

SBOM (software bill of materials)

The SBOM is available for the QIAcuityDx Platform. Customers can request the SBOM in machine-readable format from QIAGEN Technical Services.

Legal statement

See the *QIAcuityDx System User Manual* for software license agreements and warranty disclaimers.

Attachment: MDS² form

The MDS² is available for the QIAcuityDx and can be requested from QIAGEN Technical Services.

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.

Technical Information

QIAcuityDx[®] Platform 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 Services (for contact information, visit www.qiagen.com/service-and-support/contact/technical-support/).

About this guide

As manufacturer of medical devices, we design, implement, and verify our 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 individuals 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 produced 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 transit and at rest must be provided.
- Back-up 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 Services. You can find contact information at www.qiagen.com/service-and-support/contact/technical-support/.



Trademarks: QIAGEN[®], Sample to Insight[®], QIAcuityDx[®] (QIAGEN Group); Linux[®] (Linus Torvald); Ubuntu[®] (Canonical Limited); Windows[®] (Microsoft Corporation). Registered names, trademarks, etc. used in this document, even when not specifically marked as such, are not to be considered unprotected by law.
© 2025 QIAGEN, all rights reserved. PROM-23802-001 QPRO-10529 09/2025

Purpose of this document

This security and privacy guide presents the technical aspects of the QIAcuityDx Platform 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. QIAGEN’s 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:

- Internal and external independent 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

QIAcuityDx Four Instruments supplied by QIAGEN perform digital PCR (dPCR) of externally prepared PCR reactions. These instruments are provided with an embedded computer which runs the QIAcuityDx Control Software System (CSW) to process the nanoplate or a sequence of nanoplates through the instrument according to the requirements.

These instrument capabilities to process the nanoplates require the QIAcuityDx Software Suite (Suite), which allows users to define plates, to order and monitor the process, to analyze the results and to manage the result data.

Both CSW and Suite are parts of the QIAcuityDx Software System. Suite is extendable with QIAcuityDx Software Assay Plugins (SAP), which need to conform to the interface defined by Suite.

QIAcuityDx Software Assay Plugin (SAP) controls the mode of operation (IVD and Utility Mode) and determines the assay specific behaviors unique to each SAP. QIAcuityDx Software Suite sends the data to SAP to be analyzed according to its configuration, to produce reports and to manage the results.

Suite runs in a set of containers that isolates it from the host server, while CSW is embedded in the instrument.

Hardware specifications

Suite must be installed on a conventional notebook. To ensure correct performance, users shall use exclusively the notebook provided by QIAGEN. Suite runs under Windows® 11 LTSC OS. Thus, the notebook provided by QIAGEN uses OS “Win_11_IoT_Enterprise_LTSC_2024_24H2_x64”.

Table 1. Suite requires the following minimum hardware specifications to run

Feature	Value
CPU	Intel® Core™ Ultra 7 165U 1.70GHz
Memory	32 GB
L3 Cache	12 MB
Hard disk	512 GB SSD

CSW operates on the multi-plate instrument with four (4) plate configuration. The hardware configuration of the QIAcuityDx Four Instrument includes:

- A tray with capacity for 4 plates
- A 3 degree-of-freedom arm with a barcode scanner attached
- A priming and rolling unit
- One thermocycler
- An imager sub-system

The operating system designed to be used on the QIAcuityDx Four instrument is Linux® Ubuntu® 18.04.4, or later. The hardware specification of the instrument is:

