cvi42®

v.5.14.3

Client Server Installation and Configuration Guide

circle CARDIOVASCULAR IMAGING

CVi42

CLIENT SERVER INSTALLATION AND CONFIGURATION GUIDE

November 2022

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

Telephone: 1 (587) 747-4692

Support: support@circlecvi.com

http://www.circlecvi.com

Table of Contents

1. Installing cvi42

IMPORTANT: When deploying and configuring a **cvi42** server, you *must* use the Enterprise Installer package of **cvi42**

Before installing the latest version of **cvi42**, *uninstall* any previous versions of **cvi42** that may exist on your system.

1.1. Installing cvi42 on Windows Platform

The **cvi42** client is supported on Windows 10 and Windows 11. **cvi42** server can be installed on Windows Server 2012 R2, 2016, 2019 or 2022.

Before starting the installation process, it is recommended that you first uninstall the current deployment. To do so, go to `Start→Settings→Apps→Uninstall`.

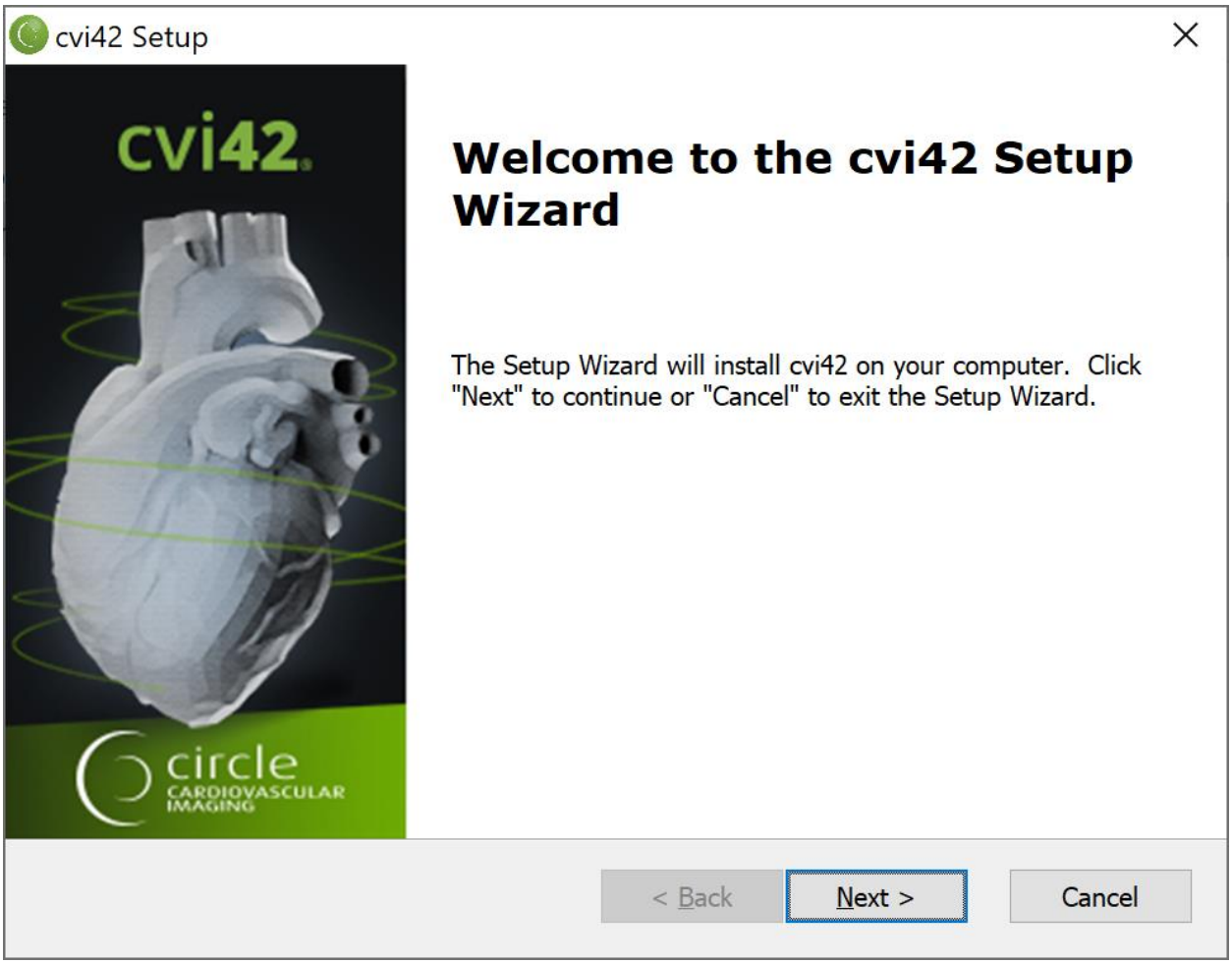
If you intended to re-install the same version of **cvi42** on top of the existing installed version, you should stop any existing **cvi42** servers/services and any license servers that may have been configured for **cvi42**. Go to `Start→Control Panel→System→Administrative Tools→Services` and stop the **cvi42** Server/Service.

RLM licensing server services for **cvi42** should also be stopped (if one has been configured).

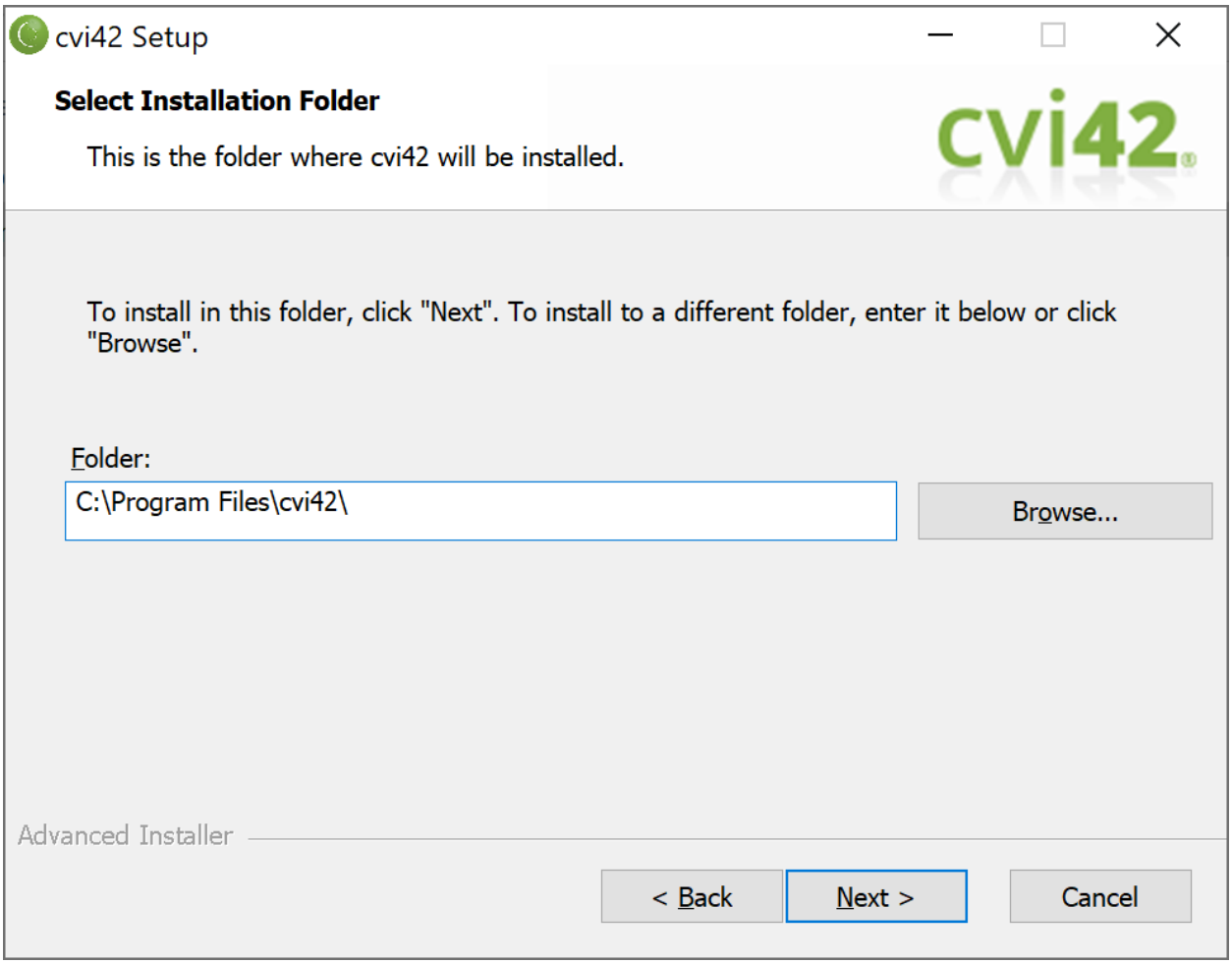
1.1.1. Installing the Server/Client Using the Setup Program

The easiest way to install **cvi42** is to run the **cvi42** setup program, which will automatically perform all the necessary configuration steps.

