Technical Information

QIAcube® Connect Security and Privacy Guide

Introduction

Organizations operating QIAGEN devices usually have requirements for the safe and secure operation of devices on their premises and the networks that they are connected to, as well as privacy requirements for the data that these devices generate, receive, transmit and store. As only the organization using these devices can assess their requirements, the organization must ensure compliance of the devices. In addition, many organizations must augment the technical measures implemented in the QIAGEN devices with organizational measures, such as regulation of access to export folders and properly securing networks that carry sensitive data.

To help our customers fulfill their privacy and security responsibilities, we provide in this document information about the technical implementation and its limitations as well as details for potential additional mitigation measures that can be taken in the case that 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, there may be necessary information that is not included. If you require any additional information, contact QIAGEN Technical Support (visit **www.qiagen.com/service-and-support/contact/technical-support/**).

About this guide

As a manufacturer of medical devices, QIAGEN designs, implements, and verifies products in 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 offers the necessary information to those persons and organizations who are responsible for ensuring secure operation of the device.

In particular, the following must be ensured:

- Confidentiality of customer and patient data
- Integrity of the product and generated data
- Availability of the intended functionality

The below are requirements for ensuring secure operation:

- The system must allow control of user access.
- Information about data in transfer and at rest must be provided.
- Backup and recovery capabilities must be available.
- Responsibility disclosure for users and service personnel must be available.

This guide also aims to provide all security information necessary for selecting and purchasing the medical device.

Contacting QIAGEN regarding product security

Please report any security or privacy issues in conjunction with our products to 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 of QIAcube Connect Software 2.0.0 that are relevant for IT security and data privacy. 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

Customer security and privacy requirements 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 customer environment.

The secure product development lifecycle contains 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

QIAGEN is dedicated to continually improving our security efforts.

System Information

System overview

QIAcube Connect is designed to perform automated isolation and purification of nucleic acids. The QIAcube Connect system is intended to be used only in combination with QIAGEN kits for applications described in the respective kit handbooks. The QIAcube Connect system is intended for use by professional operators, such as technicians and physicians trained in molecular biology techniques and the operation of the QIAcube Connect System.

The QIAcube Connect is a stand-alone instrument with a touchscreen interface.

Hardware specifications

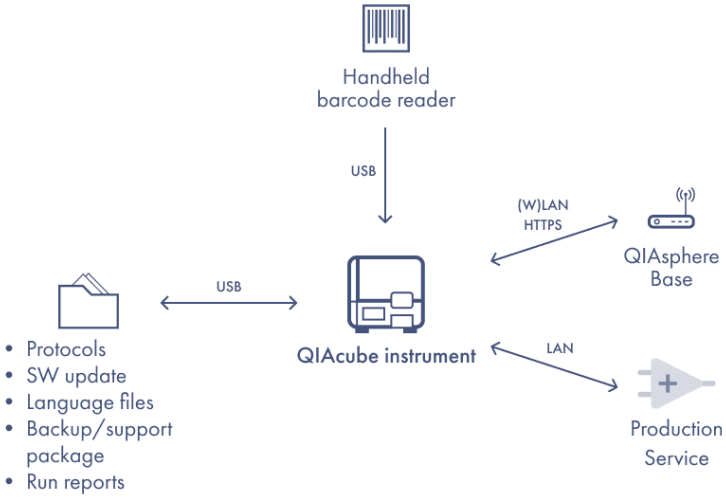
The QIAcube Connect is powered by quad-core ARM® Cortex® A9-based SoC (Freescale i.MX 6) with 1 GB of RAM, 4 GB of eMMC memory, and Cortex-M4 MCU, which does not have external connectivity (only connected to the main SoC).

