WATCHMAN™ TruPlan™
CT IMAGING SOFTWARE

Boston Scientific
Advancing science for life™

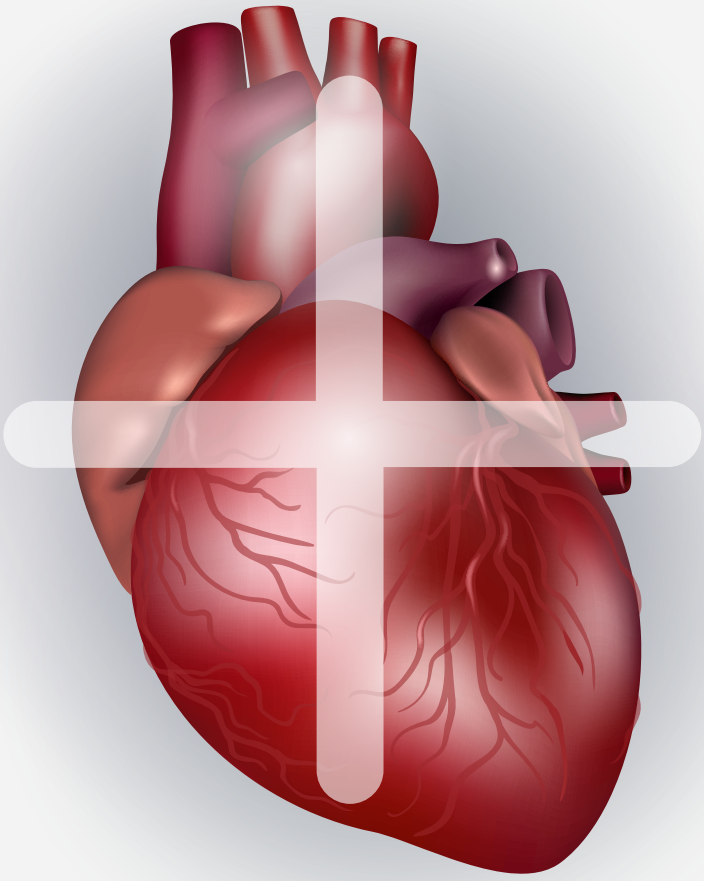
circle CARDIOVASCULAR IMAGING

INSTALLATION AND CONFIGURATION GUIDE

JANUARY 2023

VERSION 3.1

TruPlan Computed Tomography (CT) Imaging Software Application



WATCHMAN™ TruPlan™ software is developed and owned by Circle Cardiovascular Imaging Inc.(Calgary, AB, Canada), and Boston Scientific is the exclusive reseller of WATCHMAN™ TruPlan™ software.

TABLE OF CONTENTS

01

System requirements for TruPlan

The minimum system requirements for TruPlan are:

Requirement	Standalone app	Desktop Client (in enterprise solution – 3 CCU)	TruPlan Server
CPU	Windows:Intel i5 7th Gen Mac: Intel Core i5 7th gen+, Apple silicon	Windows: Intel i5 7th Gen Mac: Intel Core i5 7th gen+, Apple silicon	4-core Xeon
RAM	16GB	8GB	16GB
DISK	200GB SSD-class storage	2GB SSD-class storage	200GB SSD-class storage, capable of 500 IOPS, storage should support the ability to grow over time dependent on local workflows
VIDEO	Intel Integrated HD Graphics 630+	Intel Integrated HD Graphics 630+	n/a
MAC	macOS 11.X, 12.X	macOS 11.X, 12.X	n/a
WINDOWS	Windows 10, 11	Windows 10, 11	Windows Server 2016 or newer
NETWORK - LAN	1 Gb	1 Gb	1 Gb minimum, 10 Gb preferred
DISPLAY	1920x1080	1920x1080	n/a

It is advised to install the latest GPU driver when using TruPlan.

02

Cybersecurity & Network Security

To protect the patient information, it is advised to make sure the operating system of the computer is protected with a password and the patient information is stored on an encrypted disk partition. TruPlan is tested with the security suite of Windows Defender, there are no known limitations. It is advised to install the latest security updates for the operating system. TruPlan is not meant as the single storage location of the DICOM data, therefore there are no requirements for making backups of the system. TruPlan logs errors in the log.txt and user actions regarding patient information in the audit.log, both files can be found in **C:\Users\AppData\Roaming\Circle Cvi\ TruPlan.**

03
Supported installations

TruPlan 3. can be installed as:

1. Standalone

2.Client/Server

On the Standalone type, all the components are installed in the local machine.

On the Client/Server, server components can be installed on a separate box and having clients connected to it. Server installation is only supported on Windows systems. Windows and Mac clients can both connect to the Server.

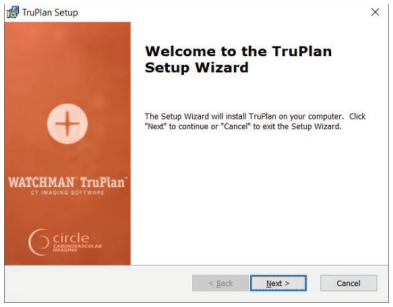
Important: You cannot connect TruPlan 2.X clients to TruPlan 3.X Server, since Client/Server architecture has been introduced only in TruPlan 3.X.