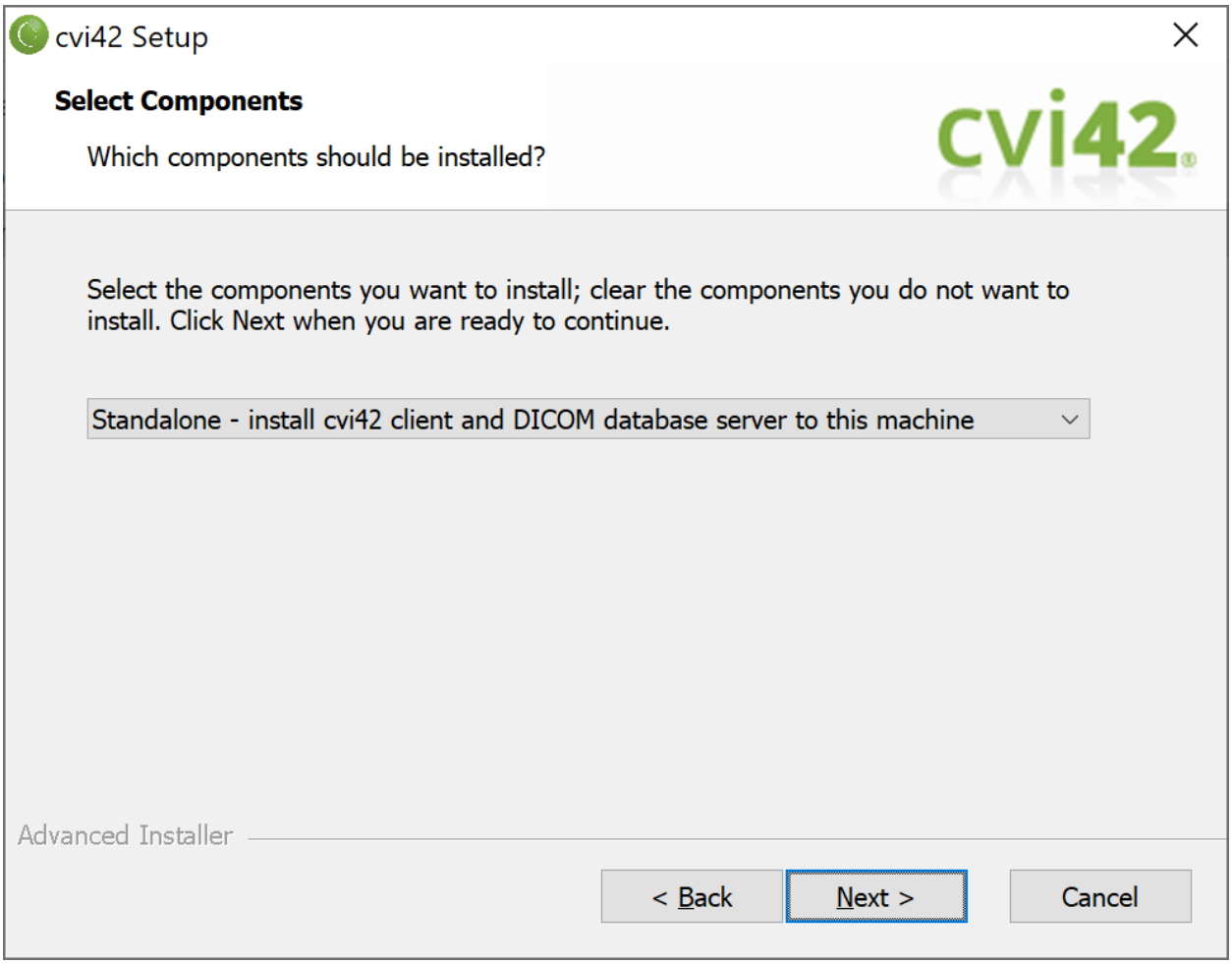
You will need to log in to an account with administrator privileges on the machine you are installing to.



Click *Next* to continue.

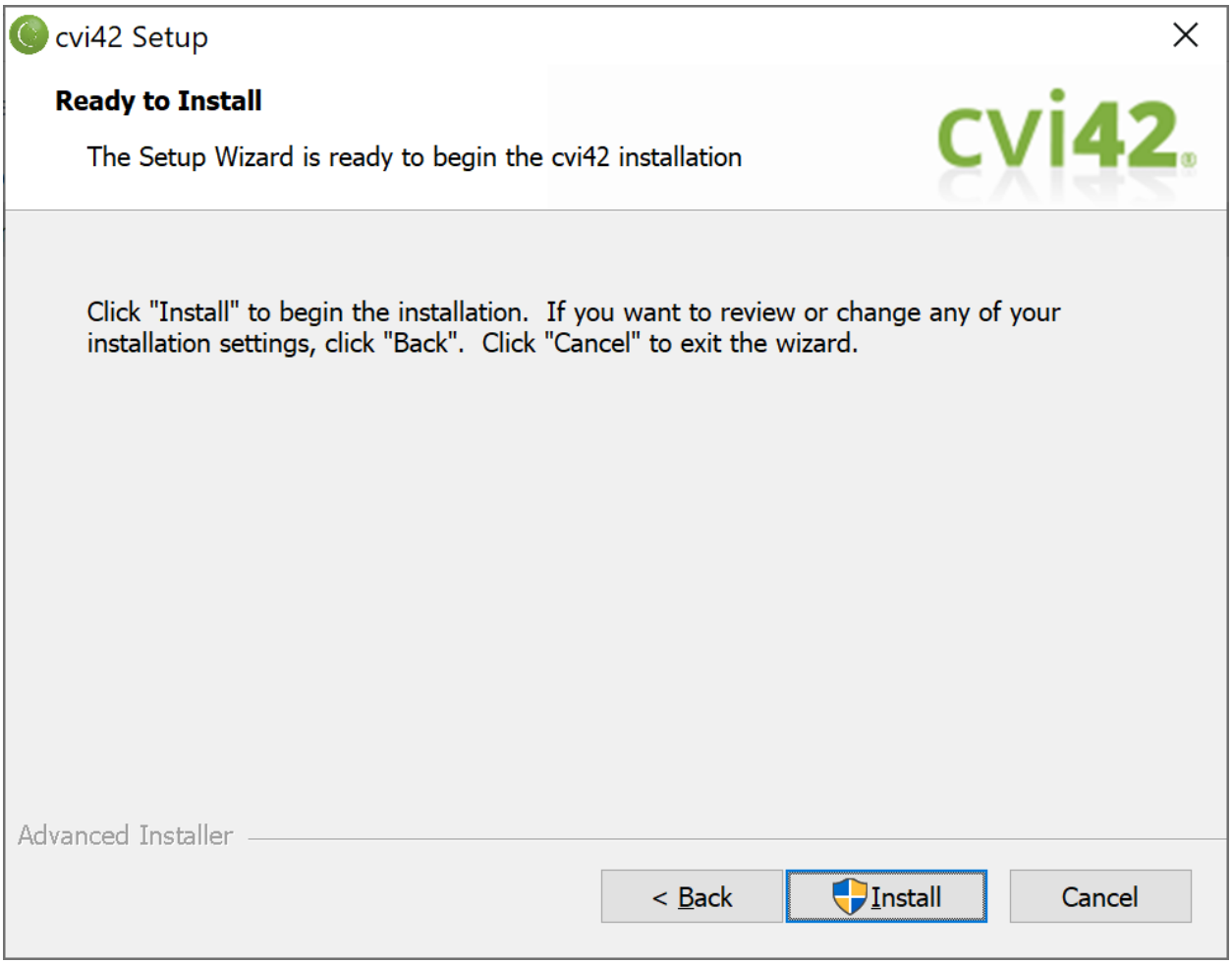


Select the folder location for installation. Click *Next* to continue.

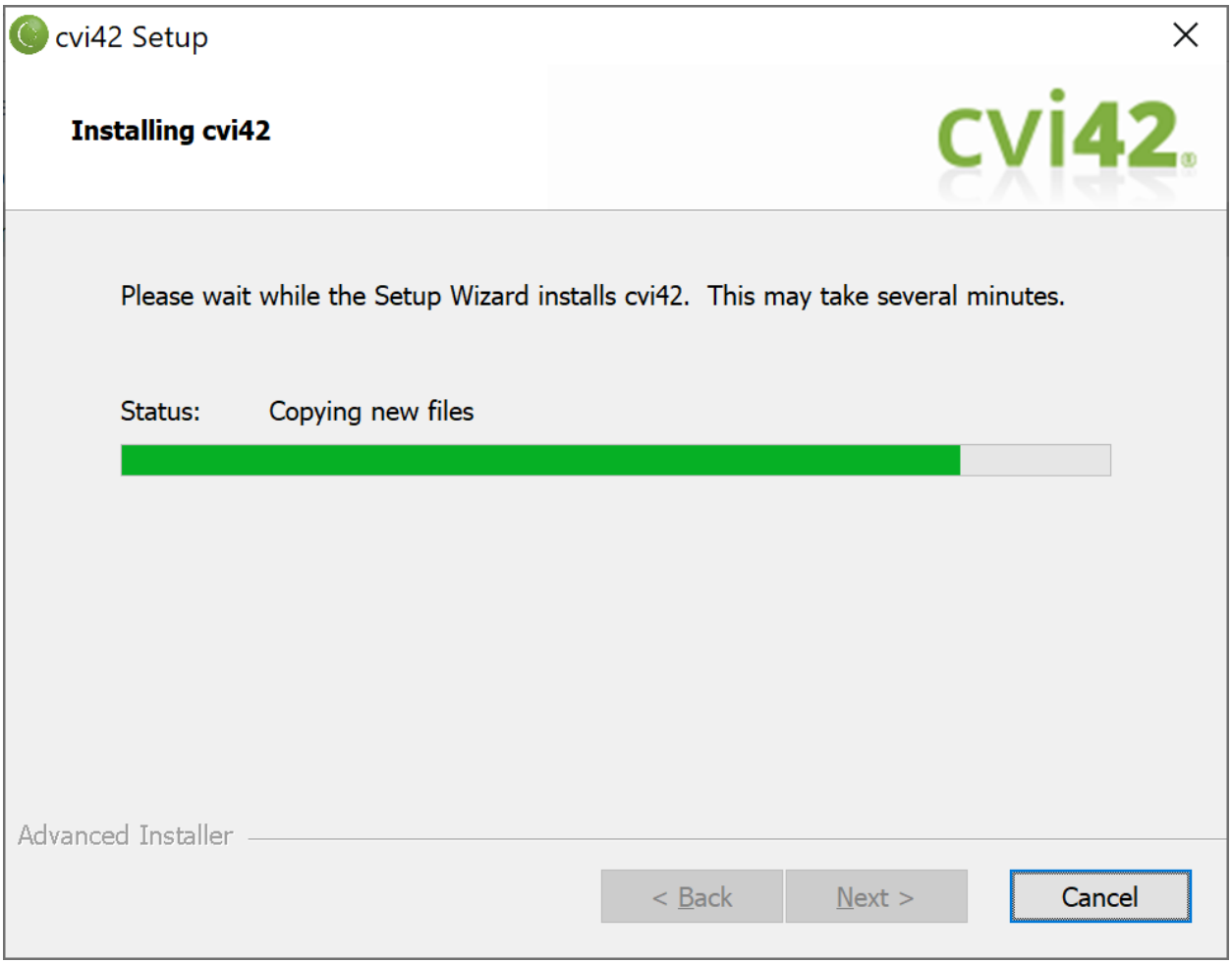


Select which components should be installed. Click *Next* to display the Software Usage Terms & Conditions.