It includes the following features:

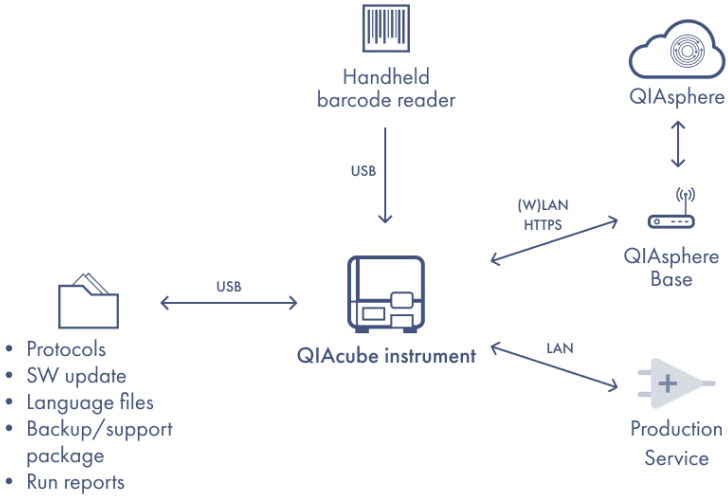
- Touchscreen providing user interface
- 5 USB 2.0 external ports (2 on instrument frame, 3 under touchscreen) for connecting
  - USB drive (for reports download and software updates)
  - Wi-Fi adapter (for wireless connectivity)
  - Handheld barcode reader (optional for some workflows)
  - Keyboard (optional)
- RJ45 ethernet port for network connectivity
- Power supply connector

Network diagram

Network diagram of the solution



Network diagram of the solution in a client environment



Information security model

The QIAcube Connect provides built-in security measures enabling confidentiality, integrity, and availability.

Preventing direct access to underlying OS

Interaction with the instrument is performed using graphical user interface on the instrument's touchscreen. Direct access to the underlying operating system and file system is prevented.

Role-based user management

The QIAcube Connect comes with built-in user management functionality. Users must have at least one role assigned: administrator or operator. Only administrators can manipulate other users' privileges or access system configuration. Service users are granted separate access options.

Audit trail and support packages

Audit trail provides insight to the operations done on the instrument, including pseudo-anonymized operator data. Support package includes logs and events from the device operations and configuration to help the service with troubleshooting. Optionally, audit trails can be transferred to local QIAsphere® Base or QIAsphere cloud.

Software updates and patches

Software update mechanism through USB stick allows QIAGEN to provide bug fixes and security patches. Software update works as separated OS booted from USB stick to allow the system to update even in case of severe issue with existing software version.

Reports

Protocol run reports are created after every protocol run and can be downloaded and backed up. Also, these reports can be transferred to QIAsphere.

Connectivity

The QIAcube Connect does not directly access external networks. However, it can optionally connect to QIAGEN's QIAsphere cloud via QIAsphere Base.

QIAsphere connection allows the user to access the status, run reports or log data of the instrument through local network or cloud service. QIAsphere connection allows the user to receive notifications and protocol update packages.

Operating system

The following table provides information about the configuration of the underlying operating system (OS) or necessary configuration that the customer is required to provide to run the solution.

Table 1. Quick summary of certain aspects of the operating system software.

Aspect	Comments
Operating system information	Custom Linux-based on kernel version 4.19.100 configured and build using buildroot-2020.02.8
Patch level and patch policy	DREAD analysis is used to help identify and classify the possible threats to the device. DREAD analysis includes following categories: • Damage – how bad would an attack be? • Reproducibility – how easy is it to reproduce the attack? • Exploitability – how much work is it to launch the attack? • Affected users – how many people will be impacted? • Discoverability – how easy it is to discover the threat? In addition, the software and its dependencies are scanned against the National Vulnerability Database (NVD, **https://nvd.nist.gov/**). The assessment is using base CVSSv3 score. Any vulnerability with a score of 7.0 or higher is mitigated or further assessed in DREAD model. The vulnerabilities of lower score are considered as acceptable risk. When a new vulnerability of critical or high CVSSv3 score is detected, the software team makes the risk assessment. To mitigate the risks, additional patch release might be scheduled or patch might be applied for the next software release. Every newly identified vulnerability will be reported to **https://nvd.nist.gov/** and all vendors are responsible to release a mitigation (such as patch) accordingly.

