Server/Client
Installation and Configuration Guide
Manufactured by
Circle Cardiovascular Imaging Inc.
250, 815 - 8th Avenue SW Calgary, AB. T2P 3P2

Telephone: 1 (403) 338-1870
Fax: 1 (403) 338 1895

Support: support@circlecvi.com

http://www.circlecvi.com

© Copyright 2017 Circle Cardiovascular Imaging Inc.
cmr® and cvi® are registered trademarks 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.
# Table of Content

1. Installing cvi\textsuperscript{42} (Windows Platform) ................................................................. 5  
   1.1 Installing the Server/Client Using the Setup Program ...................................................... 5  
   1.2 Alternate Manual Steps for Installing the Server .............................................................. 10  
   1.3 Alternate Manual Steps for Installing the Client .............................................................. 18  
2. Setting up the License ............................................................................................................. 19  
   2.1 Setting Up The RLM License Server ................................................................................... 22  
3. Configure DICOM Networking (PACS Connections) ............................................................ 31  
4. Configure Single Sign On ....................................................................................................... 31  
5. Configure Single Sign On using TLS\SSL (for Windows) ..................................................... 33  
   5.1 Inspecting a Certificate ......................................................................................................... 33  
   5.2 Installing a Certificate .......................................................................................................... 34  
6. Server Configuration (cvi\textsuperscript{42}serverconfig.ini explained) ......................................... 41  
   6.1 General Properties .............................................................................................................. 41  
   6.2 Performance ....................................................................................................................... 43  
   6.3 PPUProperties ...................................................................................................................... 43  
   6.4 License ............................................................................................................................... 44  
   6.5 DicomNetwork .................................................................................................................... 44  
   6.6 Single Sign On ..................................................................................................................... 45  
7. Housekeeping ......................................................................................................................... 45  
   7.1 Overview ............................................................................................................................ 45  
   7.2 Rules ................................................................................................................................... 46  
   7.3 Rule Editor ............................................................................................................................ 51  
   7.4 Settings ................................................................................................................................ 54  
   7.5 Log and Control .................................................................................................................. 55  
8. Importing Workspaces from cmr\textsuperscript{42} Version 3.x ...................................................... 56  
9. Installing cvi\textsuperscript{42} (Mac OS Platform) ......................................................................... 56
1 Installing cvi\textsuperscript{42} (Windows Platform)

Before installing the latest version of cvi\textsuperscript{42}, you should uninstall any previous versions of cvi\textsuperscript{42} that may exist on your system.

On Windows 7 or 2008, go to Start→Control Panel→Programs→Uninstall a Program, or on Windows XP, Start→Control Panel→Add/Remove Programs to uninstall cvi\textsuperscript{42}

If you intended to re-install the same version of cvi\textsuperscript{42} on top of the existing installed version, you should stop any existing cvi\textsuperscript{42} servers/services and any license servers that may have been configured for cvi\textsuperscript{42}. Go to Start→Control Panel→System→Administrative Tools→Services and stop the cvi\textsuperscript{42} Server Service

RLM licensing server services for cvi\textsuperscript{42} should also be stopped (if one has been configured).

1.1 Installing the Server/Client Using the Setup Program

The easiest way to install cvi\textsuperscript{42} is to run the cvi\textsuperscript{42} 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 install option: *Standalone* – client and server install, or *Client only* – install. 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.

1.2 Automating the MSI Installer

The MSI installer can be automated using Windows’ system command -- msiexec.exe – along with various installer parameters. Here are the following installer parameters accepted by the MSI installer:

IAgree – Indicates that the user agrees with the stated software usage terms and conditions. This parameter accepts the following values: “Yes”/“No”

i.e. IAgree=“Yes”

TARGETDIR – Specify where cvi42 will be installed on the hard drive.

i.e. TARGETDIR=“C:\Program Files\cvi42”

COMP – Specifies whether this is a standalone or client only installation. This parameter accepts the following value: “Standalone”/“ClientOnly”

i.e. COMP=“ClientOnly”

