Technical Information

QIAstat-Dx® Analyzer 2.0 Security and Privacy Guide

Introduction

We understand that organizations like yours have specific requirements for the safe and secure operation of QIAGEN® devices and connected networks on your premises. You must protect the privacy of the data these devices generate, receive, transmit and store. Since each organization knows its own needs best, you must ensure your devices meet your security and privacy goals. In some cases, you may need to go beyond the built-in security and add your own measures, like controlling who can access sensitive data files and keeping sensitive data networks secure.

To help you fulfill your organization's privacy and security responsibilities, here we provide information about the technical implementation of QIAGEN devices. We also discuss limitations and recommend additional mitigation measures you can take to supplement the built-in security and privacy features of our devices.

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 cover the most important topics in this guide, you may need additional information. If you have any questions, contact QIAGEN Technical Support (for contact information, visit **www.qiagen.com/service-and-support/contact/technical-support**).

About this guide

As a 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 persons and organizations (typically Health Providers) 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 transfer 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 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 the QIAstat-Dx Analyzer 2.0 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 inputs 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 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

At QIAGEN, we are dedicated to continually improving our security efforts.

System information

QIAstat-Dx Analyzer 2.0

The QIAstat-Dx Analyzer 2.0, in combination with QIAstat-Dx assay cartridges, uses real-time PCR to detect pathogen nucleic acids in human biological samples. The QIAstat-Dx Analyzer 2.0 and cartridges are designed as a closed system that enables hands-free sample preparation followed by detection and identification of pathogen nucleic acids. Samples are inserted into a QIAstat-Dx assay cartridge that contains all reagents necessary to isolate and amplify nucleic acids from the sample. Detected real-time amplification signals are interpreted by the integrated software and are reported via an intuitive user interface.

The QIAstat-Dx Analyzer 2.0 consists of an Operational Module and one to four Analytical Modules. The Operational Module hosts software that provides connectivity to the Analytical Module and enables user interaction with the QIAstat-Dx Analyzer 2.0. The Analytical Module contains the hardware and software for sample testing and analysis.

The QIAstat-Dx Analyzer 2.0 is intended to operate in a healthcare facility. Its use in the home environment is not allowed since it could be exposed to unexpected cybersecurity risks.

Figure 1
QIAstat-Dx Analyzer 2.0

Hardware specifications

- **The QIAstat-Dx Analyzer 2.0 includes the following elements:**
  - Touchscreen for user interaction with the QIAstat-Dx Analyzer 2.0
  - Barcode reader for identification of samples, patients, users and QIAstat-Dx assay cartridges
  - USB ports for assay and system upgrades, document export and printer connectivity (one port on the front and three on the back)
  - Cartridge entrance port for inserting QIAstat-Dx assay cartridges into the QIAstat-Dx Analyzer 2.0
  - Ethernet connector for network connectivity

The Operational Module embeds an iMX 8M Plus QuadLite, a 64-bit ARM64 CPU with four cores with 1.6 GHz and 2 GB RAM.