- 4 GB RAM
- 64 GB SSD
- Processor i3-8100T

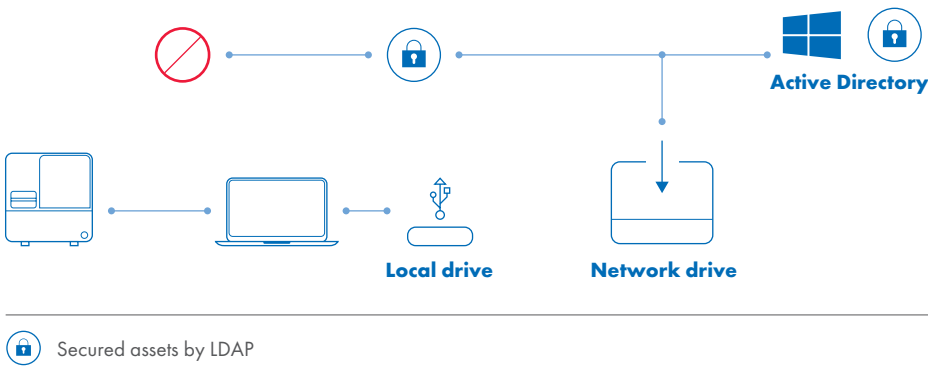
Network diagram

Direct connection (standalone)

This configuration is achieved connecting the instrument with CSW to the laptop with Suite directly with an Ethernet cable.

This scenario has the following characteristics:

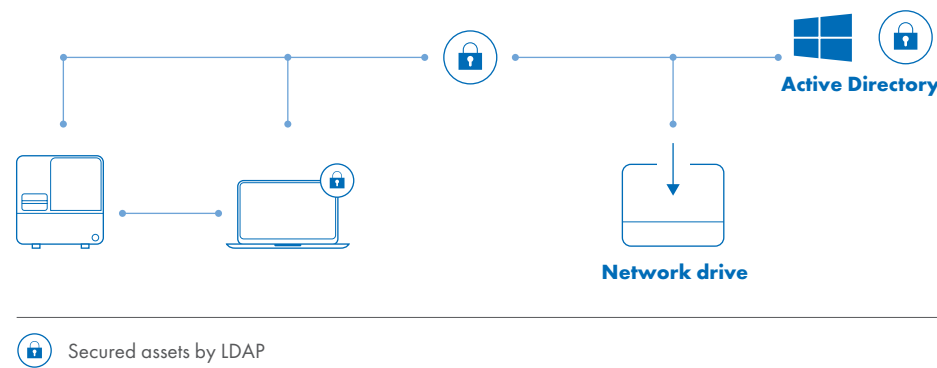
- Direct connection configuration isolated from the other local networks.
- The network connection between the instrument with CSW and the laptop with Suite is set with default IP address as defined in the Instructions for Use.
- The platform cannot be connected to any LIS (Laboratory Information System), LDAP (Lightweight Directory Access Protocol) (e.g., Active Directory) or network drive (a local drive can be used but is not provided by QIAGEN).



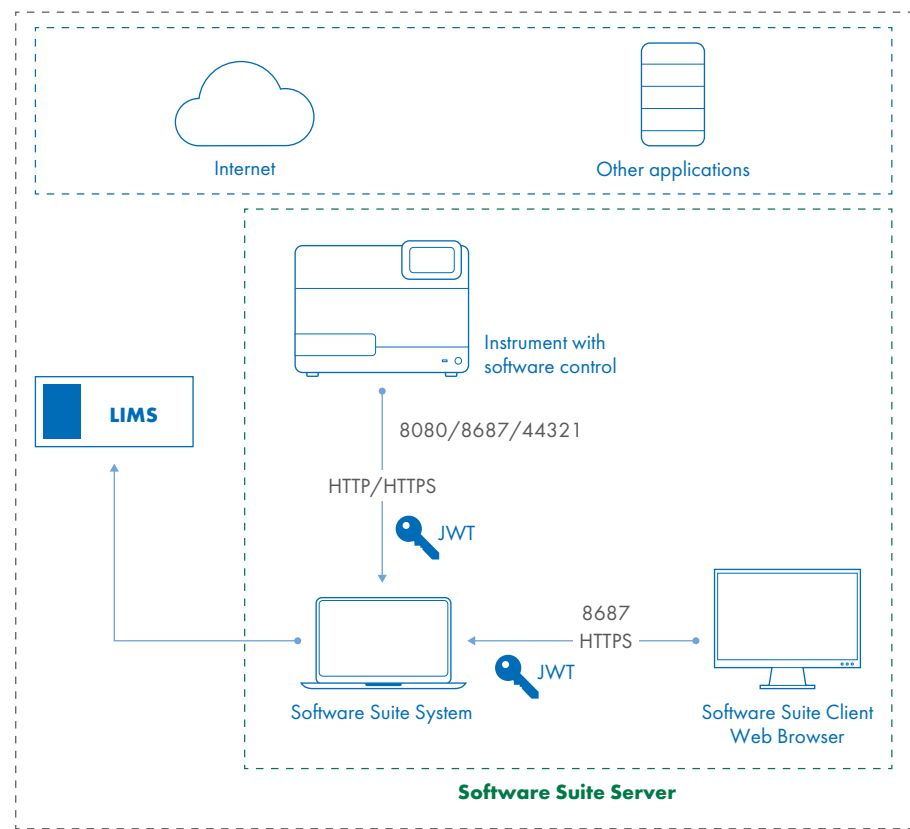
Internal network connection (network integration)

