

CVi42[®]

v.5.16

Client Server Installation and Configuration Guide

cvi42

CLIENT SERVER INSTALLATION AND CONFIGURATION GUIDE

December 2022



Manufactured by
Circle Cardiovascular Imaging Inc.
#1100, 800 - 5th Avenue SW
Calgary, Alberta
Canada T2P 3T6

Telephone: 1 (403) 338-1870

Support: support@circlecvi.com

<http://www.circlecvi.com>



© Copyright 2022 Circle Cardiovascular Imaging Inc.

cvi42 is a registered trademark of Circle International Corporation in Canada and/or other countries.

The information contained herein is subject to change without notice. The only warranties for Circle products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be constructed as constituting an additional warranty. Circle shall not be liable for technical or editorial errors or omissions contained herein.

1.	<i>Installing cvi42</i>	6
1.1.	Non-silent Client Installation	6
1.2.	Server Installation on Windows Platform	13
1.2.1.	Services Installed	25
1.3.	Silent installation of cvi42 client	26
1.3.1.	Optimizing System Performance on Windows Platform	26
2.	<i>Activating cvi42 Licensing</i>	28
2.1.	Activating Your Installation	28
2.1.1.	Offline Activation Method	31
2.2.	Configure cvi42 client to connect to the Server	32
2.3.	Enabling TLS in cvi42	35
2.4.	Setting Up User Accounts	37
2.5.	Setting Up Roles	38
2.6.	Assigning ADAS 3D User Role	39
3.	<i>Configure Antivirus Software</i>	40
4.	<i>Configure DICOM Networking (PACS Connections)</i>	40
5.	<i>Active Directory/LDAP Integrated Password Authentication</i>	42
5.1.	User Account Linking	45
6.	<i>Command-line Integration</i>	45
6.1.	Overview	45
6.2.	Client and Server Integration Workflow	46
6.3.	Command Line Parameters	47
6.4.	Launching cvi42	47
7.	<i>Server Configuration (cvi42serverconfig.ini explained)</i>	48
7.1.	General Properties	48
7.2.	PPU Properties	50
7.3.	DICOM Network	51
7.4.	AD/LDAP Integrated Password Authentication	52
7.5.	Server-side processing configuration (Node42)	53
8.	<i>cvi42 Configuration Portal</i>	53
9.	<i>Housekeeping</i>	60

9.1. Overview.....	60
9.1.1. Rule matching	60
9.1.2. Rule execution	61
9.2. Rules	61
9.2.1. Criteria	61
9.2.2. Actions	63
9.2.3. Recurrence	65
9.3. Rule Editor	65
9.3.1. Simulation	67
9.4. Settings	68
<i>Appendix A: cvi42 Default Roles.....</i>	<i>71</i>
<i>Appendix B: cvi42 Network Communications Matrix</i>	<i>72</i>
<i>Appendix C: Converting cvi42/Report Users to built-in cvi42 users.....</i>	<i>72</i>

1. Installing cvi42

This guide is designed for fresh installation only of client/server.



IMPORTANT: For all updates from 5.14 or earlier, customers will need to schedule a guided update with Circle's Customer Support Team at support@circlecvi.com



PRE-REQUISITE: When installing **cvi42** on Windows N, you should have **Media Feature Pack** installed on your Windows before installing **cvi42**.

There are two methods to install **Media Feature Pack**:

1. From Windows Settings:
<https://support.microsoft.com/en-us/windows/media-feature-pack-for-windows-n-8622b390-4ce6-43c9-9b42-549e5328e407>
2. Downloading and installing it manually:
<https://www.microsoft.com/en-us/software-download/mediafeaturepack>

After installation, you should restart your PC to install **cvi42**.

1.1. Non-silent Client Installation

Recommended System Specification for Client Installation		
Requirement	MR Requirements ³	CT / Advanced Visualization Requirements ³
Operating System	<u>Windows:</u> 10, 11 <u>MacOS:</u> 11.x, 12.x	<u>Windows:</u> 10, 11 <u>MacOS:</u> 11.x, 12.x
Network (LAN)	1 Gb/s Ethernet	1 Gb/s Ethernet
Network (WAN) for server	N/A	N/A
Display	1920x1080	1920x1080
Processor	<u>Windows:</u> Intel Core i5 7th gen+ <u>MacOS:</u> Intel Core i5 7th gen+ , Apple Silicon M1 or later	<u>Windows:</u> Intel Core i5 7th gen+ <u>MacOS:</u> Intel Core i5 7th gen+ , Apple Silicon M1 or later

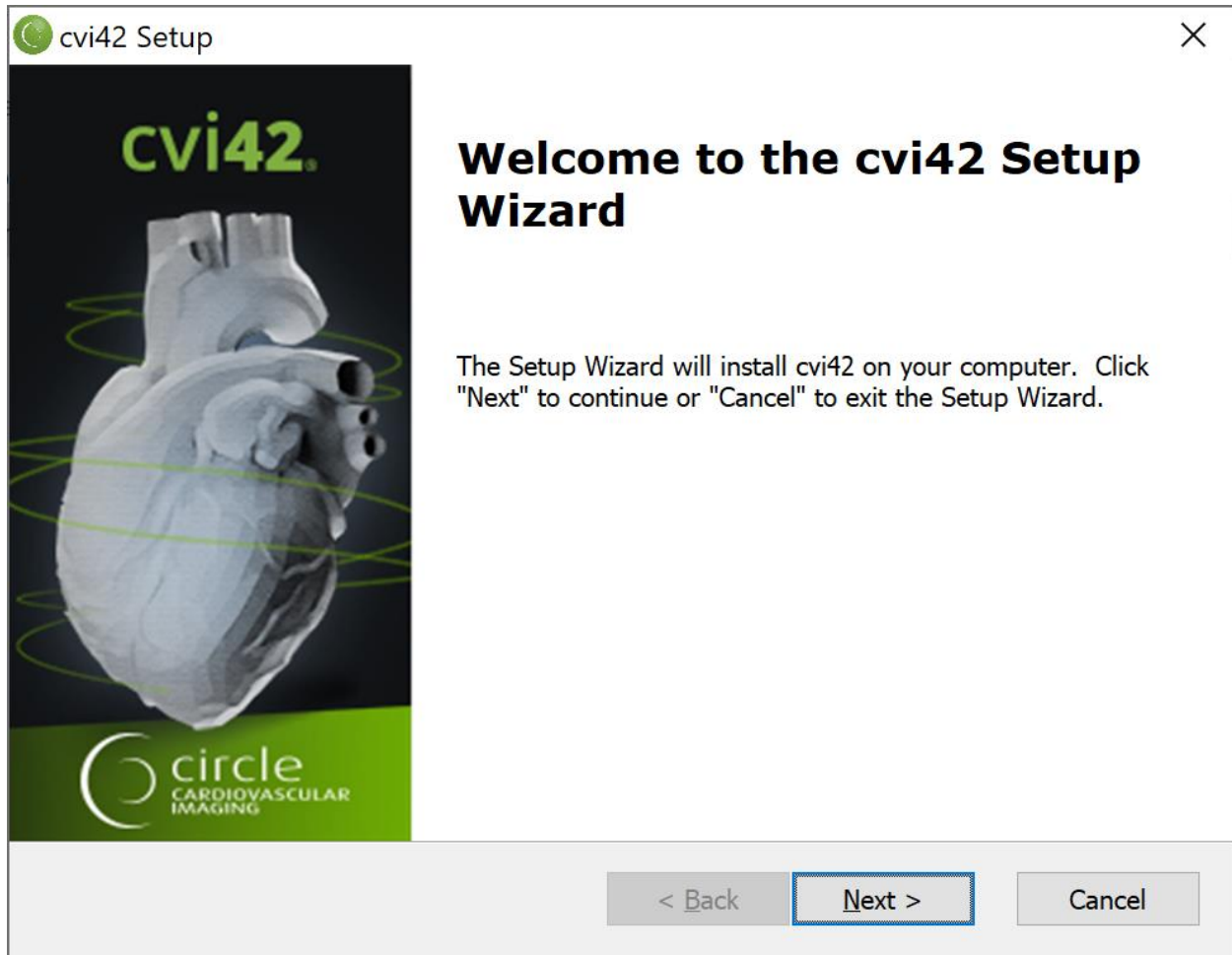
Video Card ^{1,2,3}	Intel Integrated HD Graphics 630+	Discrete nVidia GeForce 10 series, AMD Radeon R9 M370X or better
System RAM ¹	<u>4D Flow Module requires:</u> 16 GB+ <u>All other MR Modules:</u> 8 GB+	<u>CT Modules requires:</u> 16 GB+
Video RAM	N/A	2 GB+ RAM
Disk Space/Performance	5GB SSD/NVMe	5GB SSD/NVMe

Notes:

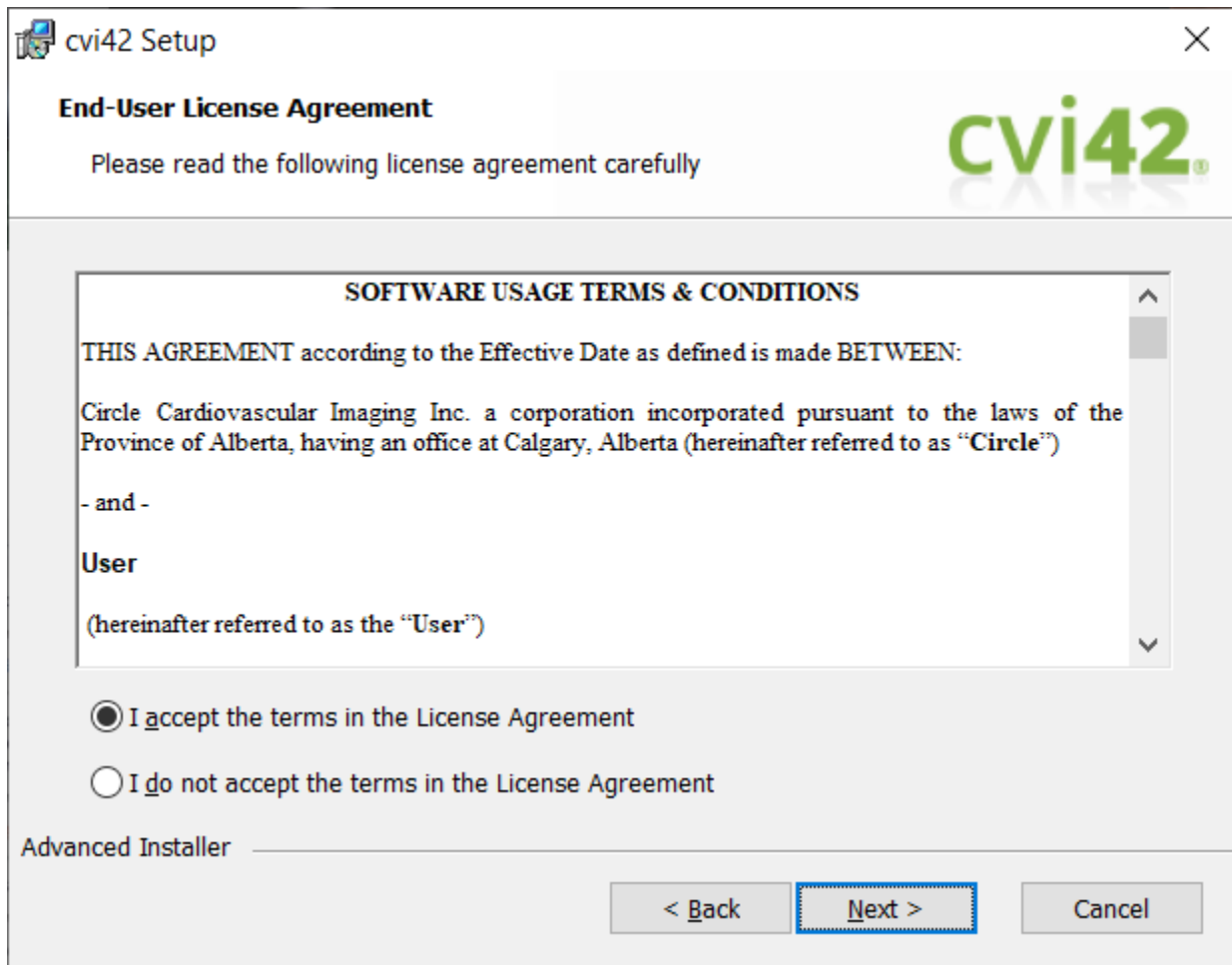
- ¹ 3D/4D dataset viewing capability varies based on series size and amount of available RAM and VRAM. A system capable of viewing 3D is automatically capable of viewing 2D images.
- ² System requires 24-bit color depth to use the client software.
- ³ Discrete graphics hardware is recommended for large datasets and modules with advanced 4D visualization capabilities.

To install **cvi42**, you should download and run the setup program, which will automatically perform all the necessary configuration steps.

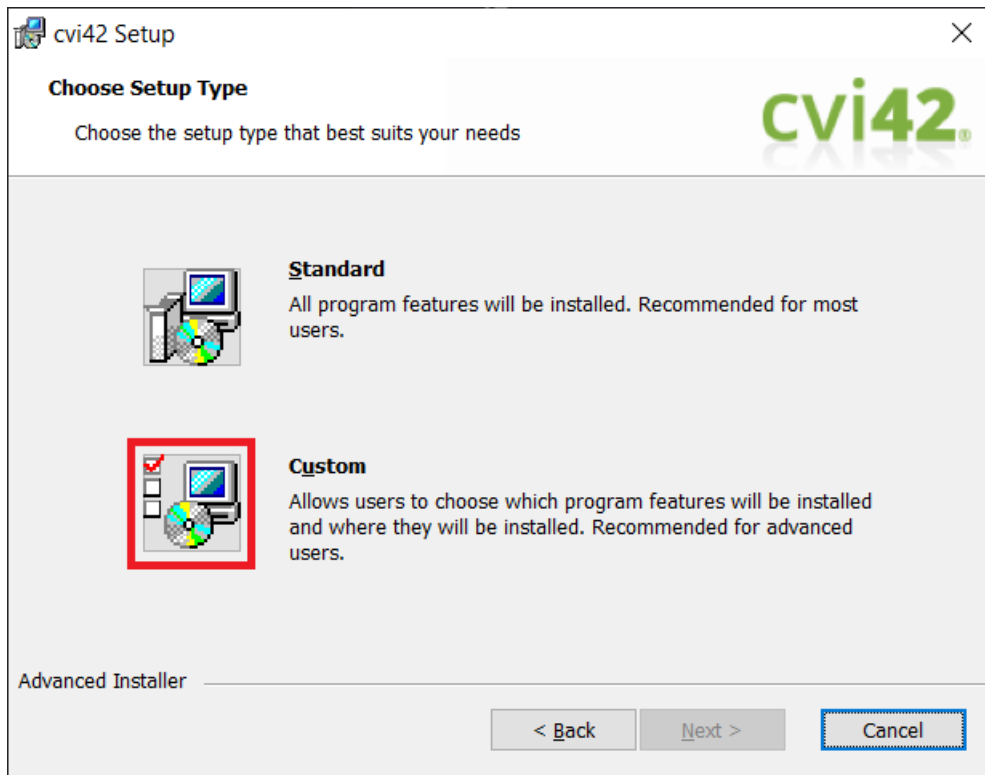
You will need to log in to an account with administrator privileges on the machine you are installing to.



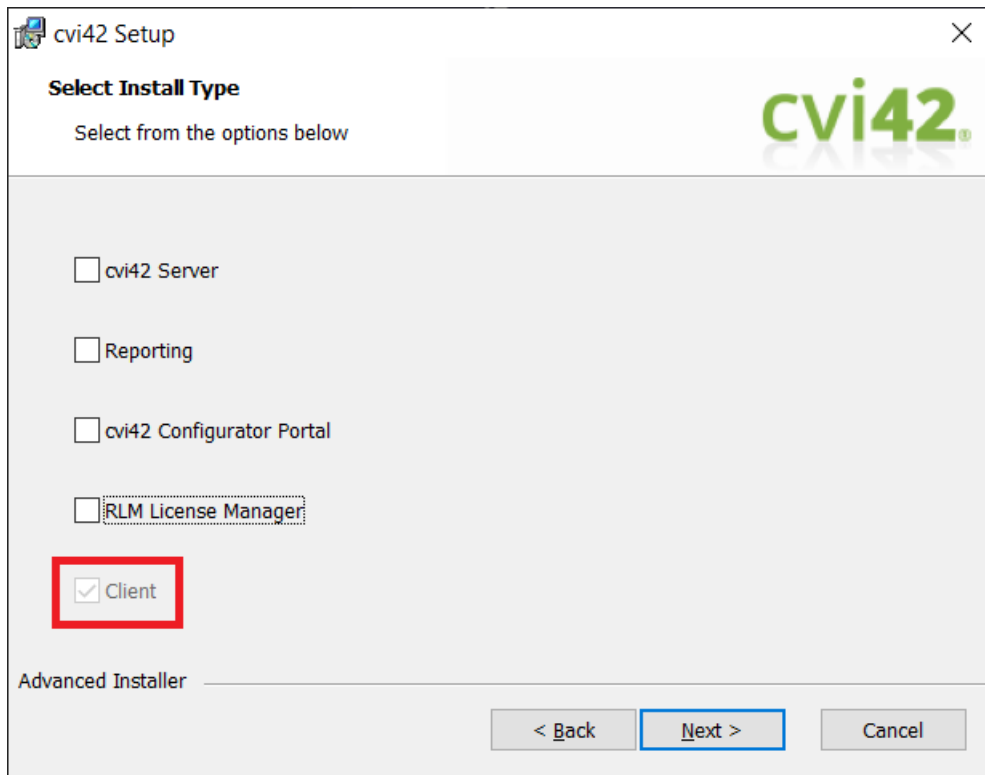
Click *Next* to continue.



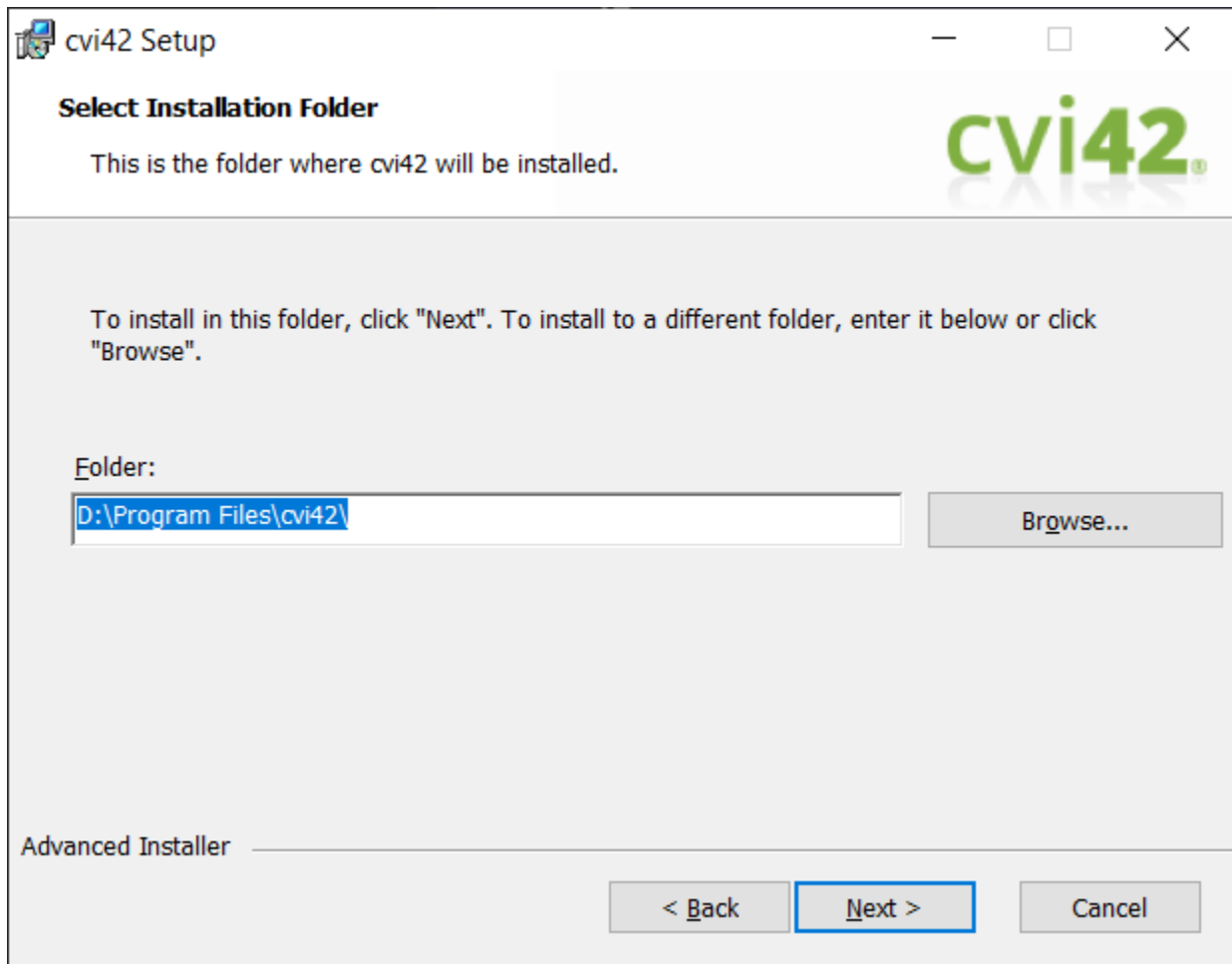
You should read, accept the License Agreement, and click *Next* to continue.



Select *Custom* option and click *Next* to continue.

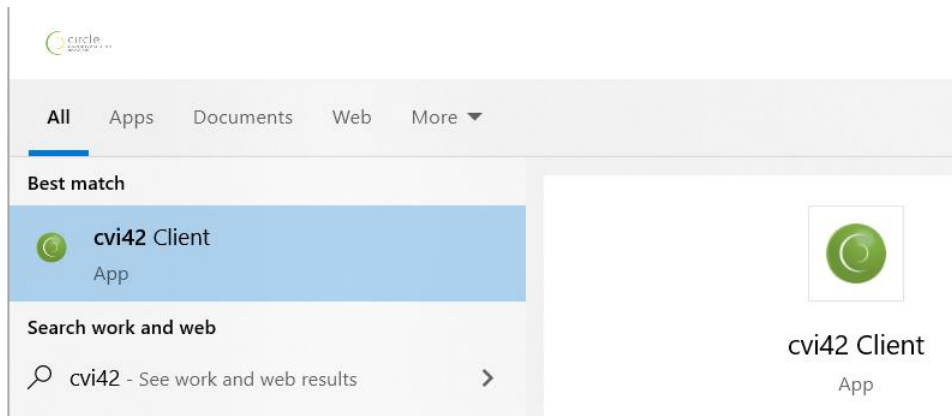


Leave just *Client* option checked, and click *Next*



Select the installation folder and click *Next*

You can now access **cvi42** from Windows Start menu:



1.2. Server Installation on Windows Platform



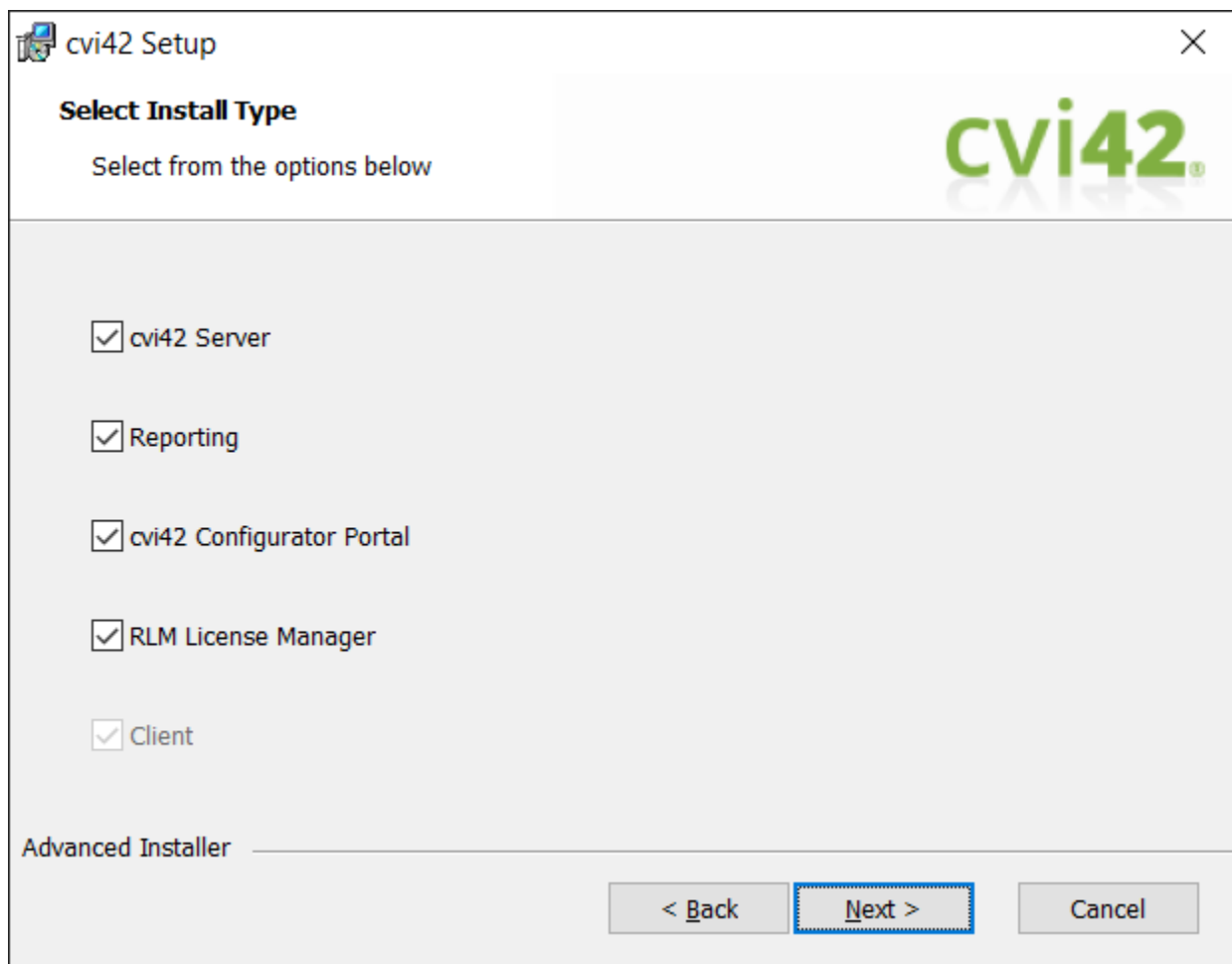
IMPORTANT: On the table below, you can find the Recommended System Specification for Server Installation with up to 4 concurrent users. For advice on larger deployments please contact Circle's Technical Support Team at support@circlecvi.com.