SERV_NAME – Specifies a name for cvi42. This name is shown to users when logging into cvi42.

i.e. SERV_NAME=“My cvi42 Server”

SERV_ADDR – Specifies the IP address/Domain name of where cvi42 is located.

i.e. SERV_ADDR=“172.16.5.12”
SERV_DOM – Specifies an Active Directory server name. This is used for single sign on, allowing cvi42 users to log in with the same user credentials found on the Active Directory.

i.e. SERV_DOM= "circle"

So from the Command Prompt a user may automate the MSI installer by typing the following commands:

```
\cd \<Location of MSI Installer> (e.g. cd Work\Downloads)
\msiexec /i "<name of msi file>" /quiet IAgree="Yes" TARGETDIR="C:\Program Files\cvi42"
COMP="ClientOnly" SERV_NAME="My cvi42 Server" SERV_ADDR="172.16.5.12"
SERV_DOM="circle" /l*v log.txt
```

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

- `/i <Product msi>` – install or configure a product
- `/quiet` – quiet mode, no user interaction
- `/l*v <LogFile>` – log all information except extra debugging information.

More information about these msiexec command line switches can be found here:


1.3 Alternate Manual Steps for Installing the Server

If the MSI installer fails to install cvi42, there is an alternative method to extract the files from the installer on to the system.

To extract the files from the MSI installer, start a Command Prompt as an administrator...
From the Command Prompt, type the following commands:

```
cd \<Location of MSI Installer> (e.g. cd \Work\Downloads)
msiexec /a "<name of msi file>" /qb TARGETDIR="C:\Program Files\cvi42"
```
After executing the command a progress bar will appear indicating the progress of the installation.

Next open Windows Explorer and browse to C:\Program Files\cvi42

From the Command Prompt, type the following commands:

```
    cd \ProgramData
    md cvi42
    md cvi42\licenses
    icacls.exe \ProgramData\cvi42\licenses /T /grant %username%:F
    copy nul > cvi42\cvi42serverconfig.ini
    icacls.exe \ProgramData\cvi42\cvi42serverconfig.ini /grant %username%:F
```
The recommended setup is to install the cvi® Server as a Windows Service.

To setup the service, start a Command Prompt as an administrator...
and type the following commands

```bash
cd "C:\Program Files\cvi42"
cvi42Server.exe -i
```

Verify that the cvi42 Server service installed by typing

- `cvi42Server.exe -v`
Open the Windows Services App by typing the following command

- `services.msc`

Find the cvi42 Server Service in the list of services and double-click on it to configure the service to start automatically.
Click on the Start button to start the service.

The Service status will change to Started. Click OK.
The Services list will now show that cvi42Server Service is *Started* and configured for *Automatic* startup.

1.4 Alternate Manual Steps for Installing the Client

It is possible to extract files and folders contained inside the MSI file to a folder of your choice (e.g. C:\Program Files\cvi42) using the following commands:

```bash
cd \<Location of MSI Installer> (e.g. cd \Work\Downloads)
msiexec /a "<name of msi file>" /qb TARGETDIR="C:\Program Files\cvi42" COMP="ClientOnly"
```
After executing the command a progress bar will appear indicating the progress of the installation.

![Progress bar with time remaining](image)

The cvi42 Client executable (cvi42.exe) will be ready to launch.

![File list with cvi42.exe highlighted](image)

2 Setting up the License

**Important:** When setting up the license for the server for the first time, the cvi42 client should be started on the same machine as the cvi42 server.
1. When you launch the cvi42 Client (cvi42.exe) you will be presented with a login dialog.

2. The default User ID is `admin`, and the default password is `password`.

3. Enter the User ID/Password information and click **Login**. cvi42 will proceed to check for a valid license and display the license request dialog.

4. 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 \ProgramData\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.

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.

Depending on license/usage needs, there are four types of licensing models available:

a) Activation/Standalone

This type of license is required to enable the cvi42 server. cvi42 will not be functional without a valid activation license. This is the only license required if the client and server will always be on same machine (standalone or workstation mode).

b) Concurrent/Floating

This type of license enables the cvi42 server to accept connections from cvi42 clients across a network. The concurrent license will allow up to the maximum number of clients to be connected as defined by your licensing terms.

