



ImageQuant™ TL GxP 11.0

Installation Instructions

Table of Contents

- 1 Introduction 3**
- 2 Install IQTL GxP module 5**
 - 2.1 Set up Secure Folder and IQTL GxP Admin tool 7
 - 2.2 HTTPS GxP setup guide 14
 - 2.3 Set up IQTL GxP application 18
- 3 Product support 20**

1 Introduction

About this document

This document describes how to install ImageQuant™ TL GxP (IQTL GxP) on Windows computers and provides the following information:

- System requirements
- Installation instructions for IQTL GxP

System requirements

To use the IQTL GxP software, the following system requirements must be met:

- Operating systems: Windows 10 (64 bit) or Windows 11 (64-bit).
- Memory: 6 GB RAM, or higher.
- Free hard disk space: minimum 10 GB.
- Microsoft .NET 8.0 installed, see instructions below.

The minimum and recommended specifications are important to provide good software performance and reduce installation and operational issues.

Note: *Admin rights are necessary to run the installation.*
 *Admin rights are **not** necessary to use the IQTL GxP software.*

Install Microsoft .NET 8.0

The Microsoft .NET package is not provided with the IQTL GxP software package.

Note: *Microsoft .NET is necessary to run the IQTL GxP software.*

Follow the steps below to Install .NET 8.0.

Step	Action
------	--------

- | | |
|---|---|
| 1 | Download Microsoft .NET Desktop Runtime 8.0 (x64) for Windows.
http://dotnet.microsoft.com/en-us/download/dotnet/8.0 |
|---|---|

Step

Action

Visual Studio 17.11.5

Included runtimes

.NET Runtime 8.0.10

ASP.NET Core Runtime 8.0.10

.NET Desktop Runtime 8.0.10

Language support

C# 12.0

F# 8.0

Visual Basic 16.9

SDK 8.0.306

OS	Installers	Binaries
Linux	Package manager instructions	Arm32 Arm32.Alpine Arm64 Arm64.Alpine x64 x64.Alpine
macOS	Arm64 x64	Arm64 x64
Windows	x64 x86 Arm64 winget instructions	x64 x86 Arm64
All	dotnet-install scripts	

Visual Studio support

Visual Studio 2022 (v17.10)

[| winget instructions](#)

.NET Desktop Runtime 8.0.10

The .NET Desktop Runtime enables you to run existing Windows desktop applications. **This release includes the .NET Runtime; you don't need to install it separately.**

OS	Installers	Binaries
Windows	x64 x86 Arm64 winget instructions	

.NET Runtime 8.0.10

The .NET Runtime contains just the components needed to run a console app. Typically, you'd also install either the ASP.NET Core Runtime or .NET Desktop Runtime.

OS	Installers	Binaries
Linux	Package manager instructions	Arm32 Arm32.Alpine Arm64 Arm64.Alpine x64 x64.Alpine
macOS	Arm64 x64	Arm64 x64
Windows	x64 x86 Arm64 winget instructions	x64 x86 Arm64
All	dotnet-install scripts	

2

Double-click the downloaded .NET package to run the installation.

2 Install IQTL GxP module

Introduction

IQTL GxP is a module designed for use in regulated lab environments and needs only to be installed if you are going to use these features and have the appropriate licenses.

Note: *IQTL GxP is currently only available for Windows.*

GxP components

IQTL GxP needs to be configured by setting up a **Secure Folder** using the **IQTL GxP Admin** tool, and installing the **IQTL GxP** application.

- **Secure Folder** is created and maintained by the **IQTL GxP Admin** user. The secure folder stores image files and analysis files. It also contains the database file that stores the user data and user roles/privileges. The admin user responsible for the **IQTL GxP Admin** tool creates and maintains this secure storage.
- **IQTL GxP Admin** tool maintains and configures the **Secure Folder**, GxP users, and user data. It also controls the connectivity (e.g. HTTP and HTTPS) between **IQTL GxP Admin** (server) and **IQTL GxP** application (client).
- **IQTL GxP** application is the module where users perform image analysis in a safe, authentication-based GxP environment. Images and the performed analysis are saved as projects in the **Secure Folder** when projects are checked in for review and approval steps. The application never operates directly on the **Secure Folder** maintained by the **IQTL GxP Admin** tool. Only authenticated users added by the **IQTL GxP Admin** tool can perform analysis in the **IQTL GxP** application.