Recommended System Specification for Server Installation		
Requirement	Server MR Requirements	Server CT Requirement
Operating System	Windows Server 2016, Windows Server 2019, Windows Server 2022	Windows Server 2016, Windows Server 2019, Windows Server 2022
Network (LAN)	10 Gb/s Ethernet	10 Gb/s Ethernet
Processor	Intel Server Class, >= 3rd previous generation, 8 vCPU	Intel Server Class, >= 3rd previous generation, 12 vCPU
System RAM	16 GB	16 GB
Disk Space/Performance	200GB SSD/NVMe, 500 iops A dedicated partition for data storage is recommended.	200GB SSD/NVMe, 500 iops A dedicated partition for data storage is recommended.

Notes:

- Minimum requirements are not meant to imply that the application will meet end-user performance expectations.
- Based on vendor support for operating systems, Windows version lower than what is specified are not generally supported.
- With Node42 turned on with CT studies, the CPU usage of server shows 30% increase, and 20% increase in memory usage.

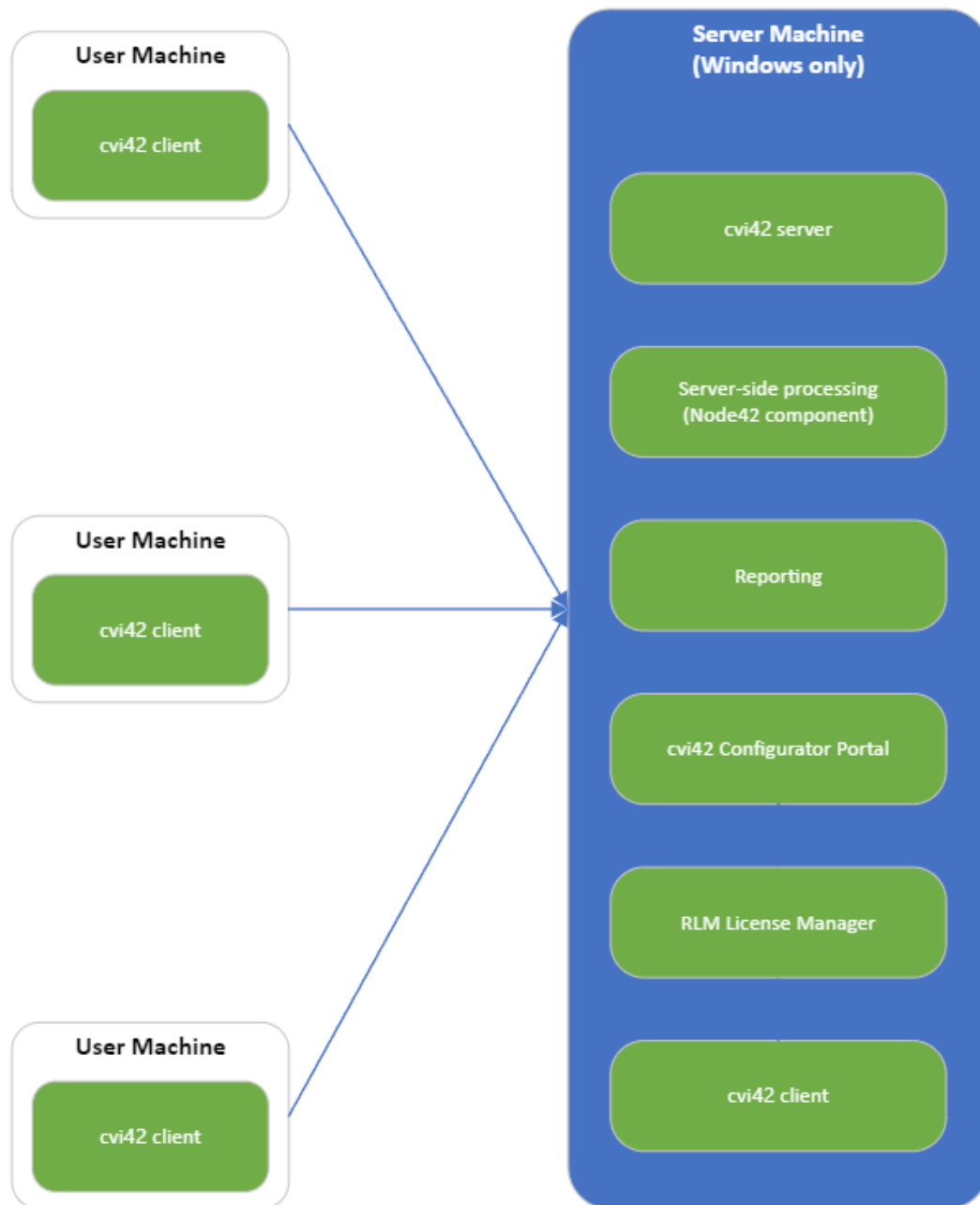
For the **cvi42** Server Installation, you may select the Custom option during installation, where you can select from a list of components to install:

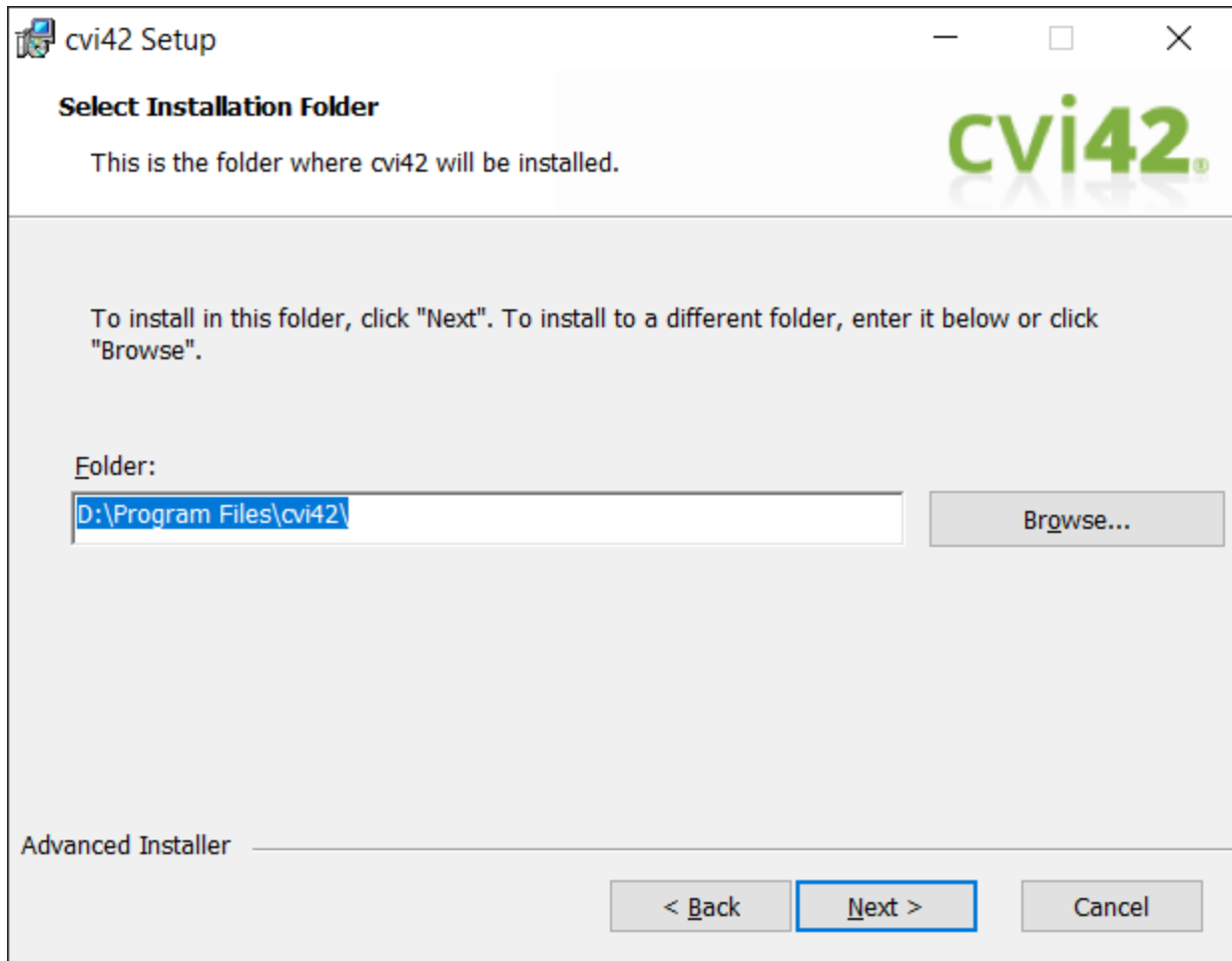


When **cvi42** is installed, the Server-side processing component (Known as Node42), is installed together, on the same machine.

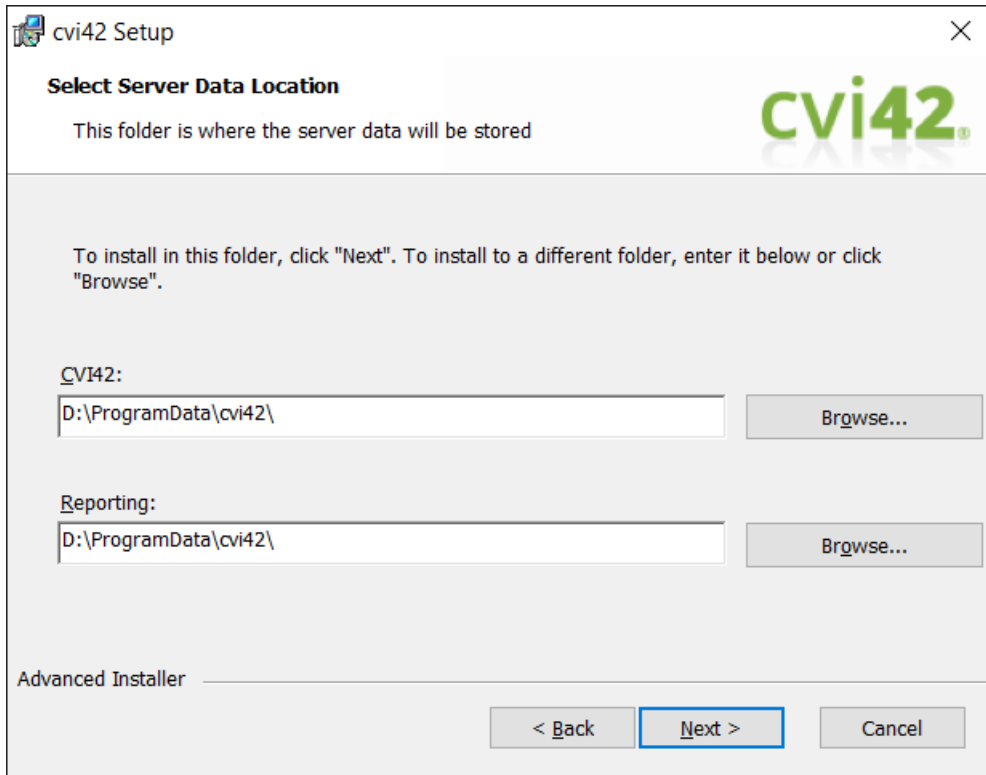
Click Next.

For the most basic setup on an Enterprise environment, you will have the server components being installed on a single server with Clients connected to it from remote computers:





Select the installation folder and then click *Next*.



The image shows a screenshot of the 'cvi42 Setup' window. The title bar says 'cvi42 Setup' with a close button. The main heading is 'Select Server Data Location'. Below it, a text box says 'This folder is where the server data will be stored'. To the right is the 'cvi42' logo. A paragraph of instructions reads: 'To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".' There are two input fields: 'Cvi42:' and 'Reporting:'. Both contain the text 'D:\ProgramData\cvi42\'. To the right of each field is a 'Browse...' button. At the bottom left, it says 'Advanced Installer'. At the bottom right, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

cvi42 Setup

Select Server Data Location

This folder is where the server data will be stored

cvi42

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

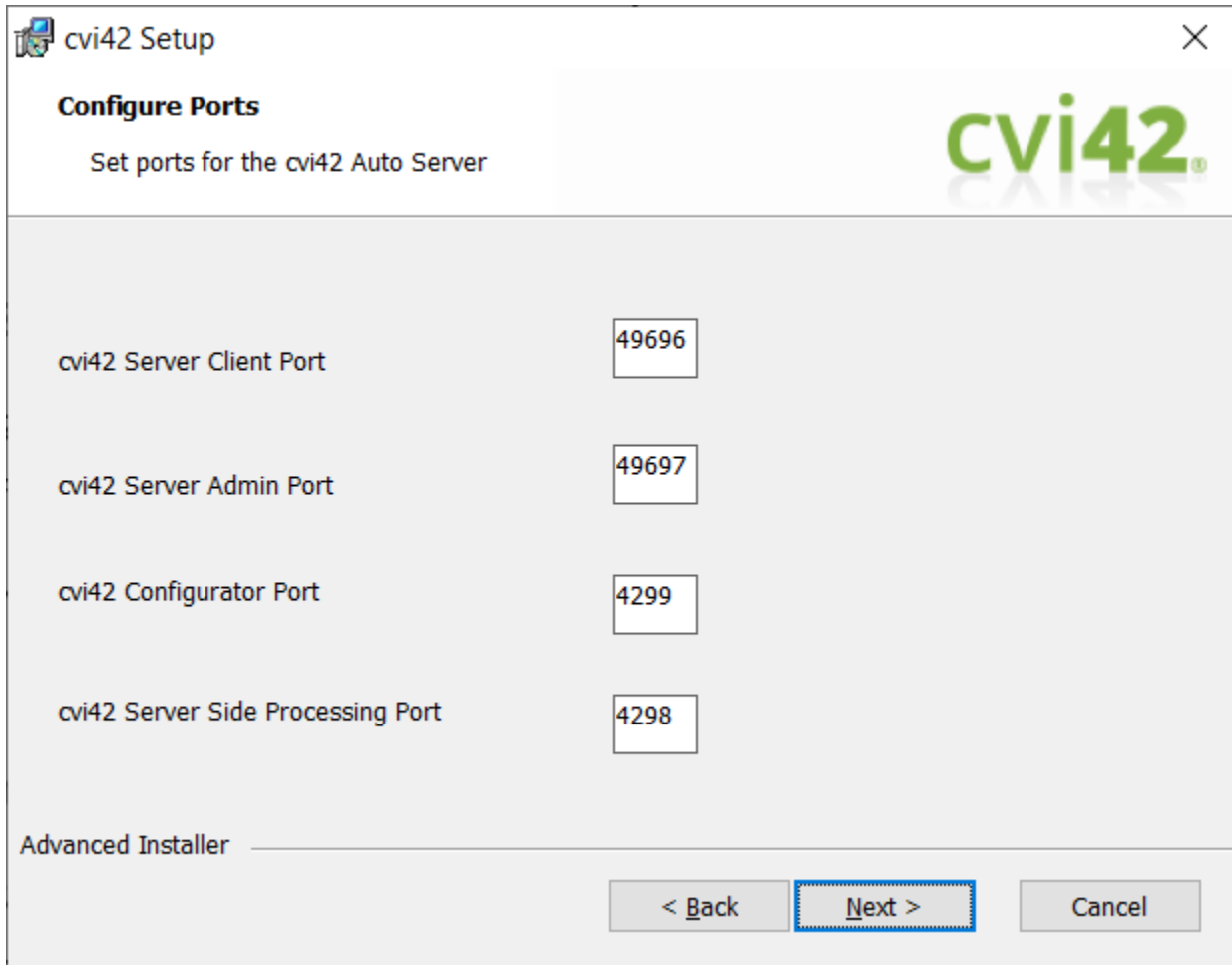
Cvi42:
D:\ProgramData\cvi42\ Browse...

Reporting:
D:\ProgramData\cvi42\ Browse...

Advanced Installer

< Back Next > Cancel

You can select different data folder for **cvi42** server and for the reporting. Then click *Next*.



The image shows a screenshot of the 'cvi42 Setup' window. The title bar says 'cvi42 Setup' with a close button. The main area is titled 'Configure Ports' with the subtitle 'Set ports for the cvi42 Auto Server'. The 'cvi42' logo is in the top right. Below, there are four rows of port configuration:

Port Name	Port Number
cvi42 Server Client Port	49696
cvi42 Server Admin Port	49697
cvi42 Configurator Port	4299
cvi42 Server Side Processing Port	4298

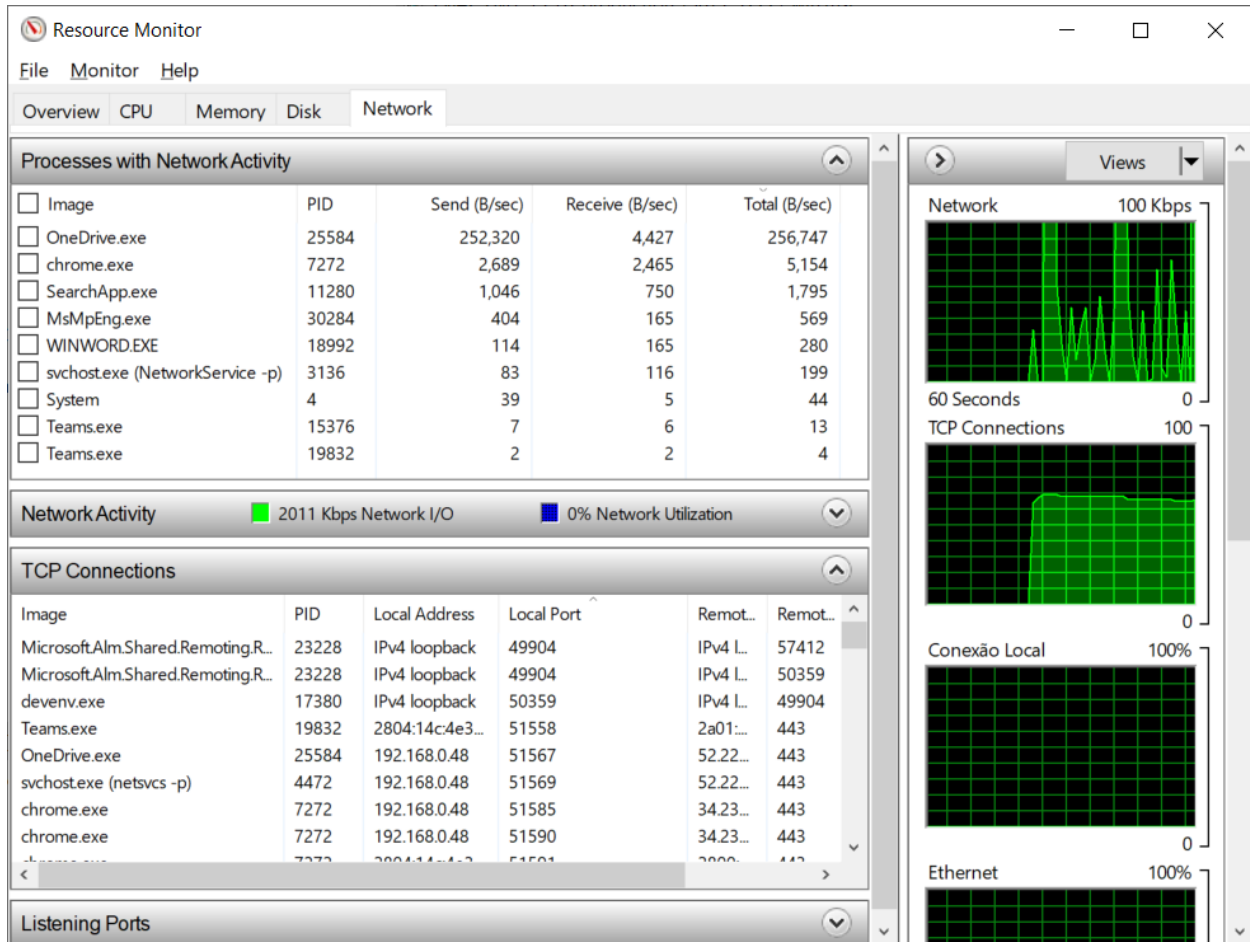
At the bottom, it says 'Advanced Installer' and has three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.



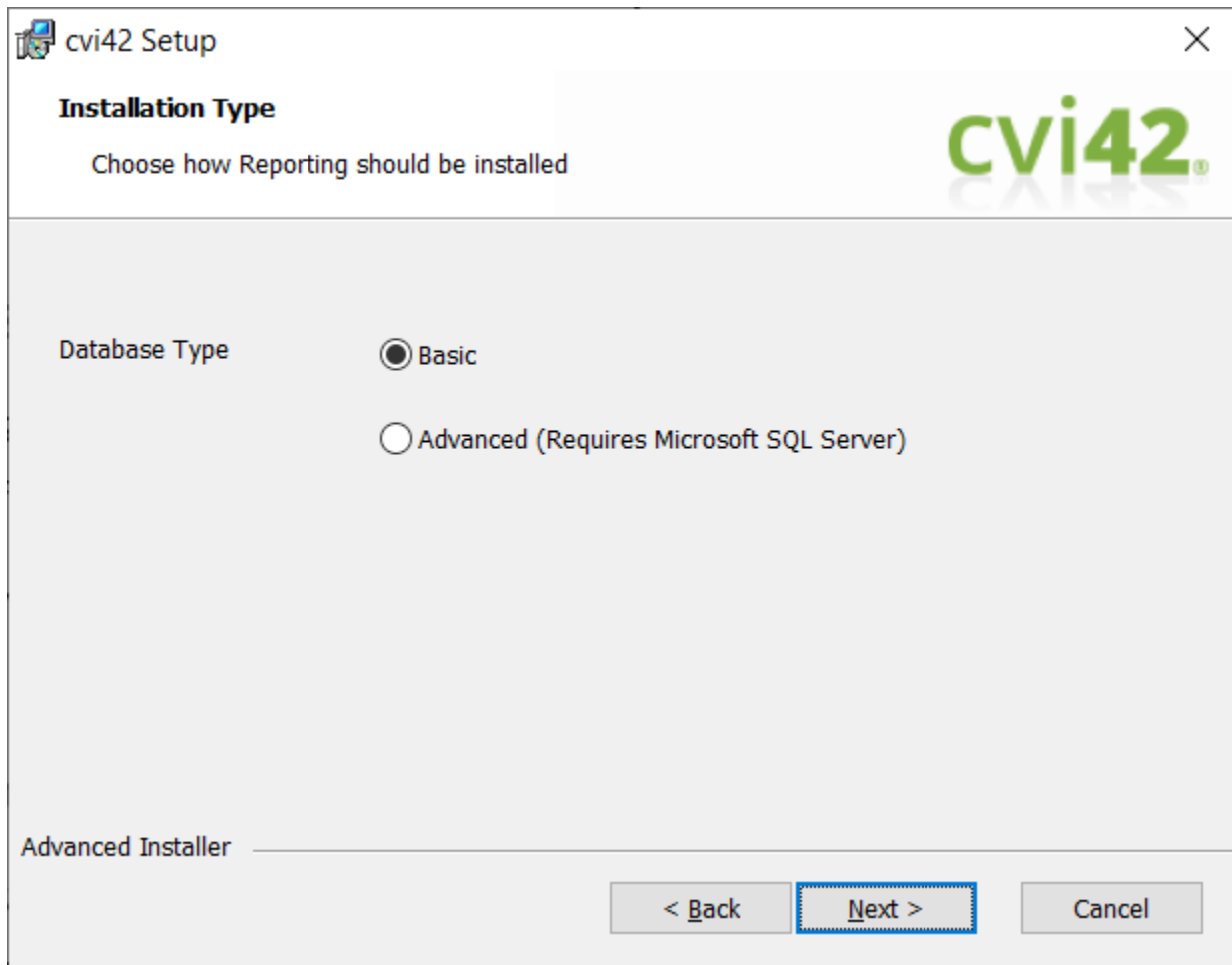
IMPORTANT: If you intend to change any of **cvi42** server ports, please be aware that this needs to be aligned in the **cvi42** client deployment.

Please ensure that the port is available on the computer, otherwise, service will fail to start.

