

Technical Information

# QIAstat-Dx<sup>®</sup>

# Analyzer 1.0 Security and Privacy Guide



## Introduction

Organizations operating QIAGEN<sup>®</sup> 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 (for contact information, visit [www.qiagen.com/service-and-support/contact/technical-support/](http://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 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 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 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/](http://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 1.0 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. 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:

- 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 name

QIAstat-Dx Analyzer 1.0



Figure 1. QIAstat-Dx Analyzer 1.0.

The QIAstat-Dx Analyzer 1.0, in combination with QIAstat-Dx assay cartridges, uses real-time PCR to detect pathogen nucleic acids in human biological samples. The QIAstat-Dx Analyzer 1.0 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 1.0 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 1.0. The Analytical Module contains the hardware and software for sample testing and analysis.

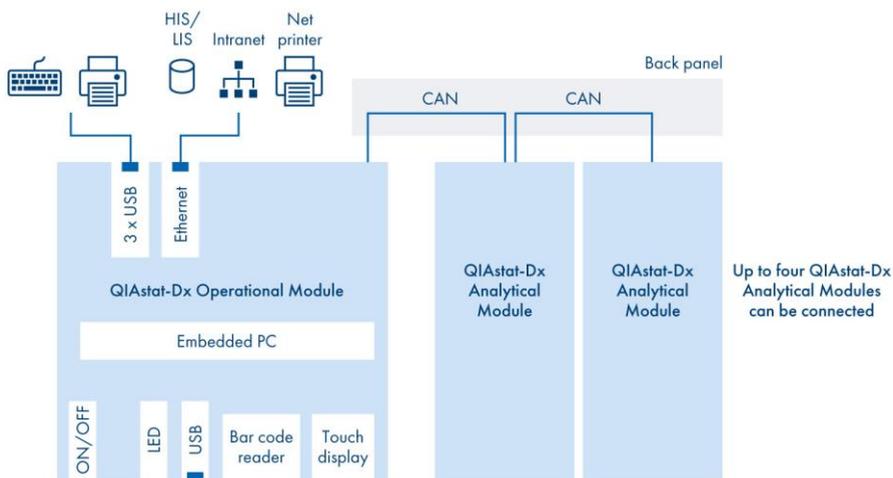


Figure 2. **Network diagram.**

## Hardware specifications

The QIAstat-Dx Analyzer 1.0 includes the following elements:

- Touchscreen for user interaction with the QIAstat-Dx Analyzer 1.0
- Bar code 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 1.0
  - Ethernet connector for network connectivity

The Operational Module embeds an ARM Cortex A8 (TI AM335x), a 32-bit RISC CPU with 720 MHz or faster and up to 1 GHz and 1 GB RAM.

## Information Security Model

The QIAstat-Dx Analyzer 1.0 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 1.0 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 of the underlying operating system (OS).

The QIAstat-Dx Analyzer 1.0 is an embedded system running in kiosk mode. The QIAstat-Dx Analyzer 1.0 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 1.0 application.

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

Aspect	Comments
Operating system	Linux System emlix GmbH.
Patch policy	Patches are distributed during the routine system updates, which are available on <a href="http://www.qiagen.com">www.qiagen.com</a> or from QIAGEN Technical Service.
Network configuration	Network configuration is accomplished with optional IPv4 or IPv6 and is DNS configurable.
DHCP requirements	IPv4 via DHCP is possible
Hardening	Hardening involves the following: <ul style="list-style-type: none"><li>● File sharing is not provided by default.</li><li>● No unneeded ports are open.</li><li>● All unneeded services and application are deleted or disabled.</li><li>● Applications cannot be auto-started from external media.</li><li>● Support of USB-based ethernet devices, WLAN and or Bluetooth is not provided.</li></ul>
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 1.4 of the Operational Module of QIAstat-Dx Analyzer 1.0.

**Table 2. Third-party components used in the software, version 1.4, for the Operational Module of the QIAstat-Dx Analyzer 1.0**

Component	Vendor	Version	License
AbsoluteLayout	Oracle Corporation	V8.0.2	CDDL v1.0
Apache Commons	Apache Software Foundation	Math V3.2, Net V3.3, Lang V2.1, dbcp V1.4.0, pool V1.5.4	Apache License 2.0
Apache HttpClient	The Apache Software Foundation	V4.5.13	Apache License, Version 2.0
Apache HttpCore	The Apache Software Foundation	V4.4.13	Apache License, Version 2.0
Apache POI	The Apache Software Foundation	V4.1.2	Apache License, Version 2.0
Apache POI OOXML	The Apache Software Foundation	V4.1.2	Apache License, Version 2.0
A-VIS Asphere	Alphagate Automatisierungstechnik GmbH	V4.0.22	Commercial
CUPS	Apple Inc.	V2.0.3	Apache License, Version 2.0
D-Bus Java	freedesktop.org, developed by Matthew Johnson	V2.7	AFL v2.1 or LGPL v2
FScript	Developed by Murlen	V1.1	LGPL v2
Hibernate	Hibernate.org	V5.4.26.FINAL	LGPL v2.1
Jackson (core, annotations, databind, datatype-jsr310)	FasterXML	V 2.12.0	Apache License 2.0

Table continued on next page.

