network diagram of RGAM system with remote database.
The specific component depicted is the external SQL Express database (e.g., in a data center, alternative option). Communication uses the Transmission Control Protocol (TCP).

▷

Network diagram of the solution within the environment where the system is used

The QIAGEN notebook can be connected by ethernet cable to the local area network (LAN).

Wireless connectivity is disabled by default for security reasons. The connected LAN must be isolated to prevent access from outside the laboratory environment.

The following figures depict three possible scenarios for how the RGAM system can be used.

In Scenario 1 (Figure 3) the RGAM system is installed in a controlled laboratory environment where operation is completely isolated from an external network because the database runs on the same notebook as the RGAM software. In this the recommended scenario, no communication to a local or external network is required.

Thus, Scenario 1 has the lowest vulnerability for cybersecurity attacks and is recommended. If sensitive patient data will be entered in the software, Scenario 1 should be the first choice to reduce the attack surface to a minimum.

In Scenario 2, a central database is set up separately (Figure 4). The advantage of this central database scenario is that one database can be hosted externally (e.g., in a secure datacenter) and shared with several RGAM instances simultaneously. Additional QIAGEN

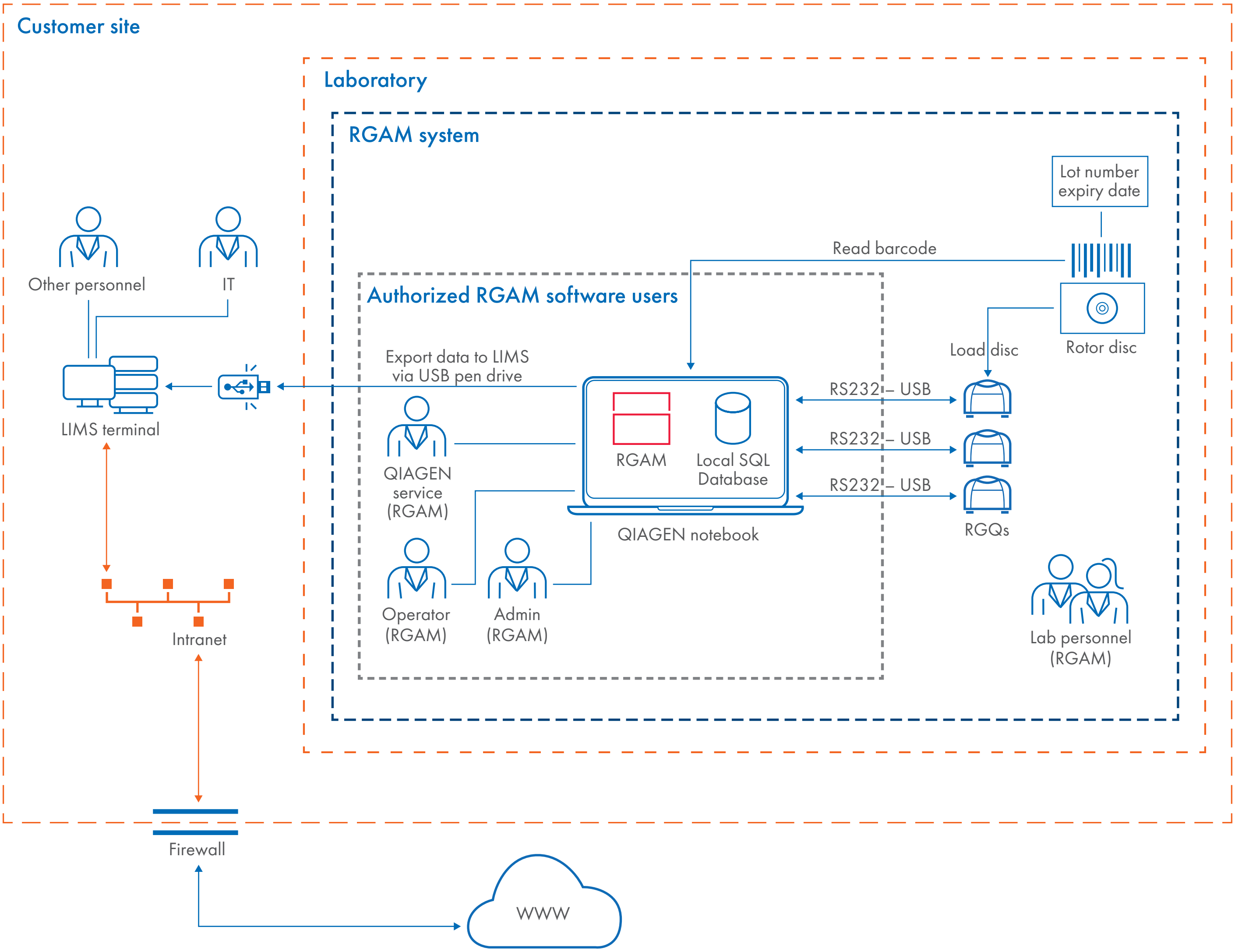

Figure 3. Scenario 1: Local database.

notebook(s) running the RGAM software, but not running the database, can be operated outside the laboratory environment to make some operations, such as approving results, more comfortable for the users of the system. As shown in the diagram, this scenario requires a connection via TCP with the isolated internal network. Therefore, it requires special attention for securing the environment and preventing cybersecurity attacks to the database. A connection to the Internet is not required and should be prevented. The external SQL server database will be the only database in this setup (i.e., no database is running on a QIAGEN notebook that runs the RGAM software).