To check if the port is being used, you can use the *Resource Monitor* on Windows:

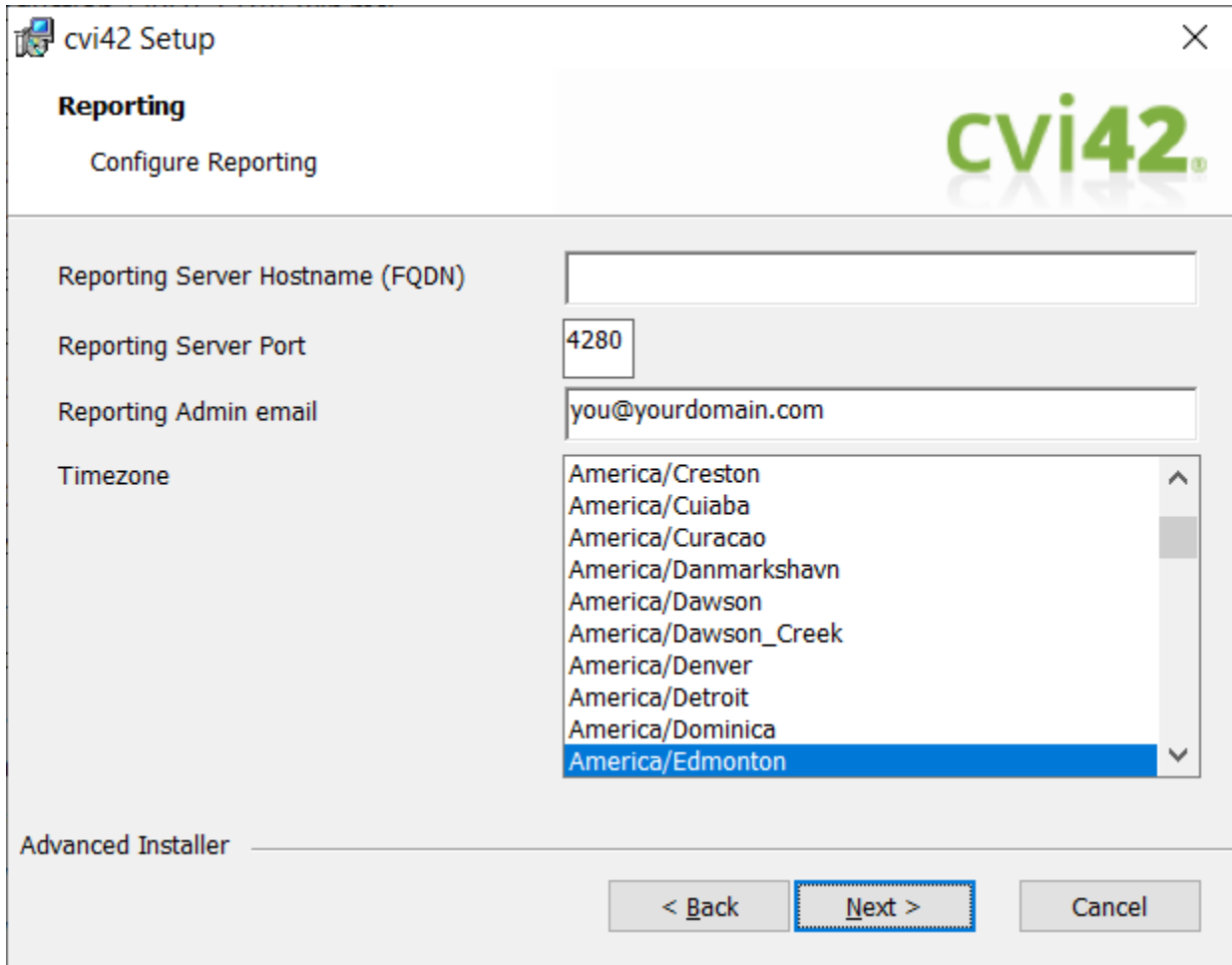


You can select Network tab, look at the TCP connections, and order the Local Port column, and just check if the port is being used there.



If you selected Reporting installation, you will be prompted to set up the report database, server, and other configuration details.

You can select a Basic Database, which is an SQLite database and no action is required in this case. Or you can select Advanced Database, which will require you to have a Microsoft SQL Server installed.



The image shows a Windows-style window titled "cvi42 Setup" with a close button in the top right corner. The window has a tab labeled "Reporting" and a subtitle "Configure Reporting". In the top right corner of the window, there is a large green "cvi42" logo. The main area of the window contains four configuration fields:

- Reporting Server Hostname (FQDN)**: A text input field that is currently blank.
- Reporting Server Port**: A text input field containing the value "4280".
- Reporting Admin email**: A text input field containing the value "you@yourdomain.com".
- Timezone**: A list box showing a scrollable list of timezones. The visible options are: America/Creston, America/Cuiaba, America/Curacao, America/Danmarkshavn, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, and America/Edmonton. The "America/Edmonton" option is currently selected and highlighted in blue.

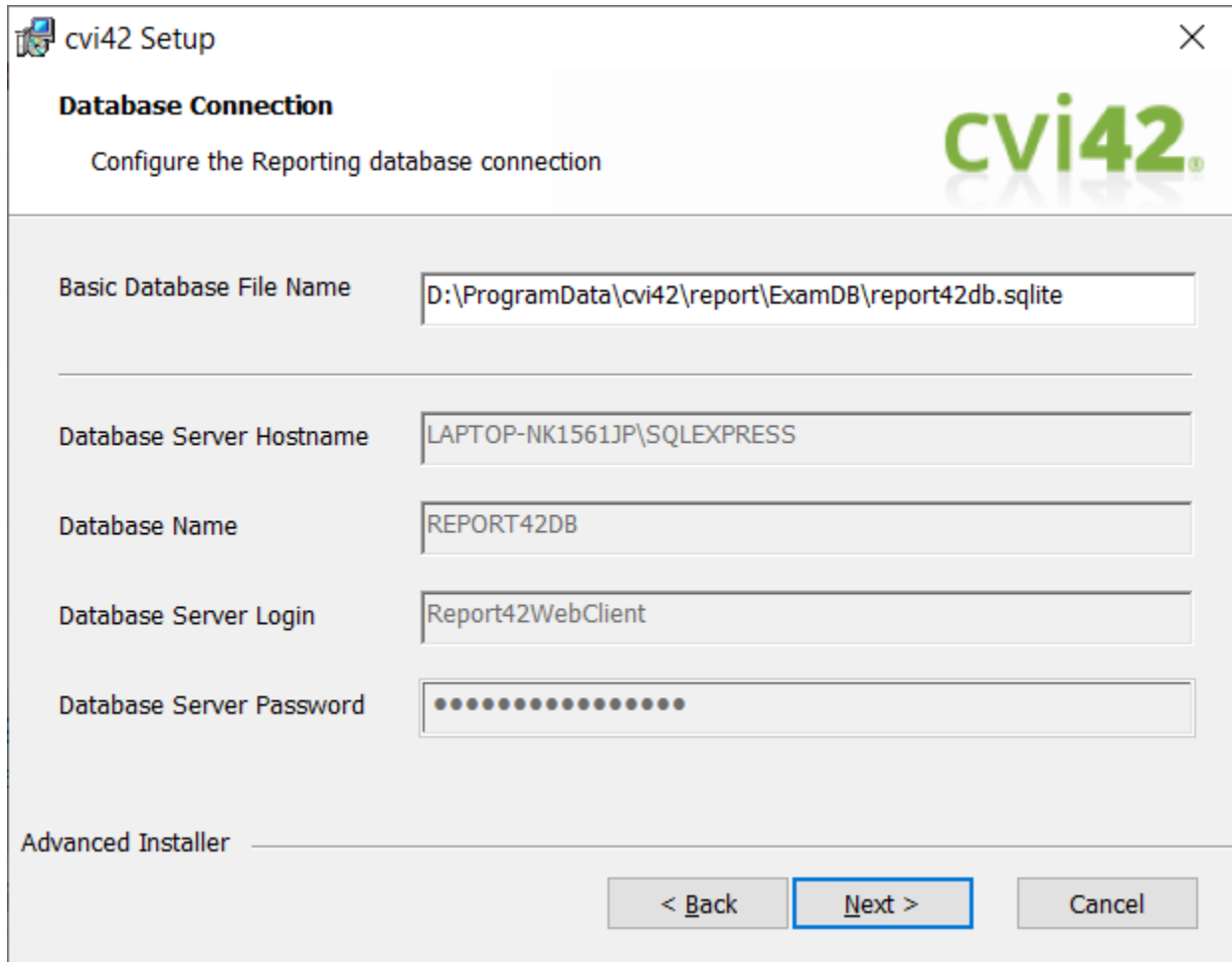
At the bottom left of the window, the text "Advanced Installer" is visible. At the bottom right, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

You can set a report FQDN or IP. If you left it blank, localhost (127.0.0.1) will be assumed.
You can also change the report port.

Report admin e-mail should be a valid e-mail, it sets the ServerAdmin field on the configuration file (httpd.conf of report Apache server)

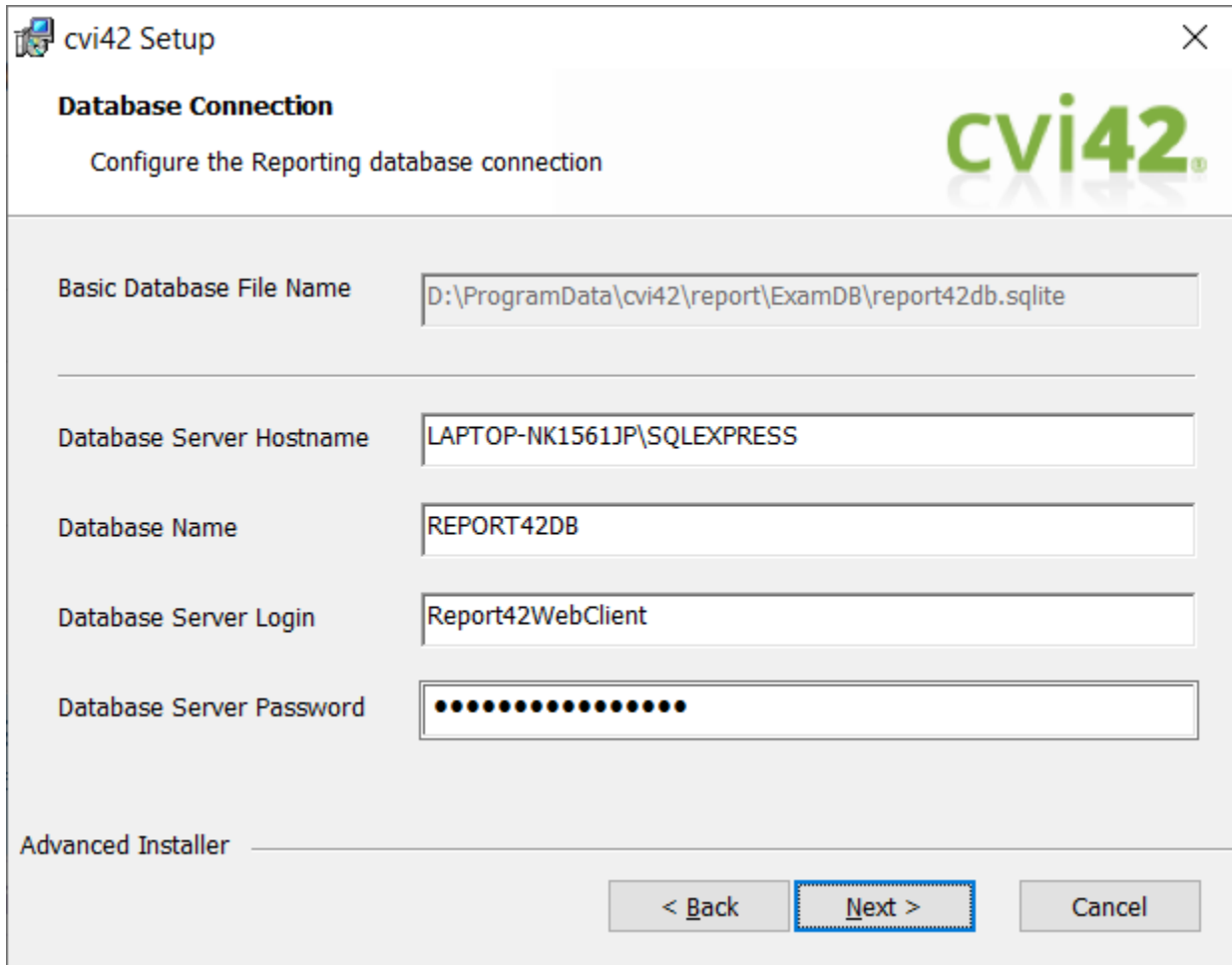
You need to select the Timezone the report date and time will be based on.

On the next screen, you can configure the database name, in case you selected Basic Database:



The image shows a Windows-style setup window titled "cvi42 Setup" with a close button (X) in the top right corner. The window has a light gray background. At the top, there is a section titled "Database Connection" with a subtitle "Configure the Reporting database connection". To the right of this section is the "cvi42" logo. Below the subtitle, there are five input fields, each with a label to its left: "Basic Database File Name" (containing "D:\ProgramData\cvi42\report\ExamDB\report42db.sqlite"), "Database Server Hostname" (containing "LAPTOP-NK1561JP\SQLEXPRESS"), "Database Name" (containing "REPORT42DB"), "Database Server Login" (containing "Report42WebClient"), and "Database Server Password" (containing a series of dots). At the bottom left, there is a section titled "Advanced Installer" with a horizontal line next to it. At the bottom right, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

Or set MS SQL Server properties in case you selected Advanced Database:



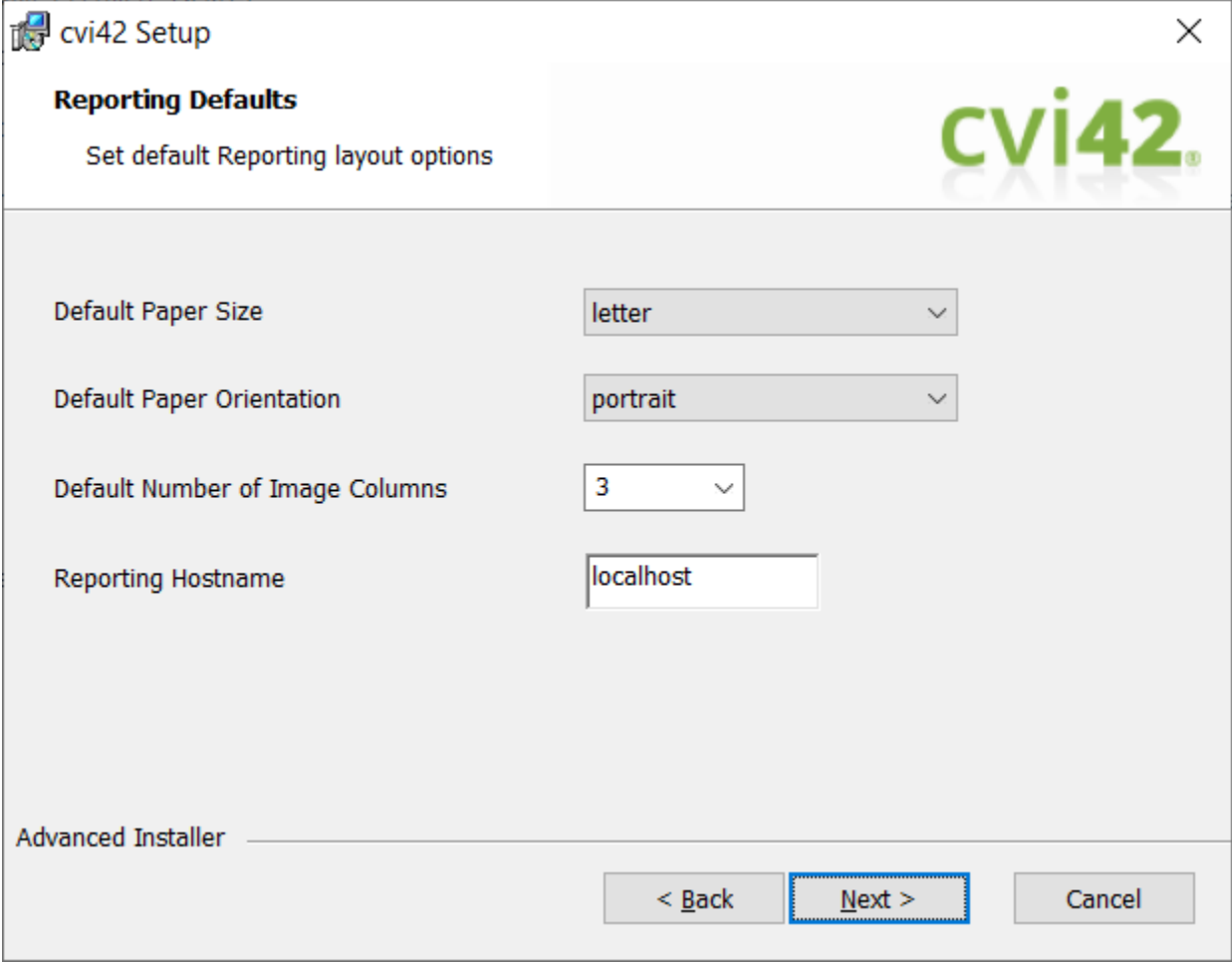
The image shows a screenshot of the 'cvi42 Setup' window. The title bar says 'cvi42 Setup' with a close button. The main heading is 'Database Connection' with a subtitle 'Configure the Reporting database connection'. The 'cvi42' logo is in the top right. There are five input fields: 'Basic Database File Name' with the path 'D:\ProgramData\cvi42\report\ExamDB\report42db.sqlite', 'Database Server Hostname' with 'LAPTOP-NK1561JP\SQLEXPRESS', 'Database Name' with 'REPORT42DB', 'Database Server Login' with 'Report42WebClient', and 'Database Server Password' which is masked with dots. At the bottom left is the 'Advanced Installer' section. At the bottom right are three buttons: '< Back', 'Next >' (which is highlighted with a blue dashed border), and 'Cancel'.

Field	Value
Basic Database File Name	D:\ProgramData\cvi42\report\ExamDB\report42db.sqlite
Database Server Hostname	LAPTOP-NK1561JP\SQLEXPRESS
Database Name	REPORT42DB
Database Server Login	Report42WebClient
Database Server Password	

Advanced Installer

< Back Next > Cancel

After the Reporting database connection setting, you can now change other configurations:



The image shows a Windows-style window titled "cvi42 Setup" with a close button in the top right corner. The window is divided into two main sections. The top section, titled "Reporting Defaults", contains the instruction "Set default Reporting layout options" and a large "cvi42" logo on the right. The bottom section, titled "Advanced Installer", contains four configuration options: "Default Paper Size" set to "letter", "Default Paper Orientation" set to "portrait", "Default Number of Image Columns" set to "3", and "Reporting Hostname" set to "localhost". At the bottom of the window are three buttons: "< Back", "Next >" (which is highlighted with a blue dashed border), and "Cancel".

cvi42 Setup

Reporting Defaults
Set default Reporting layout options

cvi42

Default Paper Size: letter

Default Paper Orientation: portrait

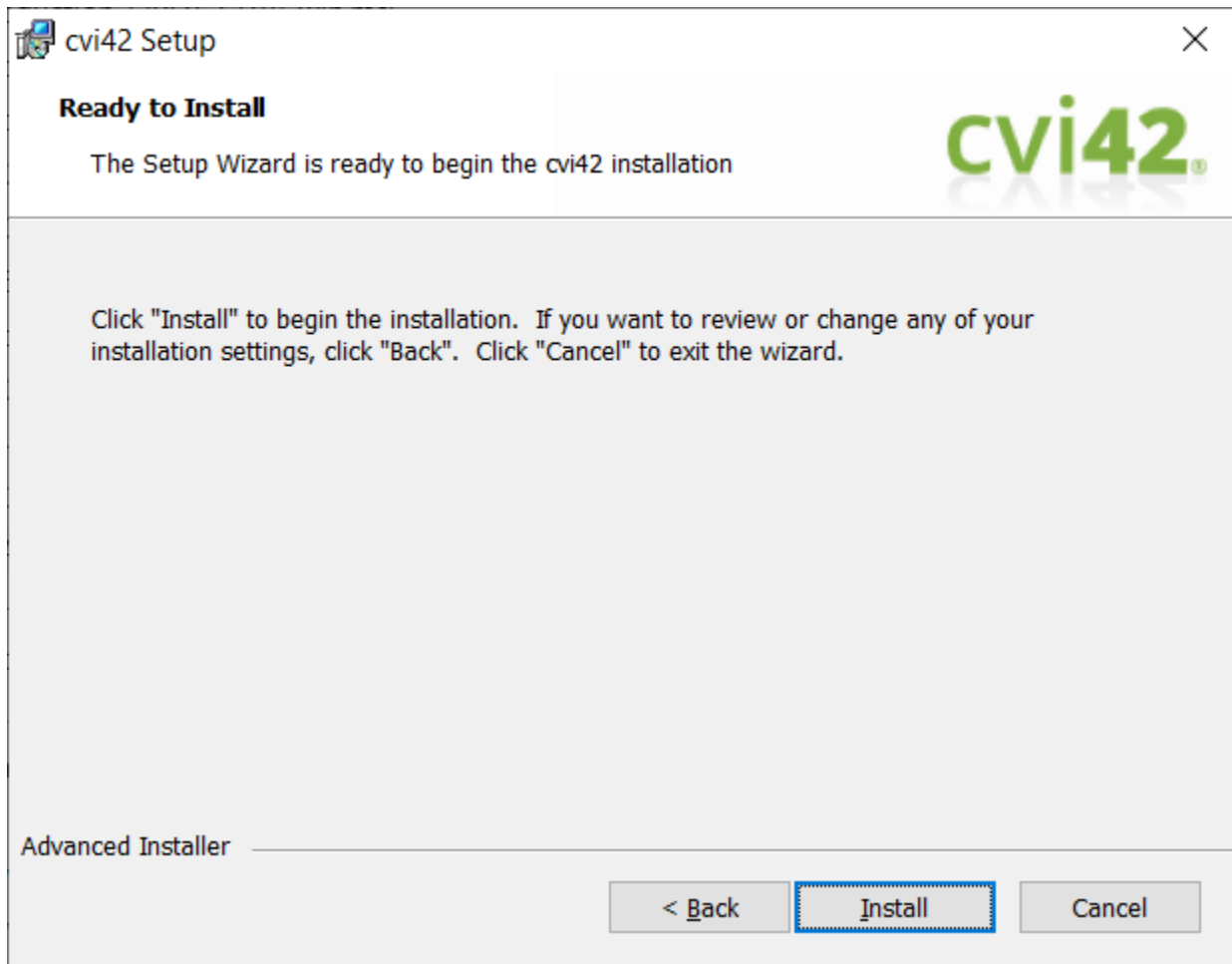
Default Number of Image Columns: 3

Reporting Hostname: localhost

Advanced Installer

< Back **Next >** Cancel

Click *Next*.



Click *Install* to complete the installation.

1.2.1. Services Installed

When all server components are installed, you will be able to see the following services running on Windows:

Installer Option	Service Name
cvi42 Server	cvi42 Server
Reporting	cvi42 Report Server cvi42 Report Go Server
cvi42 Configurator Portal	cvi42 Web Server
RLM License Manager	cvi42 License Server

1.3. Silent installation of cvi42 client

You can install **cvi42** client silently via command line.

