cytiva

# ImageQuant™ TL 10.2

## Privacy and Security Manual

cytiva.com

# Table of Contents

# 1 Introduction

## About this manual

This manual describes the privacy and security considerations of the use of ImageQuant™ TL (IQTL).

## Purpose of this manual

This manual describes the expected intended use of ImageQuant TL, the privacy and security capabilities included, and how these capabilities are configured.

## Scope of this manual

This manual is valid for the version 10.2 standard ImageQuant TL product.

ImageQuant TL consists of the following:

| Software | Description | Contained modules |
|---|---|---|
| ImageQuant TL | A software package for analysis of images in a range of experiment types in a workflow. It is possible to designate lanes, background, and bands coupled with molecular weight, calibrate and also perform optional and advanced analysis, such as lane profile comparison or normalization of both single- and multi-channel images.<br>It allows chromatograms to be imported from ÄKTA™ systems in ***Gel and Blot Analysis*** for single-channels in a new purity analysis step and improve the image export function by allowing customized exports in different image formats and resolutions. | • ***Gel and Blot Analysis***<br>• ***Analysis Toolbox***<br>• ***Array Analysis***<br>• ***Colony Counter*** |
| IQTL GxP | A separate software package for analysis of 1D electrophoresis experiments performed in a secure data environment, and supports the need for traceability and control of data. | • IQTL GxP ***Admin Tool***<br>• IQTL GxP ***Client Module*** |

## Introduction to privacy and security

This manual assumes that the reader understands the concepts of privacy and security. Security protects both system and information from risks to confidentiality, integrity, and availability. Security and privacy work together to help reduce risk to an acceptable level. In healthcare, the privacy, security, and safety must be balanced, relating to the intended use of the product.

The customer is encouraged to use risk management procedures to assess and prioritize privacy, security, and safety risks. Using the risk management, the customer can determine how to best leverage the capabilities provided within the product.

## Product description

Important user information about intended use of the product:

ImageQuant TL is not a medical device and shall not be used in any clinical procedures or for diagnostic purposes.

ImageQuant TL is an image analysis software and does not contain any associated hardware.

IQTL GxP is a separate software for archiving images and image analysis, and approving the analysis. IQTL GxP does not contain any associated hardware.

## Safety notices

This user documentation does not contain safety notices concerning the safe use of the product.

## Contact information

For specific privacy and security inquiries, use the contact form found at *cytiva.com/contact*.

## Abbreviations

The following terms and abbreviations are used in this manual:

| Term/Abbreviation | Definition |
|---|---|
| ID | Identity |
| PHI | Protected Health Information |
| PI | Privacy Information |

# 2 Privacy and security environment

## Privacy and security in the environment

ImageQuant TL has been designed for an intended use with the following expectations of privacy and security protection, that should be included in the environment where ImageQuant TL will be used:

- ImageQuant TL is used on a computer with either Windows® 10 (64-bit) or macOS® 10.15 operative systems, or higher.
- ImageQuant TL is designed to run in a network or a non-network mode. In the network mode, the system should be protected by firewall protection to prevent tampering or loss of data and therefore guarantee the security of the data.
- ImageQuant TL is designed for use in a standalone desktop environment.
- ImageQuant TL should not be used in a mobile system.

The user of the ImageQuant TL needs basic knowledge about image analysis in order to perform analyses using different applications in the software.

# 3 Authentication, authorization and audit logging

## About this chapter

ImageQuant TL includes a broad assortment of capabilities to enable privacy and security. This chapter describes the ability and use of these privacy and security capabilities.

## In this chapter

# 3.1 Access controls

## Introduction

The access control on ImageQuant TL is used to help control access to customer information on the system. Access control includes user account creation, assigning the privileges, and other features.

## Identity provisioning

The provisioning of user accounts requires the steps of account creation, maintenance, and removal of the account when it is no longer needed. A user account is created to be used by a specific individual. This user account is associated with access rights, and is recorded in system security log files.

The ImageQuant TL consists of the following:

- The ImageQuant TL software with the modules ***Gel and Blot Analysis***, ***Analysis Toolbox***, ***Array Analysis***, and ***Colony Counter*** without identity provision
- The IQTL GxP software with identity provision

The IQTL GxP software contains auditing and monitoring help features. The IQTL GxP software also contains access control features including:

- User access control
- Assigning permissions
- Other features

The IQTL GxP software is enabled with identity provision. The module IQTL GxP ***Admin Tool*** has User Account Management features, available Internally and through the Windows user domain.

