Technical Information

QIAsphere® Product and Solution Security

QIAsphere is a QIAGEN® digital platform where users can connect their QIAsphere-ready instruments for remote monitoring and other connectivity services. QIAsphere can be set up either via internet connection, using cloud services, or in local mode, within the user´s local network, with connectivity features that keep within the boundaries of a closed network.

QIAGEN puts at top priority the protection of our customers' data. Therefore, we have implemented several standards and policies to support security and help prevent unauthorized access into our QIAsphere platform.

System Overview

The QIAsphere system is the digital-service ecosystem for QIAGEN instruments. It comprises:

- Hardware and software components within the user network (i.e., gateway components, local apps available in the user WLAN)
- IoT connections to the QIAGEN cloud and to cloud-based offerings (such as status monitoring of devices) by using mobile devices independent of the user's WLAN

The system has four components (Figure 1):

- QIAsphere Cloud: Microsoft® Azure®-based solution that collects and aggregates instrument data and provides result information to the user; it also contains the website My QIAGEN, and is managed by QIAGEN
- QIAsphere Base: the on-premise component of QIAsphere, which serves as an Iot gateway device between the user's instruments and the QIAsphere Cloud
- QIAsphere App: a mobile app that is installed in the user's mobile device (iOS® or Android®) to display information from QIAsphere Cloud and QIAsphere Base
- QIAsphere Base Export Tool: an optional Windows® service that is used to export reports stored from the QIAsphere Base and deposit them in the user's directory of choice

Hardware Specifications

QIAsphere Base specifications can be found in **www.eurotech.com/en/products/iot/multi-service-iotedge-gateways/reliagate-10-12**.

Communication Methods

QIAsphere Cloud

The QIAsphere Cloud connects to the following components:

QIAsphere Base

- HTTPS, MQTT

QIAsphere App

- HTTPS
- Push notifications

QIAsphere Base

QIAsphere Base connects to the following components:

QIAsphere-ready instruments

QIAsphere Base provides the ability to connect to instruments via the user's network, using one of these methods:

▷

- HTTPS (Ethernet): Fast Ethernet, RJ45
- HTTPS (wireless connector): IEEE 802.11b/g/n

QIAsphere App

QIAsphere Base can connect to the QIAsphere App, but besides the initial configuration process, it does not need to communicate with the QIAsphere App. The QIAsphere App can get all information from the QIAsphere Cloud (recommended setup).

- HTTPS (wireless connector): IEEE 802.11b/g/n (optional)
- HTTPS (Ethernet): Fast Ethernet, RJ45 (optional)
- Bluetooth® connector (HTTP for initial setup only, disabled during operation): Bluetooth 4.0 BLE/4.0 Dual Mode, Bluetooth 3.0+HS, Bluetooth 2.1 and 3.0

QIAsphere Cloud

- HTTPS, MQTT: via Ethernet or wireless connector

QIAsphere Base Export Tool

The QIAsphere Base Export Tool connects to the QIAsphere Base and, optionally, to a Windows share on other servers:

QIAsphere Base

- HTTPS

External Windows Share folders

If the user wishes to export files to directories on other servers, they must ensure that file sharing is available between servers.

- File-sharing server message block (SMB): Requires ports 135 to 139 for UDP and TCP traffic
- Direct SMB: Uses port 445 for TCP transfer

Message queue telemetry transport (MQTT) – ports 8883

MQTT is a lightweight publish-subscribe network protocol well suited for IoT connectivity where the devices need to use low bandwidth and may not have a constant or reliable network connection. All communication uses Transport Layer Security (TLS) v1.2 encryption.