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

To install **cvi42** with all default options, you can run this command:

```
msiexec /I "<msi file>" CVI42_LICENSE_AGREEMENT=true APPDIR="C:\Program Files\cvi42"  
INSTALL_CVI42SERVER=false INSTALL_REPORT42=false INSTALL_CVI42WEBSERVER=false  
INSTALL_RLM=false SERV_ADDR=<IP or FQDN where cvi42 server is installed>  
SERV_NAME="cvi42 Server" SERV_PORT=49696 /qn /Li tmp.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
- CVI42_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, you can check in the log file for the text: *Windows Installer installed the product.*

You can also uninstall the product through command line:

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

To see if product has been uninstalled, look for this text in the log file: *Windows Installer removed the product.*

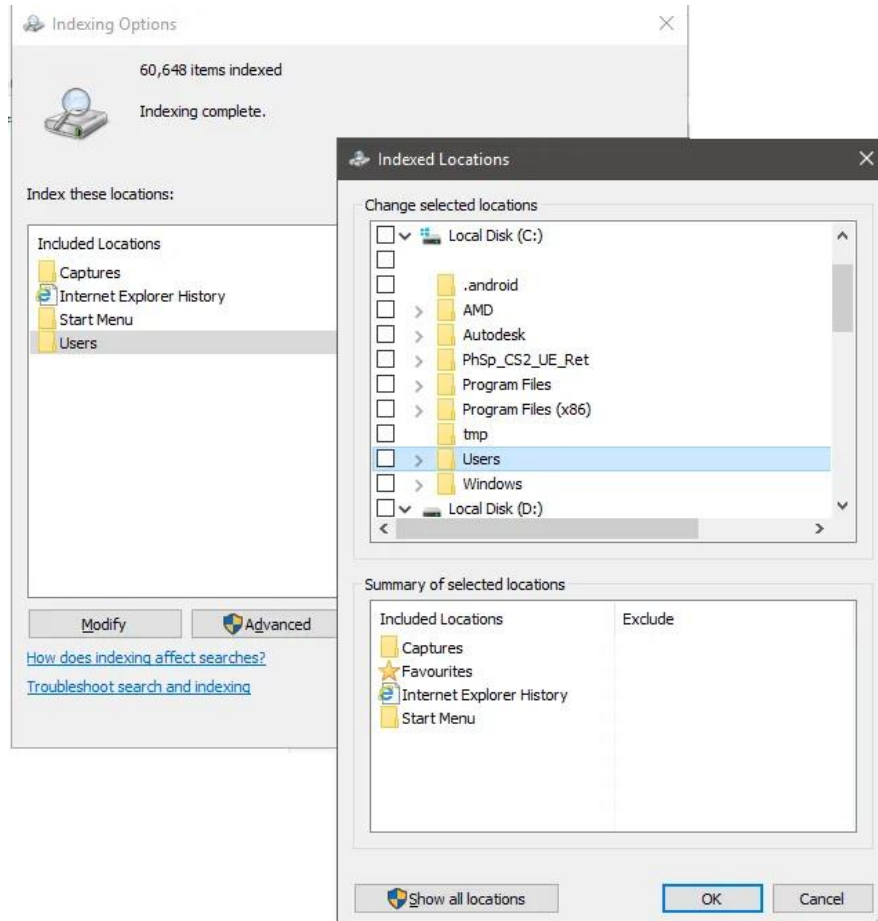
1.3.1. Optimizing System Performance on Windows Platform



IMPORTANT: In order to protect patient information, any drive directory which receives DICOM data should not be indexed.

Open the Start menu and type "Indexing", select indexing Options.

Select the "Modify" option and untick any drive directory which receives DICOM data.

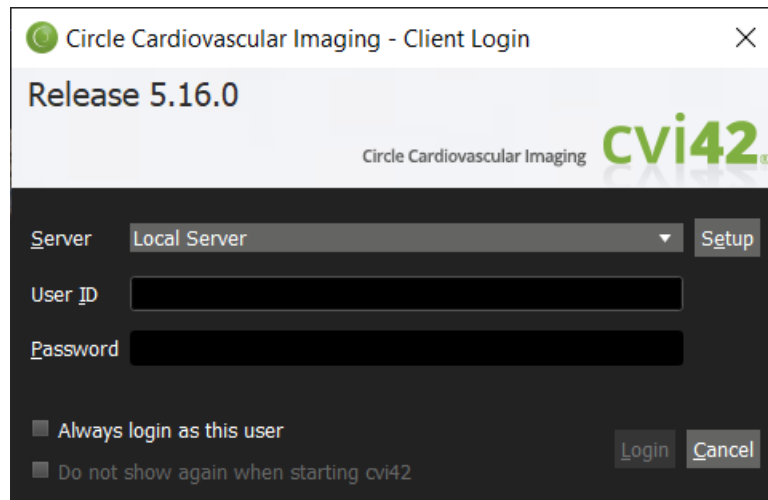


2. Activating cvi42 Licensing

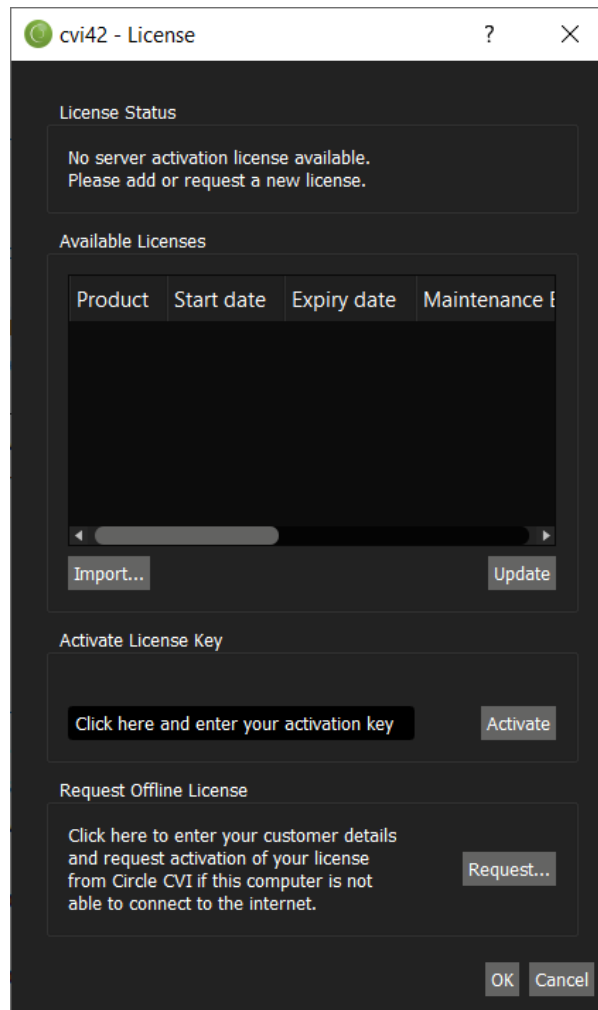
The typical way to activate **cvi42** is by obtaining an Activation Key from Circle CVI Support Team.

2.1. Activating Your Installation

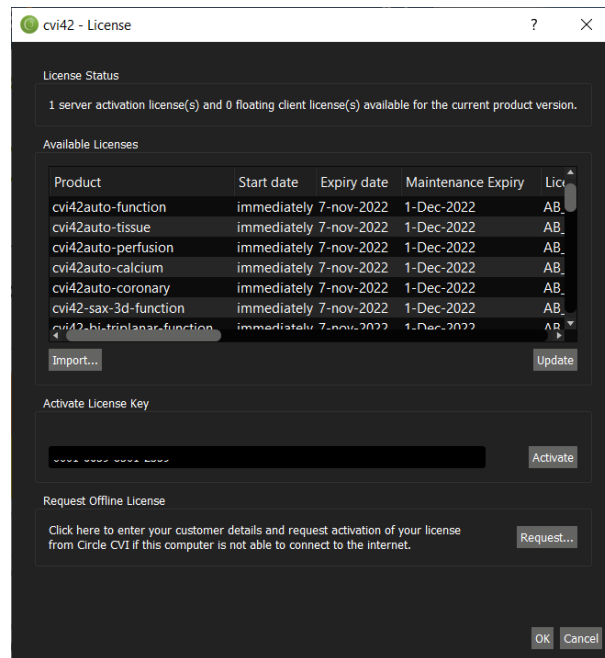
You should launch **cvi42** client on the server machine:



- The default User ID is *admin*, and the default password is *password*.
- Enter the User ID/Password information and click *Login*. **cvi42** will proceed to check for a valid license and display the license request dialogue.

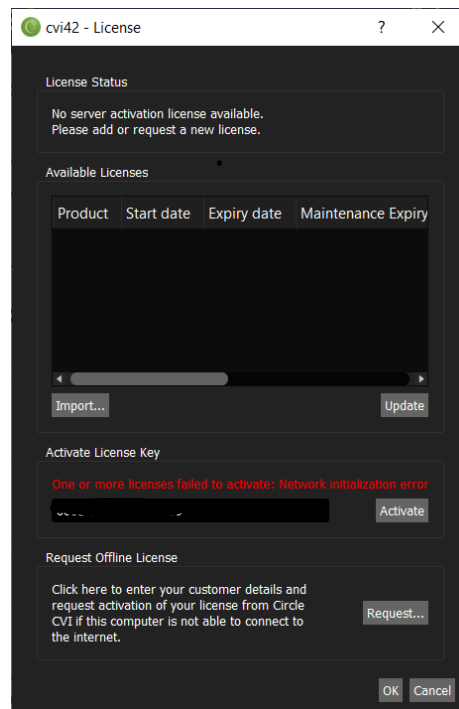


- Enter the Activation Key in the field Activate License Key field, and click *Activate*. If you are connected to the internet, you will see the list of Available Licenses filled in with all the licenses associated with your Activation Key:



By clicking *OK*, the application will open.

For any error during the activation, an error message will be presented in red color. The error message should be reported to Circle CVI Support Team, who can assist you with the problem:





IMPORTANT: If you are logged into Windows with a non-Administrator account, try to start the **cvi42** client as an administrator, by right-click on `cvi42.exe` and choose *Run As Administrator*. When you have successfully imported the license, exit the **cvi42** client, and restart `cvi42.exe` by double-clicking, as usual.

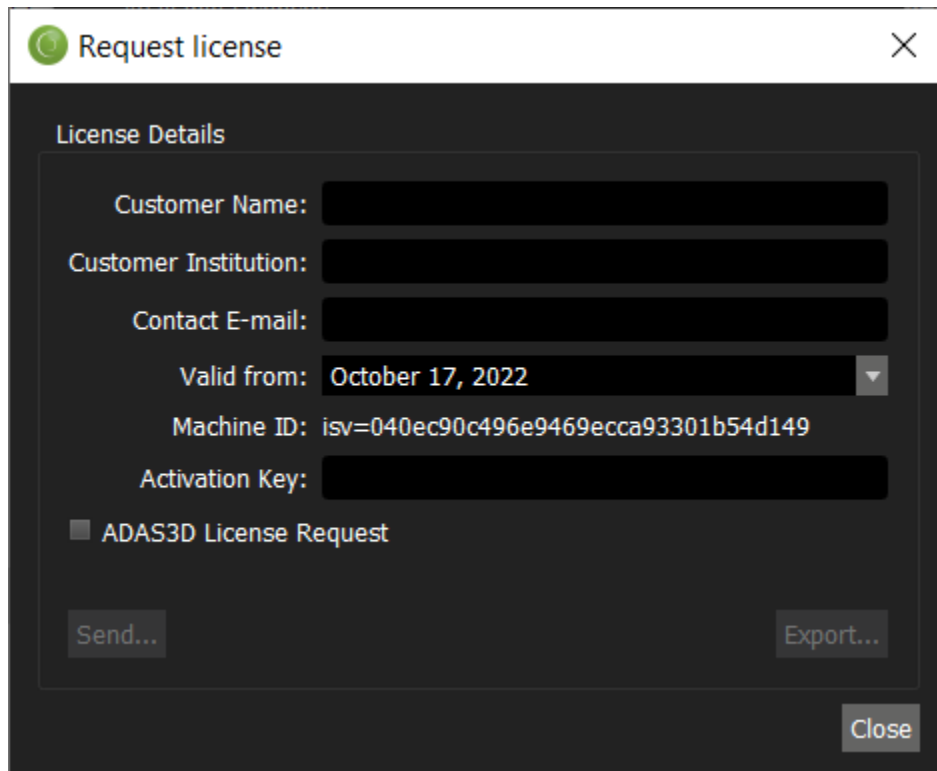


IMPORTANT: For Pay-Per-Use (PPU) licensing a reliable connection to Circle's PPU servers is required. The connection to Circle's PPU servers will be encrypted, all data will be hashed and salted, and no PHI will be transferred.

2.1.1. Offline Activation Method

If your **cvi42** server has no access to the internet, you will be able to activate with the offline activation method.

In this method, after installing **cvi42** you log in with the default credentials and in the Licence screen you click *Request...*



Request license

License Details

Customer Name:

Customer Institution:

Contact E-mail:

Valid from:

Machine ID: isv=040ec90c496e9469ecca93301b54d149

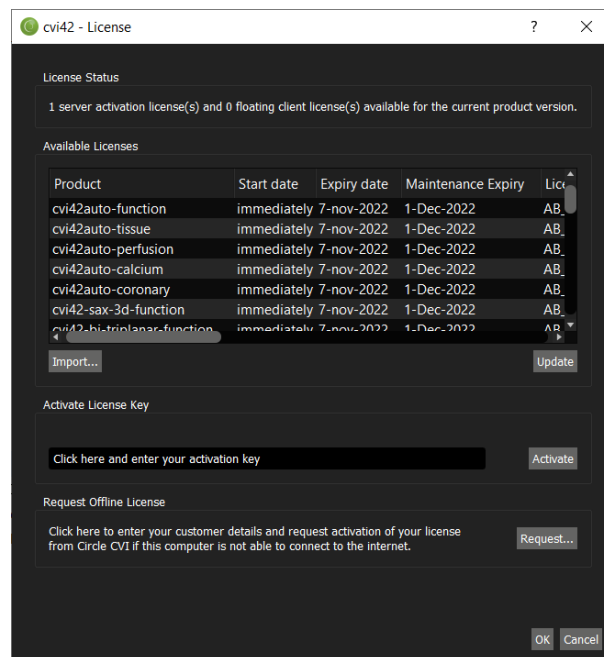
Activation Key:

☐ ADAS3D License Request

Fill in your data. The Activation Key is not mandatory, but if you have the Activation Key that Circle CVI Support provided you, you can enter it into the appropriate field.

ADAS3D License Request checkbox should only be checked if you want to request License for ADAS3D, otherwise keep it unchecked. Once completed, you can press the *Send...* button, that will open your default e-mail client with an e-mail to Circle CVI, requesting the license, or you can export the *.req* file and send it to Circle CVI later.

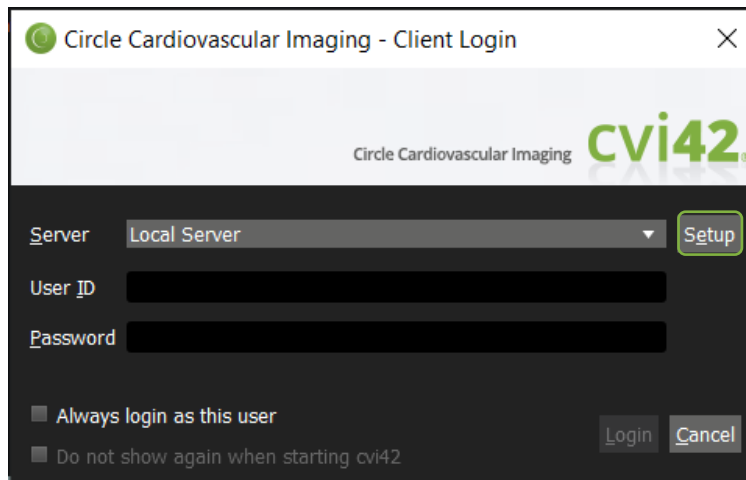
Circle CVI will generate a *.zip* file with all the licenses and send it back to you. Then, you unzip the licenses into a directory on your local computer. Click *Import...* on the *License* screen from that directory. After importing the licenses, you will have the list of licenses.



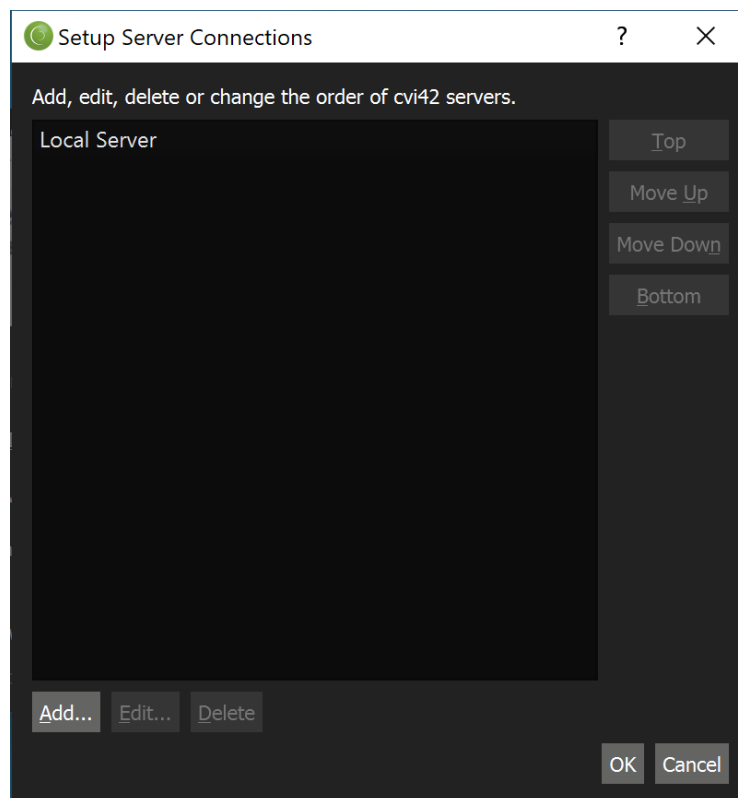
Just click *OK* to log into the application.

2.2. Configure cvi42 client to connect to the Server

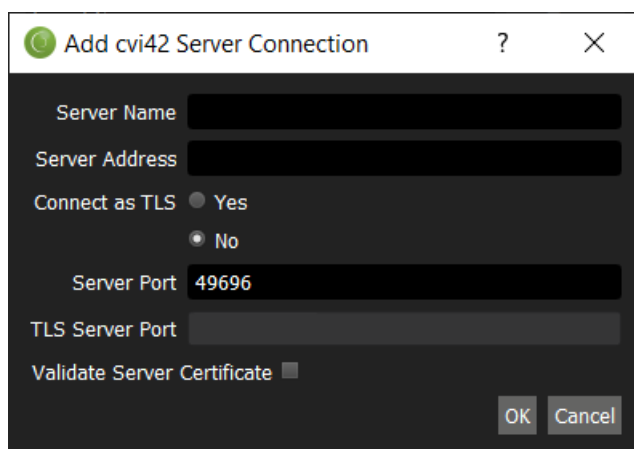
The login dialogue will be configured by default to connect to a local server.



To configure additional servers, click the "Setup" button.



Initially there will only be a Local Server connection in the list. Click "Add..." to add a new server connection.



In the Add **cvi42** Server Connection dialogue, fill in the necessary fields.

- **Server Name** – This is any name you choose to identify the server.
- **Server Address** – This is the IP address or host name of the **cvi42** server you are connecting to.
- **Server Port** – This is the communication port the server uses for connections. The default port is 49696. If the target server is configured to listen on a different port, enter the new value here.



IMPORTANT: Before configuring a secure server connection, the certificate and private keys must first be imported to the **cvi42** server. For more information on Enabling TLS in **cvi42** refer to section 2.3 below.

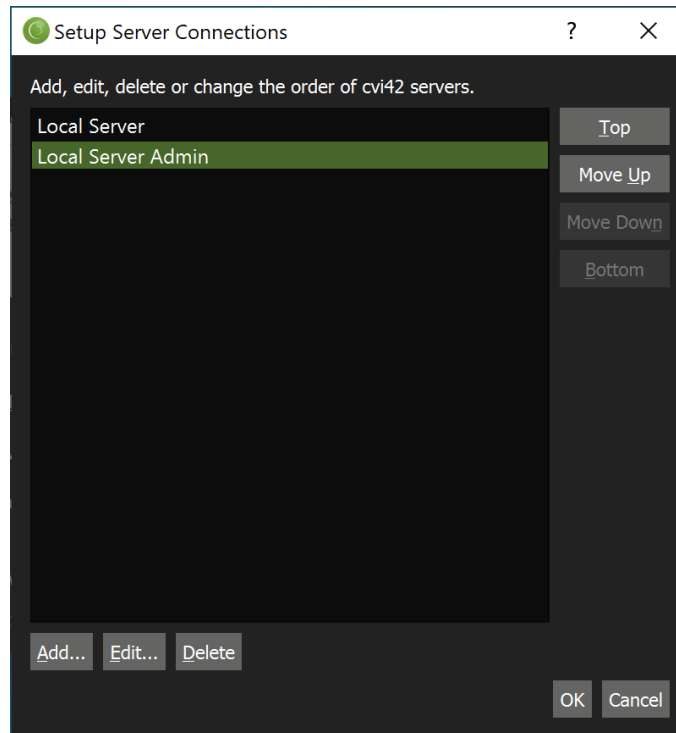
- **Server Port for Administration** – If you are required to administrate **cvi42** server, e.g. setup DICOM nodes, you will need to create a server connection pointing to port 49697. For setting up a secure connection, the default port is 4931 (secure). You will also need to log in as an admin user.



IMPORTANT: The Server Port and TLS Server Port values specified here must match the port number that is configured for the server that you want to connect to.

- **Connect as TLS** – This configuration option allows a user to connect to a secure port on the server. If enabled, the TLS Server Port field will be editable and used to specify the secure port. If disabled, the Server Port field will be editable and used to specify an unsecure port.
- **TLS Server Port** – This is the communication port the server uses for secure connections. The default port is 4390. If the target server is configured to listen on a different port, enter the new value here.
- **Validate Server Certificate** – This option is unchecked by default. When checked it means that the server should have a valid certificate, otherwise trying to login into the server via TLS will fail.

For most deployments, you can now click "OK" to finish.



To change the parameters of an existing server connection definition, select the desired server from the list and click the "Edit..." button.

To delete an existing server connection definition, select the desired server from the list and click the "Delete" button.

The "Top", "Move Up", "Move Down" and "Bottom" buttons are used to change the order of the servers in the list. This affects the order of the servers listed in the drop-down box in the Login Dialogue.

2.3. Enabling TLS in cvi42



IMPORTANT: cvi42 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.

Importing Key Pair

Before using an encrypted connection for the first time in **cvi42**, you must install a valid certificate/private key pair to the server. This can either be achieved by:

- *Importing Key Pair using cvi42 client user interface connecting to cvi42 server on the admin port*
- Or manually placing the required files in the %PROGRAMDATA%\cvi42 folder of the cvi42 server

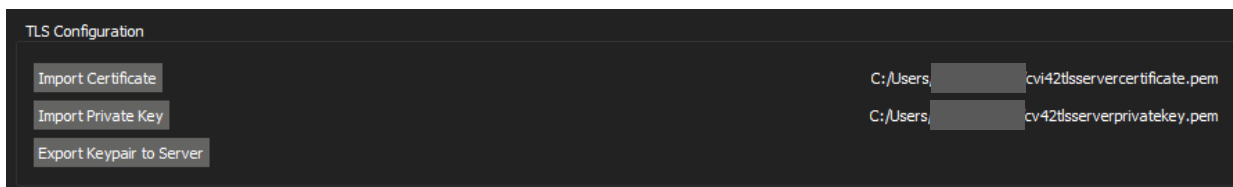
The file will need to be partitioned into separate certificate and private key files.

1. Log into a cvi42 client with cvi42 administrator credentials through the administrative port and open the preferences menu
2. Select "Server Admin"
3. Import both certificate and private key files using the client UI, 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 cvi42 will prevent you from importing certificates it does not trust.

4. Next, select "Export Keypair to Server". If this operation is successful, you will see a dialogue box confirming the files have been saved to the server.



IMPORTANT: For first time configurations, the cvi42 server *must* be restarted to enable secure connections. New key pair files may be imported without disrupting existing secure connections.

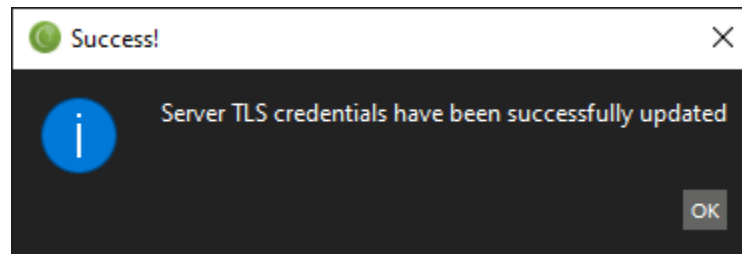


IMPORTANT: If cvi42 server has been setup for secure connection, please make sure the cvi42 client is rolled out configured for secure connection.

Configuring an Encrypted Connection

Once TLS has been enabled on the cvi42 server, a secure server connection can be configured. Follow the steps outlined in section 2.2, to either add a new connection or modify an existing one.

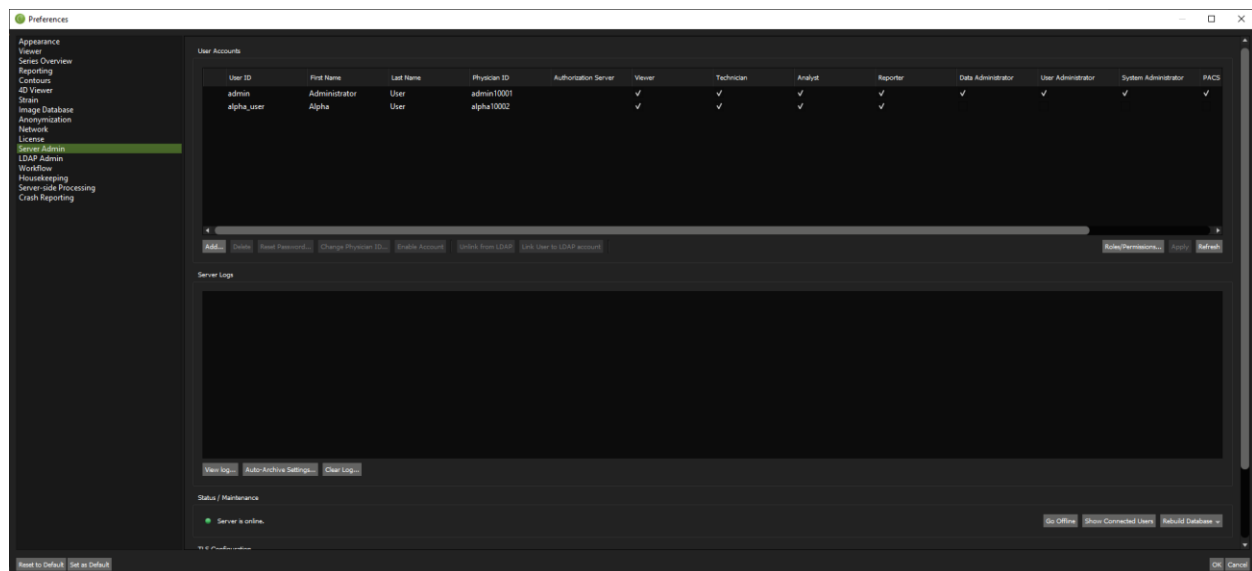
1. Select "Connect as TLS". This will disable the Server Port field and enable the TLS Server Port field.
2. Specify the TLS Server Port. NOTE the default TLS Server Port is 4391.
3. Once saved, if successful the following dialogue box will be displayed.



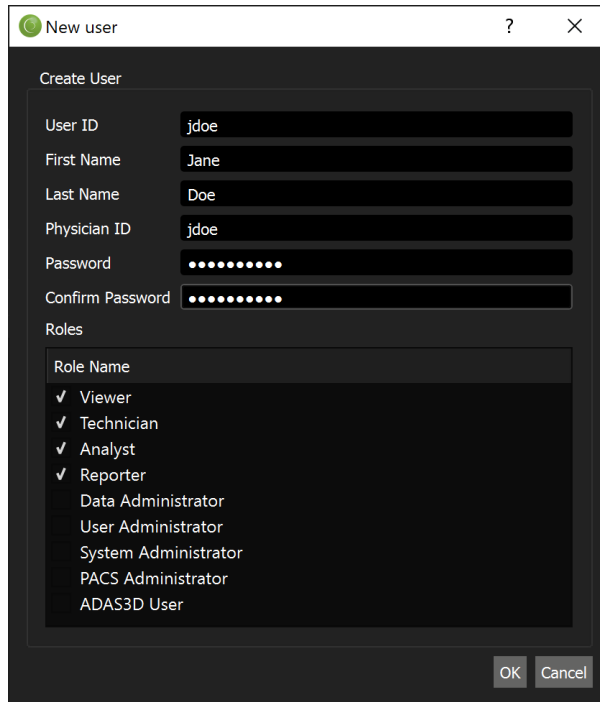
2.4. Setting Up User Accounts

To add user accounts to **cvi42**, you must login as an admin on the admin port (49697).

- Click on Preferences → Config from the menu bar (or press F12).
- Select "Server Admin" from the list.



- Click the "Add..." button, to add a new account. The *New user* dialogue will be displayed.



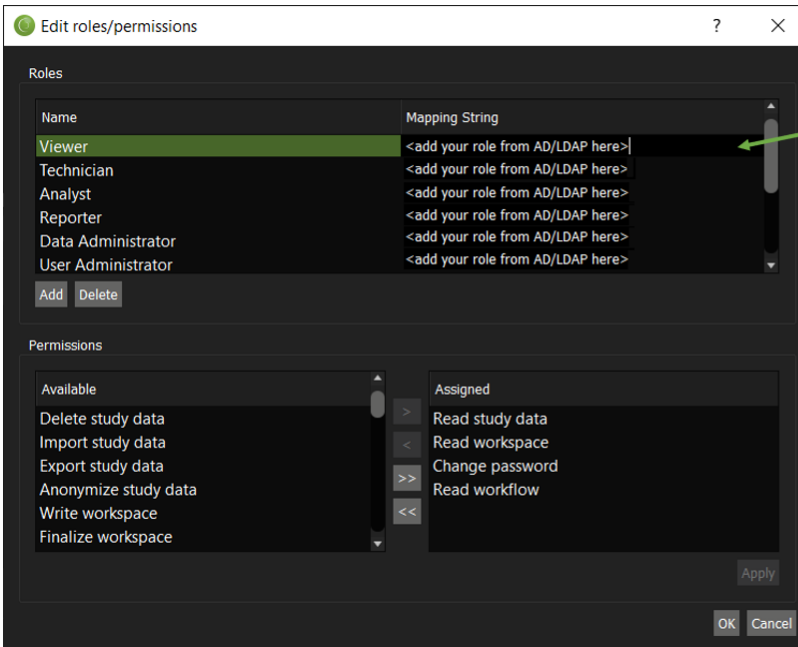
- Fill in all the user details and check the roles to be assigned to the new user.
- Click *OK* to finish.

2.5. Setting Up Roles

cvi42 defines a set of default roles that can be assigned to user accounts. The set of roles can be customized to meet your institution's needs.

From the "Server Admin" preferences page, click on the "Roles/Permissions" button.

For more information on how user accounts are linked between the local **cvi42** authorization/authentication methods and an integrated AD/LDAP server refer to section 5.1 User Account Linking.



You double click these Fields
To add the corresponding AD/LDAP
role that matches cvi42 role

If the user authorization (user roles) is not required the Mapping Strings, shown in the screenshot above, it can be ignored. The above Mapping String parameters will be mapped to the membership property of any integrated AD/LDAP server.

- To edit the permissions of an existing role, select a role from the Roles list. The Assigned box in the bottom right half of the dialogue will display the permissions assigned the selected role:
 - Select permissions from either the "Available" list or "Assigned" list.
 - Click on the ">" or "<" buttons to assign or un-assign the selected permissions. The ">>" will assign all permissions to the role, and the "<<" will un-assign all permissions from the role.
 - Click "Apply" to save the changes.
- To add a new role, click the "Add" button and enter a name for the new role. Proceed to assign the desired permissions to the new role.
- To delete a role, select a role and click the "Delete" button. A confirmation dialogue will be displayed. Click "Yes" to delete the role, or "No" to go back.



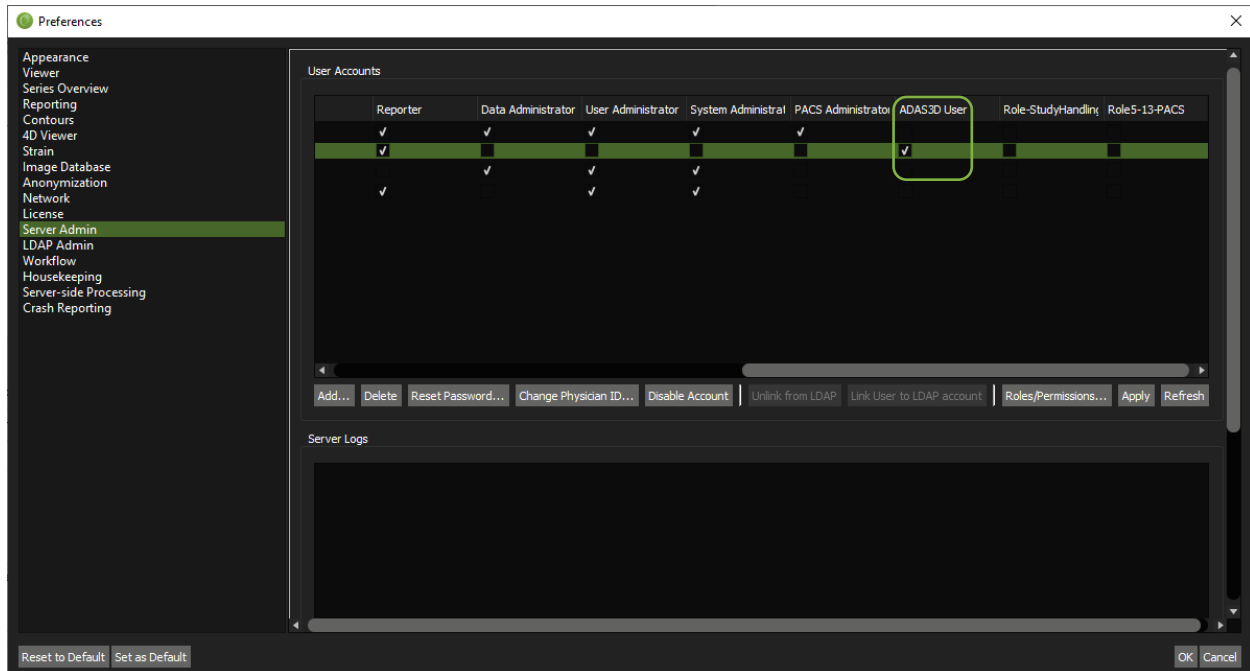
IMPORTANT: When roles/permissions of a particular user are changed, the settings will not take effect until the next time the user logs into **cvi42**.

2.6. Assigning ADAS 3D User Role



IMPORTANT: ADAS 3D is *only* available for Windows platform.

If purchased, the ADAS 3D application will be installed when installing **cvi42**. To enable user access to the ADAS 3D application, add the specific **ADAS3D User** role to each applicable user account using the process outlined in section 2.5 Setting Up Roles.



3. Configure Antivirus Software

Antivirus scanning can have a significant, detrimental effect on the performance of the **cvi42** application. Typical studies can contain thousands of individual image files and the time needed to scan each of those files can be significant. Folder exclusion or process/filetype profiling should be configured to exclude these files from any antivirus on both the **cvi42** server and client.

The paths configured in `C:\ProgramData\cvi42\cvi42serverconfig.ini` should be considered for exclusion from the designated Antivirus Software Solution in favor of system performance.

However, the recommendation is to not exclude the `\cvi42imagedb\incoming_DcmStorage\` folder as incoming DICOM traffic might not have been sufficiently scanned before on the remote system, for example an MRI / CT Scanner.

4. Configure DICOM Networking (PACS Connections)

Users with 'PACS Administrator' permissions can set up the configuration for DICOM Networking/PACS connections. The admin port (default is 49697) must be used to access the Network section of the Preferences Menu.

A remote DICOM node will need to be aware of the **cvi42** Server's DICOM AE Title, the Storage SCP Port as well as the IP address of the **cvi42** Server.

The following list presents only the most important settings of this section:

Network Settings

- **AE Title** – The Application Entity Title, is used by **cvi42** to identify itself and needs to be configured on both **cvi42** and the integrated repository. By default, the AE Title is **cvi42**. This field is case sensitive.
- **Storage SCP Port** – The network port of the **cvi42** product; this value must be defined in both **cvi42** and the integrated repository.
- **Database update interval** – This is the interval (measured in seconds) before **cvi42** will check for updates of incoming images. By default, **cvi42** will check for updates to the image database every 10 seconds.
- **Optional fields - Default MPPS Server, Default Modality Worklist Server and Default Q/R Server**

These are optional fields that can be set depending on your needs. *Default MPPS (Modality Performed Procedure Step) Server:* When a study is opened, **cvi42** reaches out to this server to obtain the Scheduled Procedure Step attributes for the study.

MWL (Modality Worklist) Server: **cvi42** sends a message to the *Default MPPS Server with the appropriate Performed Procedure Step* attributes.

Default Q/R Server: When **cvi42** is opened from a third-party application, the study identifier is passed to **cvi42**. If the study is not on **cvi42** server, it reaches out to the *Default Q/R Server* to query, retrieve and import the study.

Network Options

- **Enable Storage SCP** – Configuration option that enables **cvi42** to act as a Storage SCP. **cvi42** will listen for incoming DICOM C-STORE connections on the configured **Storage SCP Port** and **AE Title**.
- **Enable Q/R SCP** – Configuration option that enables **cvi42** to act as a DICOM Query/Retrieve SCP. **cvi42** will be able to be queried on image data by remote DICOM nodes.
- **Accept Unknown AE-Titles** – Configuration option that allows **cvi42** to operate in Promiscuous Mode and accept valid DICOM associations from any AE Title / IP address. It is recommended to configure all remote DICOM nodes properly instead of using this setting. This setting can also help when testing new connections.

- **Enable Low-Level Debug Log** – Configuration option that increases the logging level/details written to the application logs. This option is disabled by default and can generate large files.

Remote DICOM Nodes

Used to configure the necessary DICOM connection information for any remote DICOM node.

Minimum required information: Remote Node IP address, Remote TCP Port, Remote AE Title.

Fields Description

- **Address** - TCP Address or HostName of remote PACS.
- **AE-Title** - Application Entity Title of remote PACS (a single server might have several stores).
- **Port** - TCP port of remote PACS.
- **Description** - Pretty name for the cvi42 client UI.
- **Connect-As AE-Title** - Who we identify ourselves as (usually the same as the one you set above).
- **Restrict to Role** - Which user roles should be allowed to interact with this PACS.
- **Send** - Permit users to send to this PACS.
- **Anonymized Send** - Only send studies after anonymizing them (for research or consultant PACS).
- **Send Original Study** - When sending a study to a PACS, send the whole study, not just the images we may have generated.
- **Send Workspaces** - Send cvi42 workspaces when sending whole studies.
- **Send Reports** - Send cvi42 Report secondary captures when sending whole studies.
- **Report DICOM Type** - Instructs report42 whether to output DICOM reports as Secondary Capture Image Series or a DICOM Encapsulated PDF document, which is rarely supported.
- **Q/R** - Allow users to query this PACS and receive from it.
- **C-GET** - Use the older C-GET protocol for receiving images, which is better when you're using a VPN or you are behind some kind of NAT router.
- **Character Encoding** - language you claim to use when interacting with the PACS.



WARNING: The DICOM communication interfaces do not use encryption or user authentication. It is the site's responsibility to use these communication abilities in secure environments only.

5. Active Directory/LDAP Integrated Password Authentication

Users with 'System Administrator' permissions can set up the configuration for Active Directory (AD) or LDAP integrated password authentication. This feature allows users to log into **cvi42** with their existing user credentials assigned by their organization's IT team. A connection using the admin port (default is 49697) must be used to access the LDAP Admin tab of the Preferences Menu.

The LDAP Admin Tab allows the System Administrator to authenticate users against an AD or LDAP server. To connect to an AD or LDAP server, **cvi42** needs the following information.

- **Enable LDAP**– When checked this checkbox 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 **cvi42** server to communicate with the integrated AD or LDAP server.
 - Active Directory: When configuring the username value for AD, it will be a userPrincipalName(CVI42-BIND-ACCOUNT-NAME@DOMAIN-NAME) or sAMAccountName (DOMAIN-NAME\CVI42-BIND-ACCOUNT-NAME).
 - LDAP: When configuring the username value for LDAP integrations, the format of the username will be an LDAP distinguished name: (uid=<CVI42-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.
 - Active Directory: When configuring the username attribute value for AD integrations, use a unique parameter, such as sAMAccountName.
 - 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 **cvi42**, as an example:
 - memberOf=CN=cvi42, CN=Users, DC=example, DC=com
- **Use AD/LDAP groups for cvi42 role mapping** – This setting determines whether **cvi42** 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 **cvi42** user list and user permissions are determined using **cvi42**.

☒ Enable LDAP

AD/LDAP Settings

Primary Server:

Secondary Server:

☐ Use TLS/SSL to connect

Account Info for Bind

Username:

Password:

☐ Anonymous connection

☒ Use bind account for Study Request URL Authentication

AD/LDAP Specific Information

Base DN:

Username Attribute:

This is to allow you to specify the username attribute used by the AD/LDAP server. Generic LDAP usually use `uid` as an attribute to label username, while Active Directory servers uses `sAMAccountName`.

☒ Use AD/LDAP groups for cvi42 role mapping

Configuration for AD

☒ Enable LDAP

AD/LDAP Settings

Primary Server:

Secondary Server:

☐ Use TLS/SSL to connect

Account Info for Bind

Username:

Password:

☐ Anonymous connection

☒ Use bind account for Study Request URL Authentication

AD/LDAP Specific Information

Base DN:

Username Attribute:

This is to allow you to specify the username attribute used by the AD/LDAP server. Generic LDAP usually use `uid` as an attribute to label username, while Active Directory servers uses `sAMAccountName`.

☒ Use AD/LDAP groups for cvi42 role mapping

Configuration for LDAP

Once you are satisfied with the configuration click *Apply* to save the changes.

5.1. User Account Linking

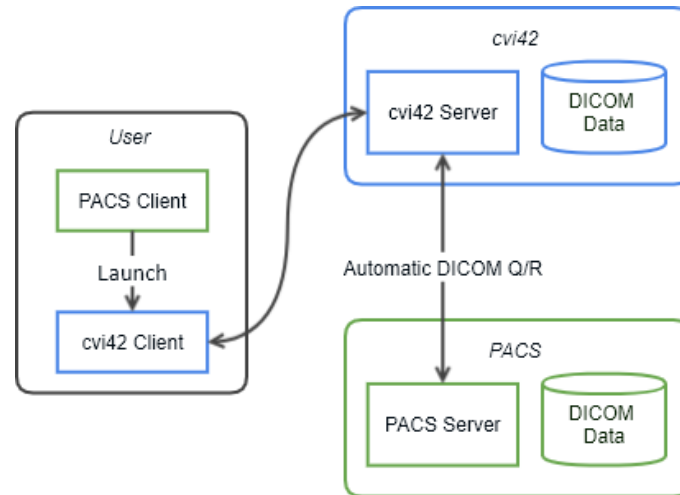
Below is a table outlining the User Account linking behaviour. For more information on configuring user accounts and user roles refer to sections 2.4 Setting Up User Accounts and 2.5 Setting Up Roles.

User in AD/LD AP	User in cvi42	User Account Linked	Password Used	Comments
Y	Y	Y	AD/LDAP	User is in both the cvi42 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 <i>only</i> in the integrated AD/LDAP server and uses the AD/LDAP password to log into cvi42 . The user will be provided access and a New User is created in the cvi42 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	

6. Command-line Integration

6.1. Overview

The Client & Server-based **cvi42** integration model provides an interface for integrating **cvi42** into third party products, using command line arguments. **cvi42** shall access studies from its own DICOM database or via DICOM Q/R to PACS/VNA.



6.2. Client and Server Integration Workflow

In a client and server-based integration, the expected user workflow is as follows:

1. User opens a study on a 3rd party vendor application (e.g., PACS, workstation etc.).
2. User launches **cvi42** within the application. **cvi42** is launched with command line arguments (e.g., Study Instance UID, Accession Number, Username, full screen etc.) provided by the application.
3. User logs on to **cvi42**.



IMPORTANT: Username is populated into the login dialogue. For security reasons, password is never passed as an argument.

4. **cvi42** client requests to **cvi42** Server to load the study with a specific Study Instance UID or Accession Number.
 - a. If the study does not exist in **cvi42** Server, the server sends a DICOM Q/R request to a designated DICOM Q/R SCP. A progress bar indicates study loading status to the user.
 - b. Once the study is retrieved and imported, the server sends back a signal that triggers the client to load the study.
 - c. If the study does not exist and cannot be retrieved, the user is prompted with a message and returned to the patient list, allowing them to continue to use **cvi42** with regular workflow.
5. User generates reports or secondary captures in **cvi42**.
 - a. **cvi42** client uploads generated DICOM files to **cvi42** server.
 - b. All files that are uploaded can then be sent to the third-party system via DICOM Storage operation either manually or using housekeeping rules.
6. User closes study and returns to patient list, or user closes **cvi42**.

6.3. Command Line Parameters

Number	Command Line	Activity	Argument
1	-accession <accession_number>	Load study that matches <accession_number>	Accession Number
2	-studyuid <study_instance_uid>	Load study that matches <study_instance_uid>	Study Instance UID
3	-unload-study	Unloads the current study	None
4	-username <username>	Sets <username> in login dialogue.	Username
5	-disable-quit-dialog	Disables dialogue message box when exiting cvi42	None
6	-disable-patient-list	Disables patient list. (cvi42 is locked to the current study)	None
7	-single-instance	Forces to run only a single instance of cvi42	None
8	-multi-instance	Forces to run multiple instances of cvi42	None
9	-study-request-url <URL>	Attempts to authenticate and load a study from the given URL	URL that provides Username and Accession Number as a response object

6.4. Launching cvi42

In order to launch **cvi42** from a third-party software, the vendor shall run **cvi42** with proper command line arguments.

As an example, the following command will launch **cvi42**, set username in the login dialogue with “-username” argument value and load the appropriate study with “studyuid” argument. If **cvi42** has already been launched, **cvi42** will close the current study and switch to the study specified in “studyuid”. Also, if a different username is passed as an argument, **cvi42** will close the current study, disconnect from current session, and present a login dialogue.