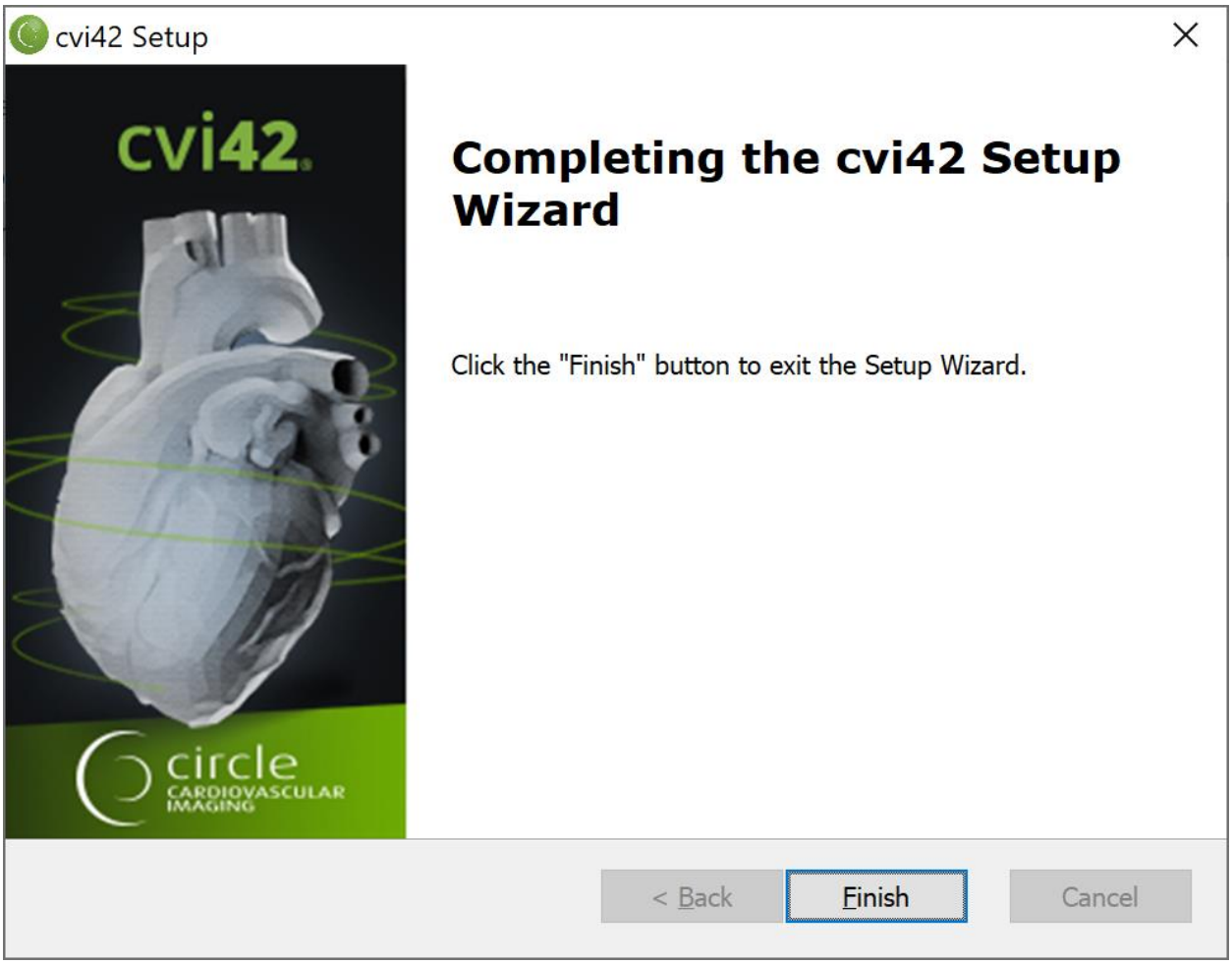
Accept the agreement and click *Next*.



Review the selected installation choices, and click *Install* to continue, or *Back* if changes are necessary.



The installer will display a progress bar during installation.



Click *Finish*, to exit the setup program.

1.1.2. Automating the `.exe` Installer

The `.exe` installer can be automated using Windows' system command along with various installer parameters. Here are the following installer parameters accepted by the `.exe` installer:

- **`IAgree`** – Indicates that the user agrees with the stated software usage terms and conditions. This parameter accepts the following values: `Yes`, `No`
  example: `IAgree="Yes"`
- **`APPDIR`** – Specify where **cvi42** will be installed on the hard drive.
  i.e. `APPDIR="C:\Program Files\cvi42"`
- **`COMP`** – Specifies whether this is a standalone or client only installation. This parameter accepts the following value: `Standalone`, `ClientOnly`
  example: `COMP="ClientOnly"`
- **`SERV_NAME`** – Specifies a name for **cvi42**. This name is shown to users when logging into **cvi42**.
  example: `SERV_NAME="My cvi42 Server"`

- **SERV_ADDR** – Specifies the IP address/Domain name of where **cvi42** is located.
  example: `SERV_ADDR="172.16.5.12"`

From the Command Prompt a user may automate the `.exe` installer by typing the following commands:

```
cd \<Location of exe Installer> (e.g. cd \Work\Downloads)

"<name of exe file>" /quiet IAgree="Yes" APPDIR="C:\Program Files\cvi42"

COMP="ClientOnly" SERV_NAME="My cvi42 Server" SERV_ADDR="172.16.5.12"

/l*v log.txt
```

The above example shows some common command line switches used by Windows:

- **/quiet** – quiet mode, no user interaction
- **/l*v <LogFile>** – log all information except extra debugging information

More information can be found here:

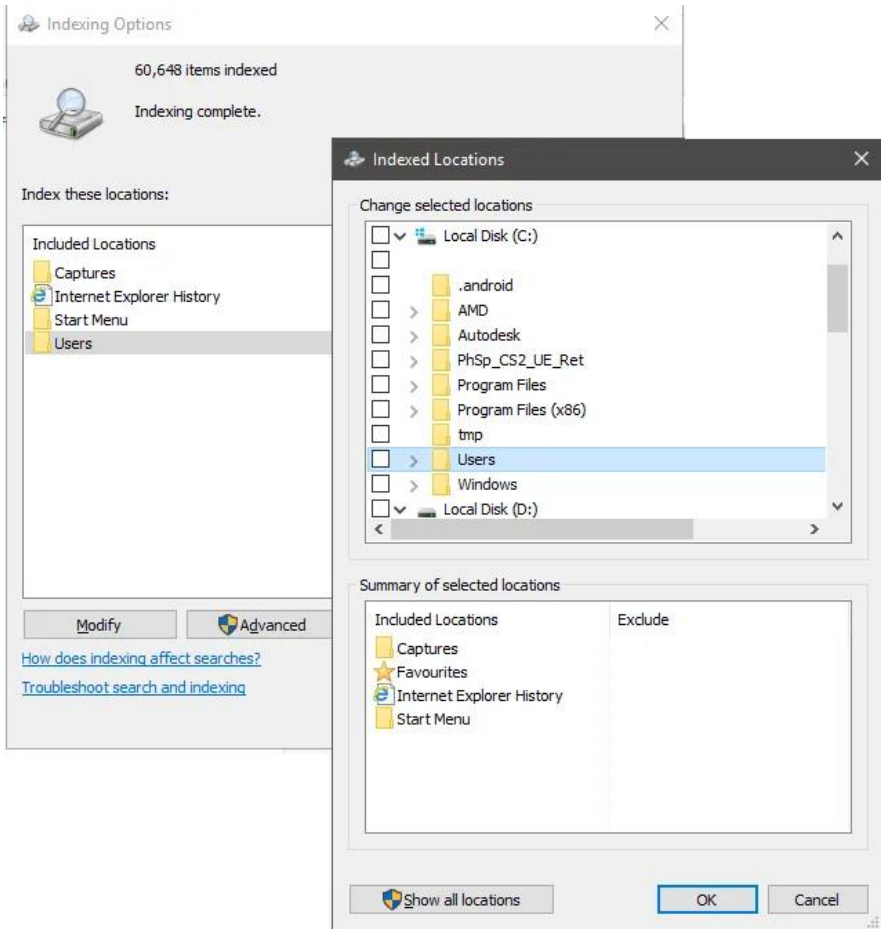
`https://www.advancedinstaller.com/user-guide/exe-setup-file.html`

1.1.3. 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.

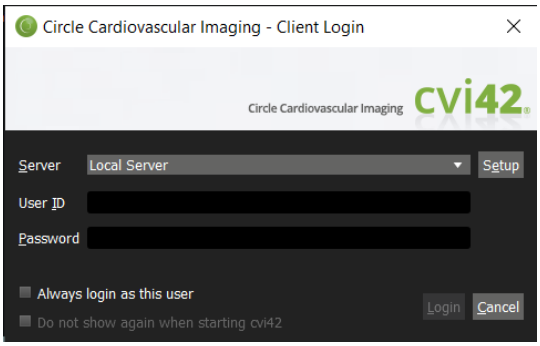
Select the "Modify" option and untick any drive directory which receives DICOM data.


Indexing Options
60,648 items indexed
Indexing complete.
Index these locations:
Included Locations
Captures
Internet Explorer History
Start Menu
Users
Modify
Advanced
How does indexing affect searches?
Troubleshoot search and indexing
Indexed Locations
Change selected locations
Local Disk (C:)
.android
AMD
Autodesk
PhSp_CS2_UE_Ret
Program Files
Program Files (x86)
tmp
Users
Windows
Local Disk (D:)
Summary of selected locations
Included Locations
Exclude
Captures
Favourites
Internet Explorer History
Start Menu
Show all locations
OK
Cancel

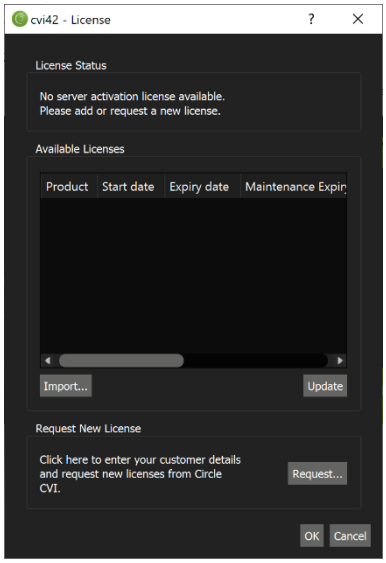
2. Setting up the License

IMPORTANT: When setting up a client-server installation, any license request needs to be performed from the server machine.

When you launch the **cvi42** client on the server you will be presented with a login dialog.



- 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 dialog.



- Click the "*Request...*" button to request a license. After you send the license request, a support representative from Circle Cardiovascular Imaging will issue a license file via e-mail. Click on the "*Import...*" button to install the license to the system.

Q When importing the license file, I received the following message: "Could not import license file... Please check permissions and disk space". What do I have to do?

A To successfully import the license, the **cvi42** client needs to be able to write the license data to:

Windows: `C:\ProgramData\cvi42\licenses`

Mac: `/Users/<current user>/<installation location>/cvi42/licenses`

Running the installer (with both client and server option), or the execution of the manual installation steps described in the previous section, should configure the necessary permissions.

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 **cvi42** client, and restart `cvi42.exe` by double-click, as usual.