The following is valid for the User Account Management in the IQTL GxP ***Admin Tool***:

- The user with local administrator privileges administers user accounts for the IQTL GxP software.
- The ImageQuant TL-GxP-Admin Tool does not have an authentication mechanism. Users are expected to run in a safe environment.
- The IQTL GxP ***Admin Tool*** is able to use Windows services to request for the Windows users. The IQTL GxP ***Admin Tool*** does a check if the Windows users are present in the system. The user names and their assigned privileges are stored encrypted in the ImageQuant TL software. No other information is stored.
- Added users can be either Internal users or Windows users. The following recommendations are valid for these user types:
  - GxP supports two kinds of user identification and login. Users can sign into the system using their Windows user credentials (so long as permissions are assigned in the ***Admin Tool***) or they can create internal user accounts managed by GxP that are not tied to the windows domain identity at all.

- Using domain accounts is more convenient because you have one less password to remember, but it can be advisable to use internal user accounts so that if the identity is compromised, the leak does not spill into your wider system.
- For this reason, it is recommended that internal user accounts are used. If Windows accounts are used, it is *strongly recommended* that they are domain accounts and *not* local PC accounts. Use of local windows accounts opens a trivial user name spoofing scheme (there is nothing that can stop creation of a user called "Supervisor" on two PCs).

The encrypted information stored by the IQTL GxP ***Admin Tool*** is used by the IQTL GxP ***Client Module***. These tools only do checks for the assigned permissions the users have and accordingly provide the information in the ImageQuant TL software. The IQTL GxP ***Client Module*** asks for the Windows user name and Windows password for authenticating the same. For Windows users, no password is stored. The Windows user name and Windows password are transferred to Windows Authentication services for verification of the user name and password.

## Passwords

The password policy is applicable to internal users added to IQTL GxP software. The password policy recommends the following restrictions:

- Password minimum length is 4 Characters and maximum 32 characters.
- Password has the option to "keep mix of upper/lower case characters".
- Password has the option to "prevent repeats", meaning that the previously used passwords cannot be reused.

It is recommended to use the above password restriction policy while creating an internal user. The password policy is not applicable to Windows users.

## User authentication

The user authentication step verifies that the user attempting to access the system is indeed the user associated with the specific account. This section describes the administration of the authentication system.

The IQTL GxP software of the ImageQuant TL product has user authentication capabilities provided through the user authentication feature. If the user credentials are deactivated, the IQTL GxP software does not allow the removed user to use the ImageQuant TL software. A deactivated user cannot log into the ImageQuant TL software.

For the user authentication feature, the following is valid:

- The IQTL GxP software supports both valid Internal user and/or Windows user authentication by using their user name and password.

The IQTL GxP software cannot change or create new Windows users and passwords.

## Assigning access rights

Assigning access rights is the administrative process for connecting permissions with user accounts.

The user permissions are applicable only for the IQTLGxP software, and with the following recommendations:

- Users should be assigned as minimal a permission set as possible. If there is a user that is tasked with scanning and introducing images into the system, other users need not have, for example, the “Add Project” permission.
- Another possibility for reducing permissions for validation that can be selected is to make sure that users only have read-only permissions. Consider a supervisor that checks and signs off work. This user can perform the task of opening and inspecting projects and analysis in a read-only capacity.

The users and their access rights are stored in encrypted files internal to ImageQuant TL security software.

## 3.2 Audit logging and accountability controls

### Introduction

Privacy and security information logging and control provide accountability through security surveillance, auditable records, and reporting.

There is no full logging mechanism in any modules of the ImageQuant TL product.

The ImageQuant TL ***Gel and Blot Analysis***, ***Analysis Toolbox***, ***Array Analysis***, and ***Colony Counter*** modules and the IQTL GxP ***Client Module*** provide a reporting feature for a performed analysis. This reporting feature is enabled only when an analysis is performed by one of the modules and the analysis is saved.

The reporting feature generates a PDF file format version of the report.

The IQTL GxP ***Client Module*** of the IQTL GxP software has version control and audit features. With the IQTL GxP ***Client Module***, users with the approval permissions can approve analyses performed by other users. The IQTL GxP ***Client Module*** provides audit reports of the actions from adding images for analysis, performing analysis and approving the analysis.

None of the other modules in the ImageQuant TL product provides auditing support features.

# 4 Patient privacy consent management

## Patient privacy

ImageQuant TL does not handle (create, transfer, or store) patient data, therefore the patient privacy consent is not applicable to ImageQuant TL.

# 5 Information protection

## About this chapter

This chapter describes privacy and security operations, and contains guidelines for the preparation of a secure environment for ImageQuant TL.

## Defense in depth

Security operations are best implemented as part of an overall "defense in depth" information assurance strategy. This strategy is used throughout an information technology system that addresses personnel, physical security, and technology. The layered approach of defense in depth limits the risk that the failure of a single security safeguard allows the system to be compromised.