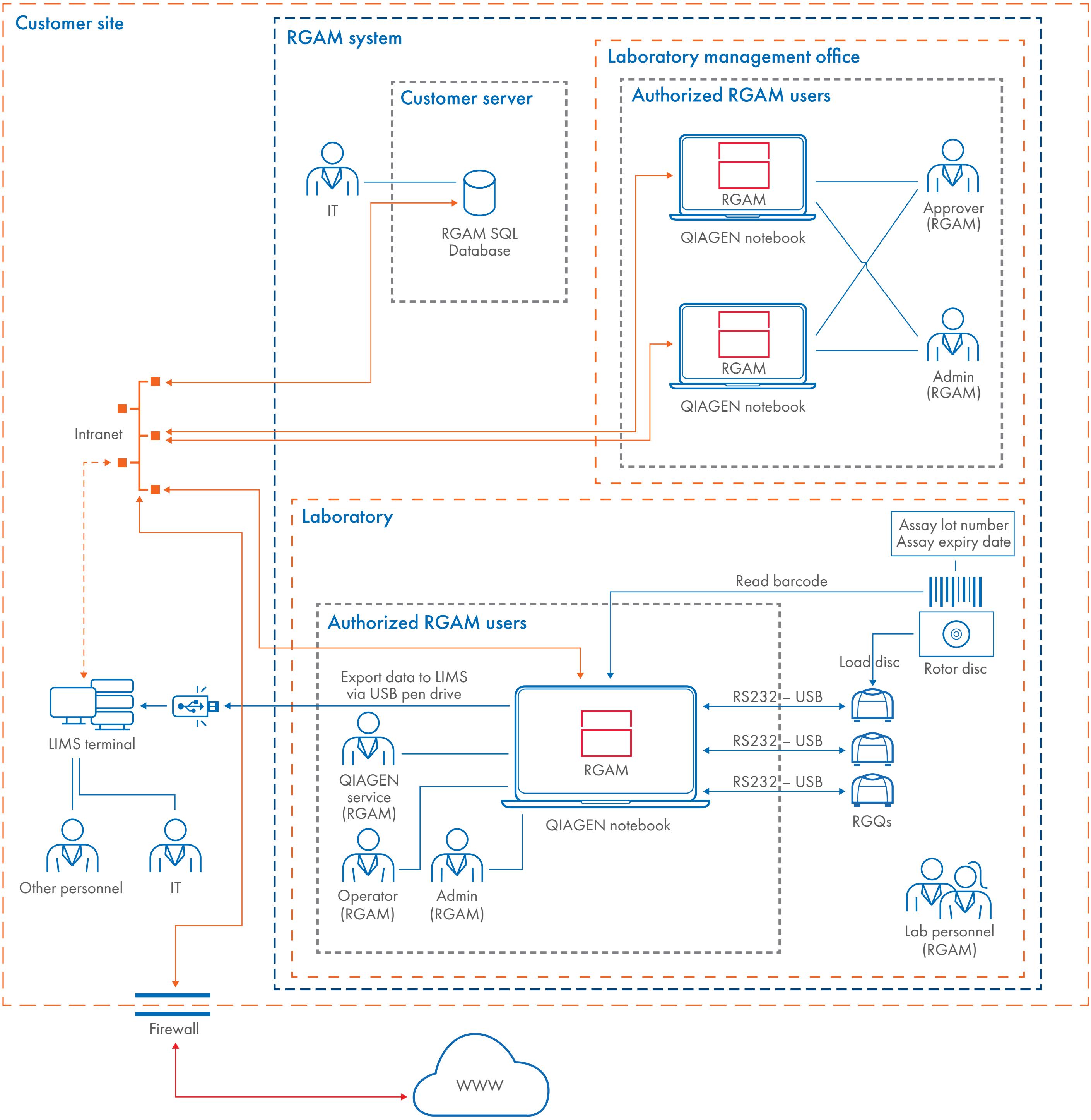

Figure 4. Scenario 2: Distributed database.

Scenario 3 (Figure 5) is a further optional scenario and similar to the central database described in Figure 4. Here, one QIAGEN notebook running the RGAM software hosts the SQL server database and shares it with other RGAM clients over the network. This scenario requires a direct TCP connection, or a TCP connection over the local network to the notebook hosting the database. Special attention for securing the network and preventing cybersecurity attacks is required. Since the database is running on a notebook, special access restrictions to the environment are required (physical access control, etc.) to prevent the notebook from theft or direct manipulation.