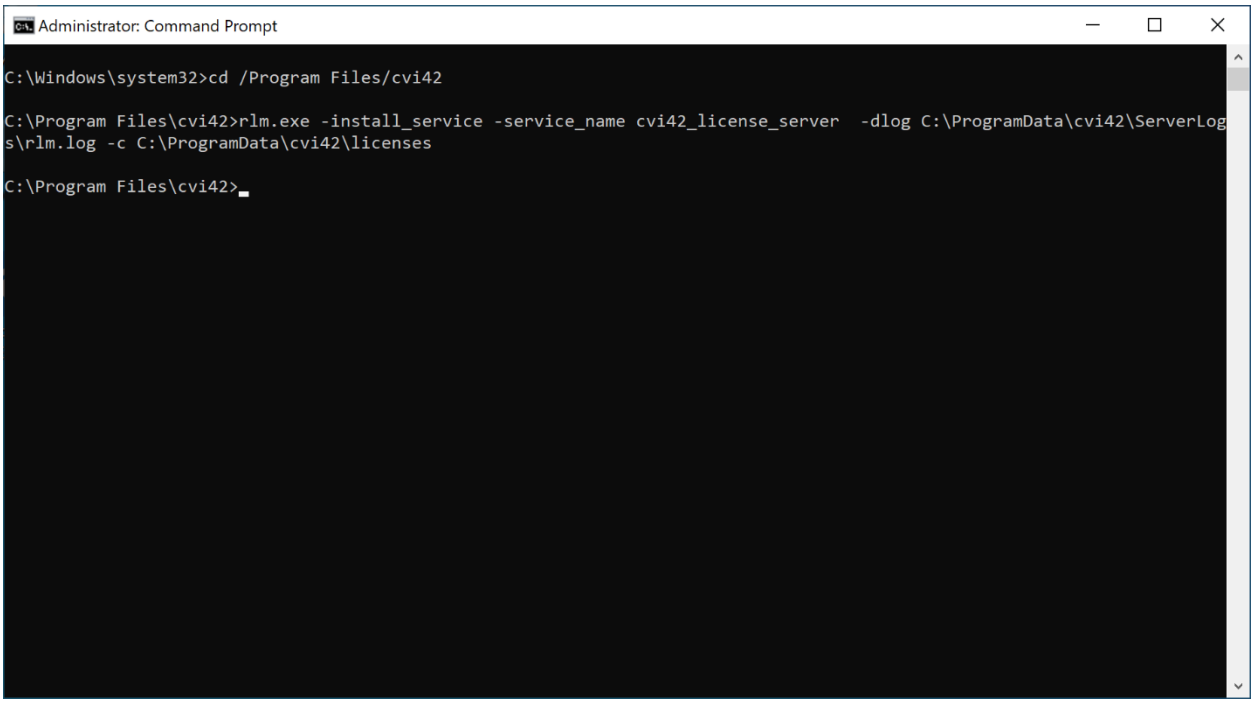
IMPORTANT: For Pay-per-use (PPU) licensing a reliable connection to Circle's PPU servers is required. The connection to Circle's PPU servers will be encrypted, all data will be hashed and salted and no PHI will be transferred.

2.1. Setting Up the License Server

The recommended setup is to install the License Server as a Windows Service. To complete this type of installation, you will need to have administrator privileges on the machine. Refer to the RLM End User Manual for additional details, `https://www.reprisesoftware.com/support/index.php`.

Open a command window and type the following commands:

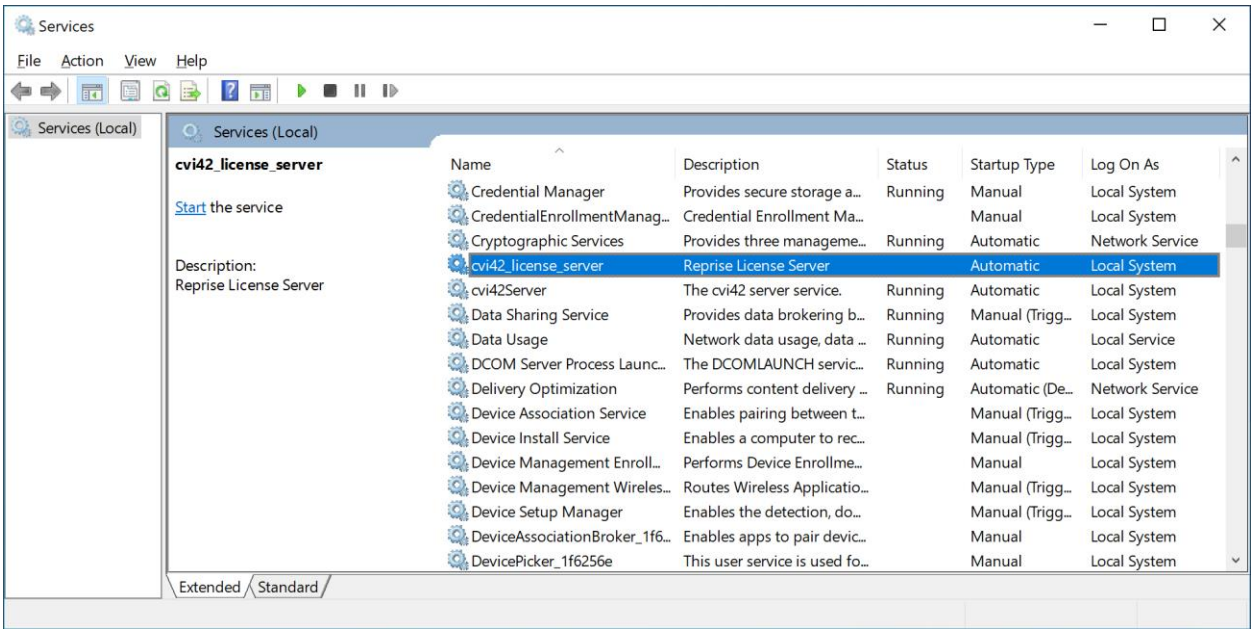
```
cd "C:\Program Files\cvi42"

rlm.exe -install_service -service_name cvi42_license_server  -dlog
C:\ProgramData\cvi42\ServerLogs\rlm.log -c C:\ProgramData\cvi42\licenses
```

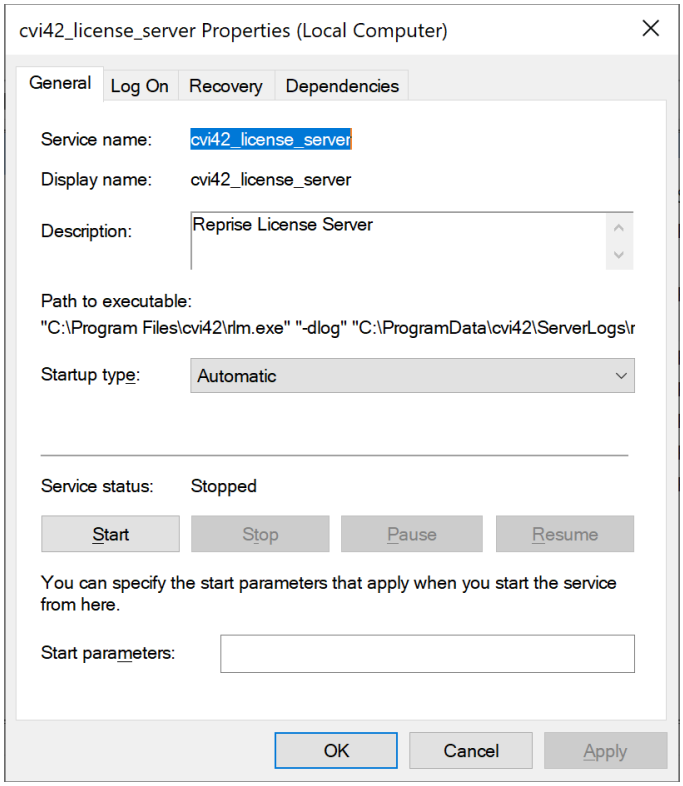


This installs RLM as a service under the name `cvi42_license_server`. When started via the Services control panel or at boot time, RLM will be passed the `"-c C:\ProgramData\cvi42\licenses"` arguments, and it will write debugging information to the file `C:\ProgramData\cvi42\ServerLogs\rlm.log`.

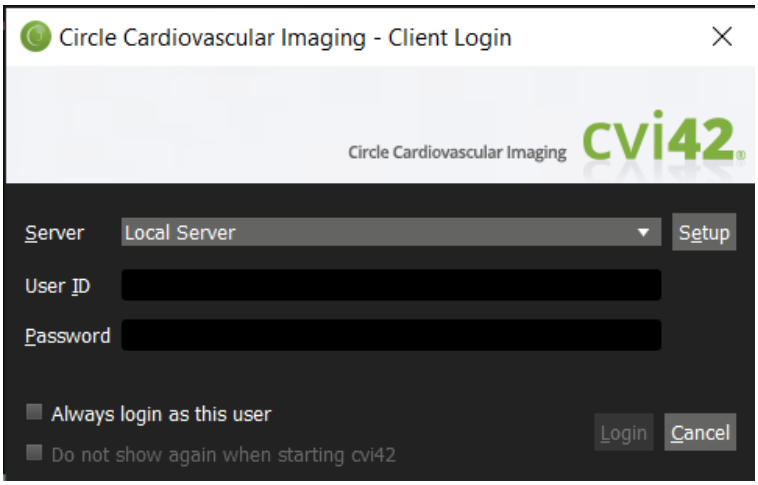
Once the licensed server is installed as a service; do the following to start RLM as a service:

1. Open the Windows Services App by typing the command `services.msc`.
2. Start the `cvi42_license_server` service by double-clicking on the item in the list, then the *Start* button.





2.2. Login Dialog

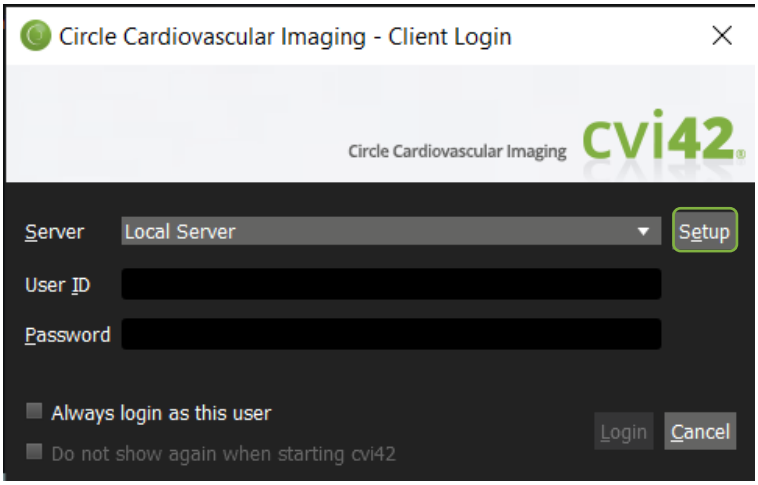


The Login Dialog is displayed when the **cvi42** client is launched. A valid User ID/Password must be entered to login to **cvi42**. For the default account:

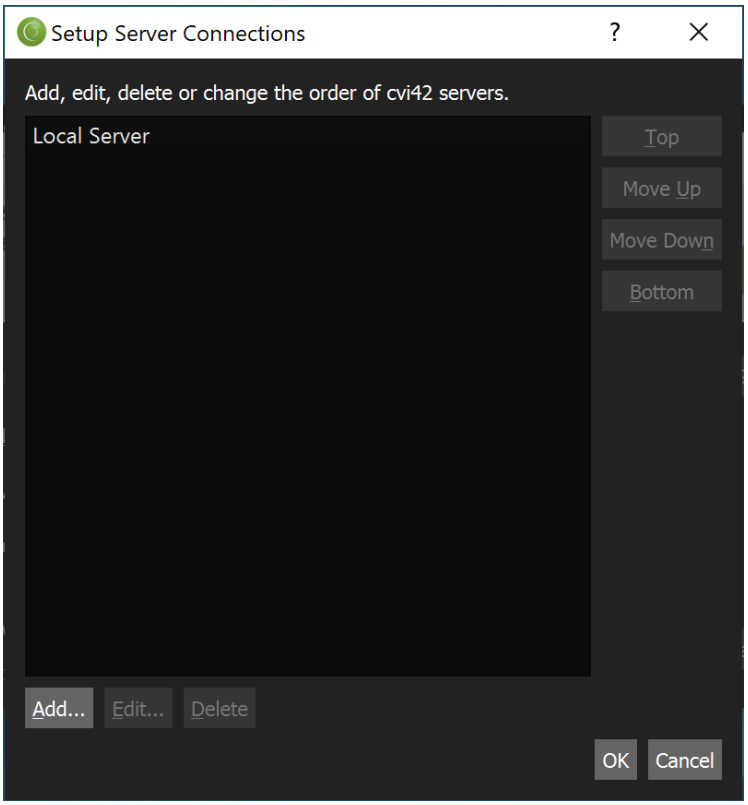
- the default User ID is *admin*, and the default password is *password*

2.3. Configure Server Connections

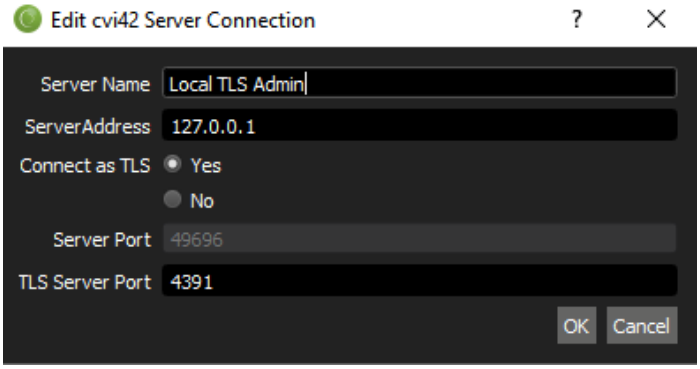
The login dialog will be configured by default to connect to a local server.



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 dialog, 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 another available **cvi42** server.
- **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.

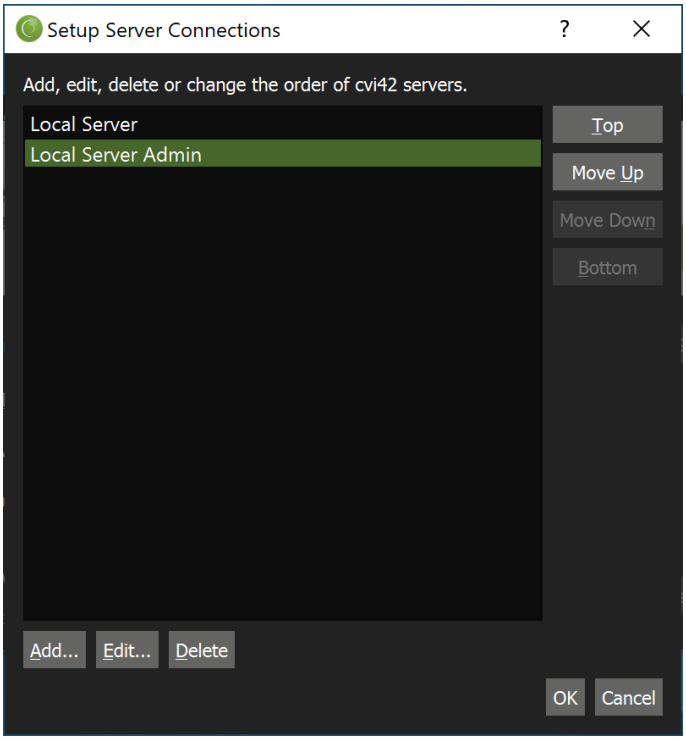
IMPORTANT: Before configuring a secure server connection, the certificate and private keys must first be imported to the **cvi42** server. For more information on Enabling TLS in **cvi42** refer to section 2.1.3 below.

- **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.

For **cvi42** administrators (users with administrator roles in **cvi42**) a dedicated port can be configured (defaults: `49697` (unsecure), `4931` (secure)) for admin-*only* access when they need to perform administrative functions on the server (for example, when taking the server offline for maintenance, adding users, setting up PACS, creating/editing roles, resetting passwords, etc.).

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.

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 Dialog.

2.4. Enabling TLS in cvi42

IMPORTANT: **cvi42** accepts `.pem` and `.der` formatted certificates and private keys.

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:

- manually placing the required files in `%PROGRAMDATA%\cvi42` of the **cvi42** server, or
- through the **cvi42** client user interface.

Manually creating a key pair for the client is not necessary as it will automatically generate them using `4096`-bit RSA. This is not done on the server side as the server must use a certificate that is trusted by the client.

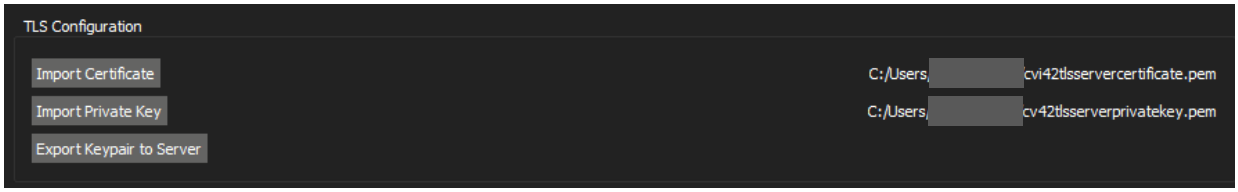
Importing Key Pair Using Client UI

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

1. Log into a **cvi42** client with **cvi42** administrator credentials and open the preferences menu
2. Select “Server Admin”
3. Import both 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 dialog box confirming the files have been saved to the server.

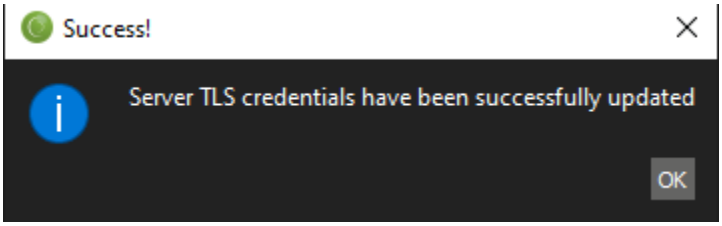


IMPORTANT: For first time configurations, the **cvi42** server ***must*** be restarted to enable secure connections. New key pair files may be imported without disrupting existing secure connections.

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 2.1.2, to either add a new connection or modify an existing one.

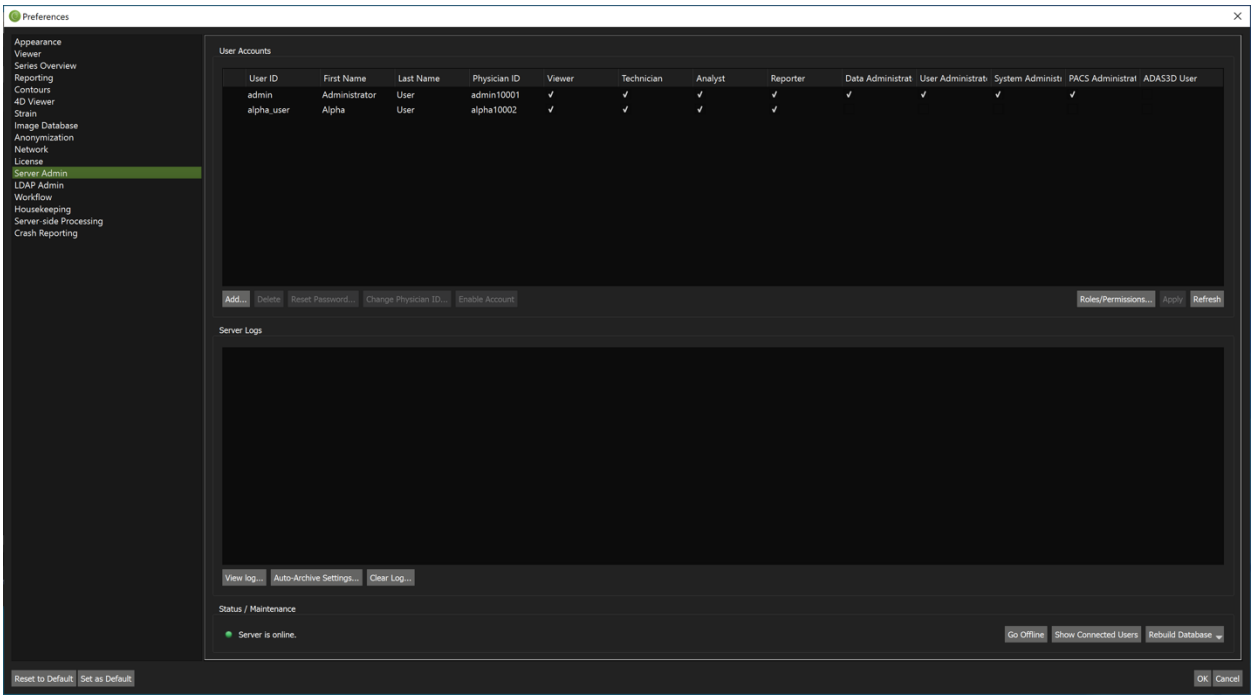
1. Select "Connect as TLS". This will disable the Server Port field and enable the TLS Server Port field.
2. Specify the TLS Server Port. NOTE the default TLS Server Port is `4391`.
3. Once saved, if successful the following dialogue box will be displayed.