To enable concurrent licensing, a license server will need to be setup. You can setup the license server on the same machine as your cvi42 Server. Please refer to the next section for details.

The license server needs to be restarted for changes to concurrent licenses to take effect.

c) Pay-Per-Use (PPU)

This type of license enables the cvi42 server to accept connections from cvi42 clients across a network. The PPU license will allow clients to connect to the server, and the studies that are opened will be tracked for usage billing.

A reliable connection to the internet on TCP/IP port is required as well as a valid key

d) Feature based

This type of license is required for activating certain cvi42 features. These licenses are distributed separately from the license used for activating additional cvi42 features.
2.1 Setting Up The RLM License Server

The recommended setup is to install the RLM 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 (http://www.reprisesoftware.com/kits/v9.3BL2/RLM_Enduser.html).

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

The format of the above command is:

```
rlm -install_service -dlog [+]logfile [-service_name sname] <rlm runtime args>
```

where:

- `logfile` is the pathname for the server debug log. This parameter is required. If preceded by the '+' character, the logfile will be appended, rather than created.
- `sname` is an optional name for the installed service. If not specified, `sname` defaults to "rlm". If `sname` contains embedded whitespace, it must be enclosed in double quotes.
- `<rlm runtime args>` are any other command line arguments to be passed to rlm when it is started.

Once RLM 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.
For older versions of cvi42 that are needed for 32-bit Windows, open a command window and type the following commands:

```bash
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
```

Open the Windows Services App by typing the command `services.msc`.

Start the cvi42_license_server service by double-clicking on the item in the list, then the “Start” button.
2.1.1 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

- User ID is “admin” and the

- default Password is “password”

The “Always login as this user” checkbox can be selected to remember the User ID/Password combination. This option is only available if you are connected to a local server (cvi42 client and server running on the same machine).

If “Always login as this user” is checked, you can also select the “Do not show again when starting cvi42” checkbox, so that the login dialog is not displayed when cvi42 client is launched. It will automatically login with the saved user credentials.

The user credentials will only be saved if the login can be successfully completed with the specified User ID/Password. When login fails, the saved user data will be cleared.

2.1.2 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 main 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.
- For cvi42 administrators (users with administrator roles in cvi42) a dedicated port can be configured (default is 49697) for admin-only access when they need to perform admin functions on the server (i.e. taking the server offline for maintenance, adding users, setting up PACS, creating/editing roles, resetting passwords, etc).
For most deployments, you can now click “OK” to finish.

Optionally, click the “Show Advanced Config” button to configure the parameter for the ancillary port, which is defaulted to 49695. The ancillary port provides an additional communications channel between the client and server. For typical installations the default value will be sufficient.

**Important:** The Server Port (and Ancillary Port) you specify here must match the port numbers that are configured for the server that you want to connect to.
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.

2.1.3 Setting Up Users

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

1. Click on Preferences ➔ Config from the menu bar (or press F12).

2. Select “Server Admin” from the list.
3. Click the “Add...” button, to add a new account. The New user dialog will be displayed.

4. Fill in all the user details, and check the roles to be assigned to the new user.

5. Click “OK” to finish.
2.1.4 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.

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

2. An Edit Roles/Permission dialog will be displayed.
3. 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 and
   - 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.

4. 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.

5. 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.

Note: When roles/permissions of a particular user are changed, the settings may not take effect until the next time the user logs into cvi42

3 Configure DICOM Networking (PACS Connections)

Users with ‘Administrate PACS’ permissions can set up the configuration for DICOM Networking/PACS connections. The admin port (default is 49697) must be used to access the Network tab of the Preferences Menu. Please see section 24.1.8 of the cvi42 user manual for a detailed description.

4 Configure Single Sign On

Users with ‘System Administrator’ permissions can set up the configuration for single sign on. Single sign on is a 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 you to authenticate users against an Active Directory/LDAP server. In order to connect to an Active Directory/LDAP server, cvi42 needs the following information.