04
Standalone Installation

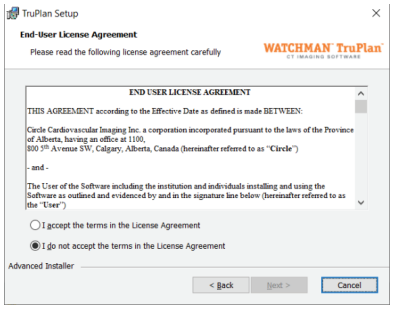
a. On Windows System

To start the installation of TruPlan, Download the msi file and:
Double-click: truplan_3.1.0<build number>_x64_win.msi

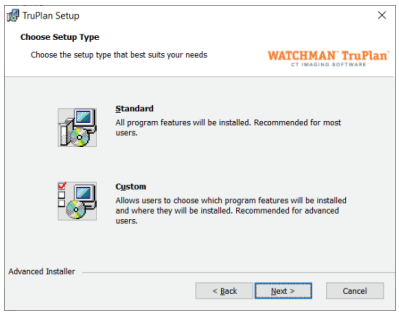
1 Click **Next**



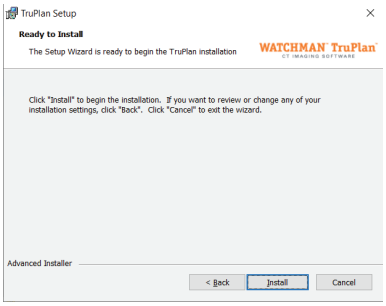
2 You need to read, accept, and click **Next** to continue



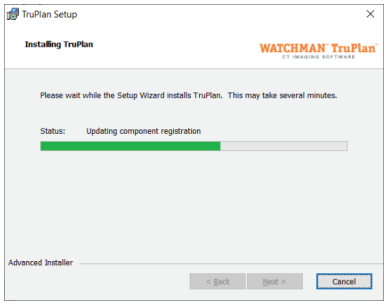
3 standalone, you select **Standard** option



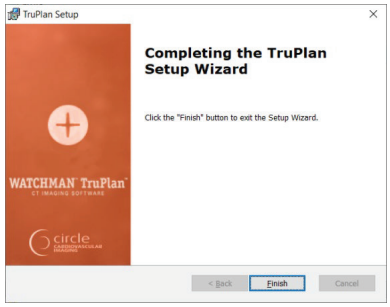
4 Just click **Install**



5 You should see installation progress indicator

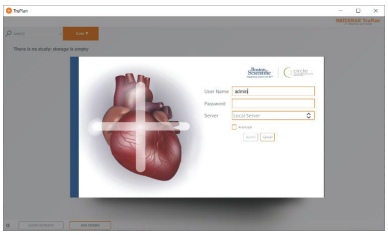


6 Installation is completed, just click **Finish**



7 You can start the application by clicking in TruPlan 3 shortcut

8 Type in:
User Name: admin
Password: password
And click **Submit**

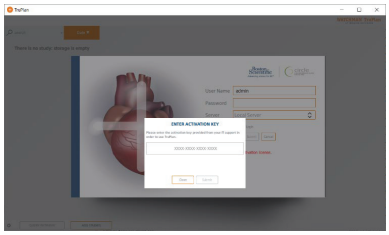


9 When selected, the installer will create a shortcut on the desktop.

Important: You should be connected to the internet, while activating the product.

10 You will be requested to enter the Activation Key you received

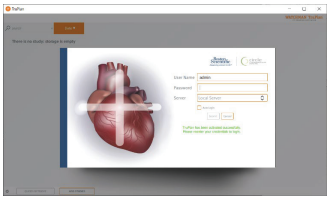
Copy and paste the activation key and click **Submit**



11 you will get success message if activation worked.

If it didn't work, you will get an error message. You need to inform Support Team about exactly error message you received.

After enter User Name and Password and click **Submit** you will be logged within the application.



12 Initial application screen after user logging in

Important:

1. TruPlan will be installed by default on the folder: C:\Program Files\Circle CVI\TruPlan
2. TruPlan data and licenses will be stored by default on the folder: C:\ProgramData\truplan
3. If you want to change these default folders, you will need to select the Custom option during the installation

i.Silent installation of TruPlan client

You can install **TruPlan** client silently via command line.

First, make sure you open the command prompt on Windows with administrative privileges.

To install **TruPlan** with all default options, you can run this command:

msiexec /I <msi file> APPDIR="C:\Program Files\Circle CVI\TruPlan" TRUPLAN_LICENSE_AGREEMENT=true INSTALL_TRUPLANCLIENT=true INSTALL_TRUPLANSERVER=false INSTALL_TRUPLANWEBSERVER=false SERV_ADDR=<IP or FQDN where TruPlan server is installed> SERV_NAME="TruPlan Server" SERV_PORT=4206 /qn /Li truplan_installation.log

- /i – installs the product
- /qn – installs the product in quiet mode with no user interaction
- /Li <logfile> - outputs the progress in a file name
- TRUPLAN_LICENSE_AGREEMENT – this is an installation parameter, and by setting it to true, you are agreeing with the EULA

Important:
Besides /i /qn /Li commands to instrument MSI installation, you can consult this link for additional options:

https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/msiexec

To see if installation completed successfully, you can check in the log file for the text: Product: TruPlan -- Installation completed successfully.

You can also uninstall the product through command line:

msiexec /uninstall "<msi file>" /qn /Li truplan_installation.log

To see if product has been uninstalled, look for this text in the log file: Product: TruPlan -- Removal completed successfully.

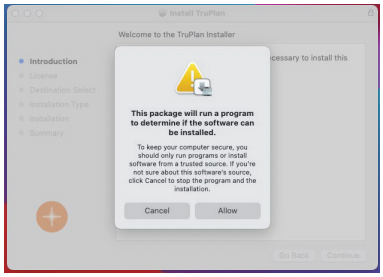
ii.Uninstalling TruPlan

Open the Apps & Features page of Windows (Select Start > Settings > Apps > Apps & features)

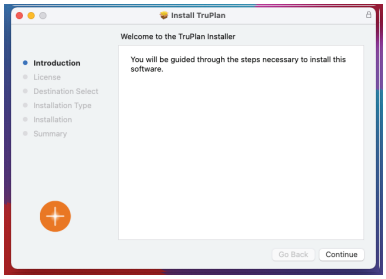
From the list of installed applications, select TruPlan, and select Uninstall. Follow the instructions in the uninstall wizard and the Application will be removed from your system.