Note: *It is recommended that an admin user configures and operates **IQTL GxP Admin** tool in a secured IT-controlled system. Therefore, the **IQTL GxP Admin** tool is a standalone application separate from the **IQTL GxP** application.*

GxP setup steps

IQTL GxP works in a true client-server environment in which multiple clients (**GxP** application users) can connect to a single server (**IQTL GxP Admin** tool user).

Two options exist, follow the one that is most appropriate:

- To configure both server and client on the **same** system/PC, with no need for network connectivity, follow all the steps in the table below.
- To configure the server on one system/PC and the clients on **different** network-connected systems/PCs, follow step 1 and step 2 in the table below. Then follow step 3 for each client PC where the GxP application must be set up.

Note: *Step 2 is needed if you choose HTTPS connectivity in the **Admin** tool. It is not needed for HTTP connectivity.*

Steps	Action
1	Section 2.1 Set up Secure Folder and IQTL GxP Admin tool, on page 7
2 (optional)	Section 2.2 HTTPS GxP setup guide, on page 14
3	Section 2.3 Set up IQTL GxP application, on page 18

In this chapter

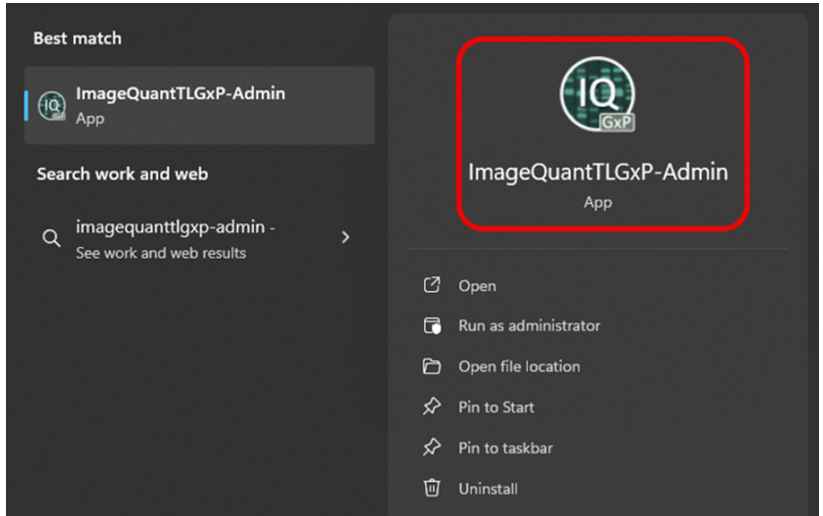
Section		See page
2.1	Set up Secure Folder and IQTL GxP Admin tool	7
2.2	HTTPS GxP setup guide	14
2.3	Set up IQTL GxP application	18

2.1 Set up Secure Folder and IQTL GxP Admin tool

Introduction

To open the ***IQTL GxP Admin*** app:

1. Type `Imagequantgxp-admin` in the search bar.
2. Open the app by clicking on the icon on the right-hand side.



Installation procedure

The ***Secure Folder*** and the ***IQTL GxP Admin*** tool are set up and administered by the GxP admin user.

Note: When upgrading the software to the latest version, from 10.x to version 11.0, first delete the GxP service already running before installing.

To terminate Windows services in GxP, follow the steps below:

1. Open the ***IQTL GxP Admin*** tool.
2. Stop the service in ***Admin*** tool.
3. Type `CMD` in the Windows search bar.
4. Right-click on the ***Command Prompt*** tool and select ***Run as administrator***.
5. Type `sc delete [service name]` and press ***Enter***.

Note: The default service name is `IQTL-GxP-Server`.

