Sante PACS Server PG

Network Configuration Guide

Copyright © 2023 Santesoft LTD, all rights reserved

Contents

Definitions 2
Configure the DICOM Server 3
Automatic CD/DVD burning and printing of received studies 4
Delayed automatic CD/DVD burning and printing of received studies 5
Program's security for DICOM TLS connections 6
How to create the cert.pem and key.pem files 6
Insert the information of the other DICOM nodes 7
Configure the Worklist Server 9
Configure the HTTP Server 10
Enable SSL Encryption 11
Study Accessibility 11
Rest of configuration 11
Troubleshooting 12
Check a port of the program 13

Definitions

DICOM Services
The DICOM protocol consists of many different services, most of which involve transmission of data over a network. The program supports the store, query/retrieve and echo services (C-STORE/C-FIND/C-MOVE/C-ECHO SCU).

Store Service (C-STORE)
The DICOM Store service is used to send images or other persistent objects to a PACS or workstation.

Query/Retrieve Service (C-FIND/C-MOVE/C-GET)
This service enables a workstation to find lists of images or other objects and then retrieve them from a PACS system.

Echo Service (C-ECHO)
This service enables a workstation to verify the connection and the communication with another workstation or a PACS system.

DICOM communication protocol
The communication protocol is an application protocol that uses TCP/IP to communicate between systems. DICOM files can be exchanged between two entities that can receive image and patient data in DICOM format.

Communication between DICOM nodes
Two DICOM nodes (workstations, PACS systems) can communicate if they know each other. That means, each system must know the AE Title, the IP address or hostname and the IP port of the other system.

AE Title
AE Title or AET is an abbreviation for Application Entity Title. An AE Title is used by an Application Entity (AE) to identify itself. AE Titles need to be locally unique and are typically managed by a system administrator. They are case-sensitive and 16 bytes long. They are to be configured prior to initializing a DICOM connection.

IP Address
An Internet Protocol (IP) address is a numerical identification (logical address) that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes. Although IP addresses are stored as binary numbers, they are often displayed in more human-readable notations, such as 192.168.100.1. Usually, can be translated into a hostname via the local hosts file, or the Domain Name System (DNS) resolver, and can be used instead of the hostname.

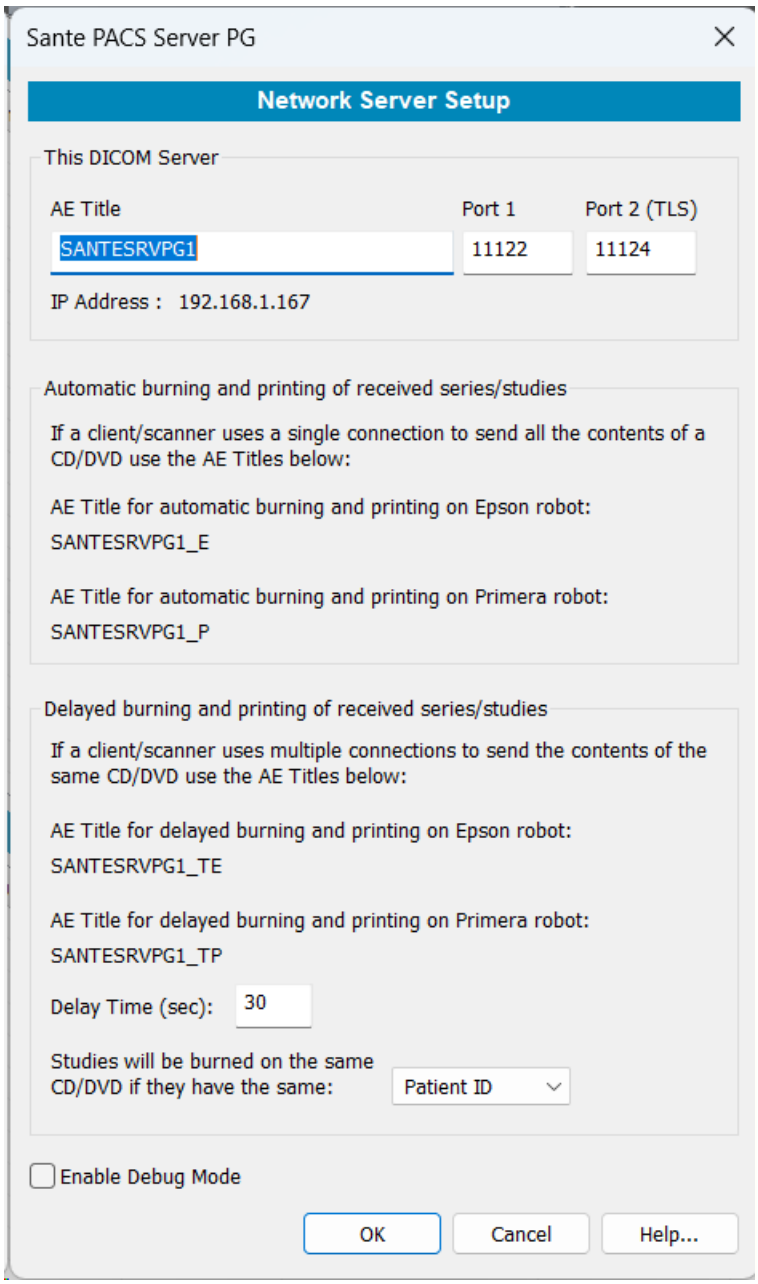
Hostname
A hostname is a domain name assigned to a host computer and is translated into an IP Address via the local hosts file, or the Domain Name System (DNS) resolver. It can be used instead of an IP Address.