The ImageQuant TL product does not claim any layered approach of defense in depth for its applications. However, the failure in security for a single application does not compromise other applications in the software.

## In this chapter

# 5.1 Network security

## System interconnections

System interconnections are not applicable as the ImageQuant TL product does not support or claim any system interconnection features.

## Wired network security

Cytiva strongly recommends that ImageQuant TL is operated in a network environment that is separated from the general purpose computing network of the owner's organization. There are many effective techniques for isolating ImageQuant TL on a secure sub-network, including implementing firewall protection, demilitarized zones (DMZs), virtual local area networks (VLANs), and network enclaves.

To assist in secure network design, the following sections describe the required network services for ImageQuant TL.

ImageQuant TL does not support or claim any wired network security features. Hence it is recommended that the user shall take care of the security for its wired network while using ImageQuant TL.

## Network setup

The following is valid for the ImageQuant TL product regarding the network setup:

- It runs in a desktop environment on Windows 10 (64-bit) or macOS 10.15, or higher.
- It uses the network setup provided by the operating system environment and does not provide any network features. It does not require the user to configure any special operating system and network features.
- It does not use any ports directly.
- It does not have any remote service or features.

**IMPORTANT**
The user still needs to make sure that the ImageQuant TL product is exposed only to a secure network environment.

The License Server application uses TCP port 62615. This server is used by the ImageQuant TL product for its floating license. This port must not be closed when using a floating license to run the ImageQuant TL product.

### HTTP vs HTTPS

If the user intends to use GxP as a fully client/server system with clients distributed over the network, it is *highly* recommended to configure the system to use HTTPS exclusively. While care is taken to reduce the amount of compromising information send over the wire, having a fully encrypted link is essential.

To configure HTTPS, please refer to the *Installation Instructions, section 3.2 HTTPS GxP setup guide*.

## Firewall

The Windows firewall must be enabled and configured by the user with a secure environment in place.

## Wireless network security

Radio signals are used in a wireless network communication, therefore wireless devices require special security consideration. Effective techniques and tools exist for improving the security of wireless communication. This section describes the characteristics for wireless connections for ImageQuant TL.

ImageQuant TL does not provide any wireless communication features. The features of ImageQuant TL can be accessed via wireless communication ports enabled by the operating system. It is recommended to secure all wireless communication ports according to the guidelines of the operating system when using ImageQuant TL.

## Removable media security

The files used in ImageQuant TL for experiments and analysis can be imported and exported to USB storage media or to any other removable device. However, this feature is an operating system feature that is not unique for ImageQuant TL software. The user is responsible for ensuring that removable devices connected to the system are free from viruses and other malware. The removable devices must be scanned with recommended antivirus software when transferring files from a computer.

## Data at rest security

ImageQuant TL does not provide any special security features for data at rest. It is expected that the files and results from ImageQuant TL and IQTLGxP are secured by the user of ImageQuant TL in a similar manner to how other system data are secured.

There is no sensitive data like PHI/PI which the ImageQuant TL product and IQTL GxP stores. However, if there is any important information as part of the analysis which the user performs, ImageQuant TL and IQTL GxP expects the user to protect that information.

**Secure Folder permissions**

IQTLGxP software has a ***Secure Folder*** storage which can be configured only by the IQTLGxP admin user.

Normal users should *not* have access to the ***Secure Folder***, not even read access. The database file should be as locked down as possible. The only access granted to the ***Secure Folder*** should be the user that the server service (the Windows service that houses the server component) is/will be running.

Ideally, a minimal number of users should have access to the folder. GxP requires *only* the service user to have access (read/write/delete) but the user may want to grant read access to additional IT-controlled users for purposes such as backup.

# 5.2 Data storage and encryption

## Data encryption

The ImageQuant TL does not support explicit data encryption measures in all of its data storage.

However, the ***Secure Folder*** in IQTLGxP software is designed to be inaccessible to all but the network services user running the IQTLGxP ***Admin Tool***.

It is recommended to the customers of ImageQuant TL to secure all the data storage with proper measures.

## Data integrity capabilities

ImageQuant TL has no capabilities to make sure that the data is not accidentally or maliciously modified.

Only the IQTL GxP application of the ImageQuant TL software has the capability to make sure that the data is not accidentally or maliciously modified. If data, like image files or experiment data, is tampered or altered outside the software, the IQTL GxP warns the user and does not allow further actions in the IQTL GxP application.

***Note:*** *This feature in the IQTL GxP application is only applicable once the file is added to the IQTL GxP application.*

Data integrity is checked every time there is a data transaction in the IQTLGxP application. And if there is any data tampering during the course of analysis in GxP software, then this will be warned and captured in audit trail.

