

CAN-8

VirtuaLab

Reference Manual

Technical guide

Revised October 2017

Table of Contents

System Overview	3
Networking Information	4
IP Protocol	4
Bandwidth.....	4
Server System Management	5
System Backup.....	5
Managing Disk Space	5
System Cleanup	6
REFRESH STUDENTS.....	7
REFRESH ALL	7
Starting and Stopping the Server	7
System Reporting/Monitoring	8
Managing Video Resources	9
Video Formats.....	9
Video Codecs	9
Video Storage.....	10
Bandwidth requirements for video in CAN-8.....	11
Calculating for the number of stations:.....	12
Calculating for 30 stations:	12
Data Rates for Audio	12
Calculating for 30 Stations:	13
System File Layout and Use	13
Registration and Menu system files.....	13
Lesson Directories	15
Deleted Directory.....	16
ACCESS CONTROL FOR USERS OF CAN-8 SERVERS.....	17
SETTING-UP THE ACCESS CONTROL.....	17
EXTENDED FORMAT.....	19
GENERAL NOTES	20
Client stations management	20
Generic Client installation	20
Create a customized Installation file.....	23
Silent Installation of the client	27
Uninstall CAN-8.....	28
Registry Keys and Values.....	28

System Overview

The CAN-8 system is designed to operate in a *client-server* environment.

The server software typically runs on Windows XP (32 and 64 bit), Windows 2003 server, Windows 2008 server, Vista (32 and 64 bit), Windows7 (32 and 64 bit) using the Intel based platform.

The client software may run on Windows 2000, Windows XP (32 and 64 bit), Vista (32 and 64 bit), or Windows7 (32 and 64 bit).

In order to operate, both the client and server machines must have *TCP/IP* loaded and properly configured.

The server system may be placed behind a firewall if *UDP ports 17180-17190* are left open to access the server or if the firewall is configured to redirect these packets from it's outside IP address to the CAN-8 server (NAT).

The CAN-8 server process provides end-to-end security between client stations and the server. This includes login authentication, user management and enforcement of single logins. There is no need to have open file shares on the machine acting as a server to allow the CAN-8 client to store student work. Likewise, it is not necessary to run web-server software as the CAN-8 server software is entirely self-contained and communicates with the CAN-8 client stations using its own protocol.

The CAN-8 server process may run either as a service process or an application on the server. The program does not display a window so there is no information to observe on the server itself. All information regarding users and operation of the system is accessed via the client station.

It is not recommended that the CAN-8 server run alongside other applications on the server machine in order to maintain good real time response to client requests. Likewise running in a virtualized environment is strongly discouraged as the performance penalty incurred due to frequent switching between hosted operating systems can degrade the response time of CAN-8 significantly.

The server hardware should have at least 4GBytes of physical RAM as the CAN-8 server software will attempt to use the bulk of it for its internal cache as needed to maintain a high performance. Virtualized or paged storage is not adequate since it will actually reduce the performance of the system as compared to not having the physical resource itself.

Networking Information

This section is intended for any person responsible of maintaining the system hardware and installation.

IP Protocol

The CAN-8 system communicates with the server using the **IP protocol**. This is the native protocol of the Internet. In the simplest case of a network, the system requires one computer that is designated as the server and another that is designated as the client. Each computer must have a **unique IP address**. The IP address or host name of the server must be **static**. After the initial login from the client station, a registry key pointing to the server's IP address or DNS name will be automatically created.

The server and client communicate using **UDP** (User Datagram Protocol) packets. This connectionless protocol is a subset of IP allowing the server and client to perform their own error handling. In order to communicate, the following ports must be available on the server for the client to attach to:

UDP Ports 17180 to 17190

In situations where the network contains firewalls, or other security measures, the firewall settings must allow passing of packets on these ports. This includes workstations, network devices and servers which must have their local firewall configured to allow traffic on these ports.

The system will work with most network address translation (**NAT**) schemes and has been tested with them. In most cases, proxy (true proxy) servers will not work unless they simulate NAT in their operation.

Bandwidth

In order to run in a satisfactory manner, a minimum required bandwidth must be available between the server and client.

This averages at **40 kbits/sec** and is at its highest **88 kbits/sec** .

If there are more stations than one, then the total maximum required bandwidth would be 88 kbits/sec times the number of stations:

1 station = between 40 and 88 kbits/sec 4 stations = between 160 and 352 kbits/sec

30 stations = between 1200 and 2640 kbits/sec
= between 150 and 330 *KBytes/sec*.

Server System Management

This section is intended for any person responsible of maintaining the Server's hardware and installation. It describes various tasks that should periodically be done to ensure smooth operation of the system.

System Backup

The CAN-8 system consists of regular files that are typically stored under the \SVSYS\... directory on one of the server disk drives. While the server program is running, various files throughout this directory will be open for writing and reading. For backup purposes, the files may be read at any time as database and student tracking files are typically appended to and not modified in place.

The backup procedure used must be capable of reading files that are currently open for writing by another process. Also, the backup program **must not ever** open any file with write access as it will potentially prevent the server program from being able to write to the same file at the same time.

