Technical Information

EZ2® Connect Security and Privacy Guide

Introduction

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

To help our customers fulfill their privacy and security responsibilities, we provide in this document information about the technical implementation and its limitations, as well as details for potential additional mitigation measures that can be taken in the case that our technical measures cannot fully mitigate potential issues.

The EZ2 Connect 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 QIAGEN 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 by visiting **support.qiagen.com**

About this guide

As a manufacturer of medical devices, QIAGEN designs, implements, and verifies products in the context of cybersecurity. To take advantage of these security features, it is important that our products are installed, configured, and maintained securely at your site. This guide offers the necessary information to those persons and organizations who are responsible for ensuring secure operation of the device.

In particular, the following must be ensured:

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

The below are requirements for ensuring secure operation:

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

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

Contacting QIAGEN regarding product security

Please report any security or privacy issues in conjunction with our products to QIAGEN Technical Support. You can find contact information at **qiagen.com/service-and-support/contact/technical-support/**

Purpose of this Document

This security and privacy guide presents the technical aspects of EZ2 Connect that are relevant for IT security and data privacy. This information is intended to support secure installation, configuration, maintenance, and operation. This document can also be used by QIAGEN personnel to support the procurement process.

Security Program

Customer security and privacy requirements are important input for our product development. Our security program covers the entire process, including the secure product development lifecycle – from design with security testing to secure integration and operation in the customer environment.

The secure product development lifecycle contains the following:

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

QIAGEN is dedicated to continually improving our security efforts.

System Information

System overview

EZ2 Connect is designed to perform automated isolation and purification of nucleic acids. EZ2 Connect is intended to be used only in combination with QIAGEN kits indicated for use with

the EZ2 Connect instrument for the applications described in the kit handbooks. The EZ2 Connect System is intended for use by professional operators, such as technicians and physicians trained in molecular biological techniques and the operation of the EZ2 Connect System.

The EZ2 Connect is a stand-alone instrument with a touchscreen interface.

Hardware specifications

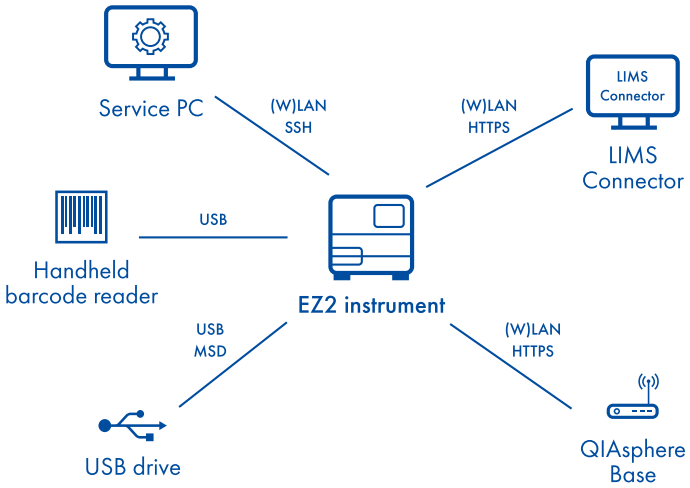
EZ2 Connect is powered by quad-core ARM® Cortex® A9-based SoC (Freescale i.MX 6) with 2 GB of RAM, 4 GB of eMMC memory, and Cortex-M4 MCU which does not have external connectivity (only connected to the main SoC).

It includes the following features:

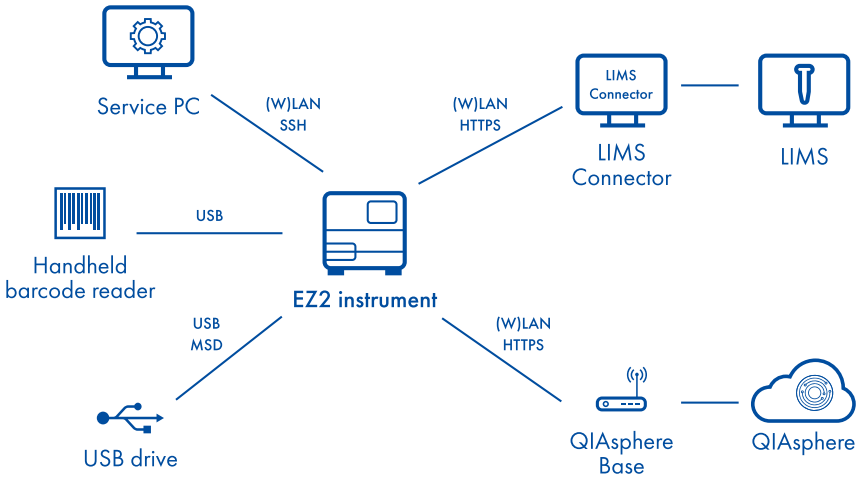
- Touchscreen providing user interface
- 3 USB 2.0 external ports for connecting
  - USB drive (for reports download and software updates)
  - Wi-Fi adapter (for wireless connectivity)
  - Handheld barcode reader (optional for some workflows)
- RJ45 ethernet port for network connectivity

Network diagram

Network diagram of the solution



Network diagram of the solution in a client environment



Information security model

The EZ2 Connect provides built-in security measures enabling confidentiality, integrity, and availability.

Preventing direct access to underlying OS

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

Role-based user management

The EZ2 Connect comes with built-in user management. Users can be added and removed and assigned a role by a user with an admin role. Roles to choose from are predefined and have different levels of privileges.

Audit trail and support packages

Audit trail provides insight to the operation of the instrument for the user and support package containing logs from device operation allows service to troubleshoot problems.

Software updates and patches

Software update mechanism allows QIAGEN to provide security vulnerabilities fixes and software bug fixes. Software update mechanism includes fallbacks in case of update problems which safeguard availability.

Reports

Protocol run reports are created after every protocol run and can be downloaded and backed up. Also, these reports can be transferred to QIAsphere®, where Sample-ID and User-ID data are pseudonymized.

Connectivity

The EZ2 Connect does not directly access external networks. However, it can optionally connect to QIAGEN's QIAsphere cloud via QIAsphere Base device and / or to a customer's LIMS through separately provided LIMS Connector service.

Operating system

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

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

Aspect	Comments
Operating system information	Yocto Project® 3.1 (Dunfell)
Patch level and patch policy	DREAD analysis is used to help identify and classify the possible threats to the device. DREAD analysis includes following categories: • Damage – how bad would an attack be? • Reproducibility – how easy is it to reproduce the attack? • Exploitability – how much work is it to launch the attack? • Affected users – how many people will be impacted? • Discoverability – how easy it is to discover the threat? Any known vulnerabilities found in the device are evaluated with the recommendation from the National Vulnerability Database (NVD). The evaluation criteria are based on the risk factor including: • Base Metrics score from NVD (refer to NVD's CVSSv3.1 Base score if possible. Otherwise, NVD's CVSSv2 will be used) • Temporal Metrics score; the current state of exploit technique or code availability, the existence of any patches or workaround, or the confidence that one has in the description of a vulnerabilities. • Environmental Metrics score; the intended use of the product and the environment in which the product would be used. The combination of the above scoring is used to calculate the final CVSSv3.1 score based on the CVSS specification. Any known vulnerabilities with a final CVSSv3.1 score higher than 7.0 are mitigated. Every identified vulnerabilities will be reported to **nvd.nist.gov/vuln** and all vendors for the Yocto Protect (TI, linux-kernel, etc.) are responsible to release a mitigation (such as patch) accordingly. Patches existing for known vulnerabilities found in the system will be applied for every EZ2 Connect Software release.