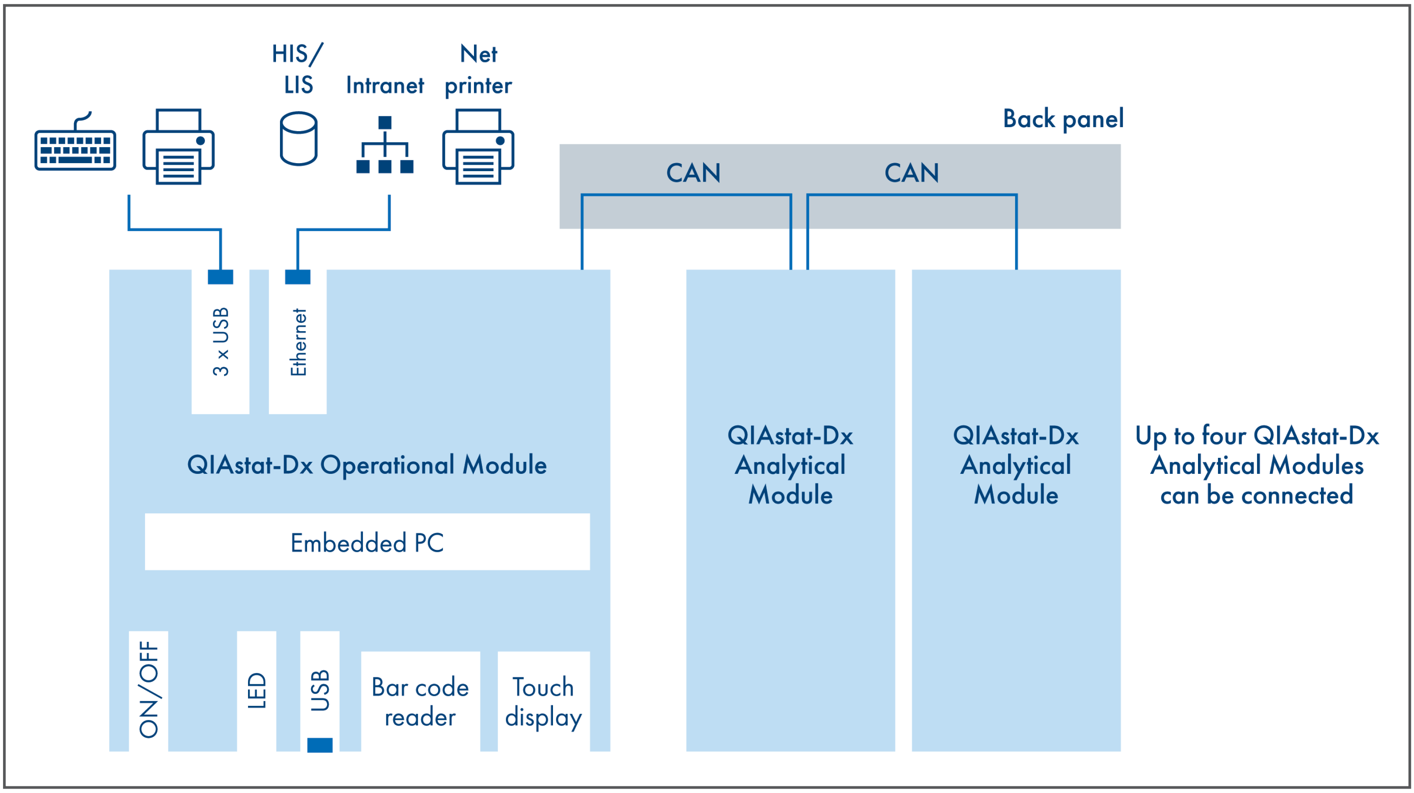
HIS/
LIS
Intranet
Net
printer
Back panel
CAN
CAN
3 x USB
Ethernet
QIAstat-Dx Operational Module
Embedded PC
ON/OFF
LED
USB
Bar code reader
Touch display
QIAstat-Dx Analytical Module
QIAstat-Dx Analytical Module
Up to four QIAstat-Dx Analytical Modules can be connected

Figure 2
Network diagram

Information security model

The QIAstat-Dx Analyzer 2.0 provides built-in security measures for enabling the following:

- Confidentiality
- Integrity
- Availability

With the built-in user management, access can be controlled according to customer needs. Role-based privilege management ensures authorization based on privileges that are tailored to the user's responsibility. The system log and support package features provide insights to the use of the system. The availability of the QIAstat-Dx Analyzer 2.0 is supported with the 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.

Operating system

The following tables and sections provide information about the capabilities or options for the underlying operating system (OS).

The QIAstat-Dx Analyzer 2.0 is an embedded system running in kiosk mode. The QIAstat-Dx Analyzer 2.0 application starts immediately after powering on the instrument. The underlying operating system cannot be accessed directly. Instead, all necessary configurations are exposed using the QIAstat-Dx Analyzer 2.0 application.

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

Aspect	Details
Operating system	Linux
Patch policy	Patches to ensure the continued security of the device are distributed during routine system updates, which are available on **www.qiagen.com**, via over-the-air updates for QIAsphere-connected instruments or from QIAGEN Technical Service.
Network configuration	Network configuration is accomplished with optional IPv4 or IPv6 and DNS is configurable.
DHCP requirements	IPv4 or IPv6 via DHCP is possible
Hardening	Cybersecurity hardening is ensured by the following: • File sharing is not provided by default • No unneeded ports are open • All unneeded services and applications are deleted or disabled • Applications cannot be auto-started from external media • Support of USB-based ethernet devices, WLAN and or Bluetooth is not provided
Customer-supplied software	No customer-supplied software can be installed.