This will remove the service and should allow you to create a new one without an error.

Note: *After upgrading from IQTL GxP v 10.x to v 11.0, IQTL GxP v 10.2 will no longer be functional and can be uninstalled.*

Follow the steps below to install and configure the **Secure Folder** and **Admin** tool server.

- | Step | Action |
|------|---|
| 1 | Download the software installation package from cytiva.com/IQTL . |
| 2 | Install the <i>IQTL GxP Admin</i> tool software:
Browse the downloaded package, open the folder <i>ImageQuantTL-GxP-[Version]-WIN</i> . Locate and install ImageQuantTLGxP-ADMIN-[Version]-WIN.msi file by following the on-screen instructions. |
| 3 | Create a new folder on your C : drive which will serve as a <i>Secure Folder</i> . Copy the path to this folder either on the same PC where the <i>IQTL GxP Admin</i> tool is installed or on a network-connected system that is accessible by an admin user operating <i>IQTL GxP Admin</i> tool.

Note:
<i>It is recommended that this folder is only accessed by admin users, not other users running the analysis module, i.e. the <i>IQTL GxP</i> application.</i> |
| 4 | Run the <i>ImageQuantTL GxP Admin</i> tool from the <i>Start</i> menu of the system by typing <code>imagequant tl gxp-admin</code> in the Windows search bar. |



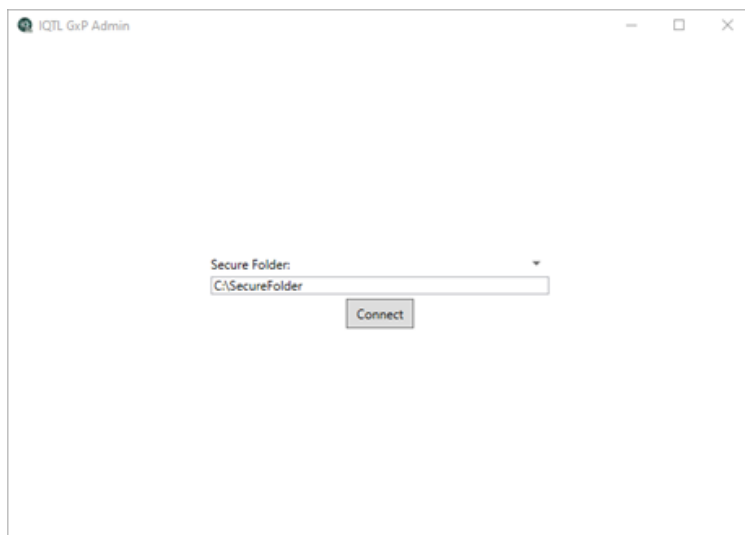
Note:
*The ***Admin*** tool is added to the ***Show hidden icons*** taskbar when the tool is minimized.*



Step	Action
5	Type the path to the Secure Folder created in step 2 and click Connect . Since this new folder does not contain any data, a No Data Found message appears. After clicking Initialize Folder the Secure Folder is ready to be used.

Note:

*This step is only required once. After the **Secure Folder** is configured, and for subsequent **Admin** tool use, click **Connect**. If version 10.x was installed on the same computer, you will not see the screen in the screenshot below, continue with [step 6](#).*



Result:

When the **Secure Folder** is created successfully, the following **Admin** tool main window opens.

Note:

*If IQTL GxP has been upgraded from version 10.x to version 11.0, follow the on-screen steps for updating the **IQTL GxP Admin** tool database.*

ImageQuant TL GxP-Admin Server 11.0.1037

SECURE FOLDER

C:\Users\Krishna Reddy\Documents\IQLT Server

SERVER Stopped

Port: 17080 ☐ Use HTTPS ☐ Local Machine ☒ Launch on Startup Start

Changes will not take effect until the server is (re)started

CLIENT OPTIONS

☐ Mandatory approval comment
☐ Require QC before analysis

PASSWORD RESTRICTIONS

NOTE: Password restrictions apply only to internal GxP users

Expire [never](#)
Minimum length: [any length](#)
Lock user account: [never](#)