1. Location of the server (i.e. domain name or IP address)
2. Enable TLS\SSL communication
3. Username/password field is used to bind to your Active Directory/LDAP server.
4. The Username field is primarily used for specifying a domain name of the Active Directory/LDAP server. There are two ways of inserting the username. First, you can specify the username as domain name\username (e.g. “srclookup\jane”). Or you can specify the username as username@domain name (e.g. “jane@srclookup.com”).
5. After you have inserted your password you can click on “Check name” to connect with your Active Directory/LDAP server. This allows you to verify the settings that you have entered.

6. BaseDN (or base distinguished name)

7. Specifies the Active Directory/LDAP tree to use for user authentication, searching for users, and looking up user information.

8. Click “Fetch DNs” to retrieve a list of DNs found on your Active Directory/LDAP server.

9. Username attribute

10. This field allows you to specify the username attribute used by the Active Directory/LDAP server during authentication.

11. Additional criteria (this is an optional setting)

12. This field allows you to specify any restriction that needs to be in place when authenticating against an Active Directory/LDAP server. For example, if the administrator has created a group on the Active Directory/LDAP server called “cvi42”, then only this group of users is permitted access to cvi42.

13. Click “Apply” to save the changes.
14. Click "Refresh" to retrieve settings from the server. Any modifications made will be reverted to the settings saved on the server.

5 Configure Single Sign On using TLS\SSL (for Windows)

In the LDAP Admin Tab, you have the option to use TLS\SSL when communicating with Active Directory/LDAP server. In order to connect to an Active Directory/LDAP server over a TLS\SSL communication channel, an SSL certificate needs to be installed on the system where cvi42 server is running.

This SSL certificate needs to be generated by the Active Directory/LDAP server, and signed by the trusted party before it can be used. Contact your Active Directory/LDAP server administrator in order to obtain this SSL certificate.

Once you have obtained an SSL certificate, you will need to install the SSL certificate in to your system. To install the certificate perform the following steps.

5.1 Inspecting a Certificate

1. Browse to where the SSL certificate is saved.

2. Double click on the SSL certificate and ensure the SSL certificate refers to a trusted party.
3. Click on “Install Certificate...”

5.2 Installing a Certificate

Once the certificate has been verified you can install the certificate. To install the certificate, start a Microsoft Management Console (MMC) as an administrator...
1. In the MMC click on File -> Add/Remove Snap-in...

2. Add or Remove Snap-ins window prompt will pop up.

3. Click on "Certificates". Click on Add >
4. Choose the "Computer account" for the certificate snap-in. Click "Next >".

5. Choose "Local Computer: (the computer this console is running on)". Click "Finish".
6. Click “OK” to add this Snap-in into the MMC.

7. On the navigation pane, browse to Certificates (Local Computer) -> Trusted Root Certification -> Certificates

8. Right click on Certificates. In the submenu click on All Tasks -> Import...
9. A Certificate Import Wizard will pop up assisting you in installing the certificate

10. Click "Next".
11. Click "Browse...". Select the folder containing the SSL certificate that you want to import.

12. Click "Open", and then "Next" to continue.
13. Click "Next", to continue.

14. Click "Finish", to complete importing the SSL certificate into your system.

15. The SSL certificate should appear in the MMC.
6 Server Configuration (cvi42serverconfig.ini explained)

On Windows, the cvi42serverconfig.ini file is in a common folder accessible by all users, typically C:\ProgramData\cvi42 (or C:\Documents and Settings\All Users\Application Data\cvi42 for WinXP).

On Mac OS, it is located in ~/Documents/cvi42/ or for Enterprise installations, /Library/Application Support/cvi42/

This file contains a list of configuration parameters for 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 the parameters is given below.