Third-party software

All software components used are part of the QIAstat-Dx application software package or preinstalled on the hardware modules. The following third-party components are used in software version 1.6 of the Operational Module of QIAstat-Dx Analyzer 2.0.

Table 2. Third-party components used in the software, version 1.6, for the Operational Module of the QIAstat-Dx Analyzer 2.0

Component	Vendor	Version	License
A-VIS Asphere	Alphagate Automatisierungstechnik GmbH	v4.0.22	Commercial
	Jaspersoft	v6.16.0	LPGL v3.0
Hibernate	Hibernate.org	v5.4.10	LGPL V2.1
SQLite JDBC	Taro L. Saito	v3.16.1	Apache License 2.0
D-Bus Java	freedesktop.org, Matthew Johnson	v2.7	AFL v2.1 or LGPL v2
Zip4J	Srikanth Reddy Lingala	v2.11.3	Apache License 2.0
Apache Commons	Apache Software Foundation	v3.2	Apache License 2.0
Apache Commons Net	Apache Software Foundation	v3.9.0	Apache License 2.0
Apache commons lang	Apache Software Foundation	v2.1	Apache License 2.0
Apache commons dbpc	Apache Software Foundation	v1.4.0	Apache License 2.0
jSSC (Java Simple Serial Connector)	Alexey Sokolov	v2.8.0	LGPL v3
TimingFramework	Chet Haase	v0.54	BSD, Apache-2.0
Spring Framework (Core, AOP, Aspects, Beans, context, context-indexer, context-support, expressions, jcl, web, jdbc, orm, tx)	Pivotal	v5.3.27	Apache License 2.0
Fscript	Murlen	v1.1	LGPL V2
Jackson (core, annotations, databind, datatype-jsr310)	FasterXML	v2.13.4	Apache License 2.0
AbsoluteLayout (Netbeans) & SwingLayout	Oracle Corporation	v8.0.2	CDDL v1.0
Apache HttpCore	The Apache Software Foundation	v4.4.13	Apache License 2.0
Apache HttpClient	The Apache Software Foundation	v4.5.13	Apache License 2.0
Apache POI	Apache Software Foundation	v5.2.2	Apache License 2.0
Apache POI OOXML	The Apache Software Foundation	v5.2.2	Apache License 2.0
SMBJ	Hieronymus (Jeroen van Erp)	v0.10.0	Apache License 2.0
Liquibase	Liquibase Inc.	v4.9.1	Apache License 2.0
jaxb-api	Oracle Corporation	v2.3.1	CDDL 1.1, GPL2 w/ CPE
OpenJDK	Oracle Corporation	v11.0.13+8	GPL-2.0+ with exception
glibc	GNU Project	v2.34-109	GPL-2.0+ (programs), LGPL-2.1+, BSD-3-Clause, MIT (library)
cups	OpenPrinting	v2.3.3op2	Apache-2.0 with GPL-2.0/LGPL-2.0 exception
xserver_xorg-server	X.Org Foundation	v21.1.2	MIT
busybox	Bruce Perens	v1.35.0	GPL-2.0, bzip2-1.0.4
cups-filters	OpenPrinting	v1.28.10	GPL-2.0, GPL-2.0+, GPL-3.0, GPL-3.0+, LGPL-2, LGPL-2.1+, MIT, BSD-4-Clause
dbus	freedesktop.org	v1.12.22	AFL-2.1 or GPL-2.0+ (library, tools), GPL-2.0+ (tools)

Connectivity

The QIAstat-Dx Analyzer 2.0 provides an ethernet connector for optional integration of the system into the customer network to connect to the HIS/LIS. See Table 1 regarding the transport protocols that can be used.