Port
TCP/IP protocol uses the notion of port numbers to identify sending and receiving application end-points on a host. Each side of a TCP connection has an associated 16-bit unsigned port number (1-65535) reserved by the sending or receiving application. Arriving TCP data packets are identified as belonging to a specific TCP connection by its sockets, that is, the combination of source host address, source port, destination host address, and destination port. Ports need to be locally unique and are typically managed by a system administrator. The numbers 104 and 11112 are usually used as IP Ports in DICOM networking, but any number between 1 and 65535 can be used, but it must be unique for the host (node/PC), and it must not be used from any other application.

Firewall
A firewall is a dedicated software, which inspects network traffic passing through it, and denies or permits passage based on a set of rules. If there is a firewall in your computer, you must unblock the application.

Configure the DICOM Server

Select the menu command **"Network → Network Server Setup"**.
A dialog box appears and lets the user insert the AE Title and the port of Sante PACS Server PG.



AE Title
The AE title of this DICOM node. The AE title must be up to 16 characters without any white character (space, enter, etc.).

Ports 1 and 2
The program opens two ports for DICOM connections. The first port must only be used by remote DICOM nodes that are not TLS enabled and the second port must be used only by remote DICOM nodes that support TLS. A mixed-up situation is not possible. If the number of an IP port is equal to 0 the program does not open the port and the program will not be able to communicate with other DICOM nodes using this port. The port number 0 can be used if the user wants the DICOM server module to be disabled.

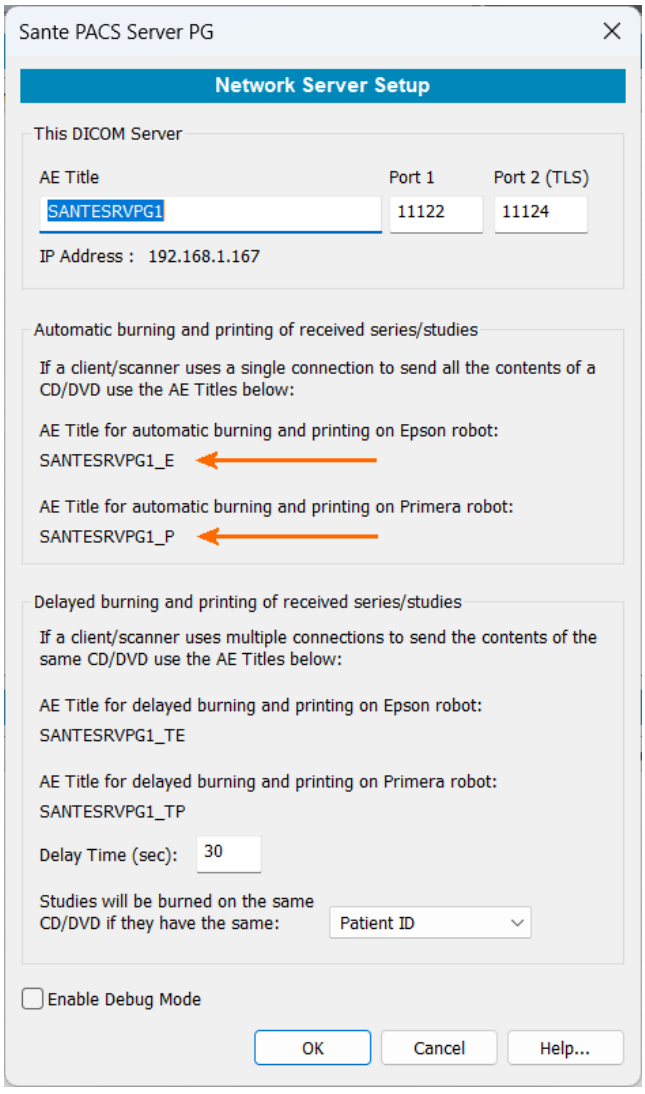
IP Address
This address is received automatically from Windows OS. The user can change this value only from the TCP/IP configuration of Windows.