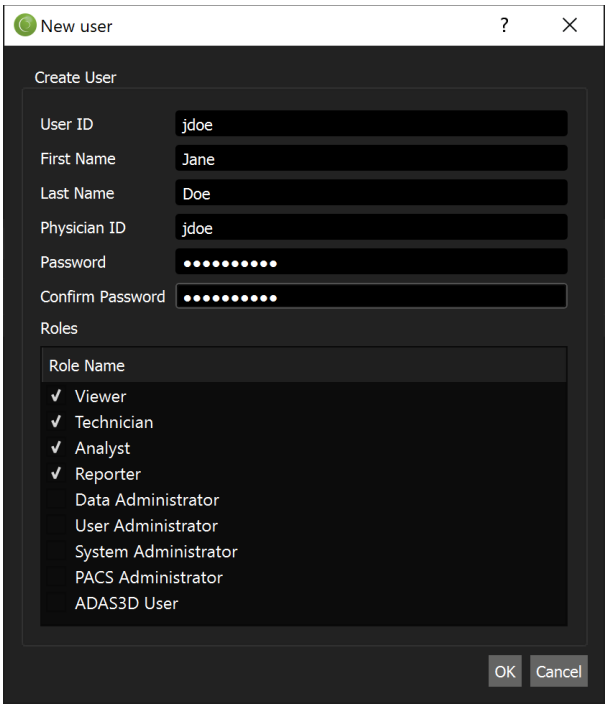
2.5. Setting Up User Accounts

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* dialog will be displayed.



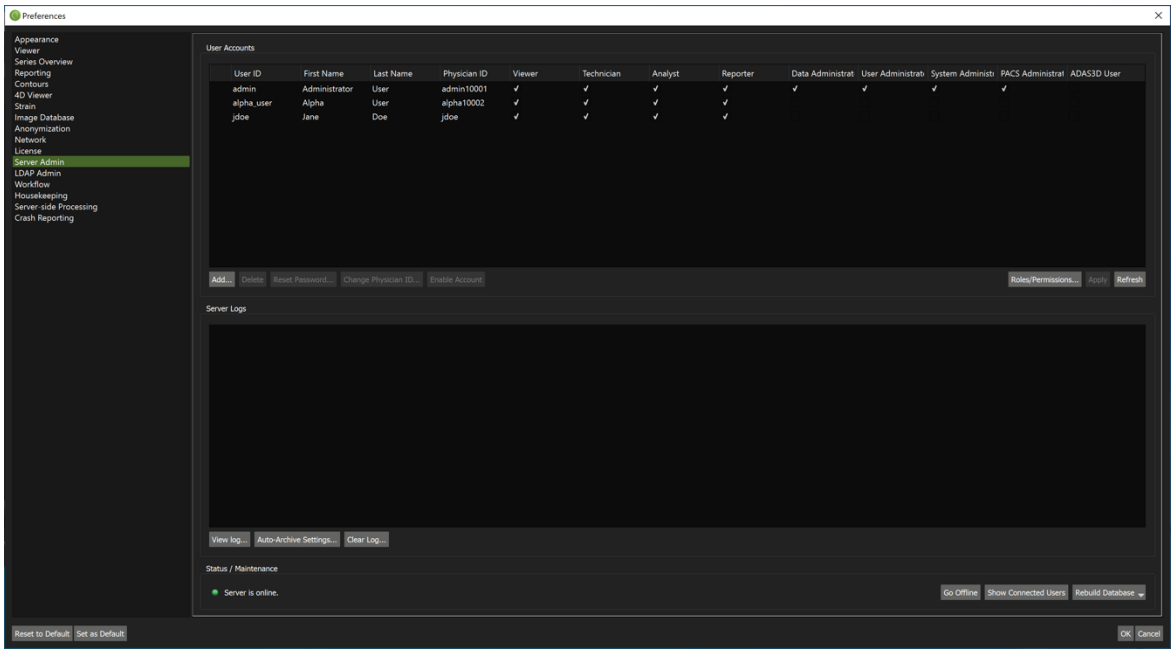
- Fill in all the user details and check the roles to be assigned to the new user.
- Click "*OK*" to finish.

2.6. Setting Up Roles

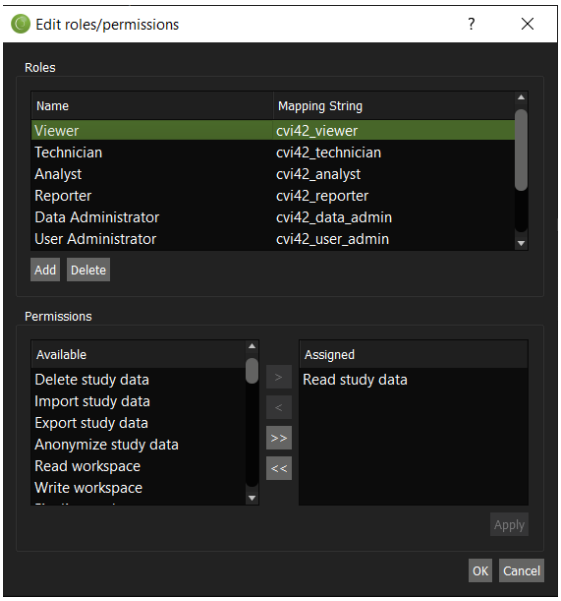
cvi42 defines a set of default roles that can be assigned to user accounts. The set of roles can be customized to meet your institution's needs.

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 or using an integrated AD/LDAP server refer to section *5.1 User Account Linking*.



An Edit Roles/Permission dialog will be displayed.



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

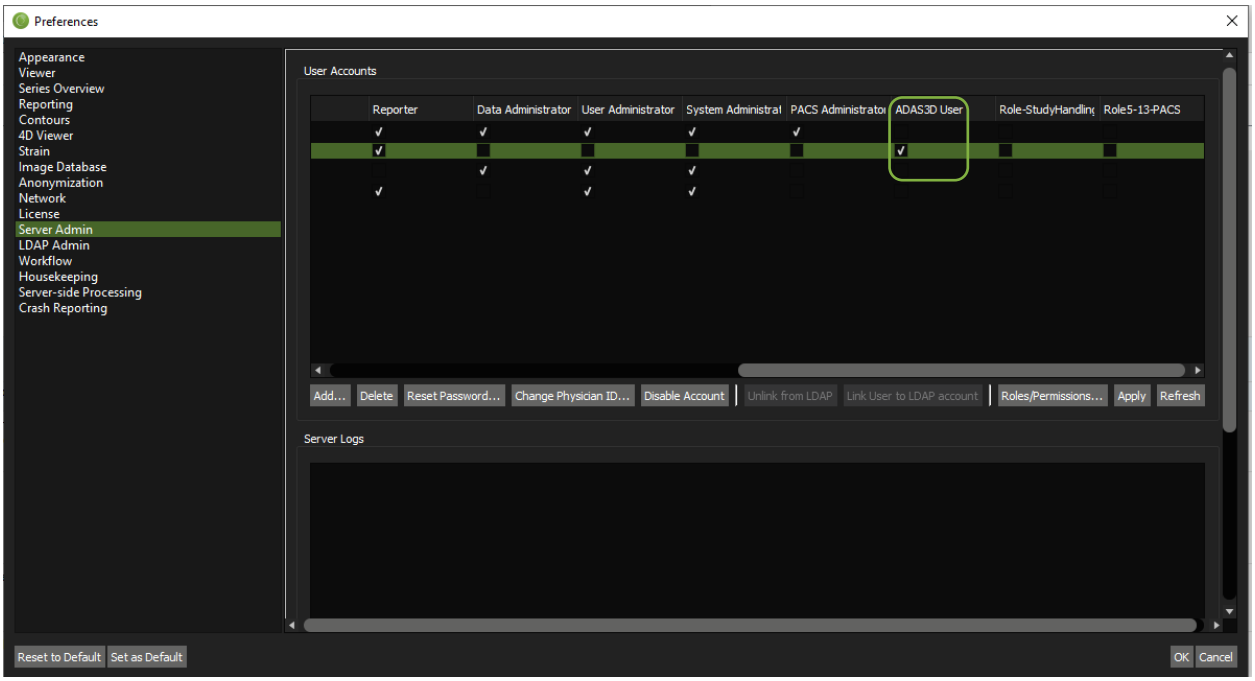
- To edit the permissions of an existing role, select a role from the Roles list. The Assigned box in the bottom right half of the dialog will display the permissions assigned the selected role:
    - Select permissions from either the "*Available*" list or "*Assigned*" list.
    - Click on the ">" or "<" 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 dialog 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 may not take effect until the next time the user logs into **cvi42.**

2.7. 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 user account using the process outlined in section *2.1.4 Setting Up Roles*.



3. Configure Antivirus Software

Antivirus scanning has 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 is 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 AET (case sensitive), 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** .
- **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 period of time (measured in seconds) before **cvi42** will check for updates for to the image database. By default, **cvi42** will check for updates to the image database every 10 seconds.

Network Options

- **Enable Storage SCP** – Configuration option that enables **cvi42** 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** 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 (for AE Title) 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.

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.

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.

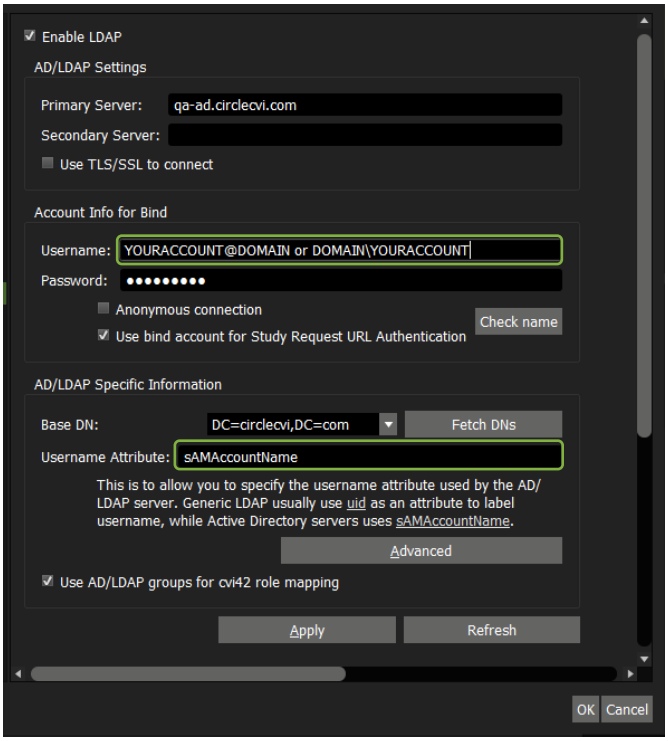
5. Active Directory/LDAP Integrated Password Authentication

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

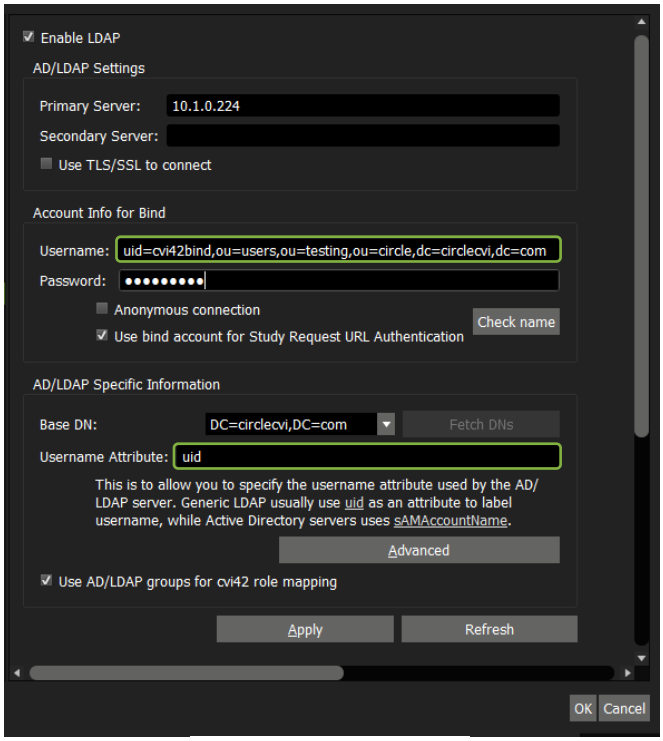
The LDAP Admin Tab allows the System Administrator to authenticate users against an AD or LDAP server. To connect to an AD or LDAP server, **cvi42** needs the following information.