6.1 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.

i.e. DataFilesPath=C:/ProgramData/cvi42

ImageDBPath – Path to the folder containing the image data for your cvi42 system.

i.e. ImageDBPath=C:/ProgramData/cvi42/cvi42imagedb

SqlDatabasePath - Path to the cvi42 server database.

i.e. 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).

i.e. 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.

i.e. 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.

i.e. FailedLoginTempLockDuration=60

**ClientPort** – Specifies the port that the server listens on for incoming connections. Default is 49696.

i.e. ClientPort=49696

**ClientAncillaryPort** – Specifies the port the server uses for ancillary communications. Default is 49695. The ancillary connection is automatically established when attempting to connect on the main client port.

i.e. ClientAncillaryPort=49695

**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.

i.e. AdminPort=49697

**ClientPortIPv6** – Specifies the port the server listens on for incoming connections when using IPv6 addresses. Default is 48696.

i.e. ClientPortIPv6=48696

**ClientAncillaryPortIPv6** – Specifies the port the server listens on for incoming connections when using IPv6 addresses. Default is 48695.

i.e. ClientAncillaryPortIPv6=48695

**AdminPortIPv6** – Specifies the port that should be used when connecting to the server to perform administrative functions when using IPv6 address. Default is 48697.

i.e. AdminPortIPv6=48697

**ThreadPoolSize** – Specifies the number of threads the server uses to handle incoming requests. Default is 10.

i.e. ThreadPoolSize=10

**BackgroundTaskThreadCount** – Specifies the number of threads the server uses for background task processing. Default is 4.

i.e. BackgroundTaskThreadCount=4

**LogFilesPath** – Path to the folder containing the log files for the server.

i.e. 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)
i.e. 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.
i.e. LogArchiveCustomInterval=1

**PasswordRulesEnforced** – Specifies whether the server shall enforce password rules. Default is false.
i.e. PasswordRulesEnforced=false

**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.
i.e. 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)
i.e. DebugLog=0

**ConfigBackupInterval** – Specifies how often the server config file will be backed up in seconds.
i.e. ConfigBackupInterval=1200

### 6.2 Performance

**DicomHeadersResponseLimit_MB=256** - This value limits the amount of compressed header data returned by the server for a single bulk header request. Its purpose is to limit the RAM usage of the server. Lower values prevent the server from running out of memory but at the cost of a higher number of smaller requests because headers not retrieved in the bulk request will be transferred individually on demand.

If set to **DicomHeadersResponseLimit_MB = -1** the size limit will be disabled.

### 6.3 PPUProperties

**HostName** – Specifies the pay-per-use server to connect to when using pay-per-use licensing.
i.e. HostName=localhost

**Port** – Specifies the port to use for connecting to a pay-per-use server.
i.e. Port=443

**Scheme** – Specifies the scheme to use for connecting to a pay-per-use server
i.e. Scheme=https
6.4 License

**LicensePath** – Specifies the location of the RLM server when using concurrent licensing. This parameter uses the format portNumber@hostname, where portNumber is the port that RLM will use to connect to the license server, hostname is the ip address of the RLM server.

i.e. LicensePath=5053@127.0.0.1

6.5 DicomNetwork

**CompressionEnabled** – This identifies whether the PACS system is being asked for compressed data or not. Default is true. Some PACS systems require this to be set to false.

i.e. CompressionEnabled=true

**RemoteDicomNodesList** – This entry defines the connections for DICOM nodes (entities) that the server can interact with.

i.e. RemoteDicomNodesList=127.0.0.1, GLENNS-MBP, 11112, PACS, 30, CVI42,, true, false, Anonymized, true, true, true, true, false, ASCII

**RemoteDicomNodesListUpdated** – This marks whether DICOM Node migration from an older format has already been performed.