This configuration is achieved by connecting the instrument with CSW to the laptop with Suite through a LAN (Local Area Network). This scenario has the following characteristics:

- The platform is integrated with the other local networks.
- The platform can have local IPs assigned by the customer.
- The platform can be connected to LIS, LDAP and network drives.



Network diagram of the solution

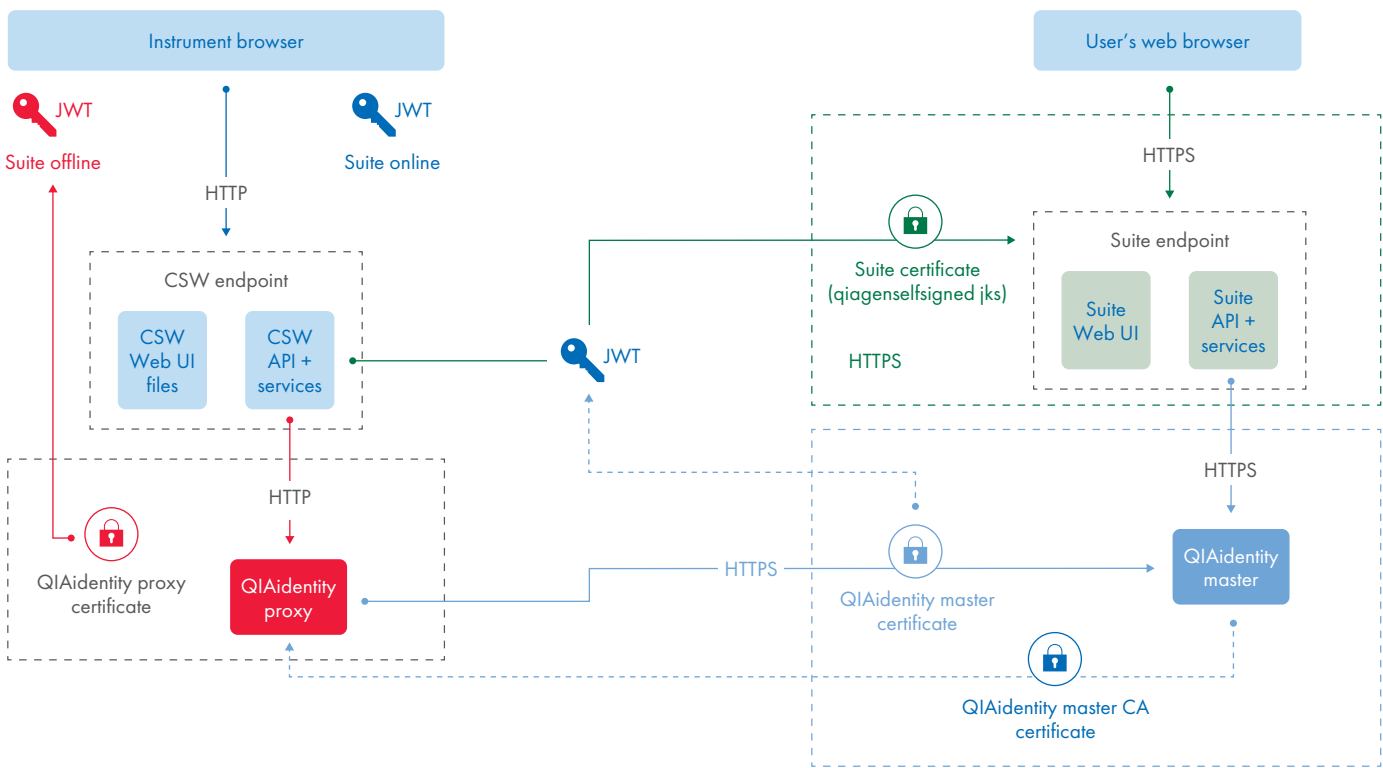


The communication occurs over HTTPS using ports 8687 and 44321, and HTTP using port 8080 for specific purposes:

- Port 8687: Incoming TCP port used to retrieve and send application data of QIAcuityDx System.
- Port 44321: Incoming TCP port used for user management, authentication and authorization.
- Port 8080: Incoming TCP port used by the instrument to time sync.

Network diagram of the solution within the customer environment

QIAcuityDx System, including QIAcuityDx Four platform, Suite, CSW and SAP, operates isolated in its own network with no access to/from internet and external applications (except LIMS (optional)); see "Network diagram of the solution, page 4".



Information security model

CSW and Suite rely on the same authentication provider to ensure consistency between users and profiles available and authorized on each process. The communication happens over HTTPS and the requests need to carry the token received after login. The token lifecycle is managed by the authenticator server.

QIAcuityDx System has a microservice to centralize the audit trail data. It stores in a database the necessary information to provide a clear overview of the executed flows and their parameters collected from Suite and CSW. From this reports can be generated to make the analysis easier.

A support package can be exported from Suite. It provides a zip file (password protected) that contains data related to the plate and updates received from the instrument (e.g., temperature, states) to help with troubleshooting. It does not include any kind of personally identifiable information (PII) or personal health information (PHI).

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 2. Brief summary of some aspects of the operating system software