Enable Debug Mode
This check box enables the debug mode of the program. The program in debug mode generates large debug data and it must be used if there is a problem and in consultation with the support team of Santesoft LTD.

Automatic CD/DVD burning and printing of received studies

Sante PACS Server PG when receiving studies, apart from storing them on the disk it can also send them automatically for CD/DVD burning and label printing to robotic disk publisher devices of EPSON and PRIMERA.

For this purpose, it uses two additional AE Titles, one with the addition of "_E" suffix in the original AE Title and one with the addition of "_P" suffix. **E.g.** If the defined AE Title is **SANTESRV1**, the program creates the AE Titles **SANTESRV1_P** and **SANTESRV1_E** as well. These additional AE Titles are used for automatic CD/DVD burning and printing.



If a client DICOM node (a CT/MR/US/DX or other medical scanner, a DICOM workstation etc.) instead of using the original AE Title of Sante PACS Server PG it uses the AE Title with the **"_E"** suffix, then Sante PACS Server PG stores the received series/studies on the database and automatically sends them for printing and burning to an **EPSON** producer.

If a client DICOM node (a CT/MR/US/DX or other medical scanner, a DICOM workstation etc.) instead of using the original AE Title of Sante PACS Server PG it uses the AE Title with the **"_P"** suffix, then Sante PACS Server PG stores the received series/studies on the database and automatically sends them for printing and burning to a **PRIMERA** producer.

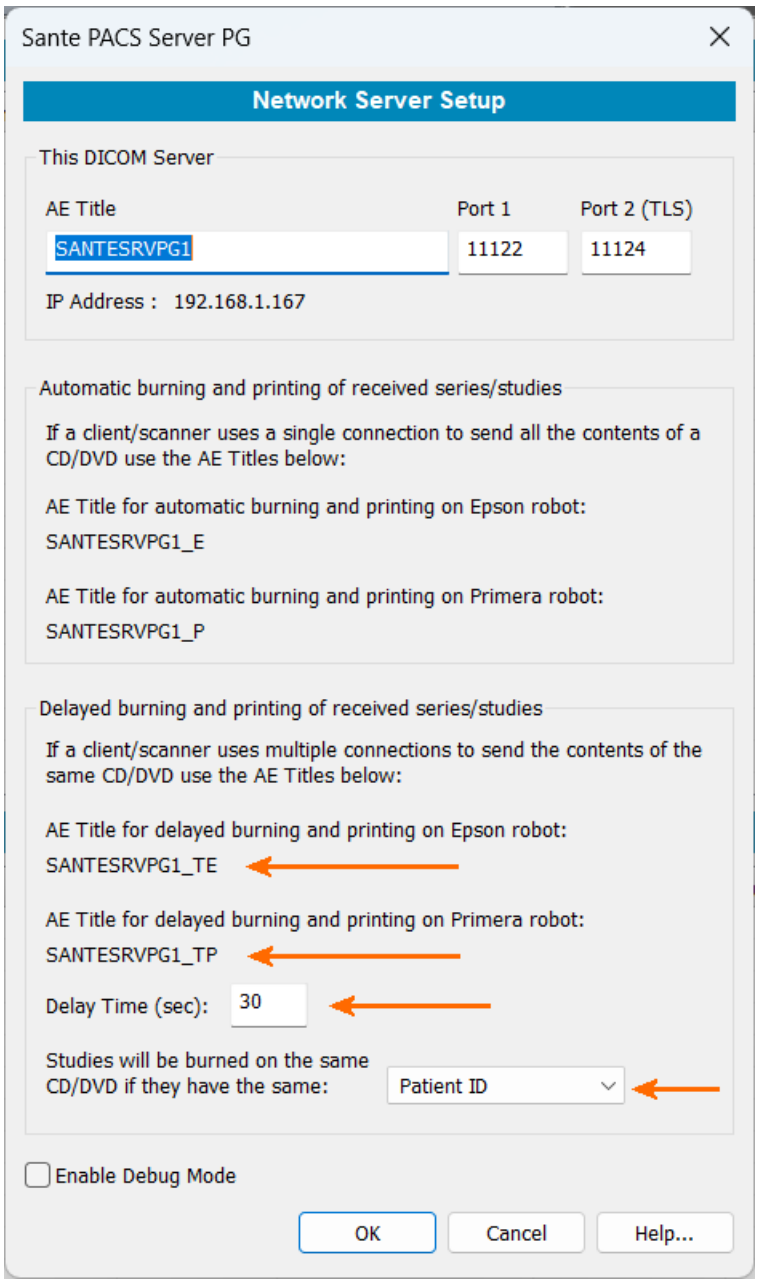
Delayed automatic CD/DVD burning and printing of received studies

Some medical scanners use multiple connections to send a whole study (usually one connection per series of the study). In that case, the program by using the AE title with **"_E"** and **"_P"** suffixes that described in the previous paragraph, will create one CD/DVD per connection, that is one CD/DVD for every series, and not one CD/DVD for the whole study that contains all the series of the patient.