Table 3. Connectivity options for the QIAstat-Dx Analyzer 2.0

Purpose	Protocol	Port	Authentication
Hospital information system (HIS) or laboratory information system (LIS)	Health Level 7 (HL7)	User-defined	–
Printer configuration	Hyper Text Transfer Protocol (HTTP)	631	Password
Printing	Internet Printing Protocol (IPP/IPPS)	631/443	TLS (IPPS only)
Support	Secure shell (SSH)	22	Password
QIAsphere Base	Hyper Text Transfer Protocol Secure (HTTPS)	443, configurable	Password
Network share	Server Message Block (SMB)	445	Password

HIS/LIS configuration

The QIAstat-Dx Analyzer 2.0 can be connected to a HIS or a LIS. This connection provides functionalities like the following:

- Assay configuration for sending results and requesting work orders
- Running a test based on a 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 settings. 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. The HIS/LIS connection is not encrypted. Contact QIAGEN Technical Service for details regarding the integration options. Also see the *QIAstat-Dx LIS Interface Specification*.

Printer

The QIAstat-Dx Analyzer 2.0 allows the use of networked printers or printers connected to the Operational Module through the USB ports on the back of the instrument. TCP port 631 is used temporarily for the configuration of network printers via a web browser. See the *QIAstat-Dx Analyzer 2.0 User Manual* for further details.

Printer connections can be encrypted for a higher level of security. If using IPP, printer connections are opportunistically encrypted, i.e., automatically upgraded to a TLS-secured IPPS connection, if available. IPPS enforces usage of TLS, like HTTPS.

If connecting printers over an unsecured protocol, ensure that access controls are appropriate for the relevant physical connections or infrastructure (USB cable to printer or the network connection) as well as to the printer itself. See the "Sensitive data" section of the *QIAstat-Dx Analyzer 2.0 User Manual* regarding the sensitivity of printed data.

Secure shell

For rare cases in which QIAGEN Technical Service must perform onsite troubleshooting, SSH access can be activated via ethernet. Using the graphical user interface of the Operational Module, a user with appropriate privileges can activate the SSH through the system settings. Port 22 is used for SSH. To activate SSH, a password that is valid for 24 hours is generated. See also the "Remote connectivity" section for further details.

QIAsphere

The QIAsphere Base is a secure communication gateway to the QIAGEN digital platform, QIAsphere. Users can connect their QIAstat-Dx Analyzer 2.0 to QIAsphere for remote instrument monitoring and other connectivity services. This connection is turned off by default and can be enabled by the customer. The IP address and port are configured by the customer.

QIAsphere provides various software services for the QIAstat-Dx Analyzer 2.0:

- **Basic QIAsphere Connectivity** for proactive remote monitoring of cartridge and instrument performance by QIAGEN Technical Service. Receive updates over the air directly on the instrument. With the QIAsphere App, users can monitor their instrument status and view Test Report PDFs. QIAsphere Insights provides epidemiology statistics and reporting for connected instruments.
- **QIAstat-Dx Remote Result Application** for viewing, commenting and signing the Test Report PDFs remotely
- **QIAstat-Dx Remote Settings** for viewing and maintaining instrument settings of the QIAstat-Dx Analyzer 2.0 and managing user access remotely

QIAsphere Basic Connectivity

When the user decides to connect to QIAsphere, the following information is transferred to the QIAsphere Cloud:

- Information about mechanical parts of QIAstat-Dx Analyzer 2.0
- Software version and configuration information
- Troubleshooting information in the form of log files
- Result data

For QIAsphere Basic Connectivity, the QIAstat-Dx Analyzer 2.0 ensures that, for any information transferred to QIAsphere, this information is de-identified prior to transfer. In detail:

- Usernames, user identifiers and sample identifiers are pseudonymized.
- Patient identifiers are anonymized.

QIAstat-Dx Remote Result Application

QIAstat-Dx Remote Result Application is disabled by default.

When enabling QIAstat-Dx Remote Result Application, the following data is additionally transferred to QIAsphere:

- **Test Report PDF** for viewing, commenting and signing
- **Usernames, sample identifiers and patient identifiers** as accompanying metadata for searching, filtering and sorting of the Test Report PDFs

During set-up of the QIAstat-Dx Remote Result Application, the customer can choose the storage region of the above data (data residency). QIAGEN ensures that data transferred for use with the QIAstat-Dx Remote Result Application is encrypted during transfer and stored only in the region of choice.