- **Enable LDAP Checkbox** – Check this checkbox to enable the configured LDAP for user authentication and authorization.
- **Primary Server, Secondary Server** – Network information about the AD or LDAP server (IP or fully qualified domain name).
- **Use TLS/SSL to connect Checkbox** – Check this checkbox to use secure connection for this integration; contact the site IT or AD/LDAP server administrator for certificate files and configuration steps).
- **Username** – This is 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 integrations the format of the username will be: `CVI42-BIND-ACCOUNT@circlecvi.com or DOMAINNAME\CVI42-BIND-ACCOUNT-NAME`.
    - LDAP: When configuring the username value for LDAP integrations the format of the username will be: `uid=<CVI42-BIND-ACCOUNT>,ou=<specify each OU layer>,dc=<specify each DC layer>,dc=com`.
- **Password** – The password of the LDAP Bind account.
- **Anonymous connection checkbox** – Check this checkbox to enable anonymous LDAP access.
- **Use bind account for Study Request URL Authentication checkbox** – Check this checkbox to enable authenticating Study Requests from URLs 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 button** – Hit this button to confirm whether or not the configured LDAP Bind account exists.
- **Base DN** – Base location to search for AD or LDAP users.
- **Fetch DNs Button** – Hit this button to fetch the DNs from the Base DN.
- **Username Attribute** – Specifies which element of the Users 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 a the `uid` parameter.

- **Advanced** – This is an optional setting, Additional attributes when performing AD or LDAP search. This field allows you to specify any restriction that may need to be in place when authenticating against an Active Directory or LDAP server. For example, if the administrator has created a group on the Active Directory or LDAP server called "cvi42", then only this group of users is permitted access to the **cvi42** application.
- **Use AD/LDAP groups for cvi42 role mapping** – This is setting determines whether **cvi42** should use the integrated AD/LDAP server for user authentication and authorization or just for authentication. If this option is disabled users logging in need to be listed in the **cvi42** user list and user authorization (role-mapping) are determined using **cvi42**.



Configuration for AD



Configuration for LDAP

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

5.1. User Account Linking

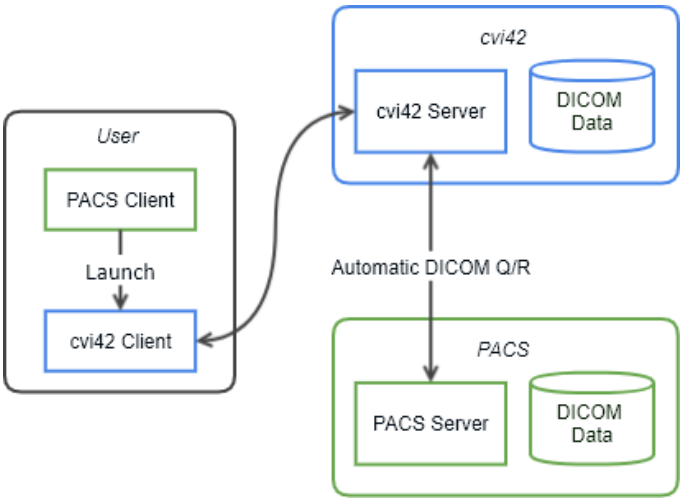
Below is a table outlining the User Account linking behaviour. For more information on configuring user accounts and user roles refer to sections *2.1.3 Setting up User Accounts* and *2.1.4 Setting up Roles*.

User in AD/LDAP	User in cvi42	User Account Linked	Password Used	Log in Status	Comments
Y	Y	Y	AD/LDAP	Y	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	Y	User is in *only* 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	Y	User will then be converted to an AD/LDAP account
Y	Y	N	Local	Y	This will not convert user to AD/LDAP user
N	Y	N	Local	Y	
Y	Y	Y	Local	N	Needs to authenticate with AD/LDAP password
Y	N	N	Wrong	N	Needs to authenticate with correct AD/LDAP password
N	N	N	Any	N	