In that case the client DICOM node (a CT/MR/US/DX or other medical scanner, a DICOM workstation etc.) must use the AE Title with a **"_TE"** or **"_TP"** suffix. With these suffixes the program waits for a specific time before sending the received series of the study for printing and burning. If it receives a new series that belongs to the study in delay, it waits again the specified time for the next series and so on. If it does not receive in the specified time a series that belongs to the study in delay, it sends the study for burning and printing.

The user specifies the delay time in the control **Delay Time (sec)** control of the dialog box below. The default value is 120 sec.

The user can specify the method (same Patient ID or same Study UID) that the program will use to group the series together so to burn them in the same CD/DVD, from the relative combo box.



Program's security for DICOM TLS connections

If the user does not use their own certification and private key files for SSL/TLS connections, for maximum security the user must replace the cert.pem and key.pem files provided by the program with others that have been created by the user. Files created this way are not suitable for use with the built-in web server and they must be used for DICOM TLS connections only.

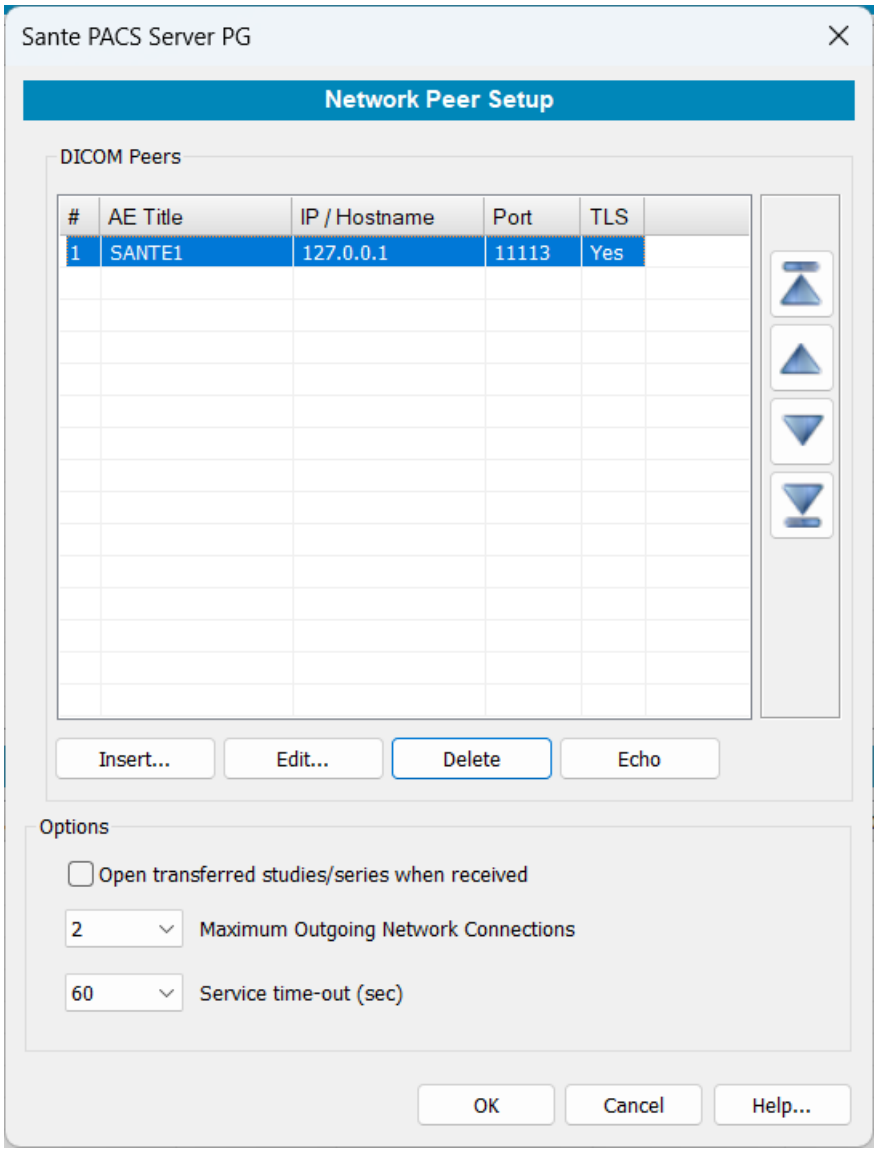
How to create the cert.pem and key.pem files

(all paths are the default paths of the programs)

- Download and install the OpenSSL utility
  https://slproweb.com/products/Win32OpenSSL.html
- Download the default configuration file
  https://github.com/openssl/openssl/blob/master/apps/openssl.cnf
  and put it in the bin folder of the OpenSSL library ("C:\Program Files\OpenSSL-Win64\bin")
- Add the path of the binaries of the OpenSSL utility to PATH system variable.
- In the command prompt run the command:
  SET PATH=%PATH%;C:\Program Files\OpenSSL-Win64\bin
- In the command prompt run the command:
  openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -sha256 -days 36500 -nodes
- Replace the files in the "C:\Sante Server DB\.Configuration Files\TLS" folder with the newly generated ones.