b.On Mac System

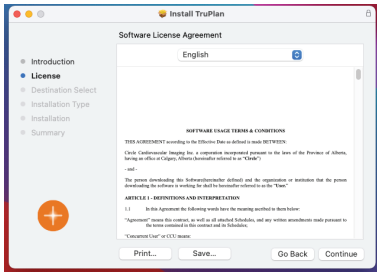
1. Click **Next**



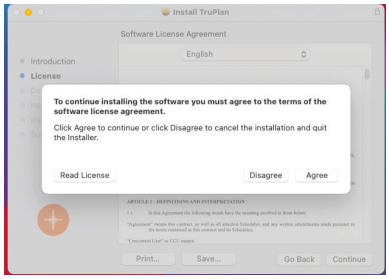
2. Click on **Continue**



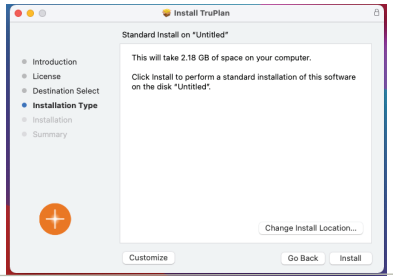
3. Click on **Agree**



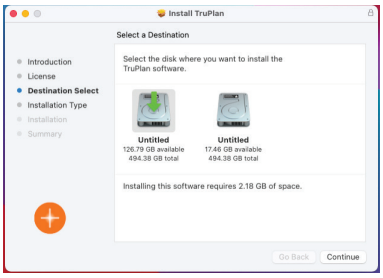
4. Click on **Continue**, you can also print or save the license if required.



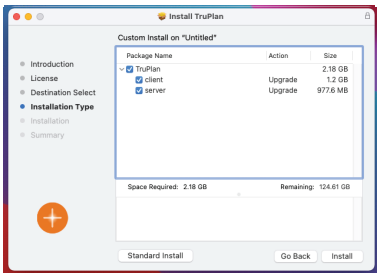
5. Click on **Install** or you can **Change Install Location**

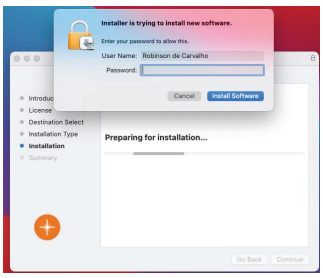


6 Change Install Location dialog

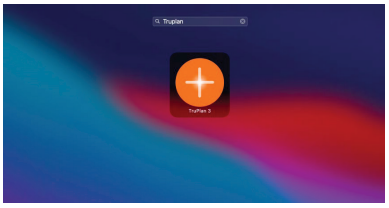


7 **Customize** dialog
After pressing install





8 Enter your password and click on **Install Software** the software will be installed on the folder / Applications/TruPlan3

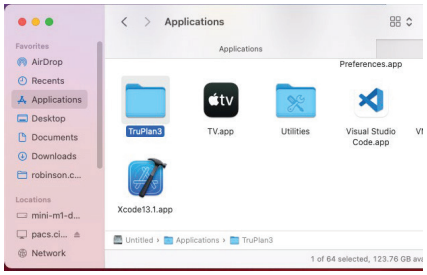


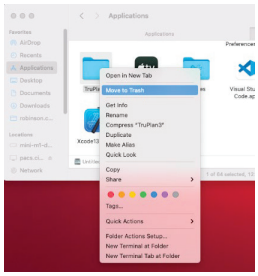
The app should show on the Launchpad

i.Uninstalling TruPlan

To uninstall go to Finder and right click on TruPlan3

1 Click on **Move to Trash** or drag and drop to your Trash on the dock



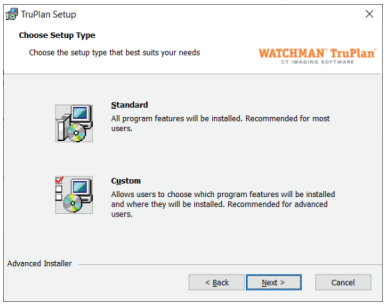


05
Client/Server Installation

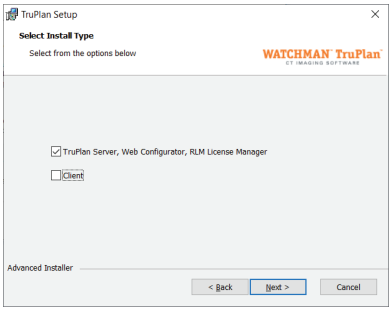
a. Installing the Server (Windows only)

To start the installation of TruPlan, Download the msi file and: **Double-click: truplan_3.1.0<build number>_x64_win.msi**

1 For the server installation, select **Custom** option

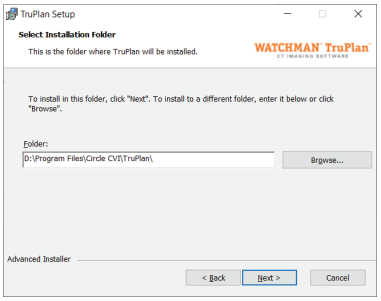


2 Select option TruPlan Server, Web Configurator, RLM License Manager Click **Next**

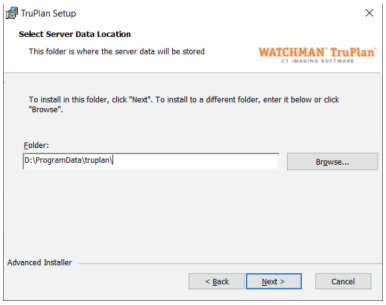


Important:
Important:
a. You don't need to install the client on the server machine
b. TruPlan server has 3 components that are installed on the same machine:
i. TruPlan Server: server component that handles the backend logic
ii. Web Configurator: Web UI that allows to configure server settings
iii. RLM License Manager: Component responsible to manage licenses