Hypertext transfer protocol secure (HTTPS) – ports 443

HTTPS is the standard protocol used for most web

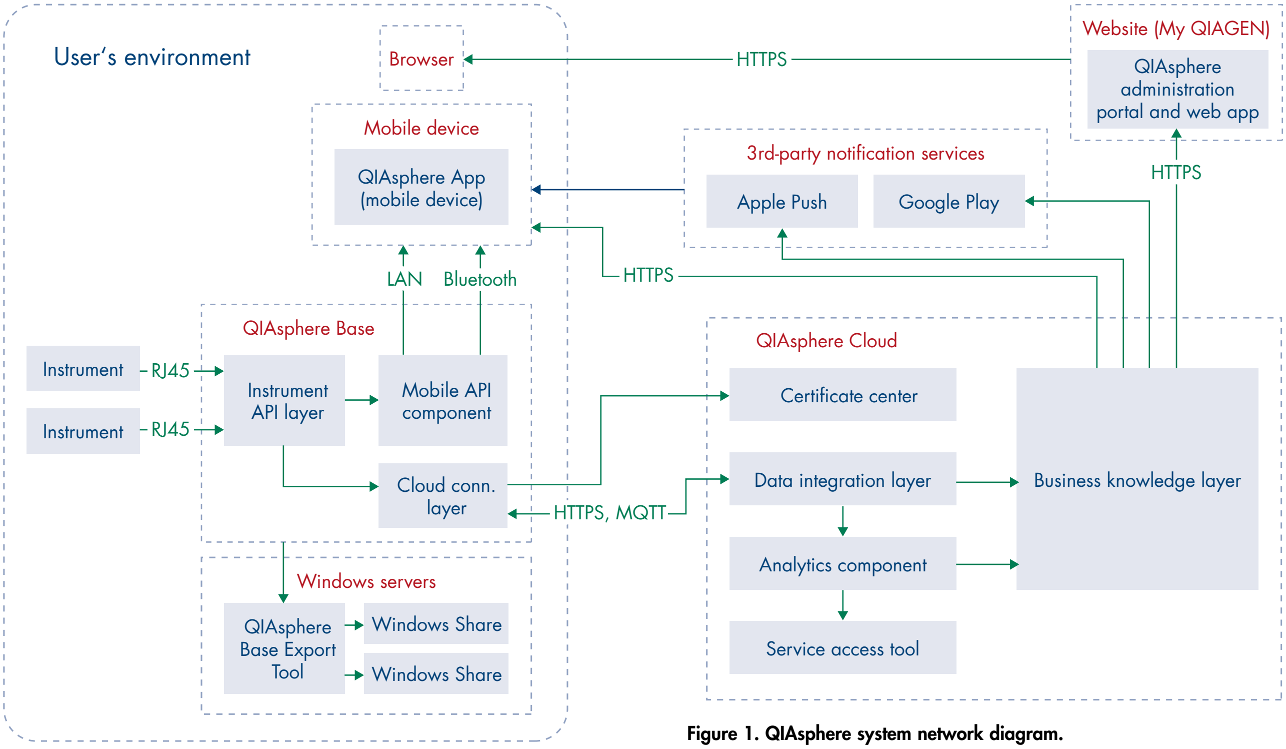

Figure 1. QIAsphere system network diagram.

communications. It leverages TLS v1.2 to encrypt the information being transferred.

QIAsphere Base wireless connection methods

- IEEE 802.11b/g/n
- Bluetooth 4.0 BLE/4.0 Dual Mode
- Bluetooth 3.0+HS
- Bluetooth 2.1 and 3.0

Certificate-Based Authentication

Both QIAsphere Cloud and QIAsphere Base use certificate authentication in their communications to identify the source of the data. Each QIAsphere Base has a separate certificate that uniquely identifies it from any other possible providers.

Each QIAsphere Base must be separately registered in QIAsphere Cloud via a two-step registration process, to ensure the correct identification and ownership of each QIAsphere Base. Certificates are issued by our certificate-provisioning system after correct identification.

For communications between the QIAsphere App and the cloud, we use a public certificate provided by DigiCert® (SHA256).

If the user needs to use the intranet mode, then a QIAGEN-signed certificate must be installed on the mobile device. (Documentation is provided separately.)

Note: The intranet mode is not required for the application to work correctly.

Anonymization

The QIAsphere system does not directly use anonymized data. Rather, it relies on the instruments to anonymize the data and to flag as *anonymized*, *none*, or *identifiable* the data that is being sent to the QIAsphere system.