```
>> cvi42.exe -studyuid "1.3.12.2.1107.5.2.12.21106.4.0.6321606317547884" -username "admin" -single-instance
```

or

```
>> cvi42.exe -studyuid="1.3.12.2.1107.5.2.12.21106.4.0.6321606317547884" -username="admin" -single-instance
```

If a study was closed or patient was changed in the vendor's software, it can pass the following arguments to **cvi42**.

```
>> cvi42.exe -unload-study -single-instance
```

This command will launch a **cvi42** process in the background, pass the arguments to the existing **cvi42** process and terminate itself. It is recommended to always pass "-single-instance" to avoid popup messages asking for launching **cvi42** in multi-instance mode.

7. Server Configuration (**cvi42serverconfig.ini** explained)

On Windows, the **cvi42serverconfig.ini** file is stored in `D:\ProgramData\cvi42.`

This file contains a list of configuration parameters for the **cvi42** server.

Whenever changing the **cvi42Serverconfig.ini** file, the **cvi42** server should be stopped, take a backup of the file, make the necessary changes, then restart the **cvi42** server.

The parameters should only be edited by a server administrator, who needs to change the defaults of a particular server installation.

A description of each parameter is given below.

7.1. General Properties

Use a text editor to change the following parameters when configuring a **cvi42** server.

- **DataFilePath** - Path to the folder containing the data for your **cvi42** system.
example: `DataFilePath=D:/ProgramData/cvi42`
- **ImageDBPath** - Path to the folder containing the image data for your **cvi42** system.
example: `ImageDBPath=D:/ProgramData/cvi42/cvi42imagedb`
- **SqlDatabasePath** - Path to the **cvi42server** database.
example: `SqlDatabasePath=D:/ProgramData/cvi42/cvi42sqlldb/cvi42Db.sqlite`
- **ConnectionTimeout** - The number of seconds that a connection can be idle (no activity on the server connection) before it will be automatically closed. The default is 86400 seconds (24 hours).
example: `ConnectionTimeout=86400`
- **FailedLoginsBeforeTempLock** - Specifies the allowable number of failed login attempts before the account is temporarily locked-out. Default is 3. The lock-out duration is specified by the `FailedLoginTempLockDuration` parameter described below. If this parameter is set to -1 then the user will be locked out of the system until the administrator re-enables their account in the Server Admin preferences page. So, the lock-out duration parameter will be ignored in this case.
example: `FailedLoginsBeforeTempLock=3`

- **FailedLoginTempLockDuration** – Specifies the lock-out duration in seconds when an account is temporarily locked due to exceeding the maximum number of failed login attempts. The default is 60 seconds.
example: FailedLoginTempLockDuration=60
- **ClientPort** – Specifies the port that the server listens on for incoming connections. Default is 49696.
example: ClientPort=49696
- **AdminPort** – Specifies the port that should be used when connecting to the server to perform administrative functions. Default is 49697. Users with administrator permissions have exclusive access on this port.
example: AdminPort=49697
- **ClientPortIPv6** – Specifies the port the server listens on for incoming connections when using IPv6 addresses. Default is 48696.
example: ClientPortIPv6=48696
- **AdminPortIPv6** – Specifies the port that should be used when connecting to the server to perform administrative functions when using IPv6 address. Default is 48697.
example: AdminPortIPv6=48697
- **ThreadPoolSize** – Specifies the number of threads the server uses to handle incoming requests. Default is 10.
example: ThreadPoolSize=10
- **BackgroundTaskThreadCount** – Specifies the number of threads the server uses for background task processing. Default is 4.
example: BackgroundTaskThreadCount=4
- **LogFilePath** – Path to the folder containing the log files for the server.
example: LogFilePath=D:/ProgramData/cvi42/ServerLogs
- **LogArchiveIntervalType** – Specifies the automatic archive interval type. Default type is 1 (daily archive). Possible values are:
 - 1 - daily (archive of logs is created daily)
 - 2 - weekly (archive of logs is created weekly)
 - 3 - monthly (archive of logs is created monthly)
 - 4 - custom interval (archive of logs is created after a custom number of days)example: LogArchiveIntervalType=1
- **LogArchiveCustomInterval** – Specifies the number of days that will elapse before the server logs are archived. Default interval 1. The custom interval is used only when the LogArchiveIntervalType is 4.
example: LogArchiveCustomInterval=1
- **PasswordRulesEnforced** – Specifies whether the server shall enforce password length and character requirements. Default is false.
example: PasswordRulesEnforced=false

If you set this parameter to `true`, then the system will check that passwords:

- Must be at least 6 characters in length
 - Must contain at least one lower case alpha character
 - Must contain at least one upper case alpha character
 - Must contain at least one numeric character
- **PasswordExpiryThreshold** – Specifies the number of days that will elapse before users are prompted to change their password. Default is 0 days. Users will not be prompted to change the password when the PasswordExpiryThreshold is 0.
- **RecentPasswordListSize** – Specifies the number of recent passwords that cannot be re-used when selecting a new password. Default is 0. The system will allow users to re-use any password when the RecentPasswordList size is 0.
- **PasswordChangeRequiredAfterReset** – Indicates whether users must change their password the first time they login after an administrator has assigned (or reset) the password. Default is false.
example: PasswordChangeRequiredAfterReset=false
- **DebugLog** – Specifies where debugging output from the server is to be captured. Default is 0 (debug output disabled). Possible values are:
 - 0 – none (debug output disabled)
 - 1 – save to file
 - 2 – console (displayed only if server is running in a command window)example: DebugLog=0
- **ConfigBackupInterval** – Specifies how often the server config file will be backed up in seconds.
example: ConfigBackupInterval=1200
- **TrustedHosts** – Specifies a comma separated list of trusted host servers. When configuring this value provide the IP or fully qualified hostname.
example: TrustedHosts=server1.abc.com, server2.abc.com
- **EnableLdap** – A Boolean value used specifies whether or not cvi42 should use the configured LDAP settings for user authentication/authorization. Default value is false.
example: EnableLdap=false
- **ForceTrustedUrlLogin** – A Boolean value parameter used to enable/disable the authentication/authorization of non-admin users with the cvi42 user list. Default value is false.
example: ForceTrustedUrlLogin=true

7.2. PPU Properties

- **HostName** – Specifies the pay-per-use server to connect to when using pay-per-use licensing.
example: HostName=ppu-z01.circlecvi.com
- **Port** – Specifies the port to use for connecting to a pay-per-use server.
example: Port=443
- **Scheme** – Specifies the scheme to use for connecting to a pay-per-use server
example: Scheme=https

7.3. DICOM Network

- **CompressionScpEnabled** – This identifies whether the **cvi42** provides compressed transfer syntaxes for requests. Default is `true`.
example: `CompressionScpEnabled=true`
- **CompressionScuEnabled** – If configured, **cvi42** will ask for the supported compressed transfer syntaxes from the integrated repositories. Default is `true`. Some PACS require this to be set to `false`.
example: `CompressionScuEnabled=true`
- **RemoteDicomNodes\N\<parameter>** – This entry defines the connections for DICOM nodes (entities) that the server can interact with.
example:

```
RemoteDicomNodes\1\SendReports=true RemoteDicomNodes\1\AeTitle=HOROS
RemoteDicomNodes\1\CharacterEncoding=Unicode
RemoteDicomNodes\1\SendOriginalStudy=true
RemoteDicomNodes\1\ConnectAsAeTitle=CVI2019_2
RemoteDicomNodes\1\Id=@Variant(\0\0\0\x7f\0\0\0\x6QUuid\0\xaf\xc7\xbc\x92\x
44\xa1L\x99\xdb\xe6\xb4\xdd\x99\x8f\xbf)
RemoteDicomNodes\1\RestrictToRole= RemoteDicomNodes\1\Send=true
RemoteDicomNodes\1\SendAnonymized=false
RemoteDicomNodes\1\ReportDicomType=Encapsulated PDF
RemoteDicomNodes\1\Description=PACS RemoteDicomNodes\1\QueryRetrieve=true
RemoteDicomNodes\1\Port=11112 RemoteDicomNodes\1\AnonymizeName=Anonymized
RemoteDicomNodes\1\Timeout=30 RemoteDicomNodes\1\SendWorkspaces=true
RemoteDicomNodes\1\CGet=false RemoteDicomNodes\1\Address=10.211.55.2
```
- **LocalPacsAETitle** – Specifies the AE Title when **cvi42** server is configured to accept study data via DICOM push.
example: `LocalPacsAETitle=CVI42`
- **LocalPacsPort** – Specifies the port to use when **cvi42** server is configured to accept study data via DICOM push.
example: `LocalPacsPort=104`
- **IncomingDirMonitorInterval** – The interval, specified in seconds, that the **cvi42** server will check for incoming study data that is sent to the **cvi42** server, and update the study list. Default is 10 seconds. This does not apply to the **cvi42** client causing the change of the study list (e.g. study import, DICOM retrieve). Its study list display will be updated instantaneously.
example: `IncomingDirMonitorInterval=10`
- **EnableStoreScp** – Indicates whether the server will accept study data via DICOM push.
example: `EnableStoreScp=true`
- **EnableQueryScp** – The server acts as a Query/Retrieve SCP for study level queries.
example: `EnabelQueryScp=true`
- **EnableCGet** – Allows the use of C-GET instead of C-MOVE DICOM protocol for supported PACS.
example: `EnableCGet=false`

- **AcceptUnknownAeTitles** – Enables promiscuous mode for DICOM operations.
example: AcceptUnknownAeTitles=true
- **EnableLowLevelDebug** – Enables the DICOM debug log.
example: EnableLowLevelDebug=false
- **MaximumQueryResults** – Specifies the maximum number of results accepted from DICOM queries. Default value is 1000.
example: MaximumQueryResults=1000
- **MaximumConnections** – Specifies the maximum simultaneous number of DICOM associations that **cvi42** will allow. Default value is 10.
example: MaximumConnections=10

7.4. AD/LDAP Integrated Password Authentication

- **PrimaryServer** – Specifies the location of the Active Directory/LDAP server. **cvi42** will initially contact this server when authenticating users using Active Directory/LDAP.
example: PrimaryServer=ad-master.srclookup.com
- **SecondaryServer** – Specifies the location of the Active Directory/LDAP server. **cvi42** authenticates users using Active Directory/LDAP against the server specified by primary server. When the authentication against the primary server fails, **cvi42** will authenticate users using a secondary server, specified by this parameter.
example: Secondaryserver=second.ad-master.srclookup.com
- **TLSSSLConnection** – Instructs **cvi42** to construct a secure communication channel when connecting to an Active Directory/LDAP server using TLS/SSL.
example: TLSSSLConnection=true
- **DomainName** – Specifies the domain name, if necessary, that the user would use during login. It is important to note that Active Directory accepts two types of domain names. Firstly, define a domain name with a trailing backslash "\\" (for example, srclookup\\). Secondly define a domain name with a prepended "@" (for example @srclookup).
example: DomainName=srclookup\\
- **BaseDN** – Specifies the location of the Active Directory/LDAP tree to use for user authentication, searching for users, and looking up user information.
example: BaseDN="DC=srclookup, DC=com"
- **UserAttribute** – Instructs what Active Directory/LDAP attribute to use when searching for users. This is important during authentication, as Active Directory/LDAP needs to identify whether the user exists on the system.
example: UserAttribute=sAMAccountName
- **AdditionalUserAttribute** – Specifies an additional restriction that needs to be accounted for when authenticating against Active Directory/LDAP server. For example, the Active Directory/LDAP server administrator has created a group called "cvi42", and only users in this group are permitted access to **cvi42**. In order for **cvi42** to enforce this, this parameter needs to

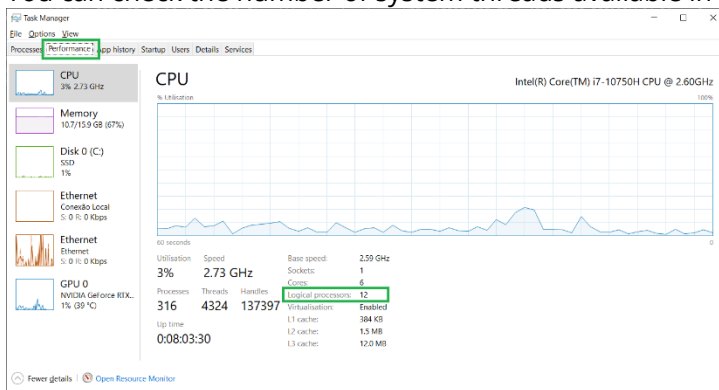
be specified.

example: `AdditionalUserAttribute="memberOf=CN=cvi42,CN=Users,DC=srclookup,DC=com"`

7.5. Server-side processing configuration (Node42)

- MaxNumberOfThreads** – Max number of threads available for the Machine Learning processing. The default value when the server creates the server config is $\min(\max(\text{system_threads} - 2, 1), 4)$. When Node42 is started, it will take the number from the `cvi42Serverconfig.ini`.
 If the configured number of threads is less than 1, it will be set to the default.
 Log message that the value has been overridden, `logNode.txt`: *UNKNOWN: Using default number of threads "4", available system threads "12"*.
 If it is more than $\max(\text{system_threads} - 2, 1)$ then it will use $\text{system_threads} - 2$.
 Log message that the value has been overwritten, `logNode.txt`: *WARNING: Too many threads configured "50", using maximum "10"*.

You can check the number of system threads available in Windows by opening Task Manager:



If Node42 is already running, you should kill node42 process in the Task Manager to reload configuration. **cvi42** Server starts a new node42 process if it's killed.

- MaxProcessingTimeSeconds** – This is the maximum number of seconds node42 will process a series before timing out, and has a default value of 600s (10 minutes). When processing times out, any in progress processing will be cancelled and no server side processing data will be stored for that series. If study has other series, node42 will continue processing the remaining series.

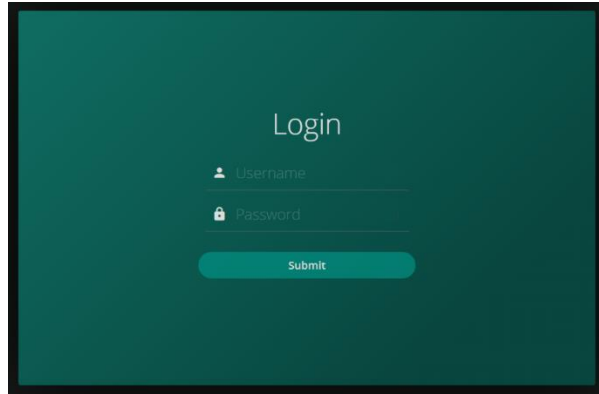
8. cvi42 Configuration Portal

In 5.16 and later releases we are introducing a new method to configure the **cvi42** server named **cvi42 Configuration Portal**.

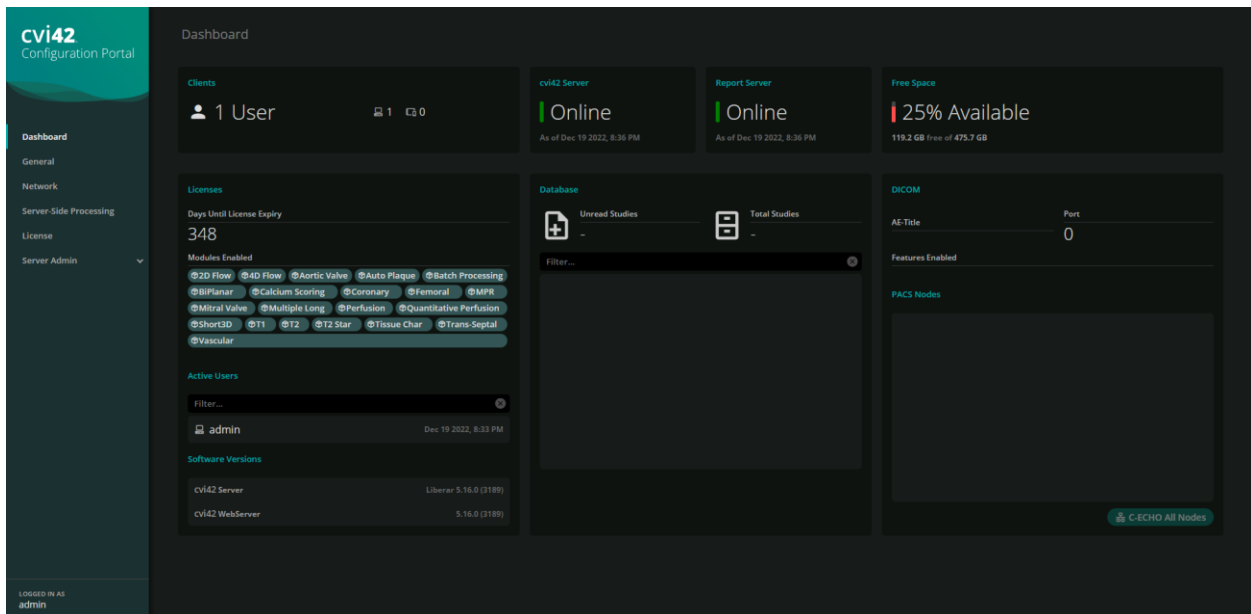


IMPORTANT: **cvi42** Configurator Portal is the new web interface to configure **cvi42** server properties. It still limited in terms of functionality, administrators can experiment it however the preferable way to configure the server is by login in the **cvi42** server admin port.

You can access **cvi42 Configuration Portal** via a browser by the url: `http(s)://<IP or FQDN>:4299`



Default credentials: admin / password



The interface is very intuitive, in the Dashboard you can check statuses of the **cvi42** server components, check licenses available, etc.

cvi42
 Configuration Portal

Dashboard
General
 Network
 Server-Side Processing
 License
 Server Admin
 Reporting

LOGGED IN AS
 admin

General

Remote Client Connection Timeout
 86400 Seconds

Failed Login Temporary Lock Duration
 60 Seconds

Failed Logins Before Temporary Lock
 3

Password Expiry Threshold
 0 Days

Recent Password List Size
 0

Thread Pool Size
 10

Data Files Path
 C:/ProgramData/cvi42/

Image Database Path
 C:/ProgramData/cvi42/cvi42imagedb

Use System Proxy Configuration
 ☐

Client Port
 49696

Admin Port
 49697

Client Port IPv6
 49696

Admin Port IPv6
 49697

Background Task Thread Count
 4

Debug Log
 None

SQL Database Path
 C:/ProgramData/cvi42/cvi42sqldb/cvi42Db.sqlite

Log Files Path
 C:/ProgramData/cvi42/ServerLogs

Password Rules Enforced
 ☐

Password Change Required After Reset
 ☐

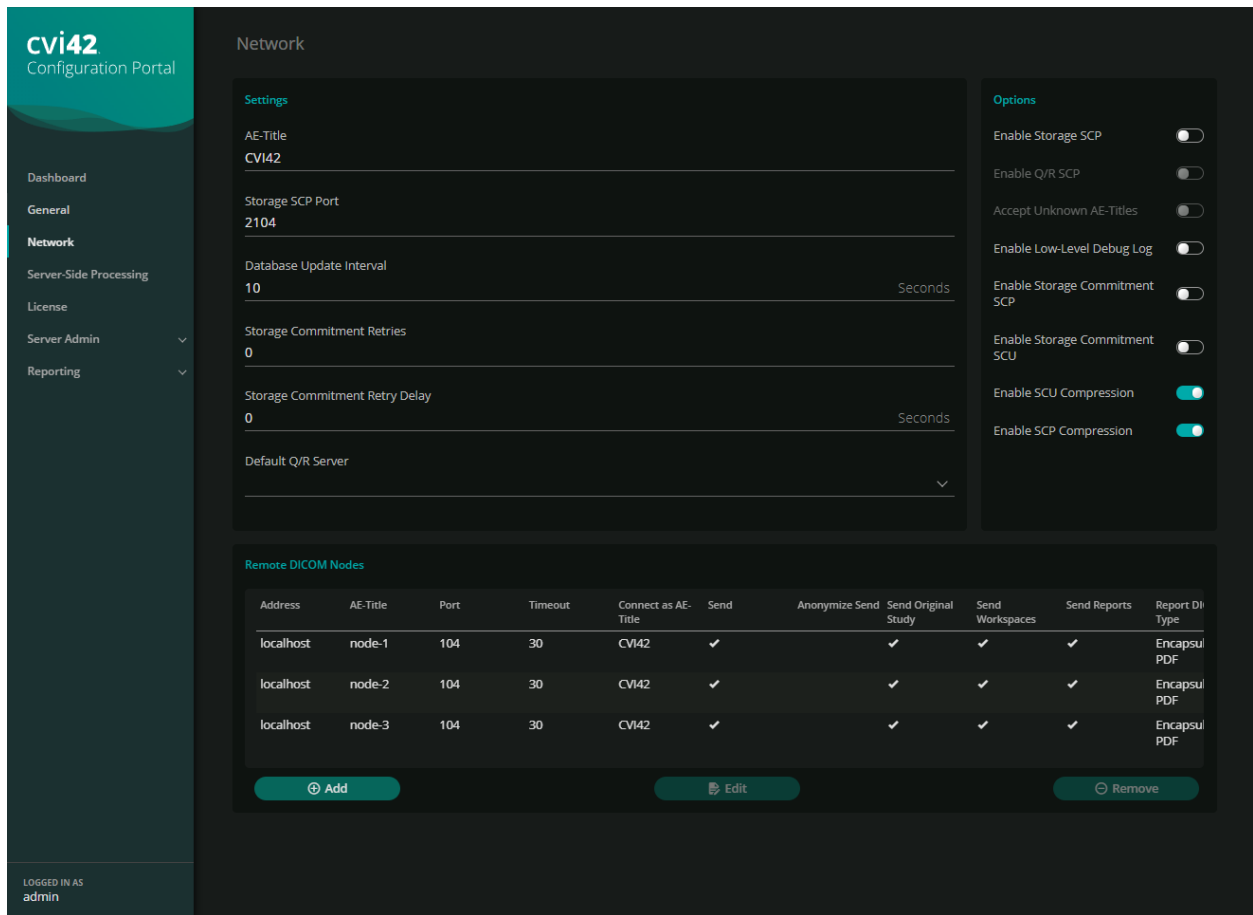
Permitted Remote Web Clients

Clients

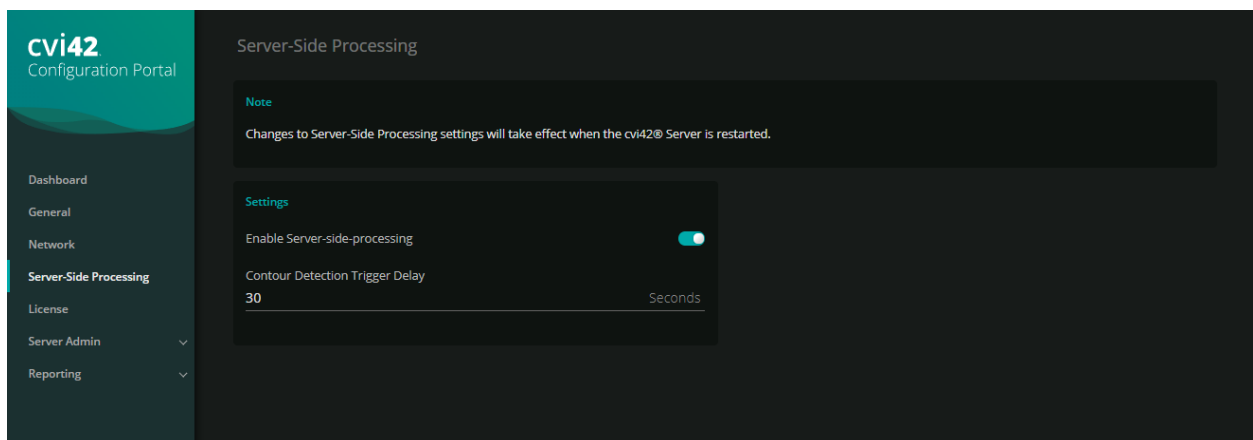
NO ENTRIES

Add Edit Remove

In the General option, you can change some of the server parameters, paths of data and database folders, ports, etc. You should restart the **cvi42** server whenever these configs are changed.



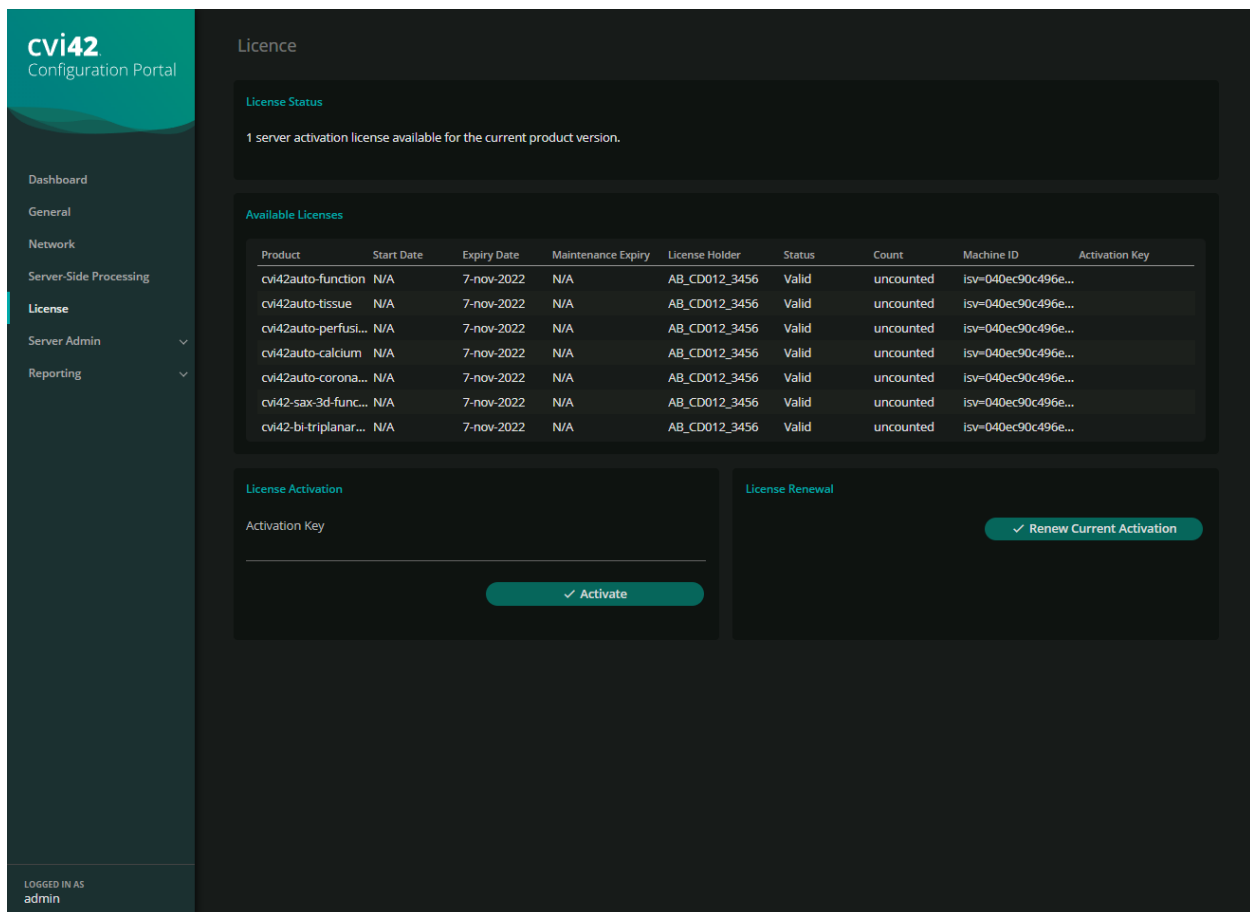
This interface has similar functionality to [DICOM Network](#).



Server-side processing enables the server to perform AI on imported studies. To enable, toggle the "Enable Server-side-processing" switch. Contour Detection Trigger Delay is the time to wait since last image for a study was received before triggering AI processing on that study. Server-side processing supports only CT studies for the 5.16 and later releases.

IMPORTANT: If **cvi42** server is installed on a separate machine, you should open TCP/4298 port on this machine, so **cvi42** client can communicate to the server-side processing component. You should open the *Windows Defender Firewall*.

For the remaining steps of the configuration, just use the defaults and in the final screen give a name for the rule.



cvi42
Configuration Portal

Dashboard
General
Network
Server-Side Processing
License
Server Admin
Reporting

Licence

License Status

1 server activation license available for the current product version.

Available Licenses

Product	Start Date	Expiry Date	Maintenance Expiry	License Holder	Status	Count	Machine ID	Activation Key
cv42auto-function	N/A	7-nov-2022	N/A	AB_CD012_3456	Valid	uncounted	isv=040ec90c496e...	
cv42auto-tissue	N/A	7-nov-2022	N/A	AB_CD012_3456	Valid	uncounted	isv=040ec90c496e...	
cv42auto-perfusi...	N/A	7-nov-2022	N/A	AB_CD012_3456	Valid	uncounted	isv=040ec90c496e...	
cv42auto-calcium	N/A	7-nov-2022	N/A	AB_CD012_3456	Valid	uncounted	isv=040ec90c496e...	
cv42auto-corona...	N/A	7-nov-2022	N/A	AB_CD012_3456	Valid	uncounted	isv=040ec90c496e...	
cv42-sax-3d-func...	N/A	7-nov-2022	N/A	AB_CD012_3456	Valid	uncounted	isv=040ec90c496e...	
cv42-bi-triplanar...	N/A	7-nov-2022	N/A	AB_CD012_3456	Valid	uncounted	isv=040ec90c496e...	

License Activation

Activation Key

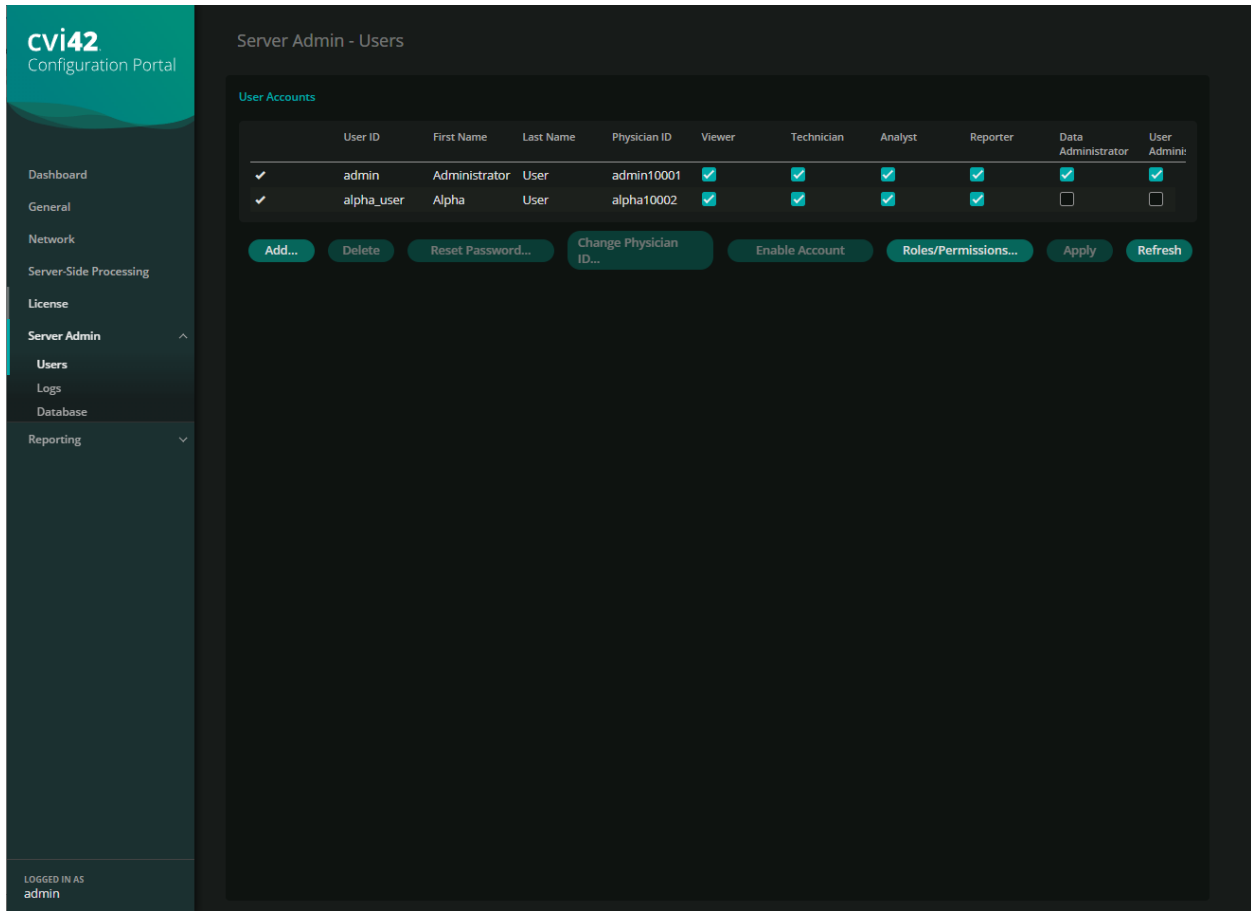
✓ Activate

License Renewal

✓ Renew Current Activation

LOGGED IN AS
admin

You can activate your licenses through entering an activation key, renew current activation or activate different activation keys for different types of licenses.



cv42 Configuration Portal

Server Admin - Users

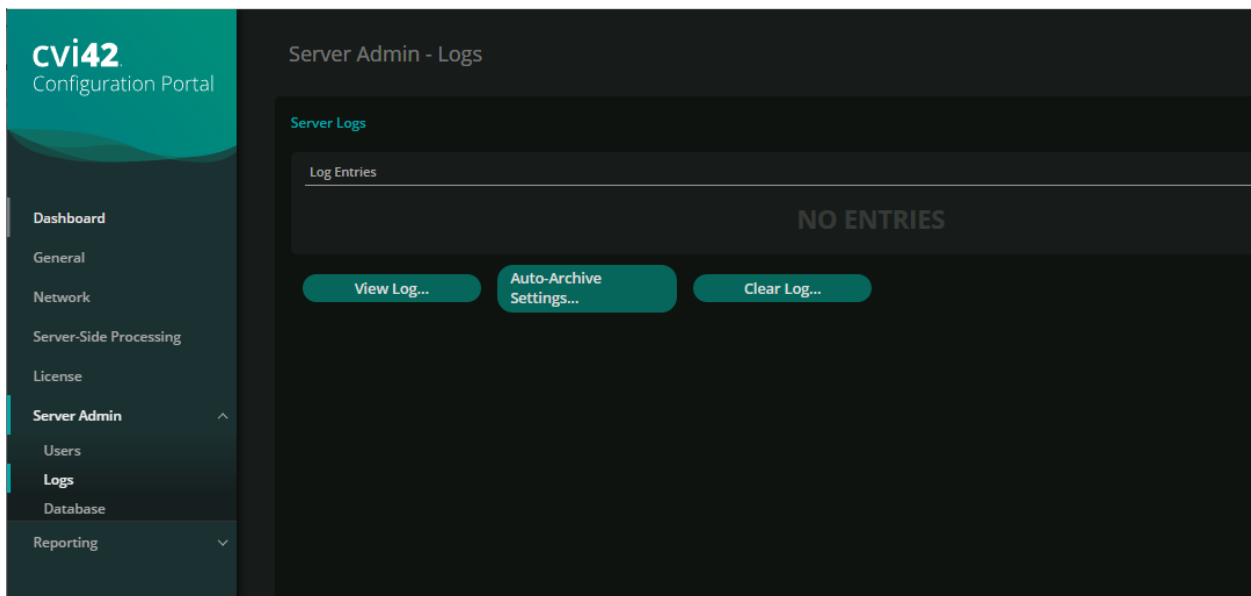
User Accounts

	User ID	First Name	Last Name	Physician ID	Viewer	Technician	Analyst	Reporter	Data Administrator	User Admin:
✓	admin	Administrator	User	admin10001	✓	✓	✓	✓	✓	✓
✓	alpha_user	Alpha	User	alpha10002	✓	✓	✓	✓	☐	☐

[Add...](#)
[Delete](#)
[Reset Password...](#)
[Change Physician ID...](#)
[Enable Account](#)
[Roles/Permissions...](#)
[Apply](#)
[Refresh](#)

LOGGED IN AS admin

In the Server Admin->Users, you have similar functionality you have in [Setting Up User Accounts](#).



cv42 Configuration Portal

Server Admin - Logs

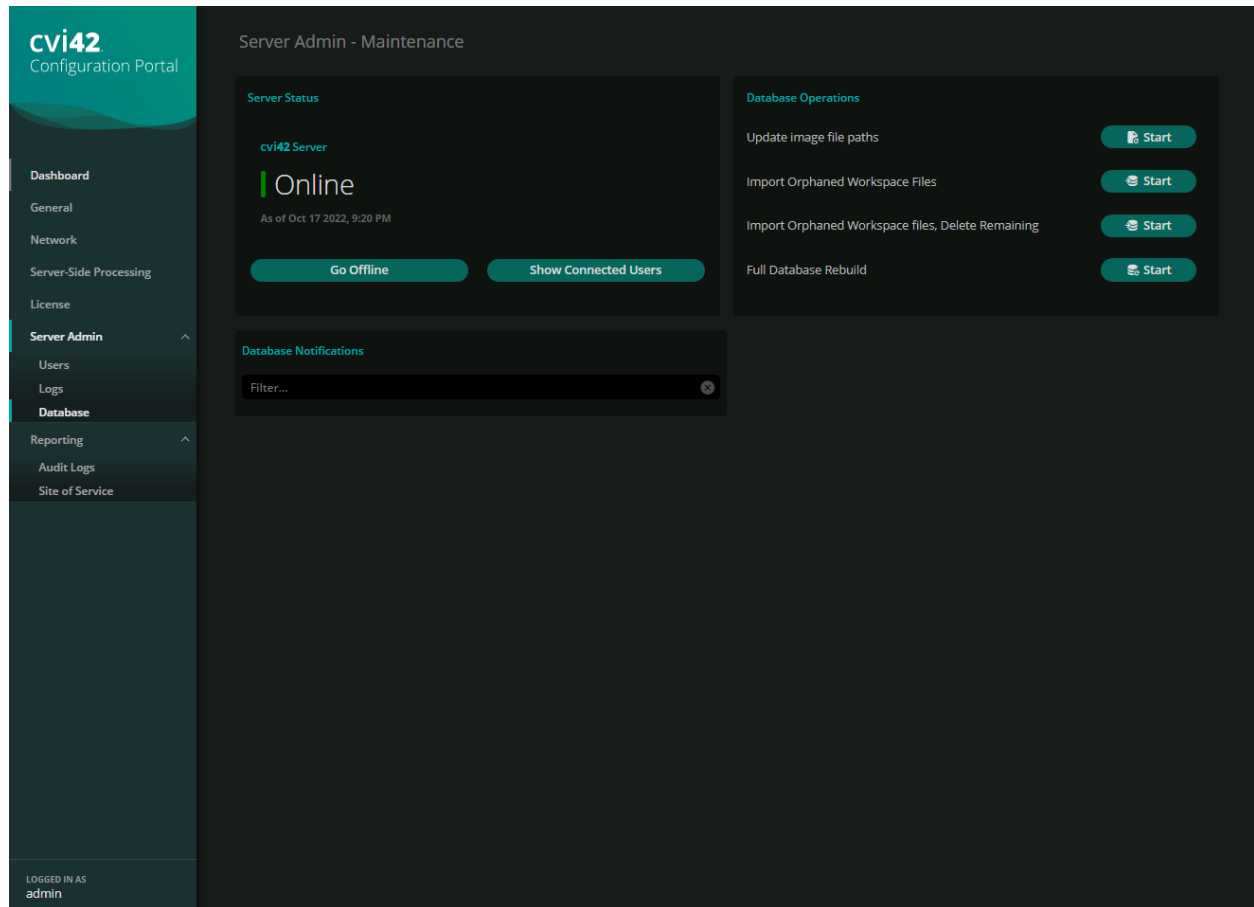
Server Logs

Log Entries

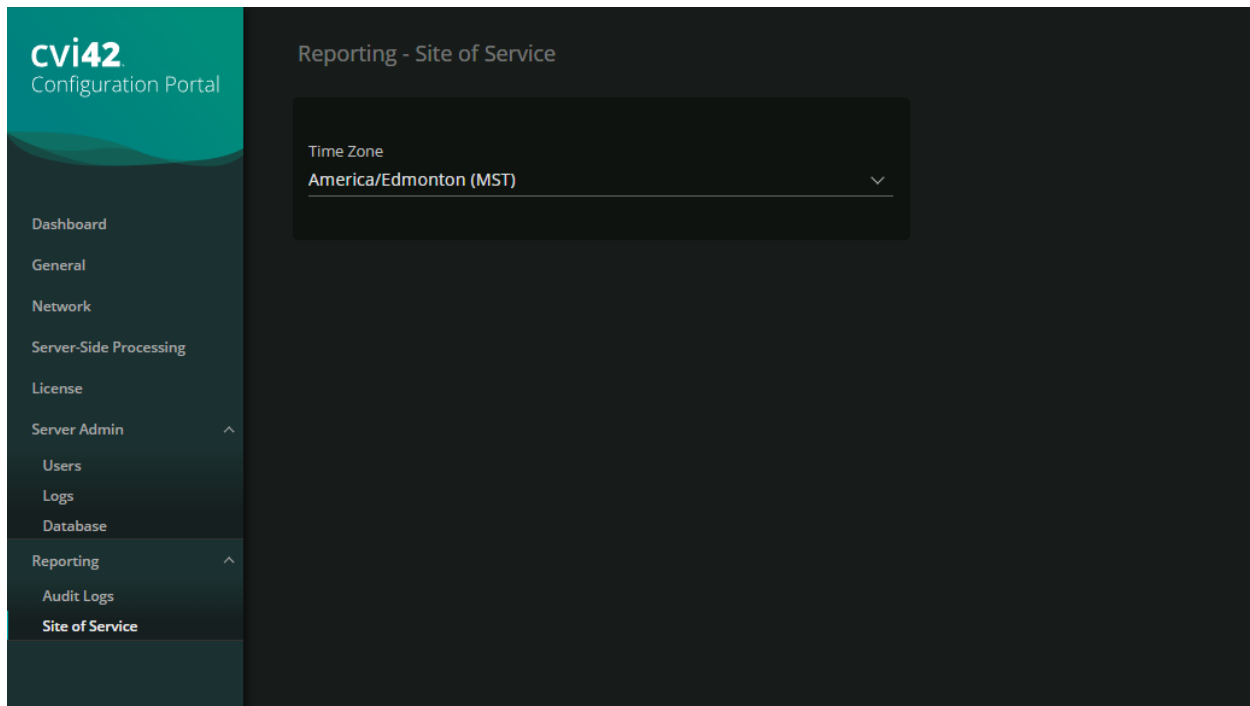
NO ENTRIES

[View Log...](#)
[Auto-Archive Settings...](#)
[Clear Log...](#)

You can manage the **cvi42** server logs.



You also have several functions to manage the **cvi42** server database.



And under *Reporting* you can set the reporting time zone.

9. Housekeeping

The housekeeping system is a rule-based system to automate maintenance of the **cvi42** DICOM study database. Typical use-cases are archival, routing and workflow.

9.1. Overview

All actions of the housekeeping system are defined by a list of rules. Each rule consists of a set of criteria and a list of actions. All criteria must be satisfied in order for a rule to apply to a specific DICOM study.

The housekeeping system is active according to a weekly schedule specified by the administrator. When the housekeeping system is active, it matches the list of rules against the **cvi42** DICOM study database periodically and executes resulting housekeeping actions. The matching interval is specified by the administrator.

9.1.1. Rule matching

The housekeeping system will periodically process the list of rules and match it against the studies present in the **cvi42** DICOM study database. For this, the system considers each study and matches its properties against the list of rules in order from top to bottom. When the criteria in a rule match, the actions specified in the rule are queued for execution. Subsequent rules will be matched against