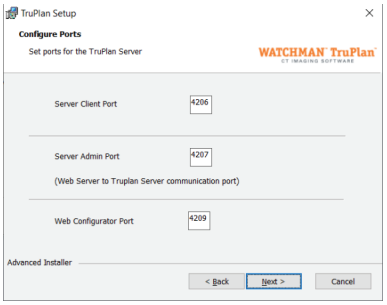
3 You can change the installation folder Click **Next**



4 You can change the data storage folder (DB, DICOM images and configuration) Click **Next**



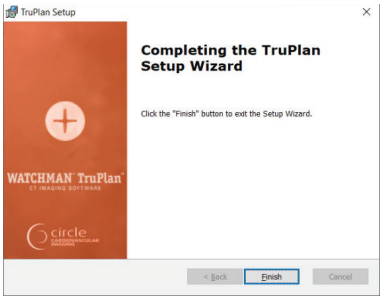
5 You can change the ports for each of the components Click **Next**



Important:

a. Server Client Port: Port where clients will connect to the server
b. Server Admin Port: This port, is the server port that the Web Configurator communicates to
c. Web Configurator Port: Port that user can connect to the configurator URL

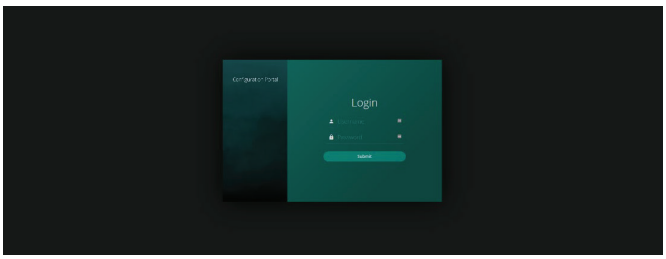
6 Installation is completed, just click **Finish**



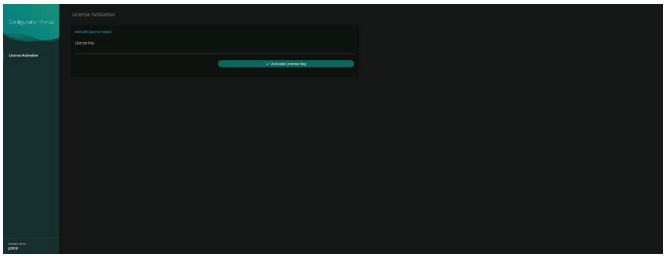
b. Activating the Server

In order to activate the server, you should access the URL: http://localhost:4209/login

If you changed Web Configurator port, please replace 4209 by the port you configured.

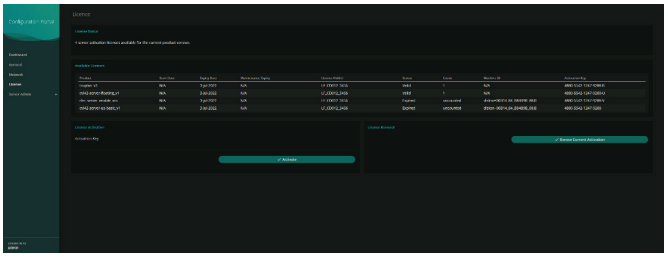


1 Type in admin / password and click **Submit**



2 Type in the Activation Key you received and click Activate License Key

Important: You should be connected to the internet, while activating the product.



3 After activation you should see 4 available licenses.

You can now install the TruPlan client on other machines and connect to the Server.

Please make sure the Server Client Port is opened in the firewall.

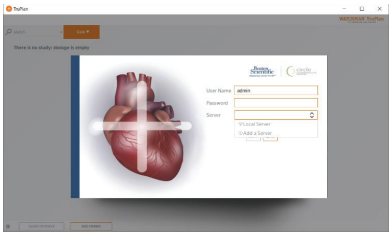
c. Installing the Client (Windows only)

Select Custom Option on the installer and select just Client component.

d. Connect the Client to the installed Server

You can start the application by clicking in TruPlan 3 shortcut

1 Select Add a Server from the Server dropdown

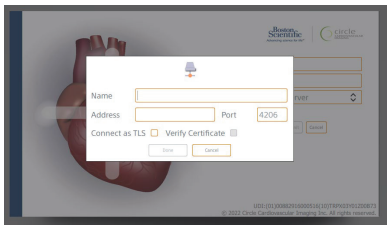


2 Name field is the name of the connection that will appear in the list of connections on the login screen.

Address can be a FQDN or an IP address. Default port is 4206 for non-secure connection.

4406 is the Default port for TLS connection. Ports can be different, depending on which ports have been configured when TruPlan was installed.

You can check “Connect as TLS” to connect to the TruPlan Server through a secure connection. If “Connect as TLS” is checked, you have the option to check “Verify Certificate” as well. By checking it, you make sure TruPlan Client only connects to a secure TruPlan Server.



Important: Even though your IT Administrator didn’t import TLS Certificate into TruPlan Server, you can connect as TLS. In this case, the TruPlan server will automatically create a self-signed certificate valid for 30 days, and will auto renew it after 30 days.

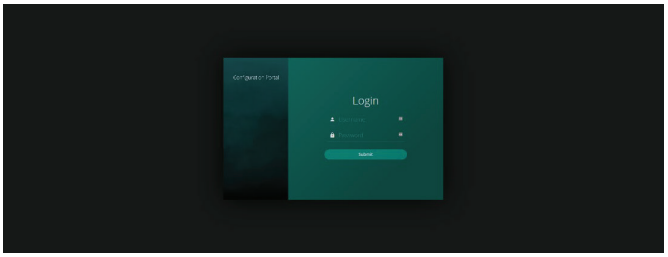
After clicking “Done”, the TLS connection you’ve just created will be available for you to select on the “Server” dropdown.
You can select the new server from on the Server dropdown, type in User Name and Password and click Submit to log in.