Aspect	Comments
Firewall	There is no default firewall setup for Yocto Project-based operating system.
Network configuration	Default static IPv4 address is set to 192.168.255.201 (user configurable in the EZ2 Connect software). Default DNS address is set to 127.0.0.1 (user configurable in the EZ2 Connect software). Supported Wi-Fi protocols: • WPA/IEEE 802.11i/D3.0 • WPA2/IEEE 802.11i (default) • WEP is disabled by default Supported IEEE 802.11 authentication algorithms: • OPEN: Open System authentication (required for WPA/WPA2) • SHARED: Shared Key authentication (requires static WEP keys) • LEAP: LEAP/Network EAP (only used with LEAP) If not set, automatic selection is used (Open System with LEAP enabled if LEAP is allowed as one of the EAP methods). Supported pairwise (unicast) ciphers for WPA • CCMP: AES in Counter mode with CBC-MAC [RFC 3610, IEEE 802.11i/D7.0] • TKIP: Temporal Key Integrity Protocol [IEEE 802.11i/D7.0] • NONE: Use only Group Keys (deprecated, should not be included if APs support pairwise keys) If not set, this defaults to: CCMP TKIP Supported group (broadcast/multicast) ciphers for WPA • CCMP: AES in Counter mode with CBC-MAC [RFC 3610, IEEE 802.11i/D7.0] • TKIP: Temporal Key Integrity Protocol [IEEE 802.11i/D7.0] • WEP104: WEP (Wired Equivalent Privacy) with 104-bit key • WEP40: WEP (Wired Equivalent Privacy) with 40-bit key [IEEE 802.11] If not set, this defaults to: CCMP TKIP WEP104 WEP40
DHCP requirements	IPv4 via DHCP possible
Hardening	Custom OS hardening was implemented, such as closing of unused ports, SSH certificates, and access control • Unneeded accounts disabled: Yes • All users in the operating system are password protected. • Unneeded file shares disabled: Yes, only TCP port 22 is enabled • Unneeded ports disabled: Yes • Unneeded services disabled: Yes • Unneeded applications disabled: No access to deploy other application besides EZ2 Connect Software • Restriction of external (USB) devices: Yes
Customer-supplied software	None

Third-party software

All software components used are part of EZ2 Connect installation package or preinstalled on the hardware modules. The following third-party components are used in software version 1.2.0.

Table 2. Third-party components used in EZ2 Connect

Component	Vendor	Version	License
Crypto++	Wei Dai	8.1.0	BSL-1.0
Log4cplus	Vaclav Haisman	2.1.0	BSD-2-Clause, Apache-2.0
Strongly typed units	Nic Holthaus	2.3.0	MIT
Wpa Supplicant	Jouni Malinen	2.7	BSD-3-Clause
QXlsx	J2doll	1.4.6	MIT
Qt	Qt Development Framework	5.7.1	Commercial

The EZ2 Connect runs on a custom distribution of a Linux operating system. Customers can request the Software Bill of Materials (SBOM) for the OS from QIAGEN Technical Service.

Connectivity

Table 3. Connectivity options for EZ2 Connect

Purpose	Protocol	Port	Authentication
LIMS Connector (LIMS integration)	Hyper Text Transfer Protocol Secure (HTTPS)	User defined	Client and server certificates
QIAsphere Base (Qiagen cloud access)	Hyper Text Transfer Protocol Secure (HTTPS)	443	Server certificate verification and client password
Support	Secure shell (SSH)	22	Private and public key pair secured with password

QIAsphere Base server authenticity is verified using preinstalled SSL certificate. LIMS Connector connection is using both client and server certificates.

The EZ2 Connect is a client in LIMS Connector and QIAsphere Base communication and server in SSH communication.

All listed connectivity options are disabled by default and are not mandatory.

Security patching

Patches are provided with standard software update packages (available on QIAGEN website or automatically if instrument is connected to QIAGEN's cloud).

The patched software components may include an operating system with libraries, third-party dependencies, and/or EZ2 Connect main application.

Sensitive data

No protected health information (PHI) or personal identifiable information (PII) data is required by the EZ2 Connect. However, the EZ2 Connect provides a way to input any data for:

- sample ID
- sample notes
- user ID
- user first name
- user last name

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

- Pseudonymized with a hash function:
  - Sample ID
  - User ID

- Removed:
  - User first name
  - User last name

- Used as is:
  - sample notes

The original data is locally stored on the instrument. If the instrument is connected to the QIAsphere Base, artifacts with unprocessed input data and artifacts with cleaned data like described above are sent to QIAsphere Base. When sending, artifacts that potentially contain PHI or PII data are marked as such so they can be processed accordingly by QIAsphere Base.

Security Controls

Security controls overview

The EZ2 Connect has a role-based user management system. Roles are predefined and are assigned to users by user with the "Administrator" role. Users themselves authenticate with a password.

When connected to the local network, the EZ2 Connect can communicate with LIMS Connector service and QIAsphere Base device. Both connections are using HTTPS protocol and are disabled by default.