Aspect	Comments
Firewall	• Iptables v1.8.3 • All unneeded ports are disabled • HTTPS 443 port is enabled • DNS 53 port is enabled • ICMP ping is enabled • Dedicated port for Service Production tool is opened only when authenticated service user is logged in.
Network configuration	External communication: • Connection to QIAsphere Base is configurable • IPv4 connection is supported LAN: • LAN connection is supported • Static IP configuration with DNS is supported WLAN • IEEE 802.11-2016 standard is supported. This includes: • WIFI 4 (802.11n) • WIFI 5 (802.11a/c) • WPA/WPA2 (802.11i) • WPA3 (SAE)
DHCP requirements	IPv4 via DHCP is supported.
Hardening	• All unneeded accounts are disabled • All unneeded ports are disabled • All unneeded services are disabled (SSH, FTP etc.) • Unneeded applications are disabled • Direct login to the operating system or service access, requires authentication • Software update packages are signed • Unneeded applications are disabled. No access to deploy other application besides QIAcube Connect software • OS access through serial port is password protected
Customer-supplied software	No customer-supplied software can be installed.

Third-party software

All software components used are part of QIAcube Connect installation package or preinstalled on the hardware modules. The following third-party components are used in software version 2.0.0:

Table 2. Third-party components used in QIAcube Connect Software 2.0.0

Component	Vendor	Version	License
Barebox (LS)	Phytec	2016.11.0-phy7	GPLv2
Barebox (MDx)	Phytec	2019.11.0-phy3	GPLv2
Linux Kernel	Linux Software Foundation	4.19.100-custom	GPLv2*
Busybox	Open source	1.35.0	GPLv2
Buildroot	Open source	2020-02.7	GPLv2*
Qt5	Qt Company Ltd.	5.7.0	Commercial
LUA	Open source	5.1	MIT
Libarchive	Open source	3.5.2	New BSD
Cryptopp	Open source	6.1	MIT
LuaBitOp	Open source	1.0.2	MIT
WPA supplicant	Open source	2.9	BSD-3-Clause
ZLib	Open source	1.2.8	FSF Permissive license
FreeRTOS	Open source / Amazon	9.0.0	MIT
TivaWare	Texas Instruments Inc.	2.1.4.178	TivaWare EULA

The QIAcube Connect runs on a custom distribution of a Linux operating system (See Operating system). Customers can request the Software Bill of Materials (SBOM) for the OS from QIAGEN Technical Service.

Connectivity

Table 3. Connectivity options for QIAcube Connect

Purpose	Protocol	Port	Authentication
QIAsphere Base (QIAGEN cloud access)	Hyper Text Transfer Protocol Secure (HTTPS)	443	Server certificate verification and client password
Service Production Tool	TCP/IP	Confidential	Service user login on the instrument required to enable the connection
DNS	DNS	53	–
DHCP	DHCP	67/68	–

QIAsphere Base server authenticity is verified using preinstalled SSL certificate. QIAGEN service is able to update the certificate if needed.

QIAsphere Base connection is optional and disabled by default. To enable the connection user has to provide IP address or host name of the QIAsphere Base and client password.

If the connection to QIAsphere Base is enabled, the instrument sends system status changes, maintenance information changes, new run reports, and audit trails. Only logs (10 minutes interval), heartbeat (1 minute interval), and notification check (1 minute interval) are sent to QIAsphere Base regularly even if the instrument is idling.

Service Production Tool service is disabled if the instrument application is not running in service mode.

Security patching

Patches are provided with standard software update packages (available on QIAGEN website).

Besides standard bug fixes and new features, the patched software may include an operating system and OTS software update (See Third-party software).

Sensitive data

No protected health information (PHI) or personal identifiable information (PII) data is required by the QIAcube Connect. However, the QIAcube Connect provides a way to input any data for:

- sample ID
- run comment
- user ID
- user first name
- user last name
- user e-mail address

The above data in artifacts intended for third-party use (e.g., support package) will be:

- Pseudonymized:
  - User ID
- Removed (except of backup package):
  - User first name
  - User last name
  - User e-mail address
- Used as is:
  - Sample ID
  - Run comment

The original data is locally stored on the instrument. Report, logs, and audit-related data might be sent to QIAsphere base (see Connectivity).