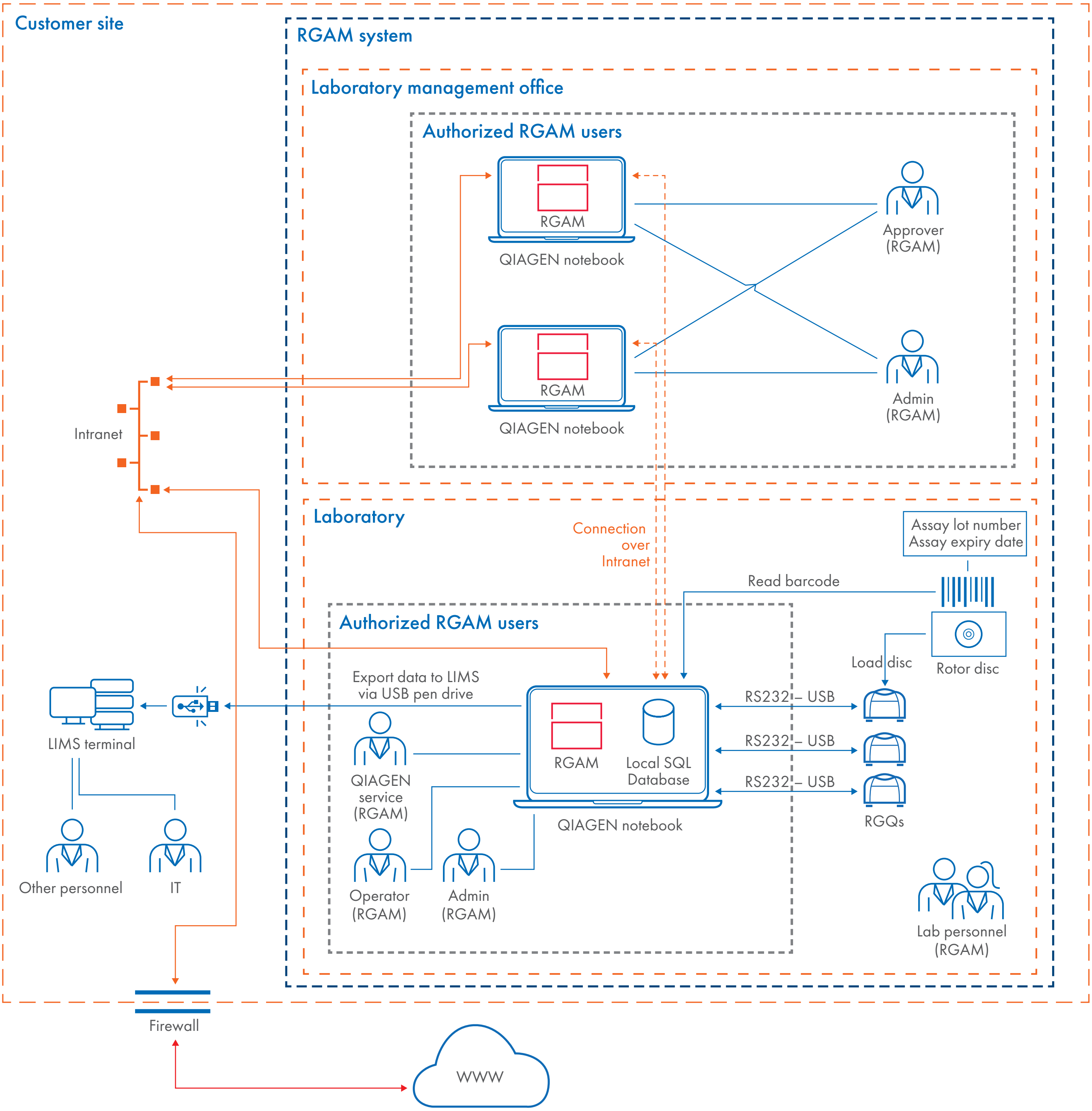

Figure 5. Scenario 3: Remote database on QIAGEN notebook.

Information security model

The RGAM software provides built-in security measures for enabling the following:

- Confidentiality
- Integrity
- Availability

All files are protected either with strong cryptographic hash values or cryptographic signatures or are password protected and encrypted. Upon import, the cryptographic hashes are verified to ensure file integrity. With built-in user management, access can be controlled according to the needs of the users of the system. Role-based privilege management ensures authorization based on privileges that are tailored to the user's responsibility. The RGAM software is supported with a further standalone application providing backup and restore functionality. In the event of a disaster in which the system is rendered inoperable, operation can be resumed in a timely manner by re-installing and restoring backups.

Third-party software

All software components used are part of RGAM installation package or preinstalled on the hardware modules. Table 1 lists the third-party components that are used in RGAM software version 2.1.

Table 1. Third-party components used with RGAM2.1

Component	Vendor	Version
DotNetZip	https://github.com/DinoChiesa/DotNetZip	1.9.1.5
Enterprise Library	http://msdn.microsoft.com/en-us/library/ff632023.aspx	5.0
iTextSharp	https://www.nuget.org/packages/iTextSharp	4.1.7
NHibernate	https://nhibernate.info/	3.1.0
Prism	http://msdn.microsoft.com/en-us/library/ff648611.aspx	2.0.1
Report Viewer	http://www.microsoft.com/download/en/details.aspx?id=6442	10.0
SQL Server 2014 Express	https://www.microsoft.com/en-us/download/details.aspx?id=42299	2014
Stateless	https://www.nuget.org/packages/Stateless/2.5.84	2.5.84
Unity	https://www.nuget.org/packages/Unity/2.1.505.2	2.1
WiX	https://wixtoolset.org/	3.5
XCeed	http://xceed.com/Index.aspx?Lang=EN-CA	4.4.0
USB to UART Bridge VCP Driver	https://www.silabs.com/developers/usb-to-uart-bridge-vcp-drivers	6.5.3 and 6.7.4
.NET Framework	https://www.microsoft.com/en-us/download/details.aspx?id=55170	4.7
Expression Blend SDK for WPF	http://www.microsoft.com/en-us/download/details.aspx?id=10801	2.0
LM-X License Manager	https://www.x-formation.com/	4.7.3
Extreme Optimization Library (math and statistics numerical library)*	http://www.extremeoptimization.com/Default.aspx	4.0
Log4Net	http://logging.apache.org/log4net/index.html	2.0.8
Adobe Acrobat Reader DC	https://www.adobe.com	20.009.20063

Users of the system can request the Software Bill of Materials (SBOM), from QIAGEN Technical Support. The document also includes details of support and anticipated end-of-life of the components.

▷

Connectivity

General network

For security and reliability reasons, cable-based network access instead of Wi-Fi shall be used. The laptop computers provided by QIAGEN have a disabled Wi-Fi adapter. If your configuration is different, a system administrator must disable the Wi-Fi adapter manually.

The QIAGEN notebooks can be connected to the isolated internal network via an ethernet cable. The notebooks are configured to allow DHCP autoconfiguration of their IP addresses. The RGAM software requires the host name or IP address of the database server upon installation. Installation can be completed only with a working database connection (i.e., when the connection to the database can be established).

Other methods of IP configuration must be performed by the IT administrator using the "Admin" account on the notebooks.

There are no minimum requirements regarding the performance or speed for the local network.

Database

RGAM can be set up to use a remote SQL database server. The software installer comes with the option to install Microsoft® SQL Server Express, which can then be used by other QIAGEN notebooks via network connections.

Two ports need to be opened in the Windows Defender firewall on the QIAGEN notebook running Microsoft SQL Server Express.

See Table 2 for connectivity options and associated network ports.

Network sharing

The on-board Windows Shares functionality can be used to exchange data with RGAM. This option must be enabled and configured by the IT administrator. Data exchange between other systems, such as LIMS, is file-based and can be managed using such shared folders and pointing RGAM installations to export files into shared folders. The TCP ports 445 and/or 139 must be allowed through the firewall for this option to work. Ensure that the access to the network is controlled by your IT organization. RGAM cannot control the confidentiality, integrity and availability of the shared folder accessed by third parties.