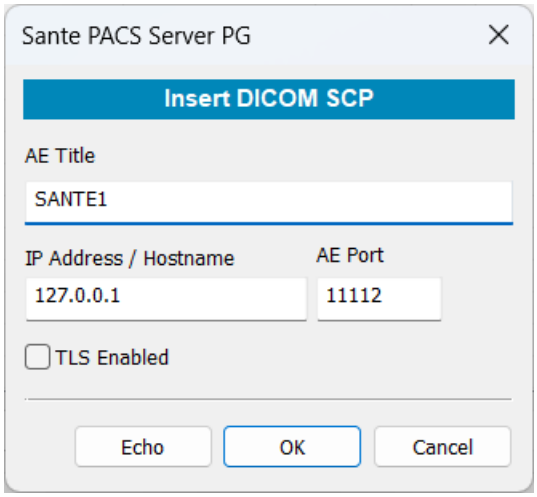
Insert the information of the other DICOM nodes

Select the server menu command **"Network ➔ Network Peer Setup"**.
A dialog box appears and lets the user insert the other DICOM servers and clients that exist in the network.
This command requires administrator privileges.



Insert/Edit a PACS system

By pressing the **"Insert"** or **"Edit"** buttons of the above dialog box, a new dialog box appears and lets the user to insert the information of the PACS system.



Select a DICOM server row and press **"Echo"** button, to check the connection with the selected server.
Select a DICOM server row and press **"Delete"** button, to delete the selected server.

Open transferred studies/series when received option
When the program receives studies and/or series it inserts them in the database.
If you wish to open them immediately after they have been received, check the checkbox "Open transferred studies/series when received".

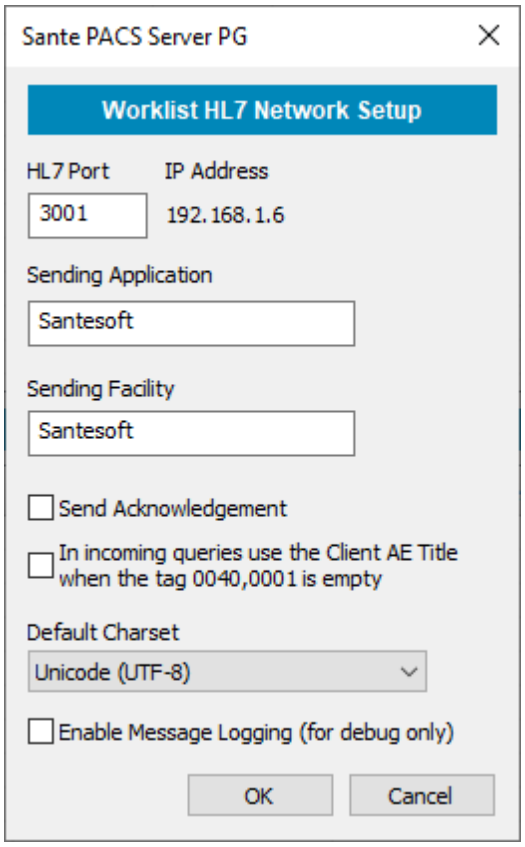
Maximum Connections option
When the program acts as a client and the user searches and retrieves studies/series from other servers, this option determines the maximum number of outgoing connections. The program starts transferring as many studies/series as the maximum connections number indicates and the rest of them are putted in a queue. The program waits for a transfer to finish and then opens another until the queue is empty.

When the program acts as a server the number of incoming connections is unlimited.
That means, any number of remote clients can connect with the program and transfer files, without any limitation.

Service time-out option
This option determines how long the program waits for a response from the peer. If this time passes the program interrupts the connection.

Configure the Worklist Server

Before the first use of the Worklist, the user must configure it. The program can receive HL7 messages about the scheduled procedures from HIS/RIS programs and for that purpose must have an IP port for communication with other HL7 nodes. For the configuration the user must use the menu command **"Network ➡Worklist Server Setup"**. This command displays the following dialog box:



HL7 Port
The IP port for the communication with other HL7 nodes like HIS/RIS software. If the number of the HL7 port is equal to 0 the program does not open the port and the program cannot receive HL7 messages. The port number 0 can be used if the user wants the Worklist server module to be disabled.