☐ Require mix of upper/lower case characters
☐ Require non-alphanumeric characters
☐ Prevent repeats

USERS +

WARNING: No admin users are configured. Assign at least one user the "Admin Login" permission to force sign-in authentication for this app. Dismiss

☐ Show Inactive Users NEW USER

- 6 Install and configure the **IQTL GxP Admin** tool (server) and **IQTL GxP** application (client), either on the same- or on different systems.
- Under **SERVER**, select **Launch on Startup** if you want the server to automatically start when the PC is restarted. If not checked, then the server needs to be started again in the **IQTL GxP Admin** application.



IMPORTANT

For normal installation, the **Local Machine** option should be unchecked. This applies for setups on both the same system and different systems.

Note:

*Only in special cases, when the user has limited admin rights and wants to install the **Secure Folder**, **Client**, and **Server** on the same PC, select **Local Machine** for the same system setup.*

If an error message occurs, or if the GxP application cannot connect to the server, try the following troubleshooting steps:

- Verify that the server is running (green light) in the **Admin** tool.
- Verify that the server is running by clicking the **Test** button.

The date and time should appear in a web browser indicating that the server is running.

- If the server is not running, start the **Admin** tool and GxP application as an administrator.
- If the GxP client cannot connect, change the port number in the **Admin** tool and re-connect with a new port number.

7 Under **SERVER**, click **Start** to create the service.

Result:

When the PC is up and running, the **IQTL GxP Admin** tool launches this service and keeps it running. After the setup, if the **SERVER** connection or **Secure Folder** configuration needs amending, then it is advised to re-start the service.

8 Under **Client Options**, set up the password policy for GxP users.

The password policy is only applicable for internal IQTL GxP users and is not applicable for Windows users. Depending on requirements, configure and enforce password restrictions, for example, expiry, minimum length, locking user accounts, upper/lower case, non-alphanumeric characters, and non-repeat options. For these first three restrictions, click on the blue links next to **Expire**, **Minimum length**, and **Lock user account** to select your preferred options. Also, if the user wants to enforce mandatory approval comments and/or QC analysis, then those need to be configured.

9 Click **New user**, to set up users.

There are three types of users that can be created and configured:

- **Internal New User:** Create an internal user by using IQTL GxP with a unique username and password governed by the password restrictions followed above.

The screenshot shows a 'User Details' window with a title bar and a close button. It has three tabs: 'New User', 'Windows AD User', and 'Local Windows User'. The 'New User' tab is active. Inside the tab, there are two text input fields labeled 'Username:' and 'Password:'. Below these fields is a section titled 'Permissions:' containing two columns of checkboxes. The first column includes 'Add Project' (checked), 'Check Out' (checked), 'Check Out (read only)' (checked), 'Emergency Login' (unchecked), and 'Access Log' (unchecked). The second column includes 'QC' (unchecked), 'Signoff' (unchecked), 'Self-Signoff' (unchecked), and 'Admin Login' (unchecked). At the bottom right of the window are 'OK' and 'Cancel' buttons.

- **Windows AD User:** Assign a user with a username and password that exists in the Windows Active Directory on the relevant domain. Passwords are not controlled by the **Admin** tool. When the domain and username are specified, click **Verify Username** to verify that the Windows user exists.

The 'User Details' dialog box has three tabs: 'New User', 'Windows AD User', and 'Local Windows User'. The 'Windows AD User' tab is selected. It contains a 'Domain:' text box, a 'Username:' text box, and a 'Verify Username' button. Below these are 'Permissions:' with two columns of checkboxes. The first column has 'Add Project' (checked), 'Check Out' (checked), 'Check Out (read only)' (checked), 'Emergency Login' (unchecked), and 'Access Log' (unchecked). The second column has 'QC' (unchecked), 'Signoff' (unchecked), 'Self-Signoff' (unchecked), and 'Admin Login' (unchecked). At the bottom are 'OK' and 'Cancel' buttons.

Wait until you see **User Verified**, then click **OK**.