Data flagged by the instruments to the QIAsphere system is handled accordingly by our systems (e.g., identifiable data is discarded when identified). Personally identifiable data is discarded upon arrival at QIAsphere Base.

Data Transfer and Storage

QIAsphere Base stores events and logs locally; these are then transferred to the QIAsphere Cloud via MQTT and HTTPS.

To ensure that sensitive data is not accessible to unauthorized third parties, QIAsphere encrypts sensitive data:

- Data in transit is always encrypted using TLS.
- Data at rest is encrypted using both application-specific methods and operating system (OS)-level methods, depending on the area being used:
  In QIAsphere Cloud, critical fields are encrypted at rest. In addition, all storage resides in a trusted zone.
  In QIAsphere Base, the data is stored on a hard drive. This data is encrypted at the OS level for ReliaGATE 10-12-61 QIAsphere Bases. This means that a potential attacker who physically removes the said hard drive cannot access its information.

Warning: The reports stored in Windows folders by the QIAsphere Base Export Tool are not encrypted. The use of this tool is optional, and it is the responsibility of the user to ensure proper access control in the destination directory if they choose to use this tool.

QIAsphere Base Hardening

QIAsphere Base has been hardened to ensure enhanced security against tampering by malicious actors.

The device is closed. No applications can be installed by operators. SSH is cut off.

- Update packages are digitally signed, and versioning of the components is managed by OSGI® mechanism
- All default system accounts have been disabled
- Unnecessary physical ports have been disabled; USB functionality has been disabled
- All unnecessary network communication ports have been disabled
- Unnecessary services have been disabled; Telnet® is not disabled, but it is not reachable from outside of the device

▷

- Bluetooth activates itself for 1 hour after restart to enable device configuration; it is automatically deactivated afterward

Software

QIAsphere Base

Operating system

QIAsphere Base uses the ReliaGATE Everyware® Linux® system as its main OS. This is an open-source and open-standard Linux-based distribution, based on Yocto Project® 2.6, which was developed to support IoT devices.

QIAsphere Base exists in two versions, depending on the type of deployment:

- ReliaGATE 10-12-61 uses Everyware Linux 26.0.0 as OS
- ReliaGATE 10-12-32 uses Everyware Linux 25.3.0 as OS

Details of the releases can be found at **eurotech.github.io/linux-releases/** The version number can be seen in the QIAsphere Base Setup Portal.

Third-party software

Everyware Software Framework (ESF)
(https://www.eurotech.com/en/products/iot/iot-edge-framework/everyware-software-framework):

a development framework that allows IoT devices to easily and securely communicate with external systems.

QIAsphere App

Ionic Framework (**ionicframework.com/docs**): a complete open-source SDK for hybrid mobile app development, built on top of Angular and Capacitor. JavaScript® open-source libraries: JavaScript does not have access to storage or network resources.

Security Patching and Updates

QIAsphere Cloud

The QIAsphere Cloud is constantly updated by the QIAGEN team to improve its functionality and to patch any security weaknesses found. Every change is made backward compatible before deployment to ensure that the QIAsphere App and QIAsphere Base functionalities are not impaired.

QIAsphere Base

Automatic updates are provided to QIAsphere Base on an as-needed basis.

These updates are generated in the QIAGEN Cloud and pushed to all QIAsphere Bases, where the update is scheduled for after-hours deployment without the need for human intervention. This ensures that the devices have the latest and most secure version available.

Important: All updates are digitally signed by QIAGEN and validated for authenticity by QIAsphere Base prior to deployment.

QIAsphere App

Patches or updates are provided on an as-needed basis. Because updating applications on the mobile phone requires user intervention, QIAGEN aims to keep the number of updates low. For this reason, security features are either bundled up with new features if its priority is low, or will be deployed as separate updates in case critical vulnerabilities or security updates are needed.

Note: QIAGEN is only responsible for the QIAsphere App and has no control of the underlying OS or other apps that may reside in the user's mobile device.

Important: New updates are distributed through the Apple App Store, Google Play, and the QIAGEN website. New updates will also be communicated to the users via push notification or during the login process to the application.