IP Address
This address is received automatically from Windows OS. The user can change this value only from the TCP/IP configuration of Windows.

Sending Application / Sending Facility
The program can send HL7 messages to other HL7 clients. The program will use these values in the corresponding fields MSH.3 and MSH.4 of the HL7 messages.

Send Acknowledgement
Some HL7 servers require to receive an acknowledgement as proof that the client received the message. With this option enabled, the program sends this acknowledgement to the server.

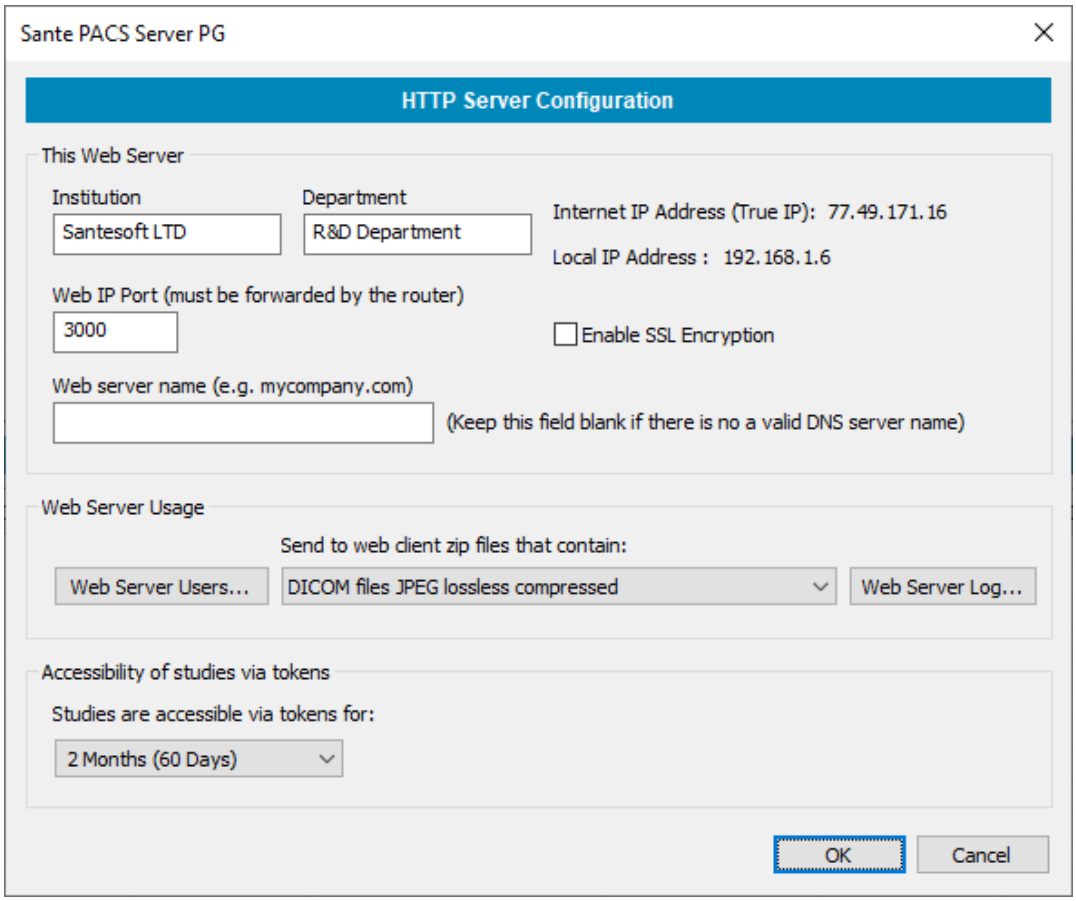
Default Charset
If the HL7 message does not contain any information about the used charset, the program uses the value of this box.

Enable Message Logging (for debug only)
By default, the C-FIND requests from medical scanners to worklist are not logged in the log database of the program and they are not displayed in the SCP report lists. That is because many medical scanners send periodically C-FIND requests in very small time-frame (usually every 15 sec) and this way the log database becomes huge. The user must enable the C-FIND message logging of the worklist for debug reasons only and turn them off again after debugging.

Rest of configuration
For the rest of configuration and for the usage of Worklist server module, please read the manual **"Built-in Worklist Guide"**.

Configure the HTTP Server

Select the menu command **"Network ➔ HTTP Server Setup"**.
A dialog box appears and lets the user configure the HTTP server module.



Institution, Department
This information appears on the web page of the server and informs the user with which server he has been connected.

Internet IP Address (True IP)
The internet IP address is received automatically from the internet service provider and it is the address with which the HTTP server goes to the internet. The user cannot change it.