i.e. RemoteDicomNodesListUpdated=true

**LocalPacsAETitle** – Specifies the AE Title when cvi42 server is configured to accept study data via DICOM push.

i.e. LocalPacsAETitle=CVI42

**LocalPacsPort** – Specifies the port to use when cvi42 server is configured to accept study data via DICOM push.

i.e. LocalPacsPort=2012

**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 30.

i.e. IncomingDirMonitorInterval=30

**EnableStorescp** – Indicates whether the server will accept study data via DICOM push.

i.e. EnableStorescp=true

**EnableQueryScp** – The server acts as a Query/Retrieve SCP for study level queries.

i.e. EnableQueryScp=true

**EnableCGet** – Allows the use of C-GET instead of C-MOVE DICOM protocol for supported PACS.

i.e. EnableCGet=false

**AcceptUnknownAeTitles** – Enables promiscuous mode for DICOM operations.

i.e. AcceptUnknownAeTitles=true

**EnableLowLevelDebug** – Enables the DICOM debug log.

i.e. EnableLowLevelDebug=false
6.6 Single Sign On

**PrimaryServer** – Specifies the location of the Active Directory/LDAP server. cvi\textsuperscript{42} will initially contact this server when authenticating users using Active Directory/LDAP.

i.e. `PrimaryServer=ad-master.srclookup.com`

**SecondaryServer** – Specifies the location of the Active Directory/LDAP server. cvi\textsuperscript{42} authenticates users using Active Directory/LDAP against the server specified by primary server. When the authentication against the primary server fails cvi\textsuperscript{42} will authenticate users using a secondary server, specified by this parameter.

i.e. `SecondaryServer=second.ad-master.srclookup.com`

**TLSSSLConnection** – Instructs cvi\textsuperscript{42} to construct a secure communication channel when connecting to an Active Directory/LDAP server using TLS/SSL.

i.e. `TLSSSLConnection=true`

**DomainName** – Specifies the domain name 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 `\` (e.g. `\srclookup`). Secondly define a domain name with a prepended `@` (e.g. `@srclookup`)

i.e. `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.

i.e. `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.

i.e. `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 “cvi\textsuperscript{42}”, and only users in this group are permitted access to cvi\textsuperscript{42}. In order for cvi\textsuperscript{42} to enforce this, this parameter needs to be specified.

i.e. `AdditionalUserAttribute=memberOf=CN=cvi42,CN=Users,DC=srclookup,DC=com`

7 Housekeeping

The housekeeping system is a rule-based system to automate maintenance of the cvi\textsuperscript{42} DICOM study database. Typical use-cases are archival, routing and workflow.

7.1 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.

7.1.1 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.

7.1.2 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, e.g. assignment/removal of study tags.

7.2 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

7.2.1 Criteria

7.2.1.1 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 e.g. "older than one year" will never match. It may make sense to use the "import date" criterion instead.
7.2.1.2 **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](http://qt-project.org/doc/qt-4.8/qregexp.html#introduction).

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

7.2.1.3 **Institution Name**

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

7.2.1.4 **Manufacturer**

This criterion filters studies by the DICOM "manufacturer" attribute. The matching is done as for 7.2.1.2 Study Description.

7.2.1.5 **Model**

This criterion filters studies by the DICOM "model" attribute. The matching is done as for 7.2.1.2 Study Description.

7.2.1.6 **Modality**

This criterion filters studies by the DICOM "modality" attribute. The matching is done as for 7.2.1.2 Study Description.

7.2.1.7 **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 cvi\textsuperscript{42} 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.
7.2.1.8 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.

7.2.1.9 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.

7.2.1.10 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.

7.2.1.11 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.

7.2.1.12 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.

7.2.2 Actions

7.2.2.1 Assign 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.

7.2.2.2 Remove Tags

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

7.2.2.3 Convert Workspaces 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 7.2.2.5 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.

7.2.2.4 Store DICOM Data
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 cvi. In the latter case, the action can be further limited to only store workspace DICOMs, report DICOMs and/or other DICOMs generated by cvi (e.g. 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, use 7.3.1 Simulation to verify 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.

7.2.2.5 Export DICOM Data
This action exports DICOM data to file-system. 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.

7.2.2.6 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, use 7.3.1 Simulation to verify that the rule matches only the desired studies.

Alternatively, consider to use 7.48 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.
7.2.2.7  Stop

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.

7.2.3  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, e.g. 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.
7.3 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 (see 7.5 Log and Control). To the right of the "display log button", the effect of the edited (unsaved) rule list can be simulated, see 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.