Table 2. Connectivity options for RGAM

Purpose	Protocol	Port	Authentication
Database communication	TCP/IP	1433	Password
Database communication	UDP/IP	1434	Password
NetBIOS/SMB	TCP/IP	139	Password
SMB 2	TCP/IP	445	Password

Security patching

The users of the system are informed about new security patches and software versions that can be downloaded from a qiagen.com page and installed on the QIAGEN notebook.

If a patch is deemed critical, a letter will be sent to the user of the system via standard QIAGEN processes. Users of the system are asked to sign and return the letter as confirmation that the upgrade has been completed.

QIAGEN Technical Support can help with the identification of the applicable patches and available tools. We continually develop and maintain tools that assist in ensuring a high level of security for RGAM installations.

Patching introduces changes to the software in complex environments and should always be performed with precautionary measures. We strongly recommend performing the following before adding patches to the system:

- Stop the use of the system by all connected installations (i.e., no runs should be performed while updating the database server, the RGAM software or the notebook operating system).
- Back up all data on the system being patched.
- Perform a full test run after patching to make sure the patch succeeded.

Notebook patching

We regularly provide critical operating system patches for QIAGEN notebooks running Windows 10 through the QIAGEN System Updater (QSU) program.

Users of Windows 10 systems can register for the QSU program on the QSU registration page (www.qiagen.com/clp/qiagen-system-updater) to be notified of new patch releases and to download the QIAGEN System Updater with the latest patch list from a QIAGEN web page (see the QIAGEN System Updater page www.qiagen.com/knowledge-and-support/product-and-technical-support/qiagen-system-updater). The QSU software will download the required patches from Microsoft and prepare them for subsequent installation on the user's applicable QIAGEN system(s), such as the QIAGEN notebooks used for RGAM.

Through this channel, only the Windows operating system and its components are kept up to date. Updates for antivirus software installed by a user of the system are the responsibility of the IT administrator.

Note that all installer files downloaded from our web page can be checked for integrity by a user of the system using the cryptographic hash value stated on the web page. This hash value must match the generated hash value from the downloaded file. Execute only installer files for which the hash values match; also see "Modifications to the system", page 18.

Software patching

Updates for the RGAM software are provided as necessary: either with new feature releases or patch releases as a result of the regular cybersecurity monitoring for known vulnerabilities in components contained in and used by the RGAM software.

For new known vulnerabilities, QIAGEN releases patches that contain updated third-party components and other necessary changes to the software. Monitoring for known vulnerabilities is performed every 3 months.

To be pro-actively notified of new software releases, a user of the system registers their products at qiagen.com. When critical patches are available, we inform all users of the system with a customer notification or letter.

We also include security patches for third-party components used by the RGAM software. At the software's end of life, users of the system can use the Software Bill of Materials list to monitor the cybersecurity status of these components themselves.

Database patching

We are aware that the SQL Server 2014 Express database has reached end-of-life support and is in an extended support phase. Additionally, we are aware that after the extended support phase, Microsoft will no longer provide security patches and is, instead, working on a version update. However, since the local network is isolated from the outside and the physical access to the database server is controlled, the attack vector is minimal, and the database can still be used with low risk.

Sensitive data

The software does not process sensitive data and thus does not pseudonymize or anonymize data. As stated in the *Rotor-Gene AssayManager Core Application User Manual*, the user of the system should not enter personally identifiable data as sample IDs.

The data that RGAM processes are stored on the database server, with the exception of files exported by the software and logs. The software maintains a set of configurable paths for import and export of several types of data, such as import folders for assay profiles, export folders for reports, etc.

Locally stored data must be protected by enabling BitLocker on the QIAGEN notebook. This prevents the theft of data even when the hard disk is removed from the notebook.

If a user of the system uses a custom SQL server to host the databases for his RGAM installations, the user has the responsibility of protecting the data stored there.

▷

When decommissioning RGAM systems, the IT administrator must ensure that data on the QIAGEN notebooks as well as the databases on the database server are properly wiped or securely backed up, depending on the data retention requirements in effect. Rotor-Gene Q MDx cyclers do not store data and so can be disposed of directly.

Security controls

Security controls overview

We recommend that you follow your organization's security policies for your local network, as communication with a remote database server or using Windows File Shares is not encrypted by default.

We have implemented the following security controls within the RGAM system:

- Access to QIAGEN notebooks is restricted.
- User accounts are grated permissions based on roles and required privileges.
- Signing or password-protecting exported files is required to prevent unauthorized modification.
- Audit trails and application logs are available for forensic purposes in case of problems.
- Hardening the QIAGEN notebooks against unauthorized access is performed.
- Back up and restore capabilities for disaster recovery are available.

Malware and vulnerability protection

Whitelisting software and antivirus protection

QIAGEN notebooks do not provide their own antivirus solution and the user of the notebook must select, install and maintain a suitable antivirus and malware protection solution. The RGAM software has been validated to work with certain antivirus products. An up-to-date list of validated products is available on the QIAGEN website or via customer support.

It is important to configure the antivirus software so that it does not impact the operation of the software. Certain folders should be excluded from scanning (to prevent false positives), and the system performance should not be impacted in such a way that communication with the cycler(s) can be interrupted (to prevent loss of results).

The Rotor-Gene AssayManager Core Application User Manual describes in more detail how to configure the selected antivirus solution to make it work with the RGAM software.

Updates, configuration and maintenance are performed by the IT administrator. As the RGAM system is not designed to run in an environment with Internet access, the distribution of antivirus updates is realized using USB pen drives or other means of physical transfer.

Additional security applications

We recommend that the user of the system enables the BitLocker hard-drive encryption provided by the Windows operating system.

For assistance with database backups, a separate Database Backup Tool is also available. This tool is described in the *Rotor-Gene AssayManager Core Application User Manual*; see also "Disaster prevention and recovery", page 14.

Network controls

The QIAGEN notebooks come with a firewall configuration that enables only operation with LAN and communication with the database server.