Web IP Port
With this port the HTTP server goes to the internet. If the number of the Web port is equal to 0 the program does not open the port and the program cannot communicate with web clients. The port number 0 can be used if the user wants the HTTP server module to be disabled.

ATTENTION!
The Web IP port of the HTTP server must be forwarded by the router!

Web server name
This field is used by the database for creation of fully qualified study tokens, that are used by patients to retrieve their studies. If the server does not have a valid DNS name or the **"Web server name"** field has been kept blank, the database interface of the sever uses the **"Internet IP Address (True IP)"** arithmetic value for creating a token with a valid fully qualified web address:
http://77.49.171.16:3000/token?4m5RHRCmSrWYcnmk8lCThvg0qy2KHA7K5ZldW7ZDNsEKsZ68NcJU4b83UtnYJfwx

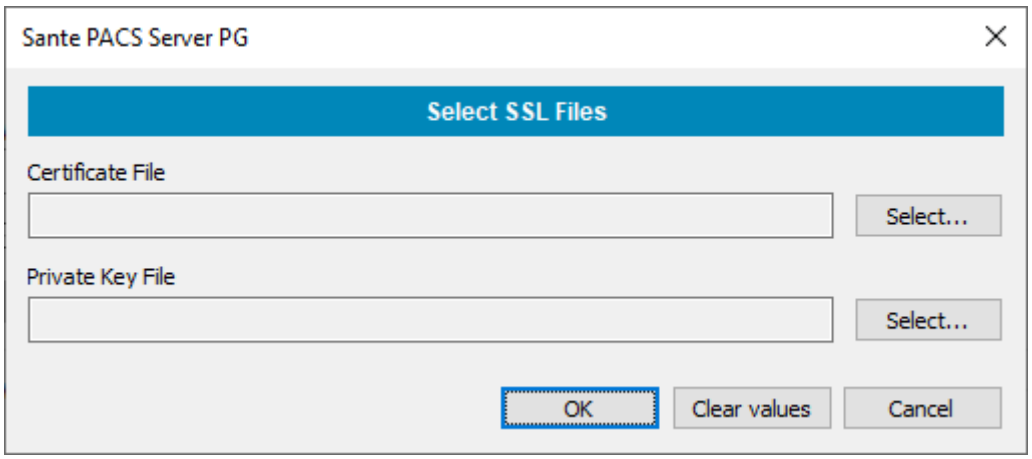
ATTENTION!
The Web server name must be kept blank if there is not a valid DNS server name!

Enable SSL Encryption

Because of the critical data contained in the server it is **strongly** recommended the HTTP server module to be used with the SSL encryption enabled and if it is possible only within VPN connections.

To get an SSL Certificate, the user must have a valid **ICAN** (Internet Corporation for Assigned Names) server name like **santesoft.com**.

When the user checks the **Enable SSL Encryption** checkbox, the program asks for the certificate file (.crt) and the private key file (.key) that the user has received from the SSL Certificate provider of his choice.



Study Accessibility

This combo box lets the user define the time that a patient or a remote physician can access studies via the mechanism of tokens. The time starts to count from the study date. With this control the user can reduce the workload of the server that is produced by remote users.