Aspect	Comments
Operating system information	•Suite: Win_11_IoT_Enterprise_LTSC_2024_24H2_x64 •CSW: Linux Ubuntu 18.04
Patch level and patch policy	•Patch level of the operating system at delivery •Vendor patch policy and interval
Firewall	The following exemptions for inbound traffic are set: •Allow – Incoming:TCP:8687 •Allow – Incoming:TCP:9087 •Allow – Incoming:TCP:8080 •Allow – Incoming:TCP:44321
Network configuration	•IPv4 and IPv6 are supported
DHCP requirement	•In case of direct connection (cable), DHCP must be disabled and a fixed IP needs to be set as instructed in the QIAcuityDx Software Suite Installation Manual
Hardening	•Unneeded accounts disabled: Admin user (local or domain) is required to install the QIAcuityDx Platform. •Unneeded file shares disabled: Any shared file/folder that is not meant to be used should be disabled. •Unneeded ports disabled: The ports 44332, 8080, 8687, and 9087 are required to be open, other than that other ports should be disabled. •Unneeded services disabled: The server is not designed to have any service other than those started during the QIAcuityDx Platform installation. •Unneeded applications disabled: The server should not have any application other than those used/installed on the QIAcuityDx Platform. •Restriction of external (USB) devices: USB devices are allowed to be used for export/import/backup features. They should be cleaned up and scanned in advance against malware. •Authentication of external devices (e.g., USB type-C) Authentication specification: This feature is not supported in the current version.

Windows authentication

There are two possible ways to authenticate.

Direct connection

A default credential for an admin user is set on the laptop provided by QIAGEN and must be changed on the first connection.

Domain

Instrument owners’ IT department needs to configure a domain user with local administrator privileges to be used on the laptop provided by QIAGEN.

Windows updates

Suite runs under Windows 11 LTSC OS, so periodic Windows updates must be planned to keep the cybersecurity risk as low as possible.