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 dialog. 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 dialog. (Not applicable to standalone)	Username
5	`-disable-quit-dialog`	Disables dialog 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 AccessionNumber 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 dialog 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 dialog.

```
>> 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 `C:\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.

- **DataFilesPath** – Path to the folder containing the data for your **cvi42** system.
  example: `DataFilesPath=C:/ProgramData/cvi42`
- **ImageDBPath** – Path to the folder containing the image data for your **cvi42** system.
  example: `ImageDBPath=C:/ProgramData/cvi42/cvi42imagedb`
- **SqlDatabasePath** - Path to the cvi42server database.
  example: `SqlDatabasePath=C:/ProgramData/cvi42/cvi42sqldb/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`
- **LogFilesPath** – Path to the folder containing the log files for the server.
  example: `LogFilesPath=C:/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 serves. When configuring this value provide the IP or fully qualified hostname.
  example: `TrustedHosts=server1.abc.com, server2.abc.com`
- **EnabledLdap** – A Boolean value used specifies whether or not cvi42 should use the configured LDAP settings for user authentication/authorization. Default value is `false`.
  example: `EnadbledLdap=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\№\<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\xf9\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.
  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`

8. 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.

8.1. 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.

8.1.1. 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.

8.1.2. 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.

8.2. 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

8.2.1. Criteria

8.2.1.1. 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.

8.2.1.2. 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.

8.2.1.3. Institution Name

This criterion filters studies by the DICOM "institution name" attribute. The matching is done as described in section *7.2.1.2 Study Description*.

8.2.1.4. Manufacturer

This criterion filters studies by the DICOM "manufacturer" attribute. The matching is done as described in section *7.2.1.2 Study Description*.

8.2.1.5. Model

This criterion filters studies by the DICOM "model" attribute. The matching is done as described in section *7.2.1.2 Study Description*.

8.2.1.6. Modality

This criterion filters studies by the DICOM "modality" attribute. The matching is done as described in section *7.2.1.2 Study Description*.

8.2.1.7. 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 when used first. 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.

8.2.1.8. 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.

8.2.1.9. 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.

8.2.1.10. 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.

8.2.1.11. 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.

8.2.1.12. Available Disk-Space

This criterion filters studies by the available disk-space (in MB) on the DICOM image database file system. 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.

8.2.2. Actions

8.2.2.1. 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.

8.2.2.2. 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.

8.2.2.3. Convert Workspace Date 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 *7.2.2.4 Store DICOM Data* or *8.2.2.5 Export DICOM Data* 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.

8.2.2.4. 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 *7.3.1 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 dialog but not yet saved to the server, the Housekeeping configuration UI will still show the names as configured on the server.

8.2.2.5. Export DICOM Data to filesystem

This action exports DICOM data to filesystem. The type of DICOM data that is exported can be limited as for 7.2.2.4 Store DICOM Data. 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.

8.2.2.6. 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 *7.3.1 Simulation* for steps on verifying that the rule matches only the desired studies.

Alternatively, refer to section *7.2.2.1 Assign 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.

8.2.2.7. 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.

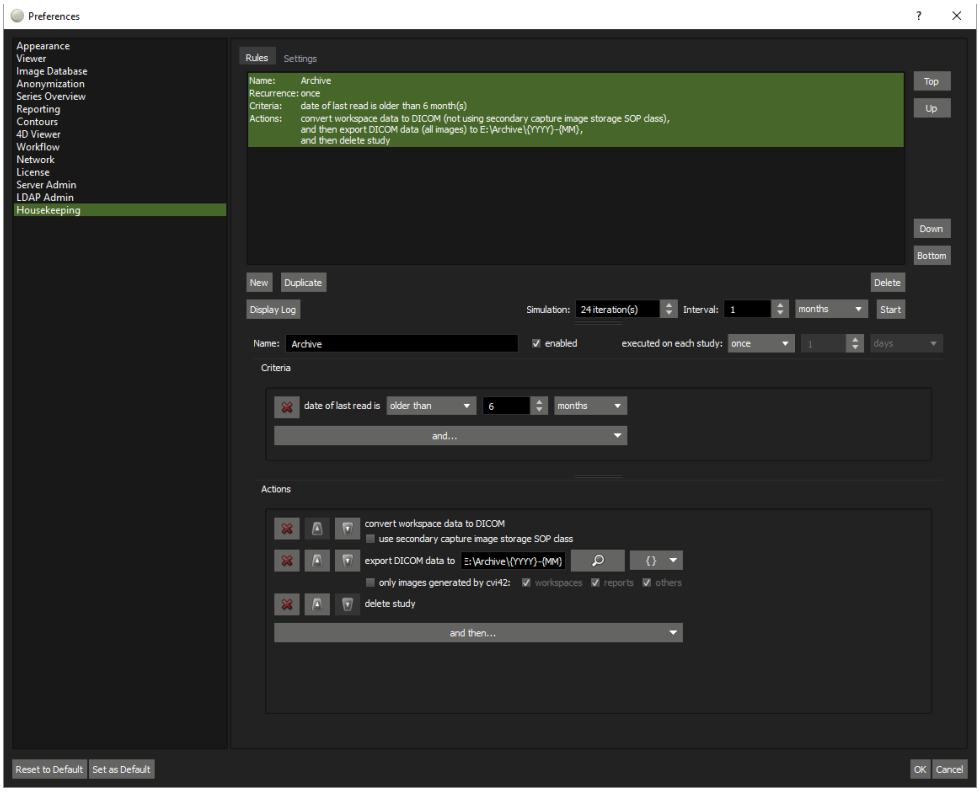
8.2.3. Recurrence

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.

8.3. Rule Editor



The rule editor is located in the "Rules" tab of the Housekeeping section of the configuration dialog. 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 *7.4.1.1 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 *7.3.1 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.

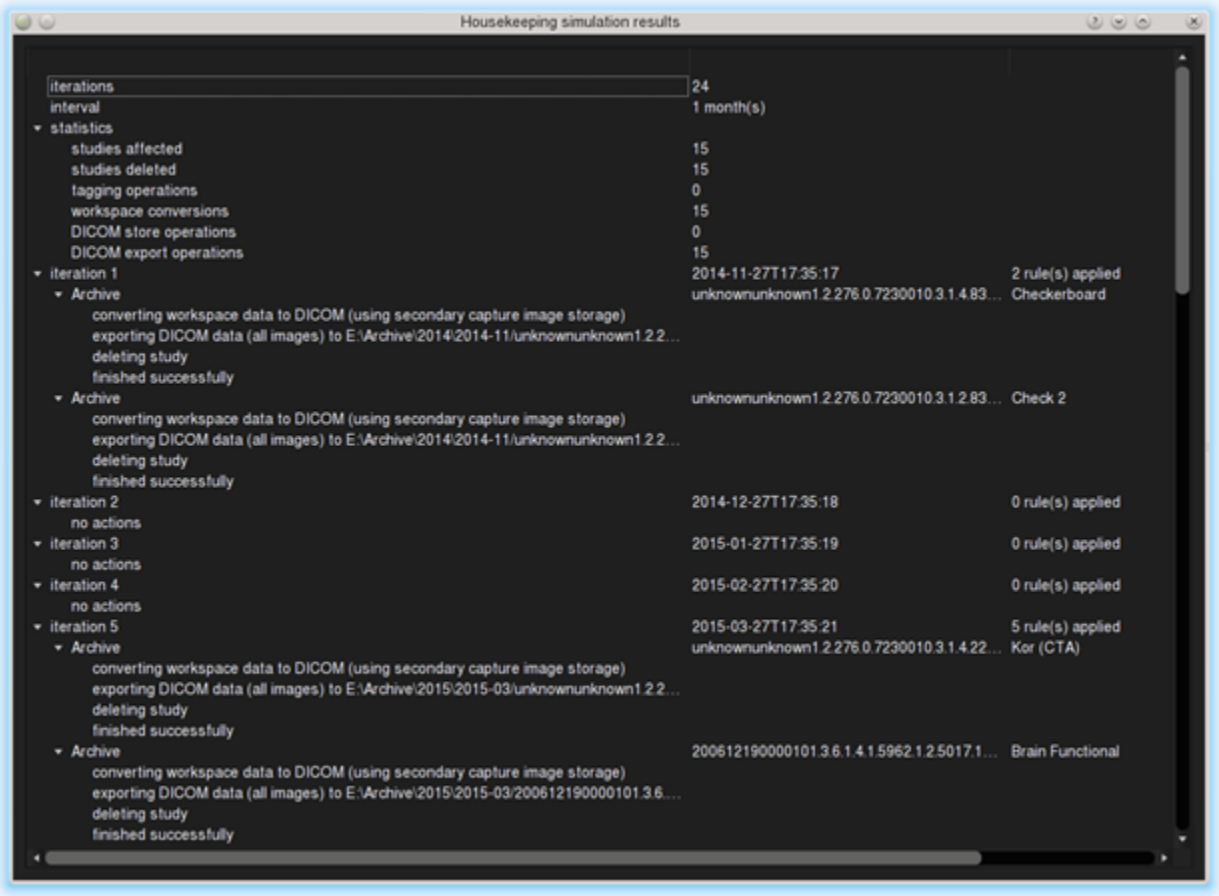
8.3.1. Simulation

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 workspaces to DICOM", "store DICOM data" or "export DICOM data" 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.

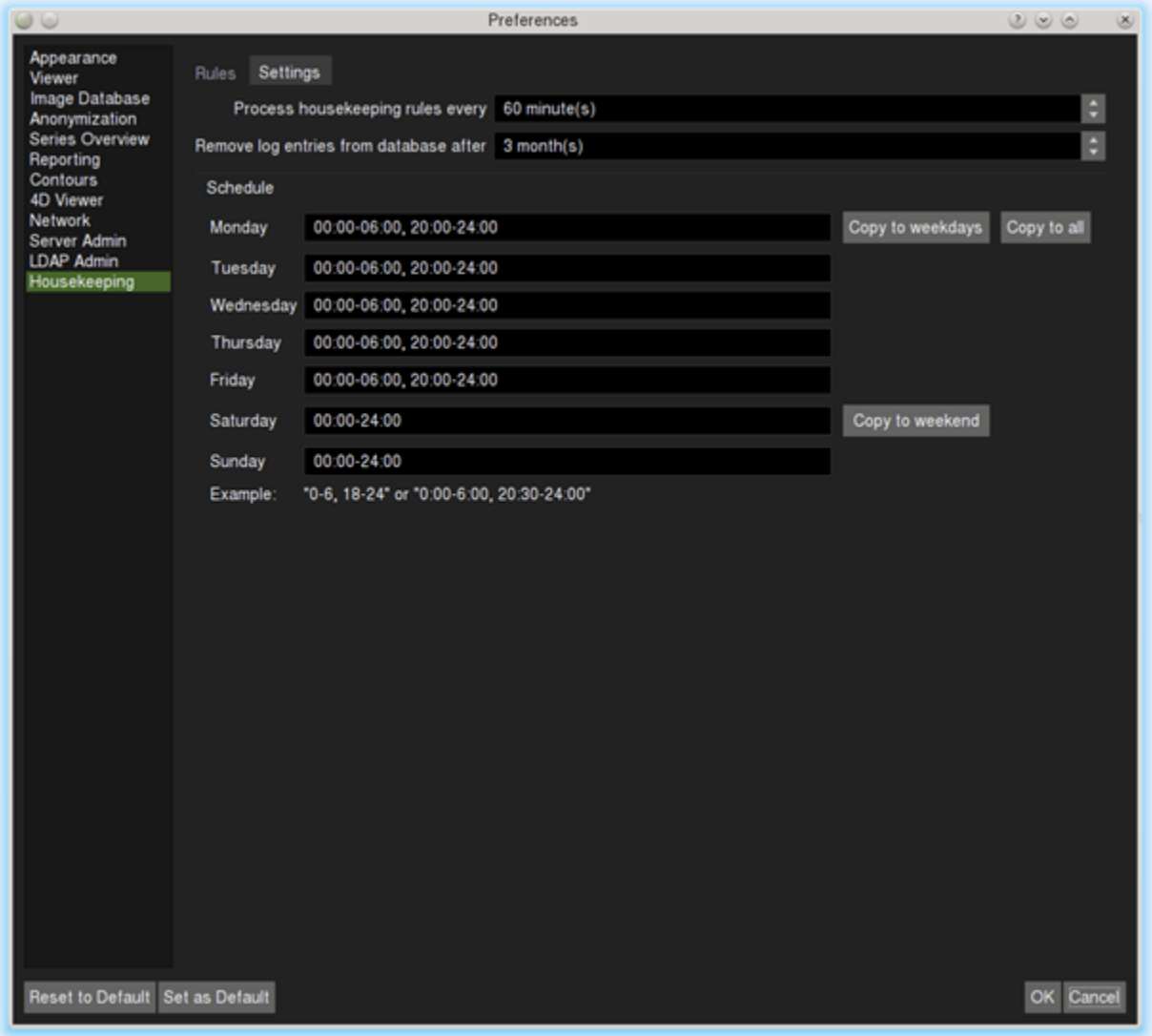


The result first lists the selected number of iterations and interval. Then a statistical summary of the simulation is given, counting the total number of affected studies and how often actions of different classes were executed (studies deleted, tagging operations, workspace conversions, DICOM store 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`" action which can potentially lead to sending data to unintended destinations.

8.4. Settings



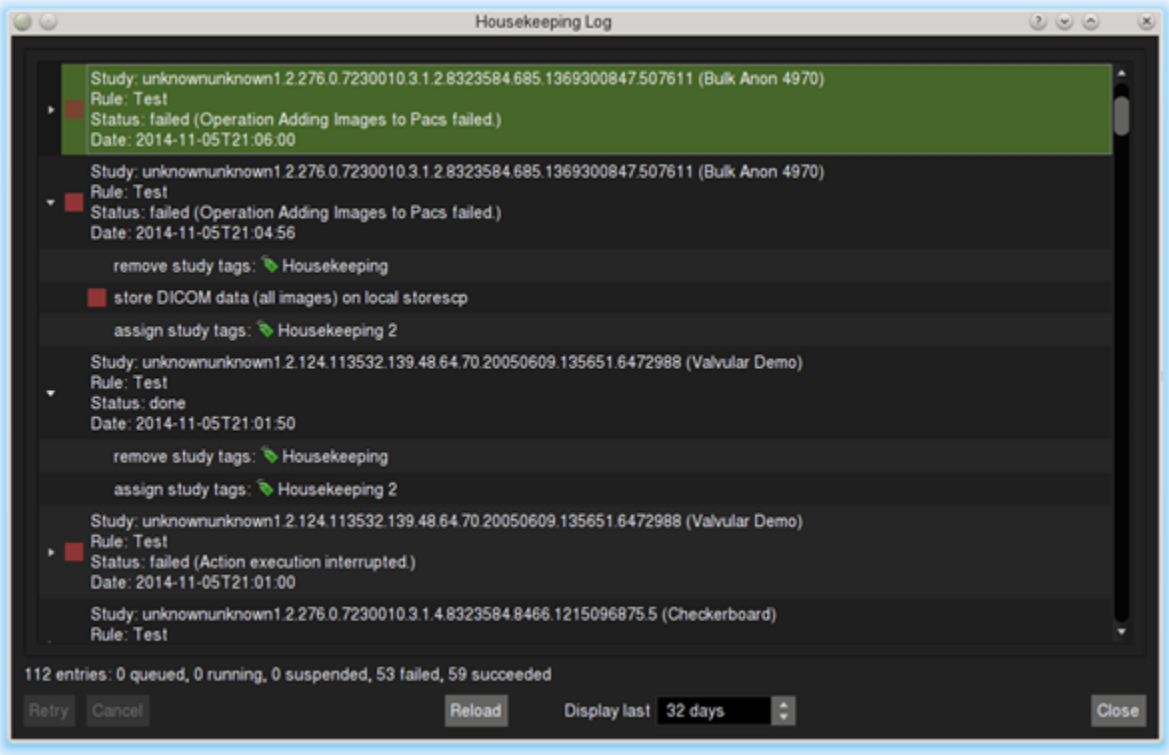
In the "Settings" tab of the Housekeeping section in the configuration dialog, parameters for the overall behaviour of the Housekeeping system are specified.

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 7.4.1 Log and Control window. 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 log 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.

8.4.1.1. Log and Control



The log and control interface displays the most recent activity 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	
cvi42 admin client	**cvi42** server	TCP/49697	
cvi42 client	**cvi42**|Report webserver	TCP/4280	
PACS	**cvi42** server	TCP/104	
cvi42 server	PPU server (cloud)	TCP/443	when licensed for PPU