Malware and vulnerability protection

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

Network controls

Only TCP port 22 is opened in the EZ2 Connect for incoming connections. No other means of protecting the EZ2 Connect and local network are provided.

Incident and vulnerability handling - software updates and security patches

Patches for the EZ2 Connect are part of the regular system update. They contain updates and vulnerability fixes for the application software and the underlying operating system. These updates undergo the typical verification and validation process according to our global quality management system. Customers are informed when updates are available. Customers can proactively obtain updates from **www.qiagen.com** or contact QIAGEN Technical Service for further support. If you suspect a cybersecurity incident impacting the EZ2 Connect has occurred, contact QIAGEN Technical Support.

Remote connectivity

Remote connectivity is possible with SSH protocol. It is meant to be used by QIAGEN service technicians. The SSH is disabled by default and only Administrator user can enable it. When enabling the public and private key is generated. Private key is moved to inserted USB stick and can be provided to service technician. The public key is kept on instrument as SSH authorized key for authentication with private key. The key is password protected. When SSH is disabled and reenabled, new public and private keys are generated and the earlier used public key is overwritten.

Authentication and authorization

Accounts

Based on available user roles there are four types of accounts:

- Administrator

Administrative account with ability to manage users and configure device.

- Operator

Account allowed to execute protocol runs (standard account for the most users)

- Advanced User (only on Fx instrument variants)

Like Operator, with the option of defining protocol run shortcuts (they allow to skip steps of the protocol run preparation).

- Service

Special account not accessible by the Administrator and not configurable by the Administrator. Used for service access.

Default accounts role-based access control

User roles have the following privileges.

User with Administrator role can:

- Configure device
- Execute protocol run
- Administrate users
- Change its own password
- Setup shortcuts for protocol runs
- Download audit files
- Configure scheduled UV run

User with Operator role can:

- Execute protocol run
- Change its own password

User with Advanced User role can:

- Execute protocol run
- Change its own password
- Setup shortcuts for protocol runs

User with Service role (not assignable by the Administrator, used for service account access):

- Configure device
- Execute protocol run
- Execute Quality Check protocol run
- Access service tab
- Administrate users
- Configure scheduled UV run

Authentication mechanisms

Users are authenticated with passwords. Passwords are hashed and locally stored. When a password is changed, it must be different to the previous one.

Password policies, expiration, and maximum login attempts are configurable by the Administrator.

In case the user is inactive the screen will be locked and require a password to unlock. The screen lock delay is configurable by an Administrator (from no lock to 30 minute delay).

Service users are authenticated by plugging in a service USB stick and providing a password.

At first login, it is strongly recommended to create at least one user account that is not assigned the “Administrator” role.

If Administrator password is forgotten, one-time password procedure exists to get one time password from QIAGEN Service. It requires Administrator to generate a challenge code and share it with QIAGEN Service. QIAGEN Service, after verifying Administrator identity and authorization, will provide one-time password which can be used to unlock the Administrator account and set the new password.

Password rules

User access is password protected. Account will be locked after a configurable number of incorrect login attempts. Password expiration is configurable (it can be off or on with a predefined number of days of password validity). One of three password policies can be assigned to a user role.

1. No policy

   Passwords can be empty. Passwords can have up to 40 characters.

2. Standard policy

   Password must be between 8 and 40 characters.

3. Strong policy

   Password must be between 8 and 40 characters and include all of the following:
   - both uppercase and lowercase characters
   - a number
   - a special character (e.g., @, #, or $)

   Strong policy is the default for all roles.

Physical protection

The customer shall set up a proper access-control system for physical protection of the EZ2 Connect instrument. Debug ports are disabled and there is no debug output being printed out from system boot.