For detection of vulnerabilities in Windows, Dependency Track Tool (a vulnerability analysis tool that audits the components used for applications) is used as well. Customers can request the SBOM in machine-readable format from QIAGEN Technical Services.

Suite will not be connected to the internet, and by default, Windows updates will not be configured to be downloaded and installed automatically. QIAGEN monitors the publicly disclosed vulnerabilities of the operating system. The vulnerabilities are assessed in the context of the usage of QIAcuityDx and actions are taken appropriately.

Notwithstanding, it is important that the customer periodically installs the last Windows updates. For that purpose, QIAGEN will send every 6 months (or if a major vulnerability is found) to all customers, the recommended updates that they need to install. Instrument owners will be requested to do a “maintenance stop” on laptops where Suite is installed, as follows:

- Responsible admin user should download the updates onto a separate PC (not the PC with Suite installed), which must have all expected security measures in place (i.e., updated to include last implemented Windows updates/security patches). Updates should be transferred to the USB/pen drive previously scanned to be free of malware by the customer.
- Prior to transferring the updates to the Suite laptop, it is vital that all runs on the instrument have been completed, and the Suite has been closed (**it is important not to install new Windows updates while the instrument is executing a run**) to avoid data loss or unsuccessful “maintenance stop” updates.
- Transfer updates to the Suite laptop with the USB pen drive.
- After the Windows updates have installed, Windows will request a restart. After the restart, Suite can be started again and the user can begin using the application safely once more.

Third-party software

All software components used are part of the QIAcuityDx System installation package or preinstalled on the hardware modules. Customers can request the third-party components list from QIAGEN Technical Services.

Connectivity

The QIAcuityDx System provides an Ethernet connector for optional integration of the system into the customer network to connect to the HIS/LIS. See Table 3, page 7, regarding the transport protocols that can be used.

Table 3. Connectivity options for QIAcuityDx

Purpose	Protocol	Port	Authentication
Hospital information system (HIS) or LIS	Health Level 7 (HL7)	User defined	–

HIS/LIS configuration

The QIAcuityDx System can be connected to a HIS or a LIS. This connection provides functionalities, such as the following:

- Assay configuration for sending results and requesting work orders.
- Running a test based on work order.
- Sending the result of a test.
- Activating and configuring communication with the HIS/LIS.

HIS/LIS connectivity is disabled by default but can be enabled or disabled as desired. The host address and port are specified in the Suite settings (Configuration > LIMS > Connection). The host address allows both an IPv4 address and a name value of the host.

The transfer protocol is currently compatible with HL7 version 2.x. QIAGEN supports encrypted HIS/LIS connectivity, helping the customer set up an environment between QIAcuityDx and the HIS/LIS system (e.g., IPsec/VPN connection). Contact QIAGEN Technical Services for details regarding the integration options.

Security patching

Security patches are provided when appropriate and are installed by the Field Service Engineer (FSE) using the package downloaded from the QIAGEN portal.

Suite packages are digitally signed, enabling the FSE to verify the integrity and authenticity of the software publisher. Digital signatures allow the FSE to be confident that the software they are installing has not been altered or corrupted since it was published.

Suite also has a cryptographic hash to validate the package. This means that a hash is created when using

the package. When the FSE downloads the package, they generate the hash again and compare it with the original to ensure that they are identical, verifying that there were no changes in the package.

CSW has a certificate added during creation of the package that allows the instrument, which knows the certificate, to verify that the package wasn't compromised.

Sensitive data

QIAcuityDx System handles only data related to the analysis. There is no personally identifiable information (PII) or health personal information (HPI) in the flow either in transit or at rest. The results are sent to LIMS, based on an order number, keeping sensitive data out of the scope of QIAGEN software.