There is no additional software (e.g., network-intrusion detection or security information and event management system) installed to protect the notebooks from network-based attacks. The IT administrator selects and deploys such mechanisms and internal cybersecurity policies for their lab environment.

Incident and vulnerability handling — software updates and security patches

Users of the system are informed when software updates are available. Users can proactively obtain updates from www.qiagen.com or contact QIAGEN Technical Support for further information. Also see "Security patching" on page 8.

If you suspect a security incident has happened or your system is running slow or shows unusual behavior, shut down the system, disconnect it from the network and contact QIAGEN Technical Support.

Remote connectivity

Remote connection to the QIAGEN notebook is optional and only intended from within the system network. In case of a remote database scenario, a TCP connection between the notebook and the database server must be established.

Authentication and authorization

RGAM makes use of Windows operating system accounts (for separating administrative permissions from regular lab use) and RGAM software accounts (for separating permissions for the individual users based on their roles). *The Rotor-Gene AssayManager Core Application User Manual* describes how both kinds of accounts are set up.

For security reasons, we strongly recommend using unique account names and passwords for each user. Account names and passwords must not be shared!

Default operating system accounts

The QIAGEN notebook is pre-configured with the following Windows operating system accounts:

- **Admin**: Administrative account with the ability to manage users and configure the operating system
- **Operator**: Account with limited privileges. Standard account for the most users

An administrator account is set up with the user name "Admin" and the password "Q1a#g3n!A6". For cyber-security reasons this password must be changed as soon as possible by an administrator. This account is intended to be used by the IT administrator for installing and maintaining the notebooks.

The standard "Operator" account is set up with limited privileges and a password that has not been set up. A user of the system is obliged to set an "Operator" password as soon as possible. "Operator" accounts are intended to be used by all non-administrative lab personnel to prevent unauthorized modifications to the system, such as installing or removing software, changing settings, etc.

Default RGAM software accounts

An administrator account for the RGAM software is preconfigured with the name "admin" and a default password "admin". The password must be changed during the first login. Contact QIAGEN Technical Support to recover the "admin" account in the case that the password has been forgotten. Additional user accounts with dedicated roles can be added through the RGAM application user management.

Role-based RGAM access control

User roles have the following privileges:

- **Operator**: Create work lists, execute a work list and view the analysis results
- **Approver**: Access analysis results and approve them
- **Administrator**: Configure the software and manage users
- **AssayDeveloper**: Create a user-defined test (UDT) mode assay
- **SuperUser**: Conveniently grant all permissions to one user
- **Service**: Maintain the software at the system site; does not have permission to approve analysis results

A user of the system can create RGAM accounts and assign the appropriate roles to the users as necessary.

▷

Authentication mechanisms

Windows accounts are local (i.e., not managed by a network-based Windows domain) unless the IT administrator chooses to set them up differently. Users of the QIAGEN notebook must log in to the system before using it. Users who are responsible for maintaining the operating system environment should log in with the "Admin" account. All other users, including RGAM application users, should use the "Operator" account.

After successful initial installation of the RGAM Core Application, version 2.1, on the notebook, user-access control to the application is activated automatically. After first login into the RGAM application with the administration account, we strongly recommend creating at least one user account that is not assigned the "Admin" or the "SuperUser" roles. For security reasons, we do not recommend using the "Admin" or the "SuperUser" roles for anything other than maintenance and administration tasks.

Password rules

We recommend following the rules of your organization's password policies when defining a new password.

The *Rotor-Gene AssayManager Core Application User Manual* describes the password rules and how they can be configured (e.g., renewal interval, enforcing passwords that are compliant with Clinical Laboratory Improvement Amendments (CLIA), etc.).

Generally, the RGAM software allows passwords of 8–40 characters. If using a CLIA-compliant password policy, the following rules must additionally be fulfilled:

- Minimum of two upper case characters
- Minimum of two lower case characters
- Minimum of two numeric characters
- Minimum of two special characters
- Password must not be the same as the user name

Physical protection

A user of the system establishes an appropriate access-control system and provides environmental conditions for physical protection of the RGAM system.

The QIAGEN notebooks as well as the optional database server must be physically accessible by authorized personnel only. This can be realized by isolating the notebooks behind access-control systems that regulate entry into certain areas or rooms (laboratory, datacenter, etc.).

Event and audit logging

The RGAM system provides logging at different levels.

Operating system logging

The Microsoft Windows 10 operating system on QIAGEN notebooks maintains event logs for application, security, setup, system and forwarded events.

Logging capabilities of RGAM

The system log of the RGAM application records general information about the use of the software, such as application starts and shutdowns, logins and logouts, password changes as well as found plug-ins, exceptions, etc.

The log files are organized as a revolving group of files on the internal file system. Data are added to the log files until the maximum size of 10 MB is reached for a file. Subsequently, the oldest file will be deleted automatically. Up to 20 files can exist simultaneously.

During the execution of experiments in the RGAM software, the application creates audit trails which are stored with the experiment data and results in the database.

Database logging

The Microsoft SQL Server Express software maintains a specific error log for the database-server instance in its installation folder. Other events can be recorded in the Windows application log; see "Operating system logging" on page 12.

Forensic logging capabilities

In case that an issue with the application occurs, users of the system can create support packages for QIAGEN Technical Support. The packages are encrypted and password protected *.zip files. These log and support package features provide insights to the use of the application software. Further insights can be gained by considering the operating system event log, see "Operating system logging" above.

Data protection

Protection of data in transit

When the recommended Scenario 1 (see Figure 3) is used and does not encrypt data in transit for remote connections itself, RGAM does not require communication to external systems.

When using a remote connection to the database, communication is not secured by default and requires that the IT administrator configure the database server appropriately.

Protection of data at rest

A user of the system enables Windows BitLocker disk encryption to protect the data stored on the QIAGEN notebooks. This protection can be enabled via Control Panel > System and Security > BitLocker Drive Encryption.

We recommend backing up the recovery keys to be able to recover data in case of hardware damage to the notebook. These must be stored safely outside of the lab environment at a place that is compliant to the applicable security standards.