Event/audit logging

Audit trail

The audit trail records general information about the use of the EZ2 Connect instrument. The following events and data are logged:

Startup of the instrument, User logged in, Login failed, Service user login, Service user login failed, Run details, Run started, Run finished, Run finished successfully, Eluate Removal, Run failed, Run aborted, Maintenance started, Maintenance finalized, Maintenance aborted, Maintenance failed, After run maintenance performed, After run maintenance skipped, Protocol update, User added, User data changed, User removed, User authorized with one time password, Abnormal shutdown, Abnormal shutdown failed, Abnormal shutdown – eluate removed, Firmware update started, Firmware update finished, Firmware update failed, SW update, SW update failed / Protocol update failed / Language update failed, OS update failed, Restricted mode enabled, User logged out, User took over the session, Load check started, Load check failed, Load check aborted, Load check finished, Load check skipped, Load check skipped at position, Report created, Report failed, Calibration started, Calibration aborted, Calibration failed, Calibration finished, System settings changed, Device configuration changed, Remote access generated new key, Remote access generated new key failed, Remote access enabled, Remote access disabled, Remote access enabled failed, Remote access disabled failed, SSH status fetch failed, Reports download, Reports download failed, Reports deletion, Reports deletion failed, Support package creation, Support package creation failed, Closing audit trail file, Too low disk space, Risk of injury, QIAsphere certificate update finished, QIAsphere certificate update failed, Language pack installation , Software language was changed, Disabling sending results to LIMS, Enabling sending results to LIMS, Instrument certificate for LIMS connection is generated, Instrument certificate for LIMS connection is not generated, LIMS Connector certificate is uploaded, LIMS Connector certificate is not uploaded, Sending LIMS results is failed, Sending LIMS results was successful, The instrument serial number is unavailable, LIMS configuration is unavailable, The user started a run after a failure in the results, Time settings changed, Canceled cooling after a run due to timeout, Notification file update failure, The download of the software update package from the QIAsphere has been started by the user, The download of the protocol update package from the QIAsphere has been started by the user, Software update package from the QIAsphere has been saved on the instrument, Protocol update package from the QIAsphere has been saved on the instrument, Software update package from the QIAsphere was downloaded but the save operation failed, Protocol update package from the QIAsphere was downloaded but the save operation failed, Problem with updating the maintenance status history file, The user imported a sample list.

Each entry is timestamped and contains user ID (after user logged in), and additional context data if required. Context data may contain sample ID. In Audit Trail for service, user ID and sample ID are pseudonymized.

Software logs

Software logs contain detailed runtime information from the EZ2 Connect application. They are part of a support package which can optionally be transferred to QIAGEN service via QIAsphere. Sensitive data present in the support package is protected by pseudonymization. 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.

Data protection

Protection of data in transit

For communication with LIMS Connector and QIAsphere Base, HTTPS protocol is being used.

Protection of data at rest

Local storage media cannot be accessed without breaking through enclosure. User passwords are hashed before storing.

Cloud/hosted solutions

The EZ2 Connect can optionally connect to QIAsphere cloud service via QIAsphere Base device. The connection is disabled by default and needs to be configured to be turned on.

Disaster Prevention and Recovery

The EZ2 Connect allows for download of reports and audit trails so they can be backed up by the user.

In case of critical software problem, the EZ2 Connect, when possible, will start in restricted mode in which software update or reinstallation is possible. The reinstallation can then be performed to mitigate potential issues.

Secure Configuration

Installation and initial configuration

Follow the installation procedure described in the EZ2 Connect and EZ2 Connect Fx User Manual. Appropriate training can be requested for safe and secure operation of the system. It is strongly recommended to use appropriate physical-access control.

Security best-practices

For safe and secure operation, the EZ2 Connect instrument can be integrated into a securely protected network. Do not expose the system to the internet. Follow the instructions carefully.

Prevent unauthorized physical access to the device.

When performing manual updates, make sure that the update packages come from the official QIAGEN website.

Do not enable SSH communication when not needed. Provide SSH key only to verified QIAGEN service personnel with a valid reason to use it. Disable SSH as soon as it is not used.

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

Regulatory Compliance and Certifications

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

GDPR requests 2 specific principles to be implemented:

- Privacy by Design

  Data privacy through technology design: the design and implementation of the system shall ensure that privacy requirements are met.

- Privacy by Default

  The configuration of the system ensures privacy out of the box: the system shall be configured in such a way that privacy is ensured directly after installation, without having to do or enable additional security settings.

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

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

Attachment: MDS² Form

The MDS2 form is available for the EZ2 Connect and EZ2 Connect Fx. Customers can request the form from QIAGEN Technical Service.

Legal Statement / Disclaimer

See the *EZ2 Connect 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** or can be requested from QIAGEN Technical Service or your local distributor.