Software Development Process

QIAsphere follows secure development practices to ensure the quality and security of our software.

- A feature roadmap is available to ensure continuity
- Changes and enhancements are internally documented and approved before being implemented

- Every change must pass through QA acceptance before deployment is approved
- All code and configuration changes are tracked and kept in a central repository
- For JavaScript, an NPM dependency vulnerability scanner is run before release
- Regular vulnerability scanner checks are performed on our website by a third-party company; all vulnerabilities are reported and internally cataloged for remediation
- Development is separated from deployment to ensure that no person can make any change and also release that change by themselves alone
- Deployments are only done after approval by product owners

Penetration testing

The cloud and application components of the QIAsphere system have been tested by independent CREST (Council of Registered Ethical Security Testers) certified penetration testers to identify any vulnerabilities that may compromise the security of the QIAsphere system. Any finding is analyzed and reacted accordingly during the software development process to ensure the protection of your data.

Security Controls

Azure platform

QIAsphere Cloud services are hosted on Microsoft Azure, fully benefiting from a wide range of security features.

- Azure infrastructure delivers high availability and reliability based on (N+1) redundancy architecture
- Azure networks are designed to provide anti-spoof protection, limiting access by using ACLs and DDoS protection by default
- User data in Azure is protected by firewalls at multiple levels

Important: Azure infrastructure meets a broad set of international and industry-specific compliance standards, such as ISO® 27001, HIPAA, FedRAMP®, SOC 1 and SOC 2. QIAsphere Cloud is hosted on the Western Europe datacenter.

QIAsphere Cloud

Logs

API calls

All API calls made to the QIAsphere Cloud APIs are logged separately. These API call logs contain:

- Originating IP address
- DateTime
- URL
- System account

Failed connection attempts are also logged.

API call logs have a retention policy of 30 days, during which period this information can be available for analysis and investigation. Usage data is collected for the pages within the QIAsphere portal that are visited by the user. However, this data is anonymized and aggregated.

Cloud resources

All changes (event) to the QIAsphere Cloud infrastructure are logged and stored as part of the audit log. The following pieces of information are stored:

- Operation name
- Status
- Time stamp
- Event initiator

Important: Exceptions and warnings to normal application execution are also logged.

The following pieces of information are logged:

- Event time
- Message
- Call stack

Password authentication

Users accessing the QIAsphere portal must provide unique credentials.

- Session timeout: 12 hours

▷

- Passwords must contain at least 8 characters, with 1 uppercase letter, 1 numeral and 1 symbol.

User passwords are protected via a password-hashing function (BCrypt). Claims are transferred to other systems using JSON web token (JWT).

JWT authentication

JWT is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as JSON objects. JWTs are used to transmit the validated identity of the users to separate systems without requiring direct communication between the system. Instead JWTs are digitally signed by a central authentication authority and transferred through the browser or app.

The JWT contains user-identity claims that are digitally signed and may not be modified without invalidating the token. The token also has an expiration date to avoid replay attacks.

Firewall

Access controls are handled via virtual firewalls, API gateways and separation in subscription to control the management of resources.

Backups

QIAGEN Cloud regularly backs up the databases using Azure's backup service, providing incremental and full snapshots at regular intervals. Copies of our production environment are regularly restored to our QA environment, ensuring the validity of our backups.

TLS

All communication from QIAGEN Cloud to external systems and components is secured via the use of TLS 1.2 and above.

Denial of Service protection

QIAsphere Cloud services utilize Azure Basic DDoS Protection, as well as content-delivery networks, which accelerate the response of often-used resources and provide protection against network-based DoS attacks.

Health monitoring

Constant monitoring of all resources informs QIAGEN of possible failures or overutilization of resources. This allows the proactive prevention of any loss of functionality or information.

QIAsphere Base

Logs

QIAsphere Base logs failure events that fall outside of normal parameters, such as errors and warnings. Errors and warnings contain the DateTime, error or warning type, description and StackTrace. The variable values are never logged.