If the RGAM database is located on a remote computer system, that system should also be protected against data loss by theft as described above. Systems other than QIAGEN notebooks require the use of the appropriate technologies supported by the corresponding systems.

As noted above, RGAM does not store or process personal health information or personally identifiable information and must not be used to do so (e.g., by misusing Sample ID entry).

User passwords are not stored in clear text in the database. For a much better security, cryptographic hash values of the passwords are generated and stored into the database instead.

Protection of exported data

Files that are being exchanged by USB removable media must be protected by using devices that are verified to be malware-free. Physical access to these devices must be controlled by, for example, restricting them to be used and stored only within the laboratory environment where physical access is controlled.

Exported files are either encrypted and password-protected or signed with strong cryptographic hashes to enable detection of tampering. Upon re-import into the RGAM software, these signatures are verified. Files from third-party systems (e.g., LIMS) have a cryptographic hash value that is not validated in the RGAM software and therefore must be validated manually.

Generated PDF reports are protected by a secret PDF owner password to prevent manipulation.

Database backups must be stored securely by the IT administrator and protected against unauthorized access and manipulation. We recommend that only authorized personnel restore such backups; refer to "Disaster recovery" on page 14.

Additional data protection

Greater data protection on removable devices can be achieved by, for example, using encrypted USB flash drives providing a keypad for unlocking the drives before use.

▷

Improving data protection on removable devices (Windows 10)

To enhance data protection on removable media, we recommend using encrypted USB flash drives using one of the two options below:

- Use a pre-encrypted USB drive
- Manually encrypt a standard USB drive using BitLocker on Windows 10 by following the steps below:

1. Insert your USB drive into the computer.
2. Open File Explorer, right-click the USB drive and select “Turn on BitLocker”.
3. Choose “Use a password to unlock the drive”.
4. Enter and confirm a secure password (minimum 8 characters).
5. Save your recovery key in a secure location. This is essential in case you forget your password.
6. Choose one of the encryption options: "Encrypt used disk space only (faster)" or "Encrypt entire drive (more secure)".
7. Select the encryption mode: "Compatible mode – recommended for removable drives to ensure broader compatibility".
8. Click "Start Encrypting" to begin the process.

Once encryption is complete, the USB drive will require the correct password to unlock and access the data.

Data handling at end of life of device

At the end of life of the RGAM system, we recommend securely wiping or destroying all media storing related data, such as notebook hard drives, USB flash drives and database server storage.

Rotor-Gene Q MDx cyclers do not require attention for decommissioning, as they do not store any data. All data are stored in the database or on the file system of the notebook(s).

Disaster prevention and recovery

Disaster prevention

RGAM v2.1 provides functionality to save reports and audit trails to the file system, so that the files can be backed up by the user of the system.

In the case that application files are corrupted, the installer of the RGAM v2.1 software provides a repair functionality that attempts to find and replace corrupted files without re-installing the entire software.

To prevent the loss of data, we provide two ways of backing up the RGAM SQL database. The first option is a built-in functionality of the Microsoft SQL Server Management Studio for manual backups. The second option is the RGAM Database Backup Tool, which we developed for automated backup creation of the RGAM SQL database. Both procedures are described in the *Rotor-Gene AssayManager Core Application User Manual*.

We strongly recommend performing backups regularly and saving the resulting backup package to a safe location.

Monitoring

As part of the disaster prevention activities, including the prevention of cybersecurity attacks, we strongly recommend monitoring the infrastructure and systems with, for example, a Security Information and Event Management (SIEM) tool. Additionally, we recommend an intrusion detection system to detect malicious and suspicious activities.

Disaster recovery

As part of disaster recovery, a user of the system implements regular back ups of the RGAM databases. We provide a dedicated tool for performing back ups regularly and automatically. RGAM database backups can also be restored using this tool. The use of this tool is described in the *Rotor-Gene AssayManager Core Application User Manual*.

In case that the user operates a database server solution that is not Microsoft SQL Server (Express), the corresponding back up and restore mechanisms of the solution used should be used.

We also strongly recommend creating system restoration images after the initial configuration of the notebooks are complete. Using such a recovery image and applying the user's own modifications, the notebooks can be restored to authenticated configurations again by authorized users. The images must be stored securely and must be protected from unauthorized access.

Secure configuration

This section describes the ways in which the QIAGEN-supplied notebooks are installed, configured and hardened.

The Rotor-Gene Q MDx cyclers come with notebooks running a QIAGEN-designed system configuration. The final steps of this configuration should be performed by a user of the system. The IT administrator department should ensure they are properly configured for integration into the IT infrastructure and all local cybersecurity policies are applied.

Notebook hardening

The QIAGEN notebooks are configured for increased security at the BIOS, operating system and firewall levels and, after installing the RGAM software, at the RGAM software level.

BIOS settings

Note that the IT administrator configures a strong BIOS password as one of the first steps when setting up the system to prevent manipulations in the BIOS settings.

Table 3 lists the settings that are applied to the BIOS of the notebooks.

Operating system hardening

Table 4 lists the settings that are applied to the Windows operating system of the QIAGEN-supplied notebooks. Firewall-configuration is described in "Windows Defender firewall whitelist configuration for inbound connections", page 17.