QIAcuityDx System uses sample identifiers (Sample ID). Sample ID is a critical identifier needed to identify each test, which may be used by the manufacturer to investigate reported events, as required by law. For data protection reasons, there is a mechanism implemented so the sample IDs are de-identified (pseudonymized) by using alphanumerical codes, which do not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. This de-identification is performed in data that are user-accessible (e.g., logfiles) but the system keeps track to the original number in the database. For that reason, QIAGEN encourages users to use sample IDs that are already de-identified (pseudonymized) by using alphanumerical codes which do not identify an individual as per the explanation above.

Security controls

Security controls overview

The whole application requires the user to be authenticated, and with a valid session to perform any task. A JWT token (JSON web token) is exchanged between services

and validated in a single provider, QIAidentity, which is a software component integrated into the QIAcuityDx Software (Suite and CSW). As standard the users have the least privilege based on their profile.

Authentication procedure

The authentication is user/password based for users in the lab. In case the user forgets their password, and no administrators are available to change it, they can contact QIAGEN Technical Services to get an OTP (one-time password). This can be used only once to change their account password and to be able to perform the authentication; the OTP code can also be used to log into the instrument to configure the connection to Suite. The FSE uses a time-based one-time password (TOTP).

Malware and vulnerability protection

Whitelisting software and antivirus

QIAcuityDx System relies on Linux Ubuntu 18.04 for CSW and Windows 11 LTSC for Suite. In the Microsoft part, an antivirus can be enabled, keeping Suite in the whitelist to avoid performance issues. For Linux, as it is an internal distribution and there is no direct access to it, and no ways for users to download or install any software, no specific protection is deemed necessary.

Additional security applications

There are no additional security applications, and the backup solution is described in the *QIAcuityDx Software Suite Backup and Restore Internal User Manual*.

Network controls

QIAcuityDx System is meant to run in an isolated network. Only the required ports must be opened in the firewall.

The firewall is a critical component in protecting the QIAcuityDx System from unauthorized access and potential cyber threats. Changes to

the firewall configuration may compromise the system security.

Incident and vulnerability handling – software updates and security patches

QIAGEN checks the vulnerabilities on a weekly basis. Based on the assessment of the vulnerability, QIAGEN may determine a need for a “hotfix” to immediately resolve and release the defect, or the defect may be scheduled for a subsequent planned release.

The update process for cybersecurity vulnerabilities is exactly the same as any normal update process for QIAcuityDx System.

In case a hotfix is needed, a fix will be implemented, and a software release will be performed following the standard process, and it will be communicated to all registered contacts associated with the system.

For version 1.0, the software update needs to be performed manually by an FSE. As soon as a software release is ready, a QIAGEN FSE will arrange a visit to update the Suite (and Utility Mode SAP if it is needed) (Notebook) and the CSW (Instrument), following the established installation procedure.

For further software versions, starting from v1.1, users with an appropriate access level will gain the option to install patches, since the functionality of updating the software will be added to Suite.

Remote connectivity

QIAGEN offers the QIAGEN Remote Support Solution (QRSS) as a primary remote connectivity for assistance in Suite (Control Software not remote supported yet).

QRSS is our solution for providing secure remote support to our customers for fast response times. The solution is hosted and managed under QIAGEN IT infrastructure. The solution offers a suite of secure support tools, encompassing features, such as chat, screen sharing, file sharing, and remote command shell. The solution enables comprehensive support services, including remote training, assistance,

troubleshooting, configuration support, monitoring and file exchange (software updates and troubleshooting files). Support sessions begin after the customer grants permission locally. All activities are subject to customer approval, ensuring a tailored support experience.

You can allow the solution by whitelisting a single port 443 to a single trusted URL <https://qsupport.qiagen.com> under full encryption TLS v1.2.

QIAGEN recommends using this solution on-demand only. For more details, see the whitepaper “QIAGEN Remote Support Solution Cybersecurity Whitepaper v1.0”. This is available from QIAGEN Technical Services.

Authentication and authorization on QIAcuityDx application

Users of the QIAcuityDx System must authenticate themselves before using the system (see the “User Management” section in the *QIAcuityDx System User Manual*). The user must provide their user ID and password before gaining access to the system.