e. Web Configurator

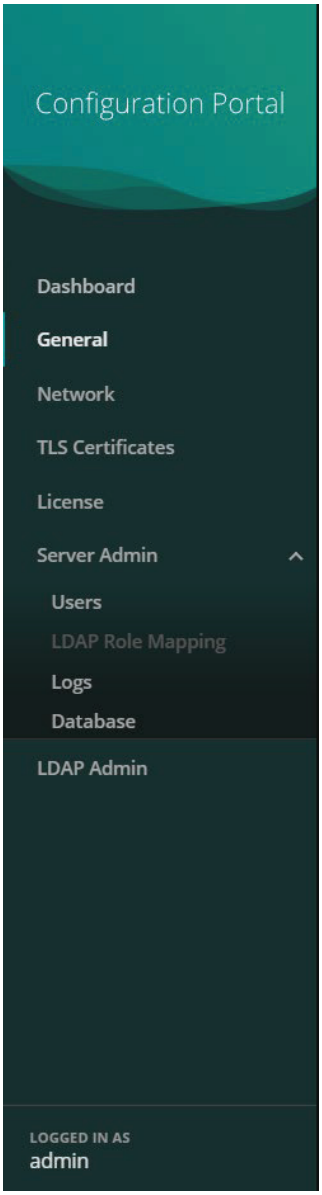
All the server configuration in TruPlan can be done through the Web Configurator interface.

You can access it in the Browser by the address: http://localhost:4209/login.

In case you have changed the Web Configurator port during the installation, or you are not accessing it from the same computer, you should change the address accordingly.



1 Type in admin / password and click **Submit**



i. What can you configure?

Dashboard:

To visualize status of TruPlan Server, number of users connected, licenses, database and DICOM.

General:

Allows several changes like connections change, TCP Ports, Password Policy and Paths.

Network:

Allows configuration of Application Entity and addition of DICOM Nodes.

TLS Certificates:

Allows to Import Public and Private Key for the TLS encryption of TruPlan Server Port.

License:

Allows to activate TruPlan and to manage Licenses.

User:

Allows to manage Users.

LDAP Role Mapping:

Allows to configure the AD Groups that will map to TruPlan Roles.

Logs:

Allows to log management.

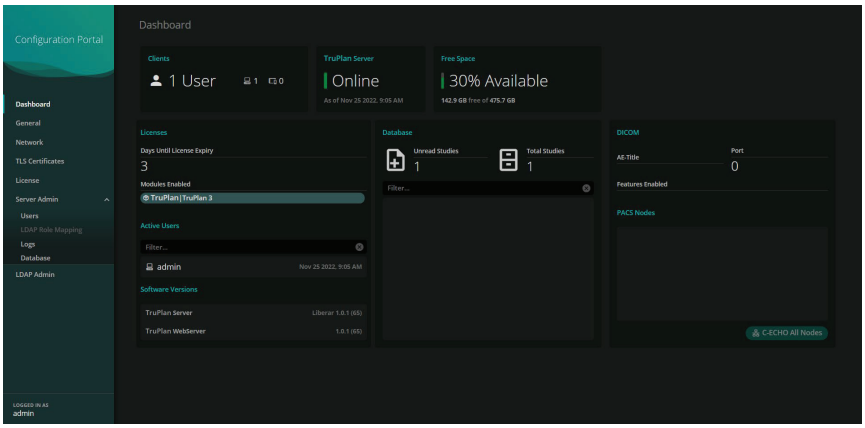
Database:

Allows to manage Database.

LDAP Admin:

Allows to Enable and configure connection to LDAP.

ii. Dashboard

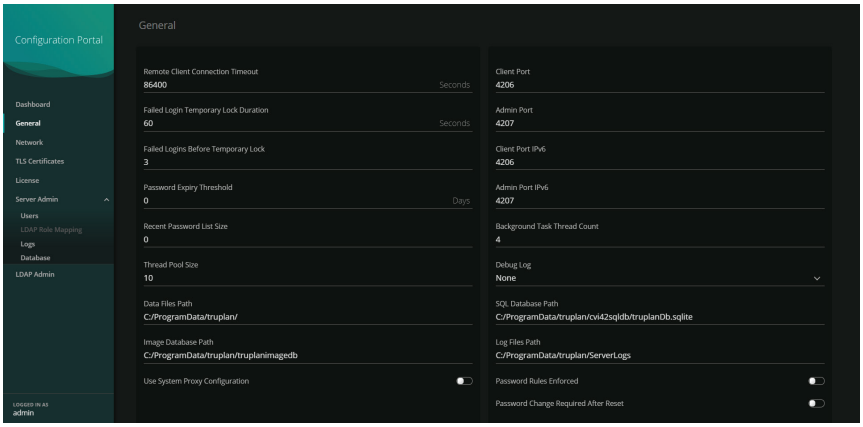


Dashboard options will present some options like:

- Number of clients logged into the server
- Server status (Online/Offline)
- Free Disk Space

> It's important to monitor free disk space on the server, when it gets closer to 20% you should plan for a server cleanup as all studies in TruPlan are stored on the server.

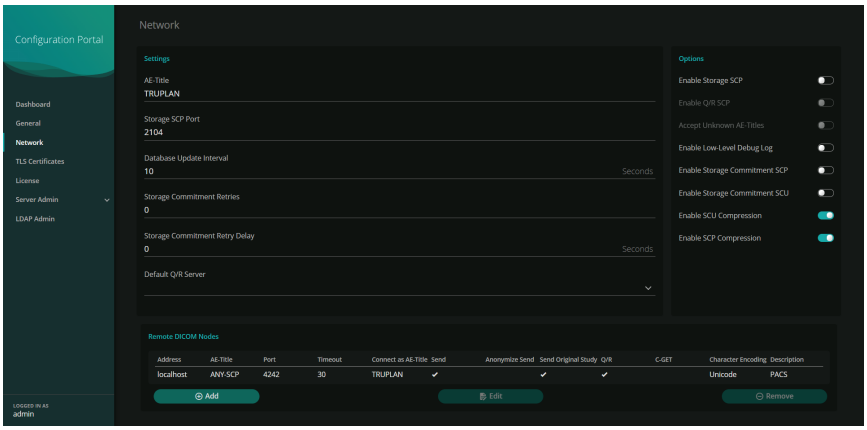
iii. General



In General, you can configure settings like:

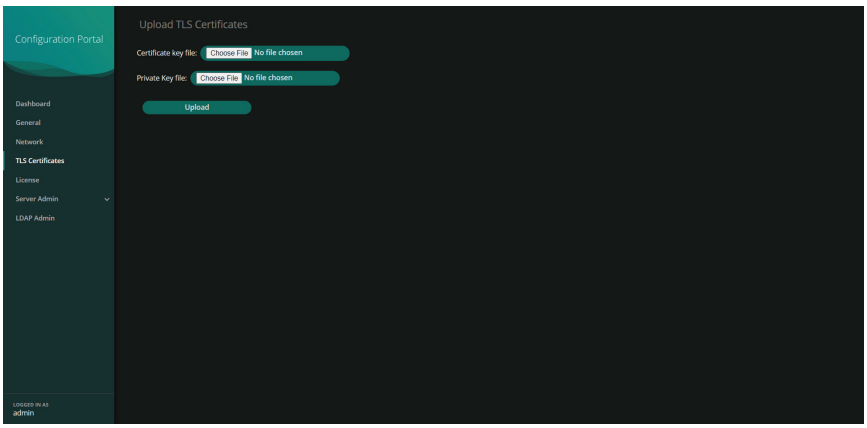
- The data files path
- The SQL Database Path
- Log Path
- etc

iv. Network



On the Network, among other options, you can add Remote DICOM Nodes by clicking Add button in the bottom left of the page.

v. TLS Certificates



On the TLS Certificates, you can setup TruPlan server importing a certificate a private key

Important: : TruPlan accepts .pem and .der formatted certificates and private keys.

Important: : It's recommended that you do not use a self-signed certificate, unless you have your own certificate authority implemented in your environment.

vi. Importing Key Pair

Before using an encrypted connection for the first time in TruPlan, you must install a valid certificate/private key pair to the server. This can either be achieved by:

- Importing Key Pair using Web Configurator interface
- Or manually placing the required files in the %PROGRAMDATA%\truplan folder of the TruPlan server

The file will need to be partitioned into separate certificate and private key files.

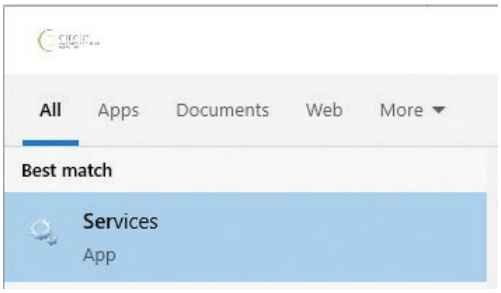
1. Log into Web Configurator and go to TLS Certificates option
2. Import both certificate and private key files as shown below

Important: : If you are using a self-signed certificate, please ensure it has been imported into the client machines trust store before completing this step as TruPlan will prevent you from importing certificates it does not trust.

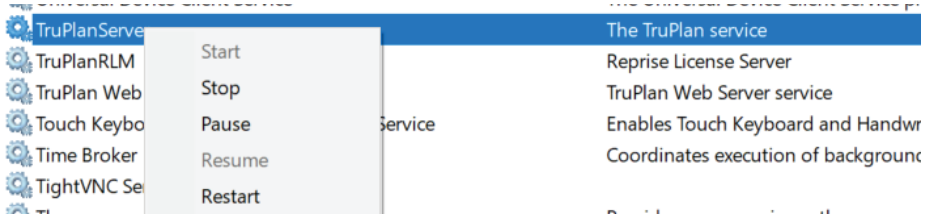
3. Next, select "Upload". If this operation is successful, you will see a success message "Certificates were successfully uploaded".

Important: : For first time configurations, the TruPlan server must be restarted to enable secure connections. New key pair files may be imported without disrupting existing secure connections.

Restarting TruPlan Server
You should open Services in Windows:

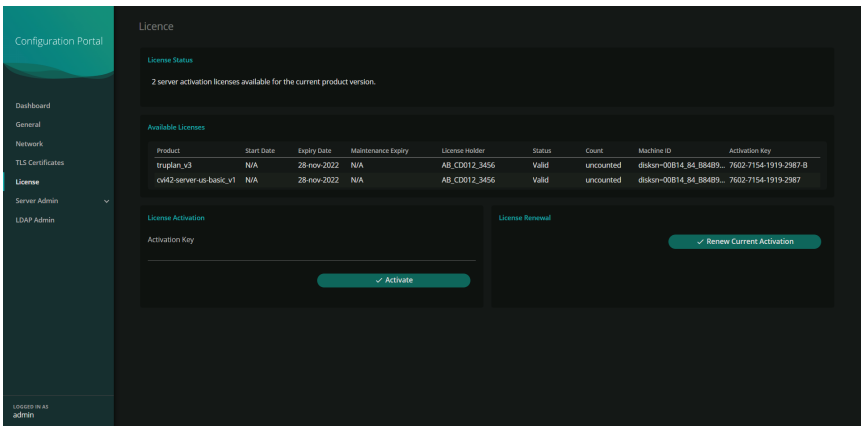


Find TruPlanServer Service, right click and select Restart:



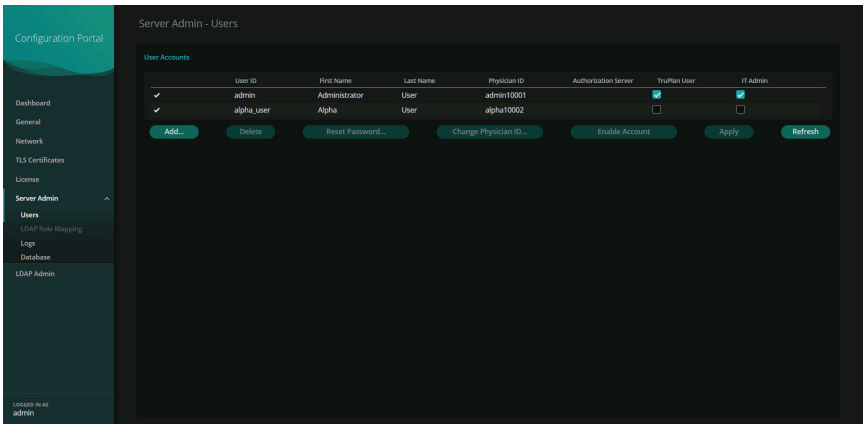
After restarting, TruPlan Server will load the new imported certificate.

vii. License



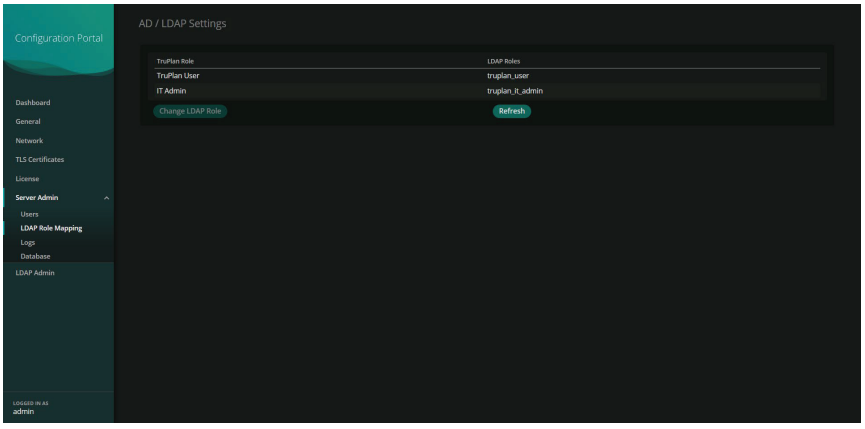
On the License, you can check the license options and take some actions like renew licenses.

viii. Server Admin -> Users



On the Server Admin, you can add new users into the server. There are two roles available: TruPlan User which gives access to all functionality except Web Configurator and IT Admin which gives access to Web Configurator.

ix. Server Admin -> LDAP Role Mapping



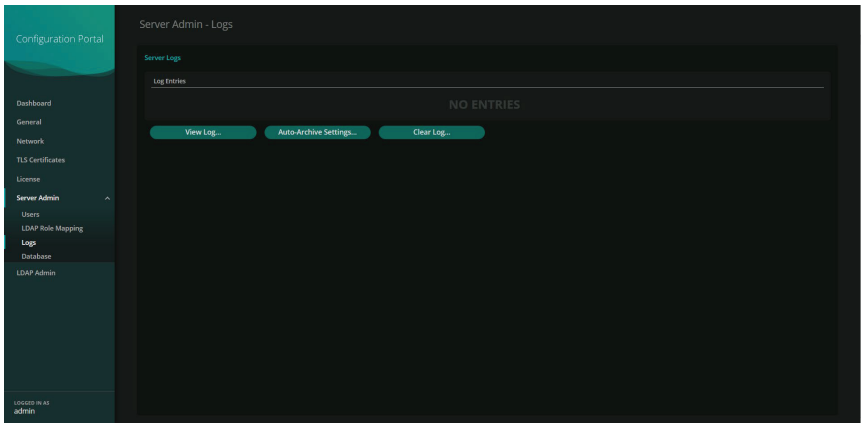
TruPlan has two roles available:

1. TruPlan User
2. IT Admin

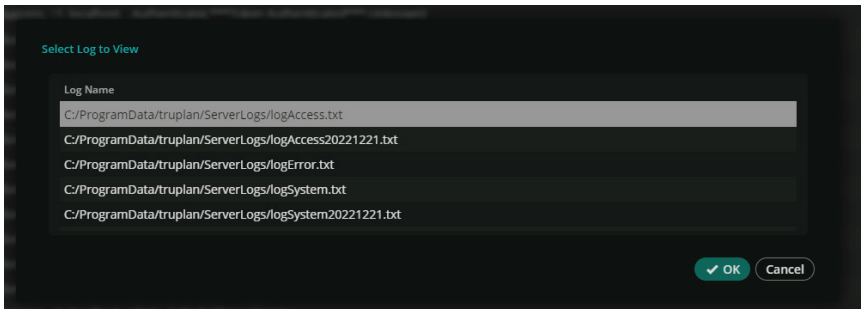
When connected to AD/LDAP, you need to make sure the AD/LDAP Roles are matching the Groups associated to TruPlan users you have setup in AD/LDAP.

You can select the role and click at ‘Change LDAP Role’ in case you need to change it.

x. Server Admin -> Logs

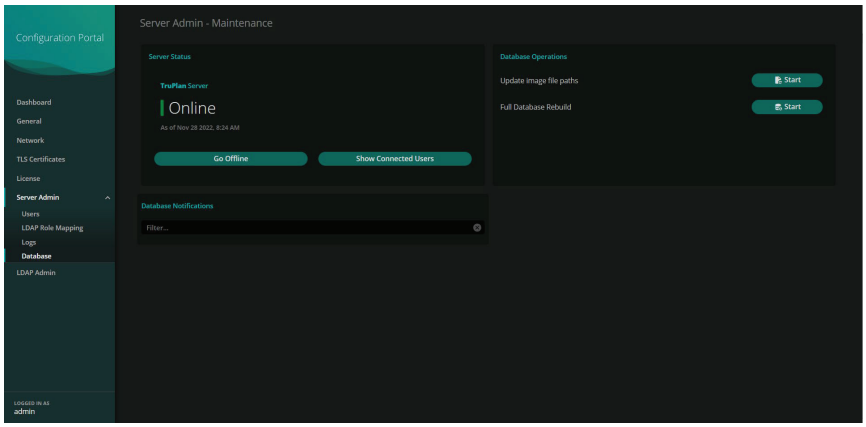


You can View and manage TruPlan server logs from this option.