Table continued from previous page.

Component	Vendor	Version	License
JasperReports	Jaspersoft	V6.16.0	LGPL v3.0
Java SE Embedded (JRE)	MicroDoc Computersysteme GmbH	Java SE Embedded 8u101 Full JRE Headless for ARMv7-A Little- endian hard-fp	Commercial
jSSC (Java Simple Serial Connector)	Developed by Alexey Sokolov	V2.8.0	LGPL v3
Launch4j	Developed by Grzegorz Kowal	V3.9	Main: 3-Clause BSD License Sub (code that is attached to the wrapped jar): MIT
Linux OS, BSP	System Industrie Electronic GmbH (S.I.E GmbH)	V1.0.0	GPL v2
SMBJ	Hieronymus (Jeroen van Erp)	V0.10.0	Apache License, Version 2.0
SpringFramework (Core, AOP, Aspects, Beans, context, context indexer, context support, expression, jcl, web, jdbc, orm, tx)	Pivotal	V5.2.12.RELEASE	Apache License 2.0
SQLite JDBC	Developed by Taro L. Saito	V3.16.1	Apache License 2.0
TimingFramework	Developed by Chet Haase	V0.54	BSD, Apache-2.0
Zip4J	Developed by Srikanth Reddy Lingala; patched by LRE Medical GmbH	V1.3.2	Apache License 2.0

## Connectivity

The QIAstat-Dx Analyzer 1.0 provides an ethernet connector for optional integration of the system into the customer network. See Table 1, page 7, regarding the transport protocols that can be used.

**Table 3. Connectivity options for the QIAstat-Dx Analyzer 1.0**

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
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 1.0 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 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 1.0 allows 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. See the *QIAstat-Dx Analyzer 1.0 User Manual* and *Printer Setup Guide* for further details.

Printer connections are generally not encrypted. 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 1.0 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 "Remote connectivity", page 16, for further details.

## QIASphere Base

The QIASphere Base is the communication gateway to QIAGEN's digital platform, QIASphere. Users can connect their QIAstat-Dx Analyzer 1.0 to QIASphere for remote monitoring and other connectivity services. This connection can be set up through an internet connection using cloud services, such as push notifications and network

---

independence, to provide full flexibility and maximize the benefits to the connected lab. This connection is turned off by default. The IP address and port are configured by the customer.

In this context following information is transferred to the QIASphere Base.

- Information about mechanical parts of QIAstat-Dx Analyzer 1.0
- Software version and configuration information
- Trouble-shooting information in the form of log files
- Result data

QIAstat-Dx Analyzer 1.0 ensures that, for any information transferred to QIASphere Base, this information is de-identified prior to transfer. In detail:

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

In addition, see Technical Information *QIASphere Product and Solution Security*, available at [qiagen.com](http://qiagen.com), for further security-related information regarding QIASphere and QIASphere Base.

## Network shares

The QIAstat-Dx Analyzer 1.0 can access shared folders via SMB. Network sharing is used to store backups outside of the system. The connection settings, including the credentials, are specified by the customer. The QIAstat-Dx Analyzer 1.0 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 1.0.

## Sensitive data

The QIAstat-Dx Analyzer 1.0 does not process or store protected health information (PHI) or personal identifiable information (PII). We strongly advise customers to not use input fields to insert PHI or PII.

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 and data sent to QIASphere do not contain sensitive data. User IDs are pseudonymized and patient IDs and sample IDs are anonymized.

The test report contains the user ID, patient ID and sample ID.

# Security Controls

## Security recommendations

It is recommended to follow your organization's security policies for your local network, as communication with HIS/LIS is not encrypted (also see "Connectivity" and "HIS/LIS configuration", pages 11 and 11, respectively).

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

User must attend system back up and creation of archive to avoid unauthorized access.

## Malware and vulnerability protection

The QIAstat-Dx Analyzer 1.0 is a closed, Linux-based system. The application runs in kiosk mode. There is no access to the underlying operating system (except by a 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 1.0. See “Operating system”, page 6, for further implemented mitigations. There is no additional malware protection provided.

## Incident and vulnerability handling — software updates and security patches

Patches for the QIAstat-Dx Analyzer 1.0 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 the typical verification and validation process according to QIAGEN's global quality management system.

Customers are informed when updates are available. Customers can proactively obtain updates from [www.qiagen.com](http://www.qiagen.com) or contact QIAGEN Technical Service for further support.