- **Local Windows User:** Assign a user with a username and password that exists in the local Windows account credentials (e.g. LDAP access). The password is controlled outside the **Admin** tool. Once the machine and username are specified, click **OK** to create the user.

The 'User Details' dialog box has three tabs: 'New User', 'Windows AD User', and 'Local Windows User'. The 'Local Windows User' tab is selected. It contains a 'Machine Name:' text box, a 'Username:' text box, and 'OK' and 'Cancel' buttons at the bottom. Below the text boxes are 'Permissions:' with two columns of checkboxes. The first column has 'Add Project' (checked), 'Check Out' (checked), 'Check Out (read only)' (checked), 'Emergency Login' (unchecked), and 'Access Log' (unchecked). The second column has 'QC' (unchecked), 'Signoff' (unchecked), 'Self-Signoff' (unchecked), and 'Admin Login' (unchecked).



IMPORTANT

A **Windows AD User** account is recommended as it has greater Windows security policies.

Note:

A username conflict issue might arise from **Internal User** accounts. A user with the same name can be configured on multiple PCs and used to accidentally (or deliberately) circumvent GxP permissions. For example, if a user named "supervisor" exists on one PC and is assigned to approve permissions, gain approval rights, or create a user on another PC named "supervisor", the GxP software is not able to distinguish between them. This not possible with a **Windows AD User** account.

- | | |
|----|---|
| 10 | Set up user permissions. Based on necessity, a minimum of one, or more, permissions or privileges need to be configured for each user, for example: |
|----|---|

- **Add Project**
- **Check Out**
- **Check Out (read only)**
- **Emergency Login**
- **QC**
- **Approve**
- **Self-Approve**
- **Access Log**
- **Admin Log**

Select which permissions to assign to the user and click **OK**. When at least one user is created, the **IQTL GxP** application is ready for use.

Note:

It is recommended to choose at least one user for admin rights by selecting the **Admin Login** option.

2.2 HTTPS GxP setup guide

Introduction

This section is for GxP administrators and describes how to set up the HTTPS connection.

Note: This section is not intended for users who want to use HTTP connectivity.

Pre-installation check

Before proceeding with the installation, verify the following:

- The **GxP Admin** tool is installed and functional.
- The **Secure Folder** is created and initialized with at least one user.
- The service is created but **NOT** running:

Click **STOP** in the **GxP Admin** tool, if necessary.

- OpenSSL is installed and accessible from the command line.
- You have permission to launch a command line with admin rights.
- You are following this guide on the PC that will host the service.

Create and install the certificates in the next section.

Create and install certificates

To configure GxP using “self-signed” certificates using OpenSSL, follow the instructions below.

Step	Action
1	Open the command prompt with admin rights.
2	<div>Create the initial certificates using the following OpenSSL command: <code>openssl req -x509 -newkey rsa:2048 -keyout gxp-key.pem -out gxp-cert.pem -days 3650</code> OpenSSL prompts you for the following details: <div><div>a. Organisation Name: this is the name that appears in the certificate manager in later steps.</div><div>b. Common Name: provide the machine name for the PC.</div></div></div>




IMPORTANT

This must match exactly what the client will use as the URL for the client connection. For an eventual URL of `https://the-server-pc:17443` provide `the-server-pc` as the common name making sure to respect case-sensitivity.

- 3 Convert the PEM files into PFX files for import into Windows certificate manager:

```
openssl pkcs12 -inkey gxp-key.pem -in gxp-cert.pem -export -out gxp-pfx.pfx
```
- 4 Open the Microsoft Management Console (MMC), click **Start** and type `mmc`.
Note:
Make sure to launch as an administrator.
- 5 Add certificates snap-in:
 - a. Click **File** → **Add/Remove Snap-in**.
 - b. Select the certificates and click **Add**.
 - c. Choose **Computer Account** and click **NEXT**.
 - d. Choose **Local Computer** and click **FINISH**.
 - e. Click **OK** to finish the snap-in selection.