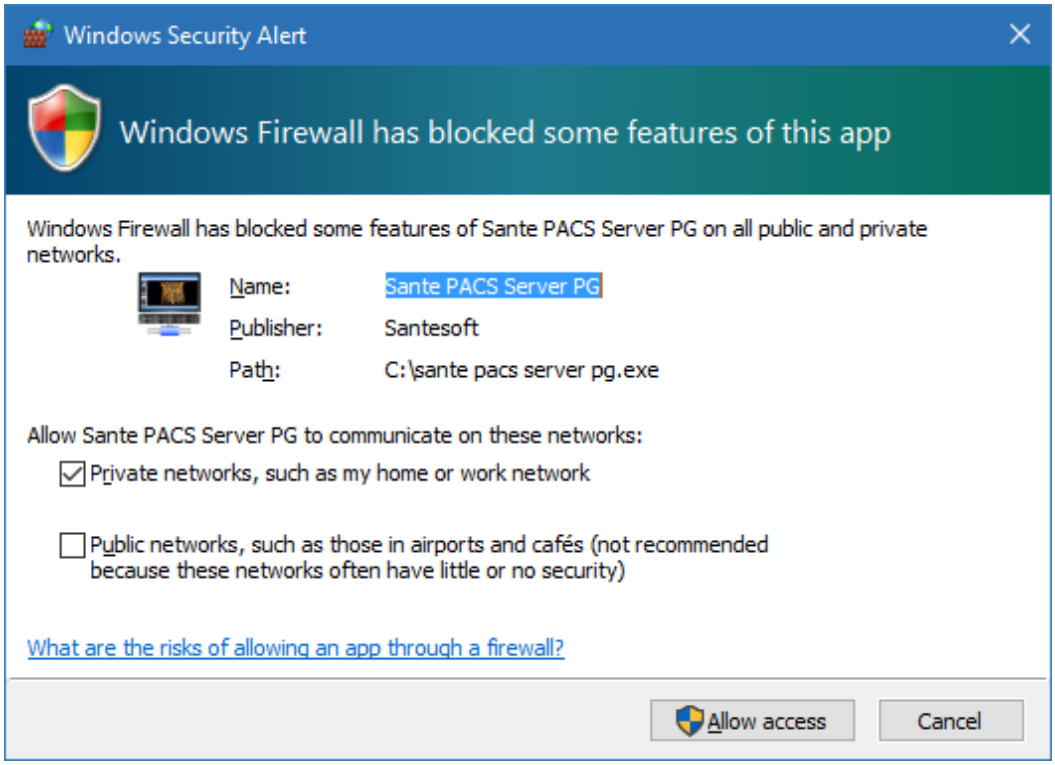
Rest of configuration

For the rest of configuration and for the usage of HTTP server module, please read the manual **"Built-in Web Server Guide"**.

Troubleshooting

If the program cannot communicate with other DICOM nodes or it cannot transfer files from other DICOM nodes, please check the following checklist:

- Ensure that the port of the program is not used by any other program.
- Ensure that the port of the program is not blocked from a firewall or an antivirus.
- When the program starts it asks for to be added in firewall exception list. If you answered no you must add it manually.



- If the two nodes (server and client) belong to different subnetworks, ensure that the port of the program is forwarded by the router.
- If the program can "ECHO" the other node (client/server) but it cannot transfer files: Both machines (server and client) must know each other. You must insert the AE Title, IP address and port of the application into "Known DICOM Nodes" list of the other node (client/server). Without this information the client/server does not know where to send the files.
- If the PC has more than one network card (physical, logical or virtual network cards) and thus more than one IP address, ensure that the client and server use an IP address of the same sub-network. E.g. If the server has two IP addresses, the addresses 192.168.1.1 and 172.91.1.1 and the client has the IP address 192.168.1.* the client must use the address 192.168.1.1 as the IP address of the server. If the client has the IP address 172.91.1.* it must use the address 172.91.1.1 as the IP address of the server. That means that the server and client must belong to the same sub-network. In case that the PC has more than one IP address, the program displays only one IP address, the first one, although it opens its IP ports in all the available network interfaces and not only in the indicated IP address. Use the command ipconfig in the command prompt to get a list of all the IP addresses of the PC.

Check a port of the program

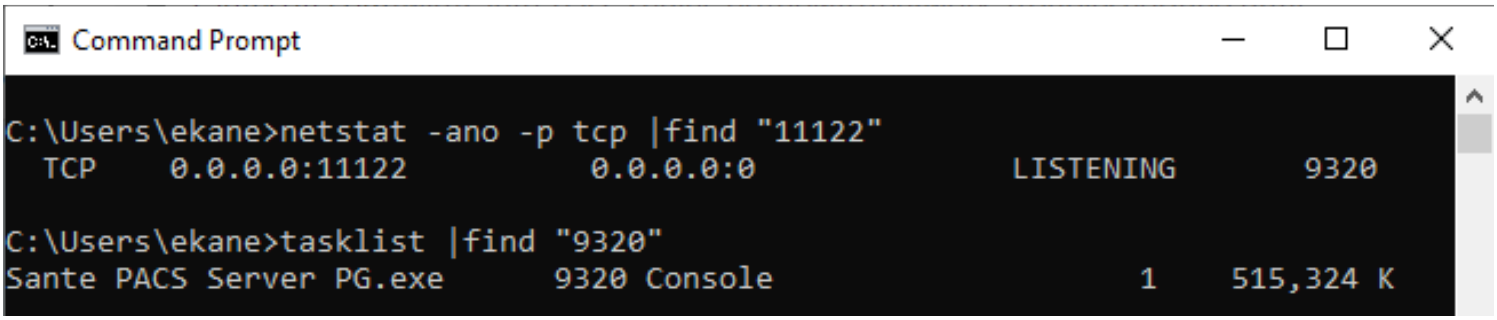
You can use the **netstat** utility in the command prompt to check if the port of the program is opened and at which IP address.

Use the menu command:

C:\>netstat -ano -p tcp |find "11122"
to check if the port 11121 of the program is opened and at which IP Address. The last number that the program prints is the PID of the application that has opened the port.

Use the menu command:

C:\>tasklist |find "9320"
to find which is this application.



With these commands you can check any one of the ports of the program, like the port of Worklist server module or the port of HTTP server module.