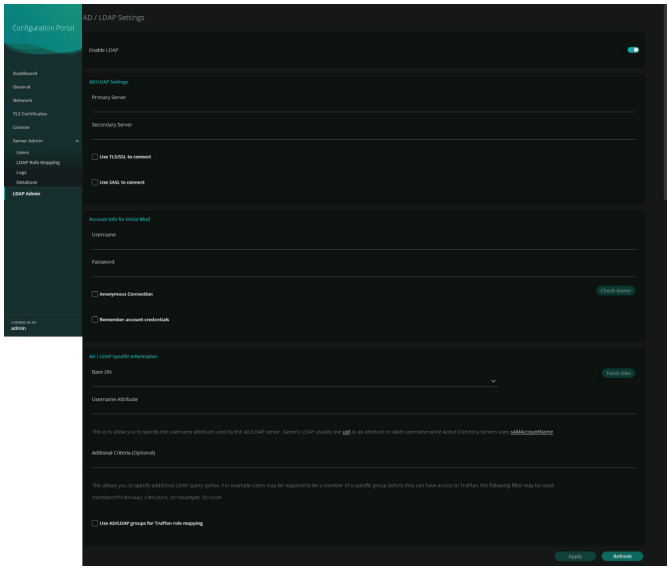
When you click View Log, you get a list of logs you can Visualize:

xi. Server Admin -> Database



In this interface, you can manage the database of TruPlan server.

xii. LDAP Admin



Users with 'IT Admin' role, can set up the configuration for Active Directory (AD) or LDAP integrated password authentication. This feature allows users to log into TruPlan with their existing user credentials assigned by their organization's IT team.

The LDAP Admin menu option allows the System Administrator to authenticate users against an AD or LDAP server. To connect to an AD or LDAP server, TruPlan needs the following information.

- Enable LDAP– When turned on enables the configured LDAP for user authentication and authorization.
- Primary Server, Secondary Server – IP address or fully qualified domain name for the AD or LDAP server.
- Use TLS/SSL to connect– When checked, the LDAP connection will be made over TLS. Contact the site IT or AD/LDAP server administrator for certificate files and configuration steps).

- Username – The username of the LDAP Bind account used by the TruPlan server to communicate with the integrated AD or LDAP server. Current only UPN format is supported (Universal Principal Name) - A UPN consists of a UPN prefix (the user account name) and a UPN suffix (a DNS domain name). The prefix joins the suffix using the "@" symbol. For example, someone@example.com:
    - o Active Directory: When configuring the username value for AD, it will be a userPrincipalName(TRUPLAN-BIND-ACCOUNT-NAME@DOMAIN-NAME) or sAMAccountName (DOMAIN-NAME\TRUPLAN-BIND-ACCOUNT-NAME).
    - o LDAP: When configuring the username value for LDAP integrations, the format of the username will be an LDAP distinguished name: (uid=<TRUPLAN-BIND-ACCOUNT>,ou=<specify each OU layer>,dc=<specify each DC layer>,dc=com)
- Password – The password of the AD/LDAP Bind account.
- Anonymous connection – When set, this will enable anonymous LDAP access.
- Use Bind Account for Study Request URL Authentication– (This is only applicable if the "shareURL" API is configured) When checked, study requests from URLs will be authenticated using the LDAP Bind Account. The LDAP Bind Account will be remembered and used to bind to an integrated AD/LDAP server for querying user accounts for each Study Request URL.
- Check Name– Use this button to verify that the configured AD/LDAP Bind Account authenticates.
- Base DN – Distinguished name of the location to search for AD or LDAP users.
- Fetch DNs – Use this button to fetch the DNs from the Base DN.
- Username Attribute – Specifies the AD/LDAP attribute used to indicate unique users.
    - o Active Directory: When configuring the username attribute value for AD integrations, use a unique parameter, such as sAMAccountName.
    - o LDAP: When configuring the username value for LDAP integrations, use the uid parameter.
- Advanced – This is an optional setting. It allows you to specify additional LDAP query syntax. For example, users may be required to be a member of a specific group to access TruPlan, as an example:
    - o memberOf=CN=truplan, CN=Users, DC=example, DC=com
- Use AD/LDAP groups for TruPlan role mapping – This setting determines whether TruPlan should use the integrated AD/LDAP server for user authentication and authorization (role mapping) or just for authentication. If this option is disabled, users logging in need to be listed in the Truplan user list and user permissions are determined using TruPlan.

Below is a table outlining the User Account linking behaviour:

User in AD/LDAP	User in TruPlan	User Account Linked	Password Used	Comments
Y	Y	Y	AD/LDAP	User is in both the TruPlan user list and in the integrated AD/LDAP server; uses the AD/LDAP password and is provided access.
Y	N	Y	AD/LDAP	User is in only in the integrated AD/LDAP server and uses the AD/LDAP password to log into TruPlan. The user will be provided access and a New User is created in the TruPlan user list and the user account is linked to the AD/LDAP user account.
Y	Y	N	AD/LDAP	User will then be converted to an AD/LDAP account
Y	Y	N	Local	This will not convert user to AD/LDAP user
N	Y	N	Local	
Y	Y	Y	Local	Needs to authenticate with AD/LDAP password
Y	N	N	Wrong	Needs to authenticate with correct AD/LDAP password
N	N	N	Any	

SUPPORT

For technical questions please contact our team by phone or e-mail:

North America
Circle Cardiovascular Imaging Inc.
1100, 800 5th Avenue SW Calgary
Alberta, Canada, T2P 3T6
P: +1 403 338 1870

Europe
Circle Cardiovascular Imaging B.V.
Europe Support Phone: + 31 (800)265 8982

Report a problem: support@circlecvi.com

Website: www.circlecvi.com