QIAstat-Dx Remote Settings

QIAstat-Dx Remote Settings are disabled by default. When enabled, the following data is additionally transferred to QIAsphere:

- Usernames, user identifiers and hashed passwords
- System configuration parameters

All passwords are transferred and stored as cryptographic hash only.

QIAsphere product and solution security

For more security-related information regarding the QIAsphere platform and QIAsphere Base, see the Technical Information document *QIAsphere Product and Solution Security*, available at **qiagen.com** or your QIAGEN sales representative.

Network shares

The QIAstat-Dx Analyzer 2.0 can access shared folders via SMB. Network sharing is used to store or restore backups outside of the system. The connection settings, including the credentials, are specified by the customer. The QIAstat-Dx Analyzer 2.0 itself does not offer remote file access.

The security of this connection relies on proper setup of SMB network sharing on the customer PC.

Security patching

Security patches are provided when appropriate and are installed by the system update mechanism of the QIAstat-Dx Analyzer 2.0.

When connected to QIAsphere, customers will automatically be notified on the QIAstat-Dx Analyzer 2.0 about new security patches for updates over the air.

Sensitive data

The QIAstat-Dx Analyzer 2.0 processes data that may be considered as sensitive information of vulnerable individuals (i.e., patients' health-related data).

We advise that customers do not insert plain identification data (e.g., patients' names and surnames) into input fields. Instead, use pseudonymized (de-identified) alphanumerical data that cannot 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 is to ensure a higher level of security and privacy by default. Notwithstanding the previous consideration, QIAGEN has implemented technical safeguards to protect data that may be considered as sensitive on the QIAstat-Dx Analyzer 2.0:

- Data access can be restricted to authorized users only
- The passwords of the user accounts are hashed, and all other information of user management is encrypted and stored on the system
- Exportable support packages do not contain sensitive data. User IDs and sample IDs are pseudonymized (de-identified) and patient IDs are fully anonymized.

Sensitive data in QIAsphere

By connecting QIAstat-Dx Analyzer 2.0 to QIAsphere, data that may be considered sensitive may be processed in the QIAsphere cloud infrastructure.

If users choose to use QIAsphere Basic Connectivity, sensitive data is pseudonymized (de-identified) on the QIAstat-Dx Analyzer 2.0 before transfer to QIAsphere to provide users with the best experience of the selected services.

If the user chooses to use QIAstat-Dx Remote Results Application or QIAstat-Dx Remote Settings, data that may be considered sensitive is transferred, as captured on the QIAstat-Dx Analyzer 2.0. This may include patient IDs, sample IDs and user IDs.

Any transferred data is securely handled and processed in accordance with best practices. Related security and privacy documentation (i.e., Data Protection Agreement) is shown before the activation of the respective service.

We have implemented numerous technical safeguards, such as data residency, encryption, pseudonymization, minimization of data, authentication and authorization, IT architecture security and application monitoring and auditing. Further, we strive to always improve organizational safeguards to make the QIAsphere platform and QIAsphere-based services compliant with privacy regulations (i.e., GDPR, HIPAA) and compliant to industry best practice.

These organizational and operational measures include all relevant compliance documentation such as impact assessment, risk mitigation planning and record of processing activities (ROPA). We ensure transparency and lawfulness of data processing (e.g., Privacy Policies, Terms of Use, Data Protection Agreements) and enforce privacy rights by implementing policies and procedures for data protection governance and training.

For more information please see the QIAsphere Terms of Use and the related Data Processing Agreement.

Security controls

Security recommendations

We recommend that you follow your organization's security policies and IT security controls (e.g., firewall, anti-virus) for your local network, as communication with HIS/LIS is not encrypted (also see the sections "Connectivity" and "HIS/LIS configuration").

To avoid operational issues, the following activities are exempt from the automatic log off that occurs after a defined period during which there are no user interactions:

- System update
- System backup and restore
- Creating, opening and viewing archives from former results

The user must attend system backup and archive creation to avoid unauthorized access.

Malware and vulnerability protection

The QIAstat-Dx Analyzer 2.0 is a closed, Linux-based system. The application runs in kiosk mode. There is no access to the underlying operating system (except by QIAGEN service technicians). Only a limited number of file types can be uploaded, and upload is controlled for authenticated and authorized administrative users through the graphical user interface of the QIAstat-Dx Analyzer 2.0. See "Operating system" for further implemented mitigations. There is no additional malware protection provided.