---

If you suspect a cybersecurity incident impacting the QIAstat-Dx Analyzer 1.0 has occurred, contact QIAGEN Technical Support.

## Remote connectivity

This section describes how the remote connections of the QIAstat-Dx Analyzer 1.0 are protected. Remote connection to the QIAstat-Dx Analyzer 1.0 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 1.0. This access is limited to QIAGEN service technicians. For this, the technician requires physical access to the device. To establish an SSH connection, the QIAstat-Dx Analyzer 1.0 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 1.0 User Manual* for details regarding configuration.

The SMB file share option allows the access of remote network resources. The QIAstat-Dx Analyzer 1.0 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 1.0.

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

---

## Authentication and authorization

Users of the QIAstat-Dx Analyzer 1.0 must authenticate themselves before using the system if the multi-user mode is activated (see the “User Management” section the *QIAstat-Dx Analyzer 1.0 User Manual*). The user must provide their user ID and the password before gaining access to the system.

The use of access control is highly recommended.

### User accounts

An administrator account is pre-configured and must be changed after the first login. Contact QIAGEN Technical Support to recover the administrator account in the case that 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. Privileges assigned by user roles**

User role	Privileges	Example
Administrator	All	Instrumentation or IT responsibility
Laboratory Supervisor	<ul style="list-style-type: none"><li>• Manage user accounts</li><li>• Introduce new assays to the assay collection</li><li>• Run assays</li><li>• View results from all users</li><li>• Generate support packages</li></ul>	Laboratory head
Advanced User	<ul style="list-style-type: none"><li>• Run assays</li><li>• View detailed results of their own user tests (e.g., amplification plots, etc.)</li><li>• Generate support packages</li></ul>	Microbiologist, laboratory technician
Basic User	<ul style="list-style-type: none"><li>• Run assays</li><li>• View non-detailed results of their own user tests (e.g., positive/negative results)</li><li>• Generate support packages</li></ul>	Healthcare provider (e.g., nurse, doctor, general practitioner)

## Authentication mechanisms

After successful initial installation of the QIAstat-Dx Analyzer 1.0, 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 1.0 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

It is recommended to follow the rules of your organization's password policies when defining a new password.

---

The QIAstat-Dx Analyzer 1.0 allows passwords of 6–15 characters. Only the following characters can be used for passwords:

- 0–9
- a–z
- A–Z
- \_ (underscore)
- (space)

User passwords do not expire and shall be changed according to the customer's security policies.

## Physical protection

The customer shall establish an appropriate access-control system and provide environmental conditions for physical protection of the QIAstat-Dx Analyzer 1.0. See the *QIAstat-Dx Analyzer 1.0 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.

---

## 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", page 11, regarding HIS/LIS data exchange.

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

The connection to network printers is not secured.

### Protection of data at rest

User passwords are hashed before storing.

### Protection of exported data

## Archives

Results from former runs can be archived to a USB storage device. The archive files are encrypted using the Advanced Encryption Standard (AES).

## Backups

Backup packages are password protected and AES encrypted. See also "Disaster prevention and recovery", page 21.

---

## Data handling at device end of life

The QIAstat-Dx Analyzer 1.0 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 1.0 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 1.0 User Manual*. Appropriate training can be requested for safe and secure operation of the system.

It is strongly recommend to use appropriate physical-access control whenever the QIAstat-Dx Analyzer 1.0 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 1.0 to a printer, download the *Printer Setup Guide* from [www.qiagen.com](http://www.qiagen.com) and configure according to your printer type.

## Security best-practices

For safe and secure operation, the QIAstat-Dx Analyzer 1.0 can be integrated into a securely protected network. Do not expose the system to the internet. Follow the instruction carefully.

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

# Regulatory Compliance

## 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 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:

- No personal data is stored.
- Options for pseudonymization and anonymization of personal data are available for exported data.
- Sensitive data is access controlled and/or stored hashed or encrypted.
- Transferred log files contain only pseudonymization and anonymization 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.

## MDS<sup>2</sup> Form

The MDS<sup>2</sup> form is available for the QIAstat-Dx Analyzer 1.0 . Customer can request the form from QIAGEN Technical Service.

## Legal Statement and Disclaimer

See the *QIAstat-Dx Analyzer 1.0 User Manual* for software license agreements and warranty disclaimers.

---

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

Trademarks: QIAGEN®, Sample to Insight®, QIAstat-Dx® (QIAGEN Group). Registered names, trademarks, etc. used in this document, even when not specifically marked as such, may still be protected by law.

1124534 06/2021 PROM-18114-010 © 2021 QIAGEN, all rights reserved.

---

Ordering [www.qiagen.com/shop](http://www.qiagen.com/shop) | Technical Support [support.qiagen.com](http://support.qiagen.com) | Website [www.qiagen.com](http://www.qiagen.com)