## De-identification capabilities

ImageQuant TL is not a medical device and does not handle (create, transfer, or store) patient data. Therefore ImageQuant TL does not contain de-identification (anonymization and pseudonymization) capabilities.

## Business continuity

In case of data corruption, the IQTL GxP software dictates and warns the user about the data corruption. The user shall delete the corrupted data and use new data for further analysis in the software.

No other ImageQuant TL module has this feature. The user is expected to use proper measures before using the data in the above mentioned applications.

## 5.3 External connections

### Connection to an external computer

Connection to an external computer is not applicable for the ImageQuant TL product.

### Security controls provided by the cloud provider

ImageQuant TL is not hosted on a third party cloud environment. Cloud security controls are not applicable.

# 6 System Protection

## Introduction

This chapter describes the guidelines for how to configure and maintain the product in a way that continuously protects privacy and security.

## Protection from malicious attacks

The computing environment is increasingly hostile, and threats continue to grow from denial of service attacks and malicious software, including computer viruses, worms, Trojan horses, and other malware. Vigilant defense on many levels is required to keep the systems free from intrusion by malicious software. In most cases, effective protection requires cooperation between Cytiva and our customers.

The ImageQuant TL product has no integrated antivirus and malware protection. There is no support from third party antivirus or anti-malware software.

It is the responsibility of the user to make sure that:

- The removable devices that are connected to the system are free from viruses and other malware.
- In case the system is used in network mode, the network infrastructure is protected with a firewall and other security measures.

For more information on malicious software protection, refer to the following two white papers by the Joint NEMA/COCIR/JIRA security and Privacy Committee:

- *Defending medical information systems against malicious software, December 2003*
- *Patching off-the-shelf software used in medical information systems, October 2004*

Both documents are available from: *http://www.medicalimaging.org/*

## Server and workstation security

ImageQuant TL contains additional features to improve local operational security. ImageQuant TL has a license server application to enable the license communication between the server and clients for license management. The application is a third party application and has its own security enabled.

## System change management

ImageQuant TL is a software-only product. It does not contain any hardware associated with it. All the updates and changes can be monitored and managed by the user and is the responsibility of their software support team.

## Patch management practices

Patch management practices are not applicable as ImageQuant TL is a software-only product and does not contain any operating system integrated with it.

# 7 Remote access

## Introduction

Often the most efficient and cost-effective ways for Cytiva to provide service is to connect to ImageQuant TL remotely. Every effort is made to make sure that this connection is as secure as possible. This chapter describes the security measures for remote access connections.

The modules in ImageQuant TL do not provide any remote access features. It is therefore recommended that the customer follows operating system guidelines to ensure no vulnerable actions through remote access software.

## Remote connection

The modules in ImageQuant TL do not contain any remote services and therefore all the services, updates, upgrades, or patches are performed by downloading the updates from Cytiva Life Sciences portal. In a case to case basis, diagnostics can be done for the modules in ImageQuant TL to reproduce the issue at the user site. This service is only used from the operating system remote service.

# 8 Personal information collected by the product

## Personal information

ImageQuant TL is not a medical device and does not handle (create, transfer, or store) patient data. ImageQuant TL does not collect personal information.

# 9 Additional privacy and security considerations

## Additional risks

ImageQuant TL has been designed with privacy and security functionality integrated into the core design. However, there exist privacy and security residual risks that must be mitigated when ImageQuant TL is integrated into the work environment. This section describes some risks that should be imported into the risk assessment of the deployment of ImageQuant TL for proper mitigation.

All modules in ImageQuant TL expect the user to maintain all security measures needed to prevent any kind of vulnerabilities. However, the IQTL GxP software has data protection and anti-tampering features enabled. The IQTL GxP software also enables audit support.

## IQTL GxP server service

The GxP server runs as a Windows service. Once configured, you should use the Windows services control panel to explicitly set a user for the server to run as so that this user can be granted special permissions to the ***Secure Folder***.

## Server and Secure Folder locality

While the only requirement for the locations of the ***Secure Folder*** and the server is that the *server* has network access to the ***Secure Folder***, it is important for good performance that they are co-located such that there is a high-speed, low latency link available. Ideally the server will be on the same PC as the ***Secure Folder***.

# 10 Product security supplemental documents

## Software Bill of Materials (SBOM)

SBOM is available for ImageQuant TL upon request. Contact the sales representative for a copy of SBOM.

Page intentionally left blank

**Give feedback on this document**

Visit cytiva.com/techdocfeedback or scan the QR code.

cytiva.com



For local office contact information, visit cytiva.com/contact

29654110 AB V:2 07/2022