the study under consideration once the actions of the applying rule have been executed. After a rule has matched or all rules have been considered for a specific study, the next study is matched against the rule list until all studies have been processed.

Once matching has completed, the queued housekeeping actions are executed.

9.1.2. Rule execution

All queued actions are processed in order of queuing. All actions are logged. Depending on the specific action, a failed action results in the execution of the whole rule to either fail or to be suspended for retry at the point of failure. Retry is supported for actions that are likely to succeed when retried such as DICOM study export (which may fail due to temporary lack of disk space) or DICOM network transmission (which may fail due to intermittent network problems or PACS server downtime).

After all queued rules have been executed, another rule matching run is invoked because rules in general depend on study attributes that are changed by rule execution, for example, assignment/removal of study tags.

9.2. Rules

Housekeeping rules consist of:

- a name (for reference)
- a flag for enabling/disabling a rule (temporarily or permanently)
- the recurrence definition:
 - "once" or "periodically" with an interval in days, weeks, months or years
- a list of criteria
- a list of actions

9.2.1. Criteria

9.2.1.1. Study Date

This criterion filters studies by the DICOM study-date attribute. Studies are filtered by their age, i.e. as "older than" or "newer than" a specified number of days, weeks, months or years.

Studies that lack the DICOM study-date are treated as "in the future" which means that rules that select studies that are i.e. "older than one year" will never match. It may make sense to use the "import date" criterion instead.

9.2.1.2. Study Description

This criterion filters studies by the DICOM "study description" attribute. The description is matched against either:

- a fixed string
- a fixed substring
- a wildcard pattern:
 - "?" matches any character
 - "*" matches zero or more arbitrary characters
 - "[...]" matches any of the characters listed inside the brackets
 - any other character matches only itself
- a regular expression:
 - Please see <http://qt-project.org/doc/qt-4.8/qregexp.html#introduction>.

Matching is set to be either case-sensitive or case-insensitive.

9.2.1.3. *Institution Name*

This criterion filters studies by the DICOM "institution name" attribute. The matching is done as described in section 9.2.1.2 Study Description.

9.2.1.4. *Manufacturer*

This criterion filters studies by the DICOM "manufacturer" attribute. The matching is done as described in section 9.2.1.2 Study Description.

9.2.1.5. *Model*

This criterion filters studies by the DICOM "model" attribute. The matching is done as described in section 9.2.1.2 Study Description.

9.2.1.6. *Modality*

This criterion filters studies by the DICOM "modality" attribute. The matching is done as described in section 9.2.1.2 Study Description.

9.2.1.7. *Study Size*

This criterion filters studies by their size (in MB). The studies are filtered by comparing the study size against a given size.

When upgrading from an earlier version of **cvi42** server, the study size database field is only initialized at first use. The first run of a housekeeping rule list that contains the study size criterion will thus take

significantly more time than subsequent runs because aggregating the study size from the DICOM image database causes high disk activity.

9.2.1.8. Import Date

This criterion filters studies by the import-date attribute. Studies are filtered by the age of the import date, i.e. as "older than" or "newer than" a specified number of days, weeks, months or years.

The import date is always present and is updated whenever new DICOM image data is added to a study.

9.2.1.9. Date of Last Read

This criterion filters studies by the date-of-last-read attribute. Studies are filtered by the age of this date, i.e. as "older than" or "newer than" a specified number of days, weeks, months or years.

The date of last read is initially empty and treated as "in the future" in this case. It is updated whenever the study is opened or closed. Display of the study in the patient list does not update the date of last read.

9.2.1.10. Date of Last Write

This criterion filters studies by the date-of-last-write attribute. Studies are filtered by the age of this date, i.e. as "older than" or "newer than" a specified number of days, weeks, months or years.

The date of last write is updated when the study is initially imported, images are added to or removed from the study or workspace data is saved.

9.2.1.11. Study Tags

This criterion filters studies by the tags assigned to the study. Studies are selected when the assigned tags "contain any of" or "miss any of" a given set of tags. Rules that require a study to "contain all of" or "miss all of" a given set of tags can be built by using multiple "Study Tags" criteria.

9.2.1.12. Available Disk-Space

This criterion relates to the available disk-space (in MB) of the storage media in which the DICOM image database file system resides. This value is not a study attribute and therefore enables or disables the rule altogether depending on the available disk-space. The available disk-space is compared to a specified value.

9.2.2. Actions

9.2.2.1. Assign Study Tags

This action assigns a given set of tags to the study. Assigning a tag that is already present is not an error. Other tags that are assigned to the study are kept.

9.2.2.2. Remove Study Tags

This action removes a given set of tags from the study. Removing a tag that is not present is not an error.

9.2.2.3. Convert Workspace Data to DICOM

This action converts all workspace data of the study to DICOM workspace format. Workspace data of all users is converted. This action is useful to run before 9.2.2.4 Store DICOM Data on PACS or 9.2.2.5 Export DICOM Data to filesystem such that the corresponding workspace data is transferred alongside the DICOM image data.

This action has the option to use the "Secondary Capture Image Storage" DICOM SOP class instead of "Multiframe Grayscale Byte Secondary Capture Image Storage" or "Multiframe True Color Secondary Capture Image Storage" DICOM SOP class if necessary.

9.2.2.4. Store DICOM Data on PACS

This action stores DICOM data of the study on a specific DICOM node. This action can either store all DICOM data or can be limited to only store DICOMs generated by **cvi42**. In the latter case, the action can be further limited to only store workspace DICOMs, report DICOMs and/or other DICOMs generated by **cvi42** (i.e. reformatted images).

As this action can potentially cause data to be sent to unintended destinations, special care must be taken when using this action. Please, refer to section 9.3.1 Simulation for steps on verifying that the rule matches only the desired studies.

Please note that if PACS names have been changed or added in the configuration dialogue but not yet saved to the server, the Housekeeping configuration UI will still show the names as configured on the server.

9.2.2.5. Export DICOM Data to filesystem

This action exports DICOM data to filesystem. The type of DICOM data that is exported can be limited as described in section 9.2.2.4 Store DICOM Data on PACS. The directory path specified as export target may contain the following placeholders which allow to automatically build up a chronological directory structure:

- "{YYYY}" is replaced by the 4-digit year
- "{YY}" is replaced by the 2-digit year
- "{MM}" is replaced by the 2-digit month
- "{DD}" is replaced by the 2-digit day of the month

Placeholders may occur multiple times. Example: "E:\DicomArchive\{YYYY}\{YYYY}-{MM}\\" will export to:

- "E:\DicomArchive\2014\2014-12\\"

- "E:\DicomArchive\2015\2015-01\"
- "E:\DicomArchive\2015\2015-02\"
- ...

Each study will be placed into an individual sub-directory of the specified export directory.

9.2.2.6. Delete Study

This action removes all DICOM data and workspaces of the given study from the database. As this action is not revertible, special care must be taken when using this action. Please, refer to section 9.3.1 Simulation for steps on verifying that the rule matches only the desired studies.

Alternatively, refer to section 9.2.2.1 Assign Study Tags in order to assign a "trash bin" tag instead of directly deleting the studies. This allows to review which studies are assigned to the "trash bin" tag and then delete those manually from the patient list.

9.2.2.7. Stop processing subsequent rules

This action causes the subsequent rules in the rule list not to be considered for the matched study. The stop is active as long as the study still matches the criteria, i.e. independently of rule recurrence.

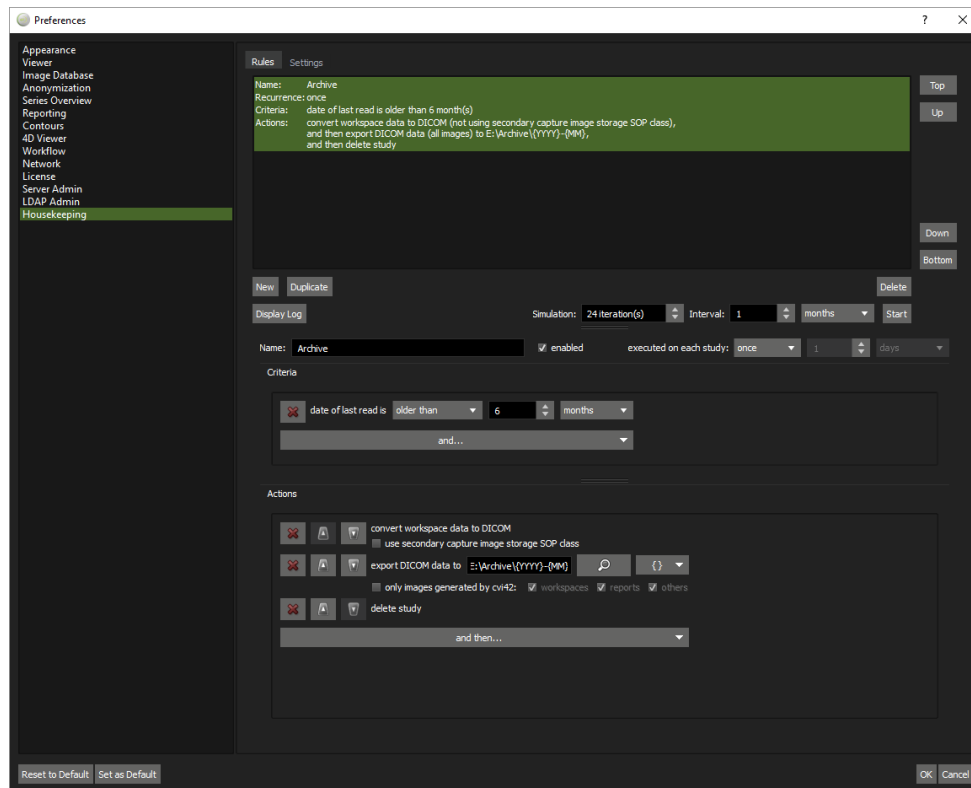
9.2.3. Recurrence

Recurrence defines whether a rule is applied repeatedly to the same study. Recurrence is defined as either of:

- "once" – the rule is only applied once to each matching study. Even if the rule criteria/actions are changed later, studies that have been processed by the rule once, are not considered again. (If it is intended that the rule shall be applied again to all matching studies once, i.e. because the criteria or actions have been changed, the rule can be duplicated, and the original rule be deleted. The duplicated rule is considered unrelated by the Housekeeping system and all studies will be considered for the rule again.)
- "periodically every N days/weeks/months/years" – the rule is considered again for a previously processed study after the specified time has elapsed after queuing of the last rule execution on the study.

Rule recurrence can be changed later. After switching from "once" to "periodically", studies that have been processed before are considered again (after elapse of the period interval). Likewise, after switching from "periodically" to "once" all studies that have ever been processed are not considered anymore.

9.3. Rule Editor



The rule editor is located in the "Rules" tab of the Housekeeping section of the configuration dialogue. The Housekeeping section is only enabled when connected to the server administrator port. In the upper part of the rule editor, the rule list is displayed. For each rule, the name, recurrence, criteria and actions are listed. The names of disabled rules are written in *italic*.

The top/up/down/bottom buttons to the right of the rule list are used to move the currently selected rule to the top/bottom or up/down in the list. The new/duplicate/delete buttons below the rule list are used to create, duplicate or delete rules.

The "display log" button is used to open the log and control interface (refer to section 9.4.1.1 Log and Control). To the right of the "display log button", the effect of the edited (unsaved) rule list can be simulated, refer to section 9.3.1 Simulation.

In the lower part of the rule editor, the currently selected rule can be edited. This section starts with the field for the rule name, the "enabled" checkbox and the specification of the recurrence. Below, there are two panes in which the criteria and actions are composed.

The criteria are composed by clicking "and . . ." and selecting the desired criterion (repeatedly). For each criterion, a line is added to the criteria pane for editing the specific properties of the criterion. A criterion can be removed again by clicking the "x" button at the start of the line. As all criteria are combined by a logical "and", the order is insignificant and cannot be changed.

The actions are composed by clicking "and then . . ." and selecting the desired action (repeatedly). For each action, a line is added to the actions pane for editing the specific properties of the action. An action can be removed again by clicking the "x" button at the start of the line. As the order of actions

is significant, actions can be reordered using the "move up" and "move down" buttons next to the "x" button.

Please note that new rules are initially set as "disabled" such that the "enabled" checkbox needs to be ticked manually after the rule has been composed.