Security Controls

Security controls overview

The instrument is shipped with default administrator account, which is forced to change its default password upon first login. Then it is possible to create additional password protected accounts.

When connected to a local network, QIAcube Connect can communicate with a QIAsphere Base device. The communication is using certificate-based secure HTTPS connection, protected by QIAsphere Base password in addition. The connection is disabled by default.

Malware and vulnerability protection

The QIAcube Connect software comes preinstalled on the instrument. Only complete software updates using software packages provided by QIAGEN are possible. Users do not have access to the underlying OS and cannot install applications.

Network controls

The only open ports are 53 (DNS), 443 (HTTPS) and 67/68 (DHCP)

The only (optional) network application is the connection with QIAsphere Base. The instrument works as a client and only HTTPS connection is allowed.

The dedicated port for Service Production tool is opened only when authenticated service user is logged in.

There is no active listening on any port on the device except for ICMP ping.

Incident and vulnerability handling – software updates and security patches

Security patches are part of the regular system updates. In case of critical vulnerability is detected via vulnerability scan, the impact will be assessed, and additional software release might be scheduled (see Patch level and patch policy for details).

These updates undergo the typical verification and validation process according to our global quality management system. Customers are informed when updates are available. Customers can proactively obtain updates from **www.qiagen.com** or contact QIAGEN Technical Service for further support. If you suspect a cybersecurity incident has occurred, contact QIAGEN technical Support.

Remote connectivity

Remote connectivity services like SSH or Telnet are disabled by default. User has no access to underlying OS to enable it.

Authentication and authorization

Accounts

Based on user roles, there are 3 types of accounts:

- Administrator
- Operator
- Service

Default accounts role-based access control

Administrator can:

- Configure device
- Administrate user accounts (except service accounts)
- Update software
- Update protocol files
- Download data from the instrument
- Perform maintenance activities
- Access system notifications

Operator can:

- Configure network connection
- Execute protocol runs
- Create protocol run shortcuts
- Download data from the instrument
- Manage own account (password change)
- Perform maintenance activities
- Access system notifications

Service user can:

- Configure device
- Execute protocol run
- Access service mode of the application with direct hardware control
- Update software and firmware
- Update protocol files
- Execute custom scripts
- Perform maintenance activities
- Access system notifications

Authentication mechanisms

Users are authenticated by unique logins and passwords. Passwords are encrypted and locally stored. The screen is locked after 10 minutes of inactivity by default. This setting is configurable and can be also disabled completely.

The default administrator account exists, but the user is forced to change its password upon first login. The user is informed about unsuccessful login attempts. Any login attempt (successful or not) is logged in the audit trail.

On MDx instruments, the account might be restricted to Research or IVD mode only. The accounts are locked after 10 unsuccessful attempts by default. This setting is configurable. Locked accounts can be unlocked using one of the following:

- Authenticated administrators can unlock any account.
- Service users can unlock primary administrator account (LS instrument) or any account (MDx instrument).
- One Time Password remote administrator unlock feature.

Password rules

The user must change their password every 60 days by default. This setting is configurable (0-360 days). When password is changed it must be different than 3 previous passwords.

The software supports the standard password policy which defines any arbitrary character with a minimal length of 8 and a maximal length of 40.

Physical protection

The customer shall set up a proper access-control system for physical protection of the QIAcube Connect instrument. Debug information is printed through physically hidden serial port connection. When connecting to the network, the instrument shall be connected to a dedicated local network.

Event/audit logging

Audit trail

The audit trail records general information about the use of the QIAcube Connect instrument. The following events and data are logged:

- Start of the instrument
- Protocol selection
- Parameter change
- Run started/finished/finished with error
- Eluate removal
- UV run maintenance started/finished/finished with error/canceled
- User creation or user data changed
- Successful/unsuccessful user login
- User manual/automatic logout
- Protocol files successful/unsuccessful update
- Protocol files removal
- Audit trail file rollover
- Support package creation
- Backup package creation
- Language files update/removal
- Full disk notification
- Full disk clean-up procedure
- Instrument settings change
- EULA accepted/declined by the user
- OTP challenge generated/access granted/access denied
- Notification created/removed from persistent storage

Software logs

Software logs contain detailed runtime information from the QIAcube Connect application. The logs are organized as a revolving group of files on the internal file system. This covers UI related actions (i.e., tab change or data input) and internal procedures (like sending data to QIAsphere Base, report creation etc.). Data is added to the log files until the maximum size is reached. Subsequently the oldest file will be overwritten after reaching the file count limit.