The use of access control is highly recommended.

Accounts on QIAcuityDx application

An administrator account must be created after the FSE finishes installing Suite, and the administrator’s account password must be changed after the first login. Contact QIAGEN Technical Services to recover the administrator account in case the password has been forgotten. Additional user accounts can be added through user management.

Default accounts role-based access control on QIAcuityDx application

In the table below you can find a description of roles and their privileges, combined with an example of the type of user that it may apply to.

General permissions mode-agnostic

In addition to the User Roles that can be assigned in each mode, there are general permissions that are mode-agnostic and are independent of the roles.

Permission	Privileges
Instrument accesses [Instrument software]	Instrument Maintenance Create Support Package Experiment Schedule Clear Module Error
Plates (Instrument and PC software)	Upload VPF Create Support Package
User Management (PC software)	Read Users and Roles Create and Edit Users and Roles Activate and Deactivate User
System configuration (PC software)	View registered Instruments Manage registered Instruments Manage Archive View Audit Trail Manage Language and Format Manage LIMS Connector Upload Labware file
Plugins (PC software)	Manage Plugins Review Run Result

These permissions can be found under the IVD and Utility Mode in the Permissions screen and include an information box above them. Users with “Create and Edit Users and Roles” permission can manually select general permissions for each user.

IVD Mode permissions

The following permissions are available for IVD Mode users under the different Roles. It is not possible to manually select a single permission independently from the role it belongs to. Roles can be selected during user creation and/or editing.

Permission	Privileges
Log in	Instrument Suite Software
Plates (instrument and PC software)	Create Plate
All plates	Run Experiment Edit Plate Data Edit Analysis Data Read Plate
Owned plates	Edit Plate Data Edit Analysis Data Read Plate
Other permissions	Import Plate Export Plate Set Plate Ownership Create Report for Analysis
Archive (PC software)	Plate Archiving Archive Overview Recover the Plate from Archive

Additional permissions can be added when installing each IVD plugin to enable signing of the plugin’s reports under a new role. Users with the “Create and Edit Users and Roles” permission can assign this new role to users. In IVD Mode it is possible to assign more than one role to each user.

Utility Mode permissions

The following permissions are available for Utility Mode users under the different roles. It is not possible to manually select permissions independently. Roles can be selected during user creation and/or edition.

Permission	Privileges
Log in (instrument and PC software)	Instrument Suite
Plates (instrument and PC software)	Create Plate
All plates	Run Experiment Edit Plate Data Edit Analysis Data Read Plate Delete Plate
Owned plates	Edit Plate Data Edit Analysis Data Read Plate Delete Plate
Other permissions	Export Plate Set Plate Ownership Create Report for Analysis Sign Report Delete Report
Templates (instrument and PC software)	Create template Edit template Read template Delete template
Archive (PC software)	Plate Archiving Archive Overview Recover the Plate from Archive

Authentication mechanisms

Users must identify themselves by logging in with their account ID and personal password to access QIAcuityDx Platform functions. If a password is entered incorrectly ten times, the user account is locked for fifteen minutes before further attempts can be made to log in.

Break-glass concept

This method of granting emergency access to a system when standard access controls are compromised is not supported on the QIAcuityDx Platform. There is no feature to allow bypassing security control in this version without contact with QIAGEN support.

Password rules

The QIAcuityDx Platform allows passwords of 8–100 characters. Only the following characters can be used for passwords, and it is mandatory to have at least one of each:

- 0–9
- a–z
- A–Z
- (-!\$%^&*()_+|~='`{ } \";<>?./#)

User passwords expire after 90 days. After that the user is redirected to the change password page and forced to change it.

Data segregation

Each plugin receives different credentials when created to ensure no other plugin or service will be able to access data directly.