Incident and vulnerability handling — software updates and security patches

Security patches for the QIAstat-Dx Analyzer 2.0 are part of the regular system update. They contain updates and vulnerability remediation for the application software and the underlying operating system. These updates undergo verification and validation activities according to the QIAGEN global quality management system prior to their release.

Customers are informed when updates are available. In addition, customers can proactively obtain updates from www.qiagen.com or contact QIAGEN Technical Service for further support. When connected to QIAsphere, customers will automatically be notified on the QIAstat-Dx Analyzer 2.0 about new security patches for updates over the air.

If you suspect a cybersecurity incident has occurred that impacts the QIAstat-Dx Analyzer 2.0 or its interoperable environment (e.g., QIAsphere), stop using the device and contact QIAGEN Technical Support immediately (www.qiagen.com/service-and-support/contact/technical-support).

Remote connectivity

This section describes how the remote connections of the QIAstat-Dx Analyzer 2.0 are protected. Remote connection to the QIAstat-Dx Analyzer 2.0 is only intended from within the customer network.

For maintenance or technical support, an SSH connection can be established to the Operational Module of the QIAstat-Dx Analyzer 2.0. This access is limited to QIAGEN field service engineers. For this, the field service engineer requires physical access to the device. To establish an SSH connection, the QIAstat-Dx Analyzer 2.0 automatically creates a random password which expires after 24 hours. No remote access from outside of the customer network is foreseen. See the QIAstat-Dx Analyzer 2.0 User Manual for details regarding configuration.

The Server Message Block (SMB) file share option allows access to remote network resources. The QIAstat-Dx Analyzer 2.0 itself does not offer remote file access.

QIAsphere connectivity is enabled through a QIAsphere Base device. The customer must configure the IP address, port and password for the connection to the QIAsphere Base device. The communication is always initiated by the QIAstat-Dx Analyzer 2.0.

The optional network printer configuration, which is based on the Common Unix Printing System (CUPS), is protected by a customer-specified password.

Authentication and authorization

Users of the QIAstat-Dx Analyzer 2.0 must authenticate themselves before using the system if the multi-user mode is activated (see the “User Management” section of the QIAstat-Dx Analyzer 2.0 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.

User accounts

An administrator account is pre-configured and its password must be changed after the first login. Contact QIAGEN Technical Support to recover the administrator account in case the password has been forgotten. Additional user accounts can be added through user management.

Role-based access control

Table 4 lists the user roles and their privileges.

Table 4. Connectivity options for the QIAstat-Dx Analyzer 2.0

User role	Privileges	Example
Administrator	All	Instrumentation or IT responsibility
Laboratory Supervisor	• Manage user accounts • Introduce new assays to the assay collection • Run assays • View results from all users • Generate support packages	Laboratory head
Advanced User	• Run assays • View detailed results of their own user tests (e.g., amplification plots, etc.) • Generate support packages	Microbiologist, laboratory technician
Basic User	• Run assays • View non-detailed results of their own user tests (e.g., positive/negative results) • Generate support packages	Healthcare provider (e.g., nurse, doctor, general practitioner)

Authentication mechanisms

After successful initial installation of the QIAstat-Dx Analyzer 2.0, User Access Control is activated automatically. At first login, it is strongly recommended to create at least one user account that is not assigned the “Administrator” role.

User Access Control can be enabled and disabled.

When User Access Control is enabled, users must identify themselves by logging in with their account ID and personal password to access QIAstat-Dx Analyzer 2.0 functions. If a password is entered incorrectly three times, the system is locked for one minute before the user can attempt logging in again.

Password rules

We recommend to follow the rules of your organization’s password policy when defining a new password. The QIAstat-Dx Analyzer 2.0 allows passwords of 6–15 characters.

Only the following characters can be used for passwords:

- 0–9
- a–z
- A–Z
- _ [ ] ; ‘ \ , . / - = ~ ! @ # ( ) + { } : “ | < > ?
- (space), but not leading or trailing

User passwords do not expire and should be changed according to the customer's security policies. Passwords of at least eight characters are recommended.