Besides that, general performance indicators of the system are constantly stored, such are general server and JVM health, CPU and memory utilization, number of threads, etc.

Password authentication

Access to QIAsphere Base (via the mobile application) requires users authenticating themselves using unique passwords.

Note: These passwords are different from the one used by the QIAsphere App.

- Session timeout: 30 min.
- Username/Passwords are changeable by the user.

Password has to be at least eight characters and must include uppercase and lowercase characters, numerals and special characters (e.g., !,#,$,*).

User passwords are protected via a password-hashing function (PBKDF2).

Cloud-registration process

Before QIAsphere Base can send information to the QIAsphere Cloud, it must first be registered via a two-step registration process, where the instrument registers itself to the cloud (while retrieving a signed certificate to validate all future communications) and the operator marks QIAsphere Base as active in the cloud.

Firewall

QIAsphere Base has an internal firewall that blocks all connections except for the preapproved ports (HTTPS and MQTT) described above.

Restoration

In case of failure, it is possible to reinitialize QIAsphere Base. Reinitialization and registration takes less than an hour.

QIAsphere Base Export Tool

Logs

Service parameter changes, filenames and the paths of exported reports are stored in the Windows Event Log.

Password authorization

To connect to a QIAsphere Base and extract the reports from this system, the user needs to to enter the password of the QIAsphere Base API. This password can be different for every QIAsphere Base.

QIAsphere App

The QIAsphere App runs on personal mobile devices. Therefore, it is important to ensure that the mobile device is properly secured.

Logs

Usage data is collected for the accessed pages in the QIAsphere App. This data is sent to the cloud, where it is anonymized and aggregated.

No data on the contents of the application is ever logged.

Password authentication

The QIAsphere App uses the QIAsphere portal as an authentication mechanism. (Note that access to the admin section of QIAsphere Base uses a separate password.) Therefore, the same password security validations are used:

- Session timeout: 12 hours
- Passwords have to be at least six characters and must include uppercase and lowercase characters, numerals and special characters (e.g., !,#,$,*).

User passwords are encrypted via a one-way hashing algorithm (BCrypt) and validated via a centralized authentication system. Claims are transferred to other systems using JWT.

Best Practices

QIAsphere Cloud

The QIAsphere Cloud is managed by QIAGEN, so no special actions need to be taken by the user regarding the general system.

However, users can create accounts in the QIAsphere web portal. Please follow the standard procedures for web accounts, e.g.:

- Use a strong password
- Keep passwords private
- Do not share your password with other people
- Use your work email address

QIAsphere Base

QIAsphere Base should reside and be operated in a physically controlled lab environment with network access to the instruments.

Although QIAsphere Base blocks all unused ports, it should be set up in a network behind a firewall.

In case of need, QIAsphere Base can be reinitialized by a physical reset button and reconfigured in a short amount of time.

QIAsphere App

The QIAsphere App needs to be installed on the user's mobile device. The mobile device should have access to the internet to access the app's full functionality. Ensure that the mobile device is properly secured. Ensure that the latest version of the QIAsphere App is installed in your device.

Do not use the QIAsphere App if you think your mobile device has been compromised.

QIAsphere Base Export Tool

Install the application on an access-restricted server. The QIAsphere Base Export Tool is a service that relies on Windows security to limit its access.

Ensure that the QIAsphere Base Export Tool is run on the same network as the QIAsphere Base, to be able to access the reports.

Ensure that the application is run under an account that has permission to access the Windows folder where you want to store the reports, because the application uses the Windows account that it is running on to request permissions.

Users that need access to the report do not need to have access to the QIAsphere Base Export Tool directly. Separate the report directories (and servers) from the QIAsphere Base Export Tool installation directory.

GDPR

QIAsphere gives you full control over all your personal data, in full compliance with the General Data Protection Regulation (EU) 2016/679 (GDPR). When you use QIAsphere, whether in local or cloud-connected mode, none of your personal identification or sensitive data is collected. QIAsphere Cloud is used only to provide you with a fully functional instrument monitoring service and other cloud services. To learn more, view the QIAsphere Privacy Policy in the QIAsphere App.

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.