7.3.1 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 (e.g. 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.
7.4 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 7.5 Log and Control window. Only log entries that are not needed for the system anymore (e.g. 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 time-spans 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 make sure, the Housekeeping system activities do not interfere with day-time usage of the system.

7.5 Log and Control

![Housekeeping Log Interface]

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 time-span to display the log for. After changing the time-span, the list is reloaded automatically.

8 Importing Workspaces from cmr<sup>42</sup> Version 3.x

Workspaces from cmr<sup>42</sup> version 3.x can be used in version 5.0 after they have been imported to the server.

For importing single workspaces for a particular study, use the following steps:

1. Double click the study to load the study list.
2. On the menu bar, select Workspace ➔ ImportWorkspace.
3. Navigate to the location of the workspace in the file dialog, and click Open.
4. The workspace will be imported to the server. The system will assume that the current user will be the owner of the workspace.

To import multiple workspaces (workspace migration) the following steps should be performed by an administrator, as it requires access to the server’s file system.

1. Use Windows Explorer, (or similar file manager program) to copy all the 3.x workspaces to C:\ProgramData\cmi42\migration\workspaces (Windows Server 2008, Windows 7), or C:\Documents and Settings\All Users\Application Data\cmi42\migration\workspaces (Windows XP).
   Note: Be sure to display hidden files and folders as C:\ProgramData folder might be hidden on your system.
2. You are allowed to use subfolders to organize your workspaces under ...
   \cmi42\migration\workspaces,
   i.e. ...\cmi42\migration\workspaces\subFolderA, ...\cmi42\migration\workspaces\subFolderB, etc.
3. The next time a user attempts to open a study from the study list, the system will attempt to automatically import matching workspaces for the current study and update the database.
4. When the study finishes loading, click on the Workspace ➔ LoadWorkspace from the menu bar, and a list of available workspaces will be displayed. Select from the list a workspace to load that contains your previous contours, measurements, etc.

9 Installing cmi<sup>42</sup> (Mac OS Platform)

To install cmi<sup>42</sup> Server as a Service (Background Process) on Mac:

This installer requires that the cmi<sup>42</sup> folder has been already dragged onto the Applications folder

1. Go into the Extras Folder on the cmi<sup>42</sup> Installation Disk Image (DMG)
Please ensure cvi42 and cvi42 Server are not currently running
Drag the cvi42 folder onto Applications
2. Run the cvi42 Enterprise Server AutoStart Installer
3. Follow the prompts and install the *cvi42Server Startup Script Installer* (Click “Continue”)
4. Please note, that any previous installations (User/Level cvi42 Database) will no longer be valid after an Enterprise installation (for dedicated server installations only!)
5. Continue (install for all users)
6. Install at the default location (current system volume)
7. Enter an Admin username and password
8. Click Close (and Restart)

(for Key installation  (Concurrent Users and/or PPU Licenses) You will need to re-log into the system as Root (Administrator) and run the cvi42 Client (to import the license key). Alternatively the license key can be copied to /Library/Application\ Support/cvi42/licenses/ directory (via the sudo command in a terminal window (e.g. sudo mv license_fileName_here /Library/Application\ Support/cvi42/licenses/)

On Mac OS X Server 10.7.3 (or later), a FQDNS is required. If the server's hostname is changed via the System Preferences (instead of the Server.app) then services on the server (including cvi42 RLM Server) may stop working properly. Solution/Workaround: Run the Server.app to edit or make changes to the Server's hostname.

Starting/Stopping/Restarting a Mac Enterprise cvi42 server

These commands will manipulate the cvi42server and RLM services on a Mac set up for Enterprise:

Stopping:

sudo launchctl unload /Library/LaunchDaemons/com.circlecvi.cvi42.plist
sudo launchctl unload /Library/LaunchDaemons/com.circlecvi.nlm.plist
sudo kill -15 `ps -Ac | grep cvi42Server | cut -c 1-5`

Starting:

sudo launchctl load -w /Library/LaunchDaemons/com.circlecvi.cvi42.plist
sudo launchctl load -w /Library/LaunchDaemons/com.circlecvi.nlm.plist