Table 3. BIOS settings

Feature	Value
BIOS > Advanced > System Options > Virtualization Technology (VTx)	Enabled
BIOS > Security > Secure Boot Configuration > Secure Boot	Disable (to make this change valid: a reboot is necessary)
BIOS > Advanced > Boot Options > Fast Boot	Disabled
BIOS > Advanced > Boot Options > UEFI Boot Order	Enabled M.2 SSD: Windows Boot Manager USB
BIOS > Advanced > Boot Options > USB Storage Boot	Enabled
BIOS > Advanced > Built-In Device Options > Wireless Network Device (WLAN)	Disabled
BIOS > Advanced > Built-In Device Options > Bluetooth	Disabled
BIOS > Advanced > Boot Options > Network (PXE) Boot	Disabled

▷

Table 4. Operating system settings

Feature	Value
Settings > Personalization > Themes > Lock Screen	Screen saver: (None) "On resume, display logon screen" disabled
Settings > Accounts	Account settings "Administrator": Administrator Password protected "Operator": Standard user
Settings > Devices > AutoPlay	Use AutoPlay for all media and devices: Off
Settings > Update & Security > Backup	No backup
Settings > Update & Security > Windows Security > Firewall & network protection	The firewall should be on for all locations and inbound connections should be turned off except the rules listed in "Windows Defender firewall whitelist configuration for inbound connections", see page 17.
Control Panel > All Control Panel Items > Security and Maintenance > Change Security and Maintenance settings	In *Security messages* Virus protection option: disabled Internet security settings: enabled (default) Network firewall: enabled (default) User Account Control: enabled (default) In *Maintenance messages* Windows Backup option: disable Windows Troubleshooting: enabled (default) Automatic Maintenance: enabled (default) Drive status: enabled (default) File History: enabled (default) Storage Spaces: enabled (default) Work Folders: enabled (default)
Edit Group Policy (gpedit.msc) > Computer Configuration > Administrative Templates > Windows Components > Windows Update	Configure Automatic Updates: disabled
Start > Windows Administrative Tools > Defragment and Optimize drives	Scheduled optimization: enabled ("Scheduled optimization is turned ON")
Indexing Options	No "local disk" indexing locations (only Favorites, Internet Explorer History, Start Menu)
Edit Group Policy (gpedit.msc) > Computer Configuration > Administrative Templates > Windows Components > Windows Error Reporting > Consent > Configure Default consent	If it is set to "Not Configured" (default) the behavior is the same as "Always ask before sending data". To set to enable: Below the "Options" set the "Consent level" (combo box) to "Always ask before sending data"
Edit Group Policy (gpedit.msc) > User Configuration > Administrative Templates > Windows Components > Store	Turn off the Store application: Enable
Disable Auto Updates on Acrobat reader Search box: Task scheduler Task Scheduler Library	Adobe Acrobat Update Task: Disable (using right mouse click)
Additionally change registry value: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Adobe\AdobeARM\ Legacy\Reader\{AC76BA86-7AD7-1033- 7B44-AC0F074E4100}	Confirm Mode data is 0x00000000 (0)
Disable Windows Bitdefender Antivirus: Edit Group Policy (gpedit.msc) > Computer Configuration > Administrative Templates > Windows Components > Windows Defender Antivirus	Turn off Windows defender Antivirus: Enabled
Disable a memory compression: Windows PowerShell (Admin)	Disable-MMAgent -mc
File Explorer Options: File Explorer > View > Options	Set Open File Explorer to: This PC Region Privacy Show recently used files in Quick access : unchecked Show frequently used folders in Quick access: unchecked
No drive indexing: File Explorer > Show properties of Local Disk (C:) > General tab	Compress this drive to save disk space: unchecked Allow files on this drive to have contents indexed in addition to file properties: unchecked
Control Panel > All Control Panel Items > Power Options > System Settings	Set When I close the lid to: On battery: Do nothing Plugged in: Do nothing
Ensure FIPS compliance is disabled: start secpol.msc (Local Security Policy App) Local Policies > Security Options > System cryptography	Use FIPS compliant algorithms for encryption, hashing and signing is disabled This setting is disabled by default.

Windows Defender firewall whitelist configuration for inbound connections

The Windows Defender firewall is generally configured to allow outbound connections but block all incoming connections by default. Exceptions to this rule are only made to allow the following:

- The notebook operates in a wired ethernet LAN
- Connections to the remote SQL database for RGAM in distributed installation scenarios, as described in Table 5.

Table 5. Allowed inbound connections

Group	Rule	Protocol	Port	Program
Core Networking	Destination Unreachable (ICMPv6-In)	ICMPv6	Any	System
	Destination Unreachable Fragmentation Needed (ICMPv4-In)	ICMPv4	Any	System
	Dynamic Host Configuration Protocol (DHCP-In)	UDP	68	svchost.exe
	Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)	UDP	546	svchost.exe
	Internet Group Management Protocol (IGMP-In)	IGMP	Any	System
	IPHTTPS (TCP-In)	TCP	IPHTTPS	System
	IPv6 (IPv6-In)	IPv6	Any	System
	Multicast Listener Done (ICMPv6-In)	ICMPv6	Any	System
	Multicast Listener Query (ICMPv6-In)	ICMPv6	Any	System
	Multicast Listener Report (ICMPv6-In)	ICMPv6	Any	System
	Multicast Listener Report v2 (ICMPv6-In)	ICMPv6	Any	System
	Neighbor Discovery Advertisement (ICMPv6-In)	ICMPv6	Any	System
	Neighbor Discovery Solicitation (ICMPv6-In)	ICMPv6	Any	System
	Packet Too Big (ICMPv6-In)	ICMPv6	Any	System
	Parameter Problem (ICMPv6-In)	ICMPv6	Any	System
	Router Advertisement (ICMPv6-In)	ICMPv6	Any	System
	Router Solicitation (ICMPv6-In)	ICMPv6	Any	System
	Teredo (UDP-In)	UDP	Edge Traversal	svchost.exe
	Time Exceeded (ICMPv6-In)	ICMPv6	Any	System
Network Discovery (all Private)	(LLMNR-UDP-In)	UDP	5355	svchost.exe
	(NB-Datagram-In)	UDP	138	System
	NB-Name-In)	UDP	137	System
	(Pub-WSD-In)	UDP	3702	svchost.exe
	(SSDP-In)	UDP	1900	svchost.exe
	(UPnP-In)	TCP	2869	System
	(WSD Events-In)	TCP	5357	System
	(WSD EventsSecure-In)	TCP	5358	System
	(WSD-In)	UDP	3702	svchost.exe
	(WSD-In)	UDP	3702	dashost.exe
Remote Assistance	(DCOM-In)	TCP	135	svchost.exe
	(PNRP-In)	UDP	3540	svchost.exe
	(PNRP-In)	UDP	3540	svchost.exe
	(RA Server TCP-In)	TCP	Any	raserver.exe
	(SSDP TCP-In)	TCP	2869	System
	(SSDP UDP-In)	UDP	1900	svchost.exe
	(TCP-In)	TCP	Any	msra.exe
	(TCP-In)	TCP	Any	msra.exe

▷

Installation and initial configuration

After the appropriate configuration of the BIOS, Windows and firewall settings, the RGAM software can be installed on the QIAGEN notebooks. The installation process depends on the installation scenario (see "Network diagram", page 3) and is described in the *Rotor-Gene AssayManager Core Application User Manual*.