Result:
 You should now see **Certificates (Local Computer)** in the list under the **Console Root** folder.
- 6 Expand the **Certificates (Local Computer)** folder.
- 7 Right-click on the **Personal** folder and choose **All Tasks** → **Import**:
 - a. In **Certificate Import Wizard**, make sure **Store Location** is set to **Local Machine** and click **NEXT**.
 - b. Click **Browse** and change the file type selector from X.509 to **Personal Information Exchange.pfx**.
 - c. Locate and select the `gxp-pfx.pfx` file from [step 3](#).
 - d. Click **NEXT**.
 - e. Enter the password you provided when you created the file, and click **NEXT**, again accepting defaults.

Step	Action
	<ul style="list-style-type: none"> f. On the next page, select Place all certificates in the following store and choose Personal, then click NEXT. g. Verify the steps and click FINISH.
8	Repeat step 7 but target the Trusted Root Certification Authorities folder instead of Personal .
9	<p>Make a note of the certificates hash:</p> <ul style="list-style-type: none"> a. In the main MMC window, expand the Personal folder and select Certificates. b. Find your certificate in the list, named according to the Organisation Name you provided in the OpenSSL process. c. Double-click (do not use right-click properties) the certificate to open the certificate info panel. d. In the Details tab, scroll down to the Thumbprint item. e. Click Thumbprint. f. Copy the thumbprint from the bottom panel to the clipboard (paste into a text editor for future reference).
10	<p>Configure network settings for the new certificate:</p> <ul style="list-style-type: none"> a. Go back to the admin command prompt. <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <div style="display: flex; align-items: center;">  <div> <p>IMPORTANT</p> <p>Only use the Command Prompt.</p> </div> </div> </div> <ul style="list-style-type: none"> b. Associate the certificate with the network port using the following command template: <pre>netsh http add sslcert ipport=0.0.0.0:[PORT] certhash=[HASH] appid={ 65f05b87- addc-4833-90b8-200642aa239b}</pre> <ul style="list-style-type: none"> a. Replace [PORT] with the port number chosen in GxP Admin tool. b. Replace [HASH] with the thumbprint from step 9f. <p>Example: netsh http add sslcert ipport=0.0.0.0:17443 certhash=1234567ETC appid={ 65f05b87-addc-4833-90b8-200642aa239b}</p> c. Add the URL to the remotely accessible list:

Step	Action
	<pre>netsh http add urlacl url=https://+:[PORT]/ user=Everyone</pre> <p>Again, replace [PORT] with the chosen port number.</p>

The certificates are now installed.

To test the server, open the **GxP Admin** tool, and click **START**.

Note: *The service might need to be created first. Refer to the main installation guide for instructions.*

1. Run a basic test by entering `https://localhost:17443` in a browser window (assuming 17443 is the port you chose).
2. Allow the browser to proceed by accepting certificates, if applicable.

Result:

A "badreq" (bad request) error message should display, verifying that the server is running.

Configure the client

For the clients to allow comms with the server, the certificate must be installed into its **Trusted Root Certificate Authorities** list. Follow the steps below for every client PC.

Note: *It is not necessary to do this on the server PC.*

Step	Action
1	<p>Open the Certificates MMC window.</p> <p>Follow steps 4, 5, and 6 from the server setup, see step 4 on page 15.</p>
2	<p>Under the Certificates (Local Computer) folder on the left, right-click All Tasks → Import and perform the same steps as before in step 7, see step 7 on page 15.</p>

Perform a quick test again using a browser. Type `https://[SERVERPC]:[PORT]` in the URL field. For example, `https://some-server:17443`. As in the previous test, a "badreq" (bad request) error message should be seen.

Launch the GxP client app and connect to the Cytiva server using the above URL.