Physical protection

The customer should establish an appropriate access-control system and provide environmental conditions for physical protection of the QIAstat-Dx Analyzer 2.0. See the QIAstat-Dx Analyzer 2.0 User Manual for required operating conditions.

Event and audit logging

System log

The system log records general information about the use of the Operational and Analytical Modules, such as the addition or removal of users, assays, logins, logouts and starting times of tests. The System Log can be exported by users assigned the Administrator, Lab Supervisor and Service Technician roles.

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 is reached for the file. Subsequently the oldest file will be overwritten. The maximum size of the log files can be configured in the settings, to meet the appropriate retention policies of the Health Provider.

Support package

If support is required, a support package can be created that contains all required run information, as well as system and technical log files. The support package can be saved to a USB storage device and provided to QIAGEN Technical Service.

Data protection

Protection of data in transit

See "HIS/LIS configuration" regarding HIS/LIS data exchange.

The connection to QIAsphere Base is secured by HTTPS transport layer security (TLS).

The connection to network printers can be secured when using IPP and is always secured with TLS if IPPS is used to connect to the printers.

Protection of data at rest

User passwords are cryptographically hashed before storing.

Protection of exported data

Archives

Results from former runs can be archived to a USB storage device or to a network share. The archive files are encrypted using a combination of asymmetric encryption (Rivest–Shamir–Adleman, RSA) and symmetric encryption (Advanced Encryption Standard, AES) to provide fast and secure operation.

Backups

Backup packages are encrypted using a combination of asymmetric encryption (Rivest–Shamir–Adleman, RSA) and symmetric encryption (Advanced Encryption Standard, AES) to provide fast and secure operation.

See also "Disaster prevention and recovery".

Support Package

The content of Support Packages is AES encrypted.

Data handling at device end of life

The QIAstat-Dx Analyzer 2.0 provides an option to restore factory defaults. The customer can request an empty database which resets the system when installed using the restore mechanism.

Disaster prevention and recovery

The QIAstat-Dx Analyzer 2.0 provides manual backup and restore functionality. Backups are saved on a USB storage device or on a configured SMB file share and can be restored accordingly. The backup packages are password protected.

It is strongly recommended to back up regularly and save the resulting backup package to a safe location.

Secure configuration

Installation and initial configuration

Follow the installation procedure described in the QIAstat-Dx Analyzer 2.0 User Manual. Appropriate training can be requested for safe and secure operation of the system.

We strongly recommend using appropriate physical-access control whenever the QIAstat-Dx Analyzer 2.0 is to be used while user management is disabled.

The customer is obliged to change the preset password of the "administrator" account after the first login when user management is enabled.

Modifications to the system

To connect the QIAstat-Dx Analyzer 2.0 to a printer, follow the instructions provided in the QIAstat-Dx Analyzer 2.0 user manual.

Security best practices

For safe and secure operation, the QIAstat-Dx Analyzer 2.0 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 Support.

Regulatory compliance

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, in particular, to enable additional security settings

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

- Sensitive data is access controlled and / or stored hashed or encrypted
- Options for pseudonymization and anonymization of personal data are available for exported data
- Transferred log files contain only pseudonymized / anonymized data
- By default no personal data is transferred to QIAGEN or any third party. Personal data is shared only if users decide to activate QIAsphere Connectivity and QIAsphere-based services (such as Remote Results Application). In this case, the processing of data is regulated by the Data Processing Agreement (DPA) accepted before the service activation, in accordance with art. 28 GDPR. Personal data is processed in accordance with best security practices and standards (art. 32 GDPR).
- User access controls allow access to personal data in the application to be controlled

MDS^2 Form

The MDS2 form is available for the QIAstat-Dx Analyzer 2.0. Customers can request the form from QIAGEN Technical Service.

SBOM (Software Bill of Materials)

The SBOM is available for the QIAstat-Dx Analyzer 2.0. Customers can request the SBOM in machine-readable format from QIAGEN Technical Service.

Legal statement and disclaimer

See the QIAstat-Dx Analyzer 2.0 User Manual for software license agreements and warranty disclaimers.
For up-to-date licensing information and product-specific disclaimers, see the respective QIAGEN kit instructions for use or user manual. QIAGEN instructions for use and user manuals are available at www.qiagen.com or can be requested from QIAGEN Technical Services (or your local distributor).