Physical protection

Although QIAGEN has implemented cybersecurity measures to keep the risks of cyberattack under control, it is not feasible to eliminate risk completely, especially if a malicious user gains physical access to the instrument. Thus, Health Providers using the QIAcuityDx Platform should have policies and controls in place to implement appropriate physical access-control measures to the laboratories where the instrument is installed. They should also restrict access to authorized personnel and establish selection, control and training measures to lower the probability that their employees could, intentionally or unintentionally, compromise system security. Specifically, Health Providers should train employees in the importance of physical security and how to recognize potential threats and establish and enforce policies for physical security, including regular audits and inspections. If physical security measures are not in place, there may be a higher likelihood of certain cybersecurity vulnerabilities being exploited. These could include, but are not limited to, unauthorized access to systems, ➤

manipulation of data, or exposure of sensitive information, potentially affecting the accuracy and reliability of results. While these risks don't guarantee issues will occur, applying appropriate physical safeguards helps reduce the chances of such scenarios and supports the overall integrity of the system.

Event/audit logging

The system log records general information about the use of the system, such as the addition or removal of users, assays, logins and logouts.

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 of 60 days. Subsequently, the oldest file will be overwritten. Log files are included in every backup and can be restored at any time.

The logs can be exported in the support package, which is password protected.

The log format applied is the following:

```
%d{yyyy-MM-dd HH:mm:ss} [%thread] %-5level  
%classname - %msg%n
```

Data protection

Protection of data in transit

To ensure the protection of data in transit, all requests are made under HTTPS protocol.

Protection of data at rest

The QIAcuityDx Platform does not use protected health information (PHI) or personally identifiable information (PII) data.

Some databases are not encrypted. We recommend limiting access to the laptop where the QIAcuityDx Platform is located to trusted users only. Data files (archived

plates and backups) in the shared directory are not encrypted. We recommend encrypting disk storage and shared directory storage.

Protection of exported data

Any data exported from the application is encrypted (e.g., support package, archived plate, exported plate, backup).

Additional data protection

For exported reports, a cryptographic hash is generated to detect tampering.

Cloud/hosted solutions

No data are stored outside of the network.

Data handling at end of life (EOL) and end of support (EOS) of device

Post-discontinuation of the instrument, an extended period of software support for a standard 7-year schedule shall be defined. After that, the EOS has been reached, and the support will finish.

At the EOS, the user needs to export all data required for archiving as per local policy and then all data should be erased from the QIAcuityDx Platform.

The QIAcuityDx Platform provides an option to restore the factory default settings. The customer can request an empty database which resets the system when installed using the restore mechanism.

In case the user decides to keep using the application after EOL, no support, updates, or cybersecurity patches will be provided by QIAGEN, although instrument withdrawal is not enforced.

The EOS will occur also when a mandatory version upgrade is delivered. In this case lower versions will not be supported further by QIAGEN.

Disaster prevention and recovery

The QIAcuityDx Platform provides a manual backup and restore functionality. Backups are saved on a USB storage device, or on a configured folder or network folder, and can be restored accordingly. The backup packages are

compressed as zip files and password protected. It is strongly recommended to back up regularly and save the resulting backup package to a safe location.

Secure configuration on QIAcuityDx application

Installation and initial configuration

Follow the installation procedure described in the QIAcuityDx System User Manual. Appropriate training can be requested for safe and secure operation of the QIAcuityDx Platform.

It is strongly recommended to use appropriate physical-access control to the QIAcuityDx Platform.

Modifications to the QIAcuityDx Platform

To modify the initial admin password, please refer to the QIAcuityDx System User Manual.

Security best-practices

For safe and secure operation, the QIAcuityDx Platform can be integrated into a securely protected network.

Do not expose the system to the internet.

Follow the instructions carefully.

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

Regulatory compliance and certifications

EU General Data Protection Regulation

This section describes compliance with 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 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 anything to enable additional security settings.

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

- QIAcuityDx does not use Protected Health Information (PHI) or Personally Identifiable Information (PII)
- Sensitive data are not stored.
 - Pseudonymization and anonymization of personal data are applied at the LIMS level as explained in the "Sensitive Data" section.
- Transferred log files contain only pseudonymized/anonymized data.
 - By default, no personal data are transferred to QIAGEN or any third party.