A user of the system also verifies that only the two Windows accounts described in the *Rotor-Gene AssayManager Core Application User Manual* and in "Default operating system accounts", page 11 (i.e., "Admin" and an "Operator" account), are present on the QIAGEN notebooks. The "Admin "account must be protected with a strong password. We strongly recommend also protecting the "Operator" account with a strong password as well.

Before installing the RGAM software on the system, the downloaded installer package should be verified by comparing its cryptographic checksum to the value we provide on the corresponding download page. We also sign installers with a digital signature, which can be verified in the Windows explorer using the "Details" dialogue for an executable file. Such verifications should also be performed for later patch or feature releases of the software and its components as well as for the operating system. Do not continue to run programs if Windows warns that the publisher could not be verified, which is a sign that the executable is missing the digital signature.

We also recommend that booting from USB be disabled in the BIOS once the system preparation has reached a stage that it is not useful for the user. Also, the boot order should be limited to only boot from the built-in hard-drive.

Once the system is prepared, the RGAM software can be installed. *The Rotor-Gene AssayManager Core Application User Manual* describes the required steps.

After the initial setup, a user of the system creates a recovery image of the Windows installation. In case of a system restoration, these steps are then quickly restored as well.

As part of the software installation, a user of the system ensures RGAM user accounts are created, the proper roles are assigned to these accounts and strong passwords are chosen.

We strongly recommend enabling the RGAM software security features described in the *Rotor-Gene AssayManager Core Application User Manual*. The software provides settings, such as auto-lock of user sessions in the software, enforcing CLIA-compliant passwords and password expiry intervals.

Modifications to the system

The user of the system is allowed to adapt the RGAM systems for integration into the local IT environment.

In addition to setting a BIOS password, the default passwords of the Windows "Admin" account and the RGAM user account(s) should be changed to strong alternative passwords (see "Password rules", page 12).

There are a number of recommended modifications to the QIAGEN notebook (drive encryption and malware protection) as it is delivered to improve the system security.

A user chooses and installs an antivirus solution. The officially validated solutions are listed in the *Rotor-Gene AssayManager Core Application User Manual*. Other solutions may need to be validated by the user, especially with respect to interference of the operation of the RGAM software and the Rotor-Gene Q MDx cycler(s) and regarding system performance. Points to be aware of when configuring an antivirus solution on the system are listed in the user manual.

A user of the system also enables a drive encryption solution, such as the Windows-integrated BitLocker software. This measure protects against data leak from stolen devices and hard-drives.

The use of printers may require special printer drivers, which a user of the system also installs and maintains.

Modifying the system will require a user of the system to revalidate the system to make sure it is not impacted (e.g., by performance drops and connection interruptions during cycler operation).

Security best practices

The following best practices should be observed:

- The systems should be used only by authorized and trained personnel.
- The lab and network environment in which the system is used should be secure.
- Disaster prevention by backups, recovery images and regular security updates should be taken seriously.

It is important to regularly check for notifications or register to receive notifications automatically about QIAGEN-approved security updates to the operating system and application software. Ensure that your systems are kept up-to-date with approved patch releases.

A major source of attack is unprotected computer networks. For this reason, wireless connectivity (WLAN, Wi-Fi) is disabled by default. The RGAM system should not be connected to the Internet or be part of wireless networks.

We strongly recommend controlling physical access to the RGAM systems and devices (e.g., by lab access-control devices).

Only use the system for its intended purpose and follow the instructions carefully.

If you encounter functional or security issues, contact QIAGEN Technical Support.

Regulatory compliance and certifications

EU General Data Protection Regulation

This section describes compliance to the European General Data Protection Regulation (GDPR) 2016/679.

GDPR requests two specific principles to be implemented:

- **Privacy by Design**: Data privacy through technology design

The design and implementation of the system should ensure that privacy requirements are met.

- **Privacy by Default**: The configuration of the system ensures privacy out of the box

The system should be configured in such a way that privacy is ensured directly after installation, without having to do anything, in particular, to enable additional security settings.

The following organizational and technical elements have been implemented to achieve GDPR compliance:

- No personal data are stored.
- Sensitive data are access controlled and/or secured with a strong cryptographic hash or encrypted or signed with a digital signature.
- Transferred log files contain only pseudonymization and anonymization data.
- No personal data are transferred to QIAGEN or any third party.
- User access controls allow access to personal data in the application to be controlled.

MDS^2 form

The MDS^2 form is available for the RGAM 2.1.x. Users of the system can request the form from QIAGEN Technical Support.

▷

Legal statement and disclaimer

See the *Rotor-Gene AssayManager Core Application User Manual* for software license agreements and warranty disclaimers.

For up-to-date licensing information or Rotor-Gene Q instrument specific disclaimers, refer to the corresponding Rotor-Gene Q instrument manual.

The Rotor-Gene Q, if used in combination with QIAGEN kits indicated for use with the Rotor-Gene Q instrument, is intended for the applications described in the respective QIAGEN kit handbooks. If the Rotor-Gene Q instrument is used with kits other than QIAGEN kits, it is the user's responsibility to validate the performance of such product combination for any particular application.

For up-to-date licensing information and product-specific disclaimers, see the respective QIAGEN kit handbook or user manual. QIAGEN kit handbooks and user manuals are available at www.qiagen.com or can be requested from QIAGEN Technical Services or your local distributor.