2.3 Set up IQTL GxP application

Installation procedure

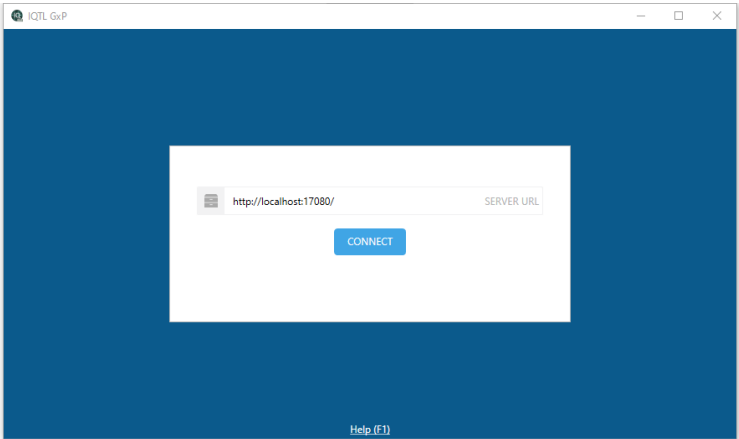
Follow the steps below to install and configure the ***IQTL GxP*** application on each client PC where IQTL GxP software will be used.

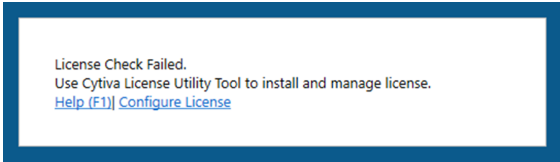
Step	Action
1	Download the software installation package from cytiva.com/IQTL .
2	Install Microsoft .NET 8.0 on each client PC where IQTL GxP software will be used.
3	<p>Install the <i>IQTL GxP</i> application software.</p> <p>Browse the downloaded package, open the folder <i>ImageQuantTL-GxP-[Version]-WIN</i>, then double-click the ImageQuantTLGxP-[Version]-WIN.msi file by following the on-screen instructions.</p> <p><i>Result:</i></p> <p>When the installation is complete, a shortcut with the name <i>ImageQuantTLGxP</i> is available from the start menu and on the desktop.</p>



4	Double-click to start the <i>IQTL GxP</i> application.
---	---

Result:
The following window opens:



Step	Action
5	<p>Activate the license.</p> <p>Note: <i>Make a reference to the document describing the license activation, otherwise an error message is shown:</i></p> 
6	<p>Specify the server URL by providing inputs in the format of “[Scheme]://[Address]:[Port]”:</p> <ul style="list-style-type: none"> • Scheme is the connectivity protocol specified in the Admin tool (see step 7 on page 11). Accordingly specify HTTPS or HTTP. • Address: Type the network DNS name or IP address of the system where the IQTL GxP Admin tool (server) is installed and configured. If the IQTL GxP application is installed on the same system as the Admin tool, specify <code>localhost</code>. • Port is the number specified in IQTL GxP Admin tool (see step 7 on page 11).
7	<p>Click Connect.</p> <p>This only needs to be done once. Subsequent use of the IQTL GxP Admin tool uses the same URL. If the server URL changes, disconnect in the next screen to reconnect with the new URL (see step 5 on page 9).</p>
8	Click Sign In .
9	<p>Log on to the IQTL GxP application with the authenticated username and password configured during IQTL GxP Admin tool user setup (see step 10 on page 13).</p>

To run the IQTL GxP application, install the ImageQuant TL application. Refer to *ImageQuant TL 11.0 Installation Instructions for Windows (29751074)*.

3 Product support

Contact us

If there are any problems with the installation or use of IQTL GxP, contact your local product support team, or use the contact form found at [cytiva.com/contact](https://www.cytiva.com/contact).

Page intentionally left blank

**Give feedback on this document**

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



cytiva.com

Cytiva and the Drop logo are trademarks of Life Sciences IP Holdings Corporation or an affiliate doing business as Cytiva.

ImageQuant is a trademark of Global Life Sciences Solutions USA LLC or an affiliate doing business as Cytiva.

Any other third-party trademarks are the property of their respective owners.

© 2025 Cytiva

ImageQuant © 2025 Cytiva

Any use of software may be subject to one or more end user license agreements, a copy of, or notice of which, are available on request.

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

29750806 AA V:4 12/2024