Event logs

For regular events (temperature check, disc space check, and QIAsphere Base heartbeat) the data are stored in a separate event log.

Data protection

Protection of data in transit

For network communication HTTPS protocol is being used. QIAsphere Base connection is protected additionally by password. For sensitive data information see Sensitive data.

Protection of data at rest

Local storage media cannot be accessed without breaking through enclosure. All passwords are salted and hashed before storing. For sensitive data information, see Sensitive data.

Protection of exported data

Data exported from the instrument is not encrypted except for protocol file data.

Additional data protection

The following files are signed with cryptographic function, which helps to check file integrity and authenticity:

- Audit trails
- User data file
- Maintenance data file
- Run report as xml file

Cloud/hosted solutions

QIAcube Connect can optionally connect to QIAsphere cloud service via QIAsphere Base. The connection is disabled by default and needs to be configured to be turned on. It is possible to configure QIAsphere Base to work without cloud connection.

Data handling at end of life of device

The decommissioning includes removal of all sensitive data including:

- Users' account and settings
- Audit trails
- Reports
- User application logs
- Maintenance history
- Notifications

This can be achieved using built-in “factory reset” functionality.

Note: the factory reset does not remove calibration data, hardware counters and logs from the updater application. The system remains operational after the procedure with the already installed software version.

Disaster Prevention and Recovery

QIAcube Connect allows for download of reports and audit trails so those can be backed up by the user. QIAGEN Technical service is able to restore user data using backup package which can be also proactively downloaded by the user.

When disc space is low, the user is first warned about the need of backing up and freeing device space. If the user continues to use the instrument regardless, the instrument will block protocol run until persistent storage cleanup. The appropriate guide on the screen will be displayed.

Oldest log files will be removed after reaching limit of 10 historical log files. Log, audit, and report files can be exported and backed up using QIAsphere Base connection.

Secure Configuration

Installation and initial configuration

Follow the installation procedure described in QIAcube Connect Software 2.0 User Manual. Appropriate training can be requested for safe and secure operation of the system. It is strongly recommended to use appropriate physical access control.

Modifications to the System

The user does not have access to the underlying OS. Custom modifications are prohibited.

Security best-practices

For safe and secure network operation, the QIAcube Connect instrument shall be integrated into a securely protected network. Do not expose the system to an open network.

Prevent unauthorized physical access to the instrument. Use the system only for intended purposes, according to QIAcube Connect Software 2.0 User Manual. Use only official software and protocol packages provided by QIAGEN.

When facing functional or security issues, contact QIAGEN Technical Service

Regulatory Compliance and Certifications

The General Data Protection Regulation (GDPR) has been released on 04 May 2016 and is applicable since 25 May 2018. The regulation enforces strict data protection rules, which are also applicable for personal health data handled by medical device software.

GDPR requests 2 specific principles to be implemented:

- Privacy by Design
  Data privacy through technology design: the design and implementation of the system shall ensure that privacy requirements are met.
- Privacy by Default
  The configuration of the system ensures privacy out of the box: the system shall be configured in such a way that privacy is ensured directly after installation, without having to do or enable additional security settings.

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

- No personal data is required
- Sensitive data is access controlled and/or stored hashed.
- Transferred log files contain only pseudonymized sensitive data.
- No personal data is transferred to QIAGEN or any third party.
- User access controls allow access to personal data in the application to be controlled.

Attachment: MDS^2 Form

The MDS^2 form is available for QIAcube Connect Software 2.0 on request at QIAGEN Technical Service for QIAcube Connect MDx instrument.

Legal Statement/Disclaimer

See the *QIAcube Connect User Manual* for warranty disclaimers.

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.