Please note that when a rule is deleted, executions of the rule which have already been queued but have not yet been processed are cancelled.

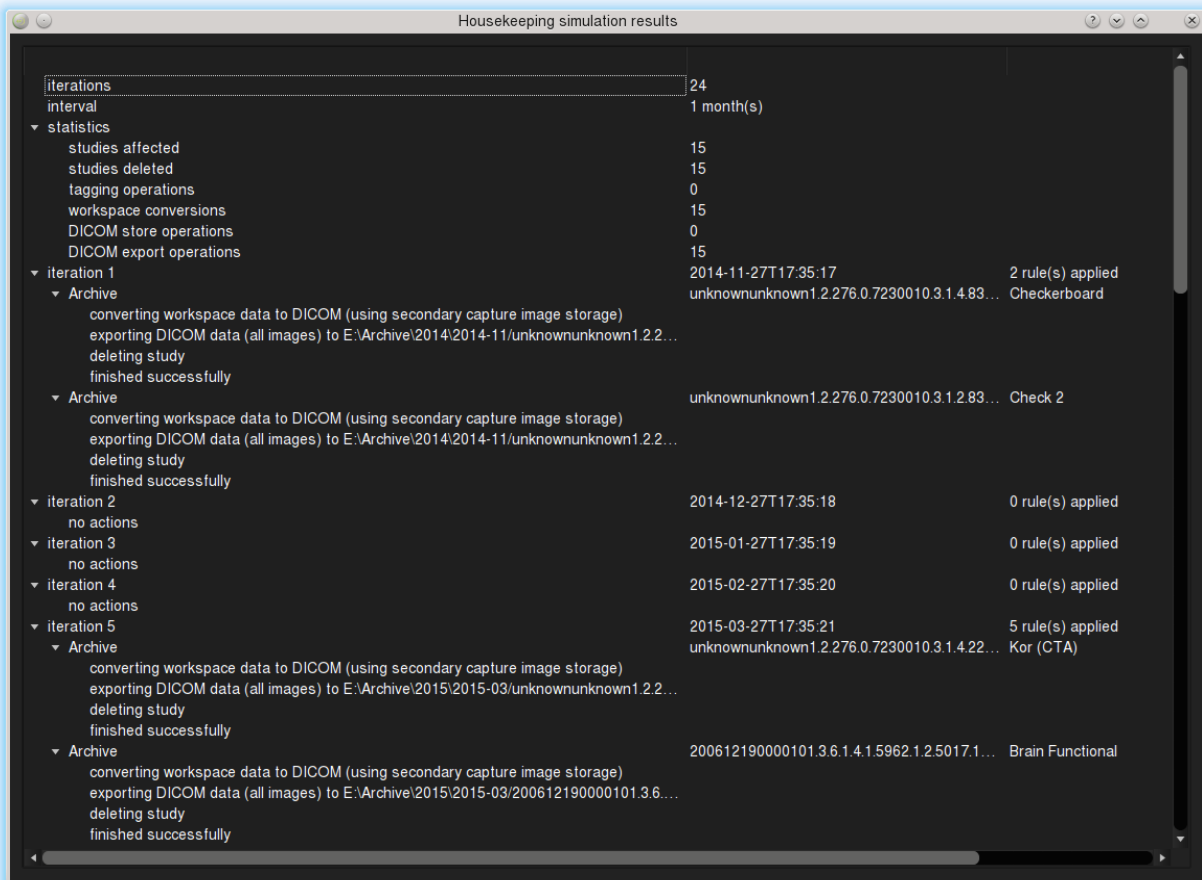
9.3.1. Simulation

The currently edited rule list can always be simulated against the current **cvi42** DICOM study database. Only rules that are marked as "enabled" are active in simulation as in execution. A simulation is started by specifying a number of simulation iterations, a time interval for each iteration and clicking the "start" button. As many rules include ages (i.e. age since study import, age since last read, ...) it is important to cover a relevant time-span for simulation. For example, when working on a rule that archives data after a year, selecting a simulation of 24 iterations with an interval of one month would be appropriate while in contrast 10 iterations with an interval of one day wouldn't give meaningful results.

Apart from the effect of the lapsed time, simulation also handles the effects of tag assignment/removal and the stop action. This can be used to simulate workflow rule sets. Simulation also handles study deletion and will not match rules against studies that are simulated as deleted again.

Other actions are merely logged for the simulation results, i.e. when simulating "convert workspace data to DICOM", "store DICOM data on PACS" or "export DICOM data to filesystem" actions, no further simulation such as checking DICOM node connectivity or checking for available disk-space is carried out.

While simulation is running, a progress indicator is shown in the "simulation" section of the rule editor. Once finished, the results are displayed in a separate "Housekeeping simulation results" window.



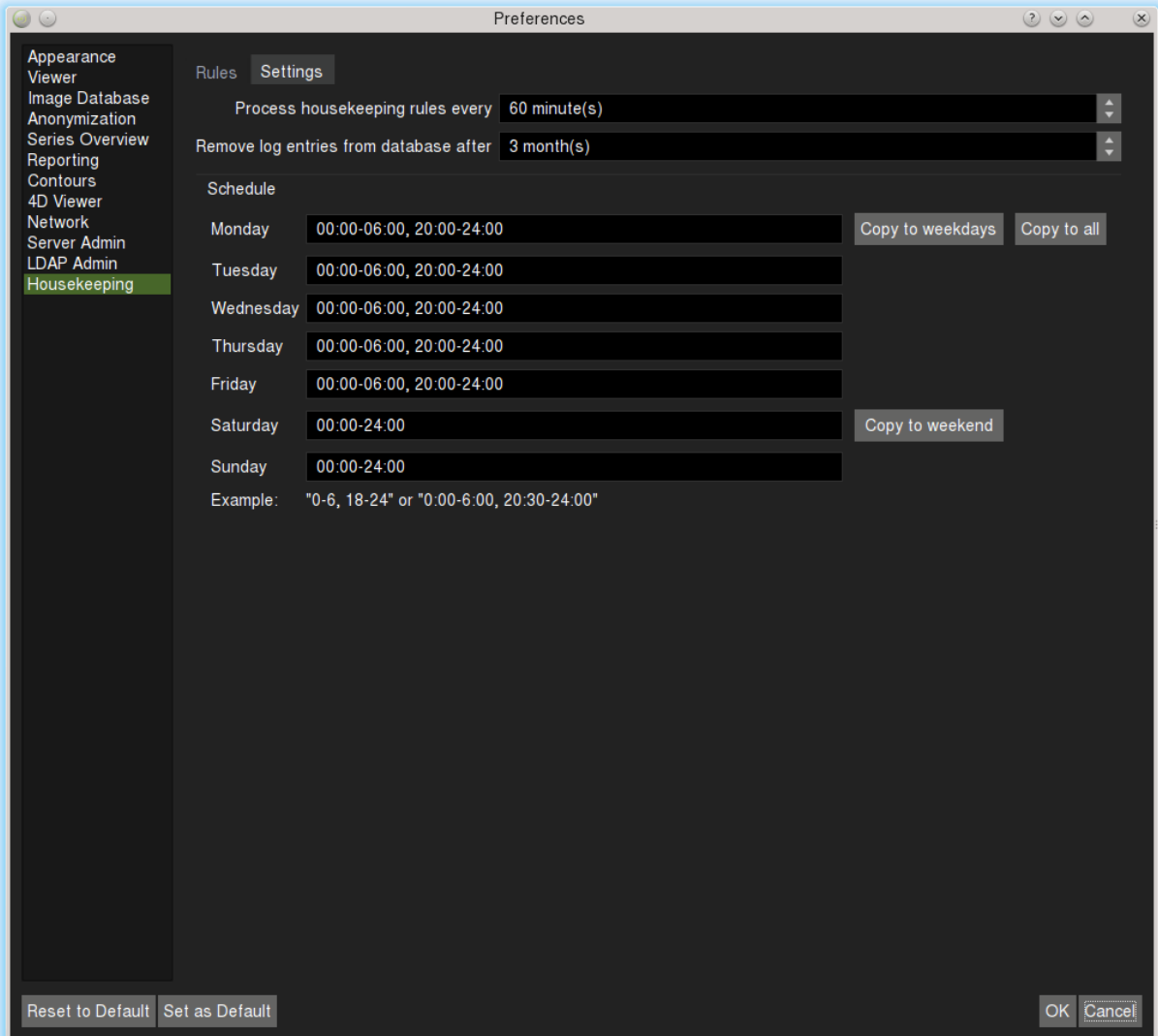
Housekeeping simulation results		
iterations	24	
interval	1 month(s)	
▼ statistics		
studies affected	15	
studies deleted	15	
tagging operations	0	
workspace conversions	15	
DICOM store operations	0	
DICOM export operations	15	
▼ iteration 1	2014-11-27T17:35:17 2 rule(s) applied	
▼ Archive	unknownunknown1.2.276.0.7230010.3.1.4.83... Checkerboard	
converting workspace data to DICOM (using secondary capture image storage)		
exporting DICOM data (all images) to E:\Archive\2014\2014-11\unknownunknown1.2.2...		
deleting study		
finished successfully		
▼ Archive	unknownunknown1.2.276.0.7230010.3.1.2.83... Check 2	
converting workspace data to DICOM (using secondary capture image storage)		
exporting DICOM data (all images) to E:\Archive\2014\2014-11\unknownunknown1.2.2...		
deleting study		
finished successfully		
▼ iteration 2	2014-12-27T17:35:18 0 rule(s) applied	
no actions		
▼ iteration 3	2015-01-27T17:35:19 0 rule(s) applied	
no actions		
▼ iteration 4	2015-02-27T17:35:20 0 rule(s) applied	
no actions		
▼ iteration 5	2015-03-27T17:35:21 5 rule(s) applied	
▼ Archive	unknownunknown1.2.276.0.7230010.3.1.4.22... Kor (CTA)	
converting workspace data to DICOM (using secondary capture image storage)		
exporting DICOM data (all images) to E:\Archive\2015\2015-03\unknownunknown1.2.2...		
deleting study		
finished successfully		
▼ Archive	200612190000101.3.6.1.4.1.5962.1.2.5017.1... Brain Functional	
converting workspace data to DICOM (using secondary capture image storage)		
exporting DICOM data (all images) to E:\Archive\2015\2015-03\200612190000101.3.6...		
deleting study		
finished successfully		

The result first lists the selected number of iterations and interval. Then a statistical summary of the simulation is given, counting the total number of affected studies and how often actions of different classes were executed (studies deleted, tagging operations, workspace conversions, DICOM store operations, DICOM export operations).

Next, the individual simulation iterations are listed: The first line lists the simulated date and how many rules applied in total. Then, each rule application is listed by the rule name, the study that the rule applied to (including the DICOM study instance UID and the patient name for reference) and the list of actions that were simulated.

Please take care to review the simulation results carefully to make sure the rule list behaves as intended. This is particularly important for rule lists that include the "delete study" action which can lead to irrevocable data loss and for rule lists that include the "store DICOM data on PACS" action which can potentially lead to sending data to unintended destinations.

9.4. Settings



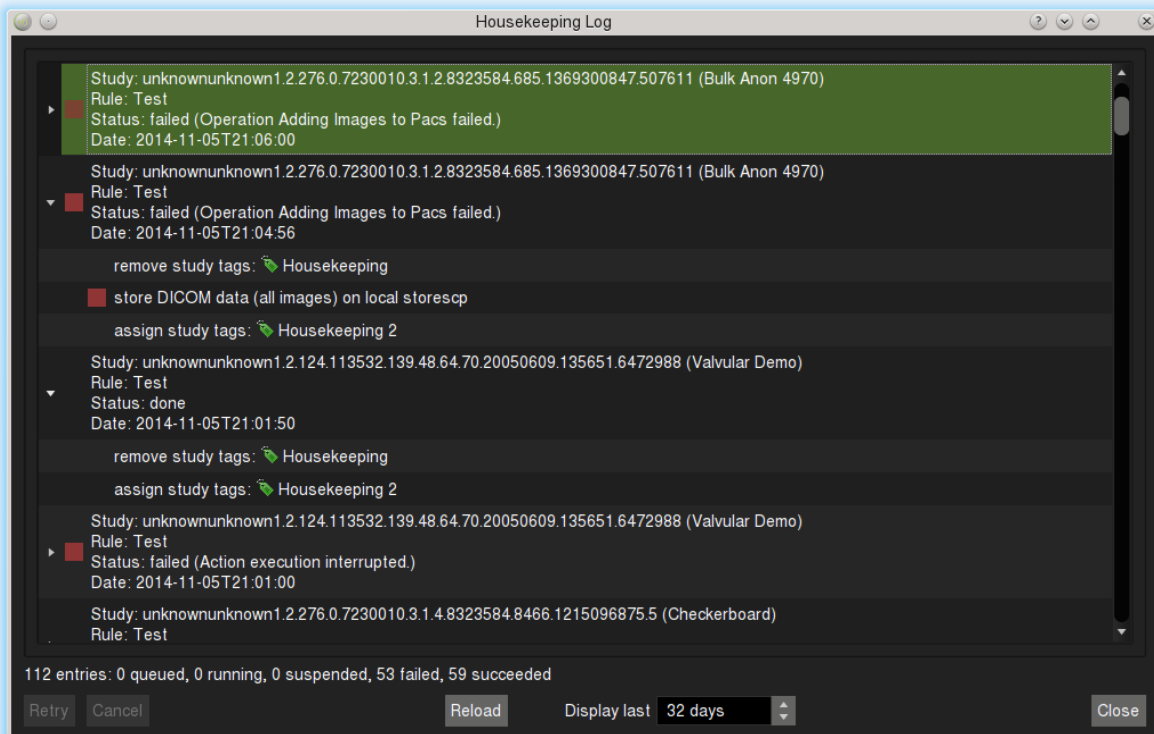
In the "Settings" tab of the Housekeeping section in the configuration dialogue, parameters for the overall behaviour of the Housekeeping system are specified.

The first setting is the interval in which the housekeeping system processes its rule list during hours of operation. Smaller values put a higher load on the server but may be desirable when using rule lists for workflow organization.

The second setting specifies how long the server will retain log entries inside the database. These log entries are displayed in the 9.4.1.1 Log and Control. Only log entries that are not needed for the system anymore (i.e. for keeping track of which studies a rule has already been applied to) are removed from the database after the specified period of time. Apart from the logs kept in the database, the Housekeeping system also logs all actions to the `logHousekeeping.txt` file to which this setting does not apply.

Below this, the Housekeeping system schedule can be defined as a list of timespans per weekday. Buttons are provided to copy the data entered for Monday to all week or all weekdays and to copy the data entered for Saturday to all weekend. The schedule can be used to ensure, the Housekeeping system activities do not interfere with day-time usage of the system.

9.4.1.1. Log and Control



The log and control interface displays the most recent activities of the Housekeeping system. For each applied rule, the study (including DICOM study instance UID and patient name for reference), the rule name, the status and the date of the entry are displayed.

While the rule is queued for execution, it is marked with a blue button. If rule execution has failed, it is marked with a red button. If it is suspended for retry, it is marked with a yellow button. Each entry can be expanded by clicking on the triangle icon to the left in order to display the specific actions.

At the bottom of the window, the retry/cancel buttons can be used to retry or cancel selected suspended rules. As studies that have a suspended rule are not considered for other rules, it is important to review the log periodically. Queued rule executions cannot be cancelled manually but are cancelled when the rule is deleted.

The reload button reloads the log from the server. The spin-box next to it is used to specify the timespan to display the log for. After changing the timespan, the list is reloaded automatically.

Appendix A: cvi42 Default Roles

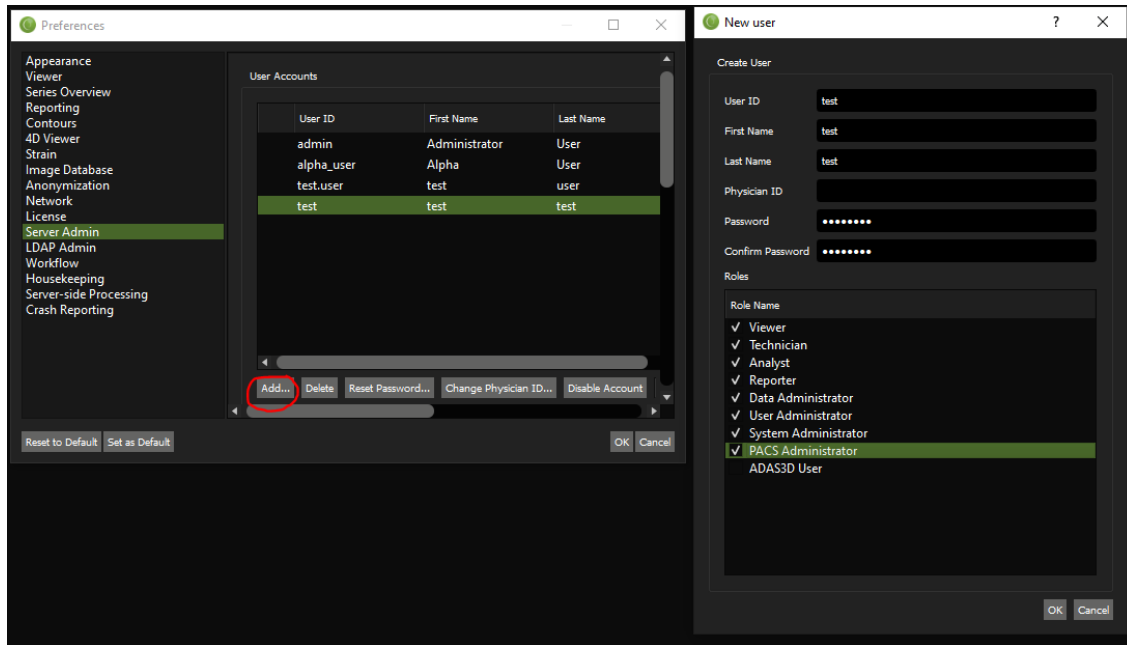
Role	Permissions
Viewer	Able to view study data and existing workspaces.
Technician	Able to import study data and enter patient biometric data.
Analyst	Able to save analysis on study data in workspaces or copy other user workspaces.
Reporter	Able to report on study data.
Data Administrator	Able to clean up the database and unlock user accounts.
User Administrator	Able to create, edit, and delete users accounts.
System Administrator	Able to alter system properties and administrate logs.
PACS Administrator	Able to manage PACS server connection properties
ADAS3D User	Able to open studies in ADAS3D

Appendix B: cvi42 Network Communications Matrix

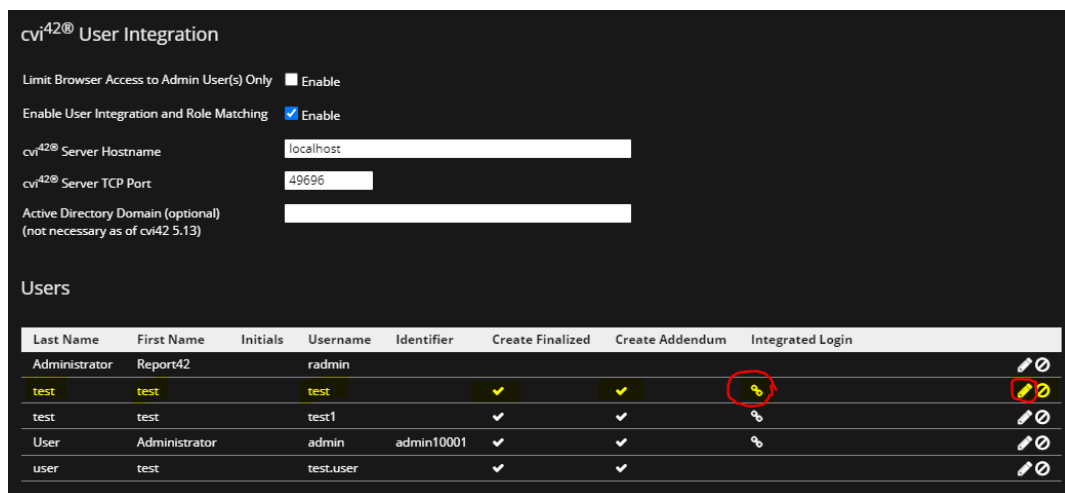
Source	Destination	Default Port	Comment
cvi42 client	cvi42 server	tcp/49696	Regular user port with no encryption
cvi42 client	cvi42 server	tcp/4390	Regular user port with TLS encryption
cvi42 client	cvi42 server	tcp/49697	Admin user port with no encryption
cvi42 client	cvi42 server	tcp/4391	Admin user port with TLS encryption
cvi42 client / web-browser	cvi42 report webserver (Apache)	tcp/4280 (http/https, websocket)	Report Web Interface
cvi42 client	cvi42 server side processing (node42)	tcp/4298 (http/https)	When server-side processing is enabled
cvi42 report webserver	MirthConnect	tcp/6680	HL7
cvi42 report webserver	cvi42 Web Configurator	tcp/4299 (http)	Server configuration web interface
PACS	cvi42 server	tcp/104	DICOM
cvi42 server	PPU server (cloud)	tcp/443 (https)	When licensed for PPU
cvi42 server	RLM Activation Pro server (cloud)	tcp/443 (https)	When activating license
Browser	cvi42 Web Configurator	tcp/4299 (http)	Server configuration web interface

Appendix C: Converting cvi42 | Report Users to built-in cvi42 users

1. Login to cvi42 as an admin user through Server Port 49697
2. Open the Config window under Preferences
3. In "Server Admin", create a new user with the following roles:



4. Disconnect from the current cvi42 server, and re-login as the new user through Server Port 49696 (verify that the user can login before moving on)
5. In a browser (e.g. Chrome), login to report through port 4280 (e.g. localhost:4280) as the new user (verify that the user can login before moving on)
6. Navigate to "Users" through "Admin Settings" -> "System/Report Content" -> "Users"
7. Locate the new user in the list and confirm that there is a linked chain symbol under the "Integrated Login" column for that user. Then click on the pencil icon in its row.



8. Click the "Convert to Local User" button, enter a new password for the user and save changes.

Username*

test

First Name*

test

Last Name*

test

Initials

User Prefix

User Suffix

Physician Identifier

Convert to Local User

Roles

☐ Viewer

☐ Analyst

☐ Data Administrator

☐ System Administrator

☐ ADAS3D User

☒ Technician

☒ Reporter

☒ User Administrator

☒ PACS Administrator

Permissions

☐ View In Progress

☐ View Complete

☐ View Preliminary

☐ View Finalized

☐ View Addendum

☐ Create In Progress

☐ Edit In Progress

☐ Create Complete

Save changes

Cancel

Username*

test

First Name*

test

Last Name*

test

Initials

User Prefix

User Suffix

Physician Identifier

Password*

Re-Type Password*

Please enter the same value again.

Roles

☒ Viewer

☒ Analyst

☒ Data Administrator

☒ System Administrator

☐ ADAS3D User

☒ Technician

☒ Reporter

☒ User Administrator

☒ PACS Administrator

Permissions

☐ View In Progress

☐ View Complete

☐ View Preliminary

☐ View Finalized

☐ View Addendum

☐ Create In Progress

☐ Edit In Progress

☐ Create Complete

Save changes

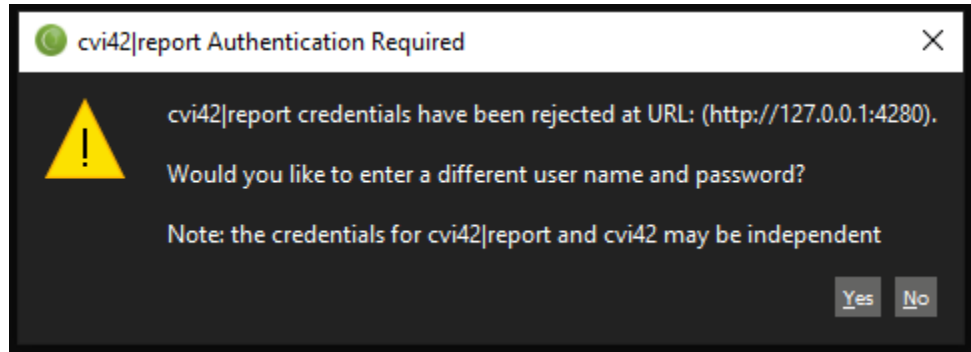
Cancel

9. Check that the linked chain has been removed from the "Integrated Login" column.

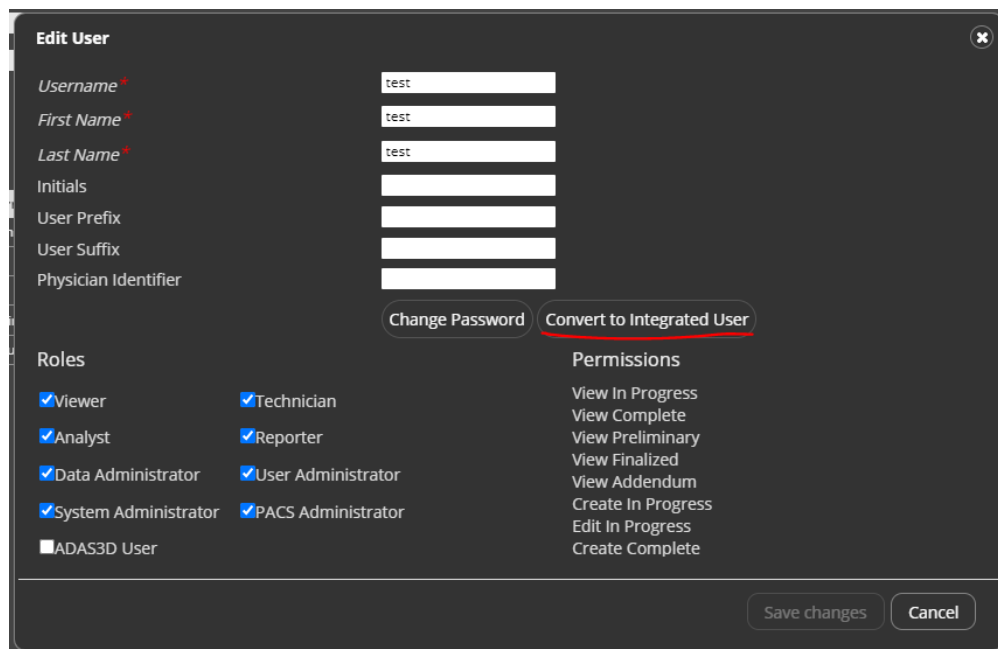
Users							
Last Name	First Name	Initials	Username	Identifier	Create Finalized	Create Addendum	Integrated Login
Administrator	Report42		radmin				
test	test	test	test1		✓	✓	
test	test	test	test1		✓	✓	
User	Administrator	admin	admin10001		✓	✓	
user	test	test.user	test.user		✓	✓	

74

10. Login as the new user through Server Port 49696 using the **original** password. Confirm that the credentials have been rejected by report by observing this pop-up.



11. In a browser (e.g. Chrome), login to report through port 4280 (e.g. localhost:4280) as an admin.
12. Navigate to "Users" through "Admin Settings" -> "System/Report Content" -> "Users"
13. Locate the new user in the list of Users and click on the pencil icon in its row.
14. Click the "Convert to Integrated User" button.



15. Verify that the admin can no longer change fields such as Username, First Name, and Last Name, then Save Changes.
16. Check that the linked chain is present in the "Integrated Login" column.

Last Name	First Name	Initials	Username	Identifier	Create Finalized	Create Addendum	Integrated Login	
Administrator	Report42		radmin					 
test	test	test			✓	✓		 
test	test		test1		✓	✓		 
User	Administrator		admin	admin10001	✓	✓		 
user	test		test.user		✓	✓		 

17. Log out and log in as the new user with the password given in step 8 ("newpassword").
Confirm the user is no longer able to log in.
18. Login as the new user through Server Port 49696 using the **original** password ("password").
Confirm the user can access report.