It is recommended that a full system backup be used rather than an incremental backup due to the large number of files that are modified during the operation of the system. Each incremental backup may be as large as the full system backup in this case.

Managing Disk Space

As a resource, the disk space on the server will be consumed by the system over a period of time. The exact amount consumed will depend on the number of students performing recordings, the length of the recordings and the amount of static course material that has been recorded on the server. In most cases the student recordings will far exceed the space used by the course material, as well, the amount of course material does not increase constantly, whereas the student recordings may do so.

The approximate disk space used by students for recordings may be calculated as follows for the purposes of example:

Average minutes spent per student recording per session

$$\begin{array}{c} * \\ \text{Number of students using system per day} \\ = \\ \text{Total minutes of recording time per day} \end{array}$$

If you take this total and divide by 60 minutes to the hour and then multiply the number of hours by 15 MBytes you will have the daily total storage requirements for the system. For example:

$$\begin{array}{l} (30 \text{ minutes per session recorded}) * (150 \text{ students per day}) = 450 \text{ minutes per day} \\ 450 \text{ minutes per day} / 60 \text{ minutes per hour} = 7 \text{ hrs per day} \\ 7 \text{ hrs per day} * 15 \text{ MBytes per hour} = 105 \text{ MBytes per day} \\ \text{Assuming classes 5 days a week} = 525 \text{ MBytes per week} \\ \text{Per month} = 2.1 \text{ GBytes per month} \\ \text{Per 4-month term} = 8.4 \text{ GBytes} \end{array}$$

As you can see, the amount of disk storage for students climbs rapidly.

In order to combat the eventual filling of the entire server disk, the instructors should be advised to remove students from the lesson tracker screens as soon as possible after they are finished scoring the work or have gone over it in class.

When the instructor deletes items from the tracker, the data is placed in a temporary recovery area where it may be archived or deleted by the system administrator. This area is to be found on the server in the directory [\SVSYS\DELETED](#) assuming the file directory layout of a standard installation.

After instructors have deleted the data from the Tracker screens, this directory may be deleted by the administrator to free up the disk space used by the student responses. This directory may be removed while the server is running.

System Cleanup

The functions available to refresh the system are accessed from the **client software**, for users with SYSTEM SUPERVISOR's privileges.

At the end of each term or year, it is sometimes desirable to remove all the users and their recordings from the system.

There are two tools available for that end. Both methods rely on using the REFRESH option via an [Import Registration File](#). The two types have different effects:

REFRESH STUDENTS

This option removes all students and their recorded data from the system but leaves instructors, and classes intact. This option is useful between terms for when it is not desired to re-create instructors or classes.

Step by step instructions on [how to use the REFRESH STUDENTS function](#) can be found in the **System Tools** section of this manual.

REFRESH ALL

This option removes all students, classes, assignments, and instructors and all users' recorded data. The MASTER user is remove and re-created with the default password of PWORD. This option is useful at year-ends when instructors and class assignments will change. This option also has the side benefit cleaning up the users database file and re-compacting it.

Step by step instructions on [how to use the REFRESH ALL function](#) can be found in the **System Tools** section of this manual.

In both of the above cases, the \SVSYS\DELETED directory should be removed to free the disk space that is used by student responses. The system will automatically re-create a DELETED directory on its own, and when necessary.

NOTE:

Do not attempt to clean up the system or recover disk space by deleting files or folders from the CAN-8 server directory (except the DELETED directory mentioned above). This would result in a corrupted file system and impact the software's behaviour.

Starting and Stopping the Server

The CAN-8 server process may run as an **application** or as a **service** on the machine that is being used as the server. In this case it is generally automatically started when the server is started or when the administrator user signs on. In some cases, it may be required to stop the server process and then re-start it.

These cases are:

- Copying files to or from the installed \SVSYS\... directory tree.
- Installing software updates/changes.
- Troubleshooting server operation.

In order to shut the server process down *if it is running as a service* (does not show in taskbar), the following steps are required:

1. Go to the control panel.
2. Double click on Services.
3. Scroll down to CAN-8 Server.
4. Press the Stop button.
5. The service manager will notify you when it has stopped running.

For information on how to install CAN-8 as a service, please contact your CAN-8 support team.

If the server process *is running as an application* (does appear on the taskbar), then use the following steps:

1. Click on the minimized taskbar box for the server, a large empty window will appear on the screen.
2. Click on the X in the upper right corner of the window
3. The empty window will disappear indicating the server process has stopped.

You may want to make sure there is no instance of the CAN-8 server running on that machine, in which case you can open the task manager and check in the process list that there is no ntserve.exe process listed.

Once stopped the system may safely be modified. Modifying the system files with the server process running may result in damaged files.

To restart the server process if it is a service, these steps should be followed:

1. Go to the control panel.
2. Double click on Services.
3. Scroll down to the CAN-8 Server.
4. Press the Start button.
5. Exit the service manager when the CAN-8 server has started.

In the case that the server application is started on the login of the administrator user, it may be simply re-started by double clicking on the CAN-8 icon on the desktop.

System Reporting/Monitoring

While operating the system tracks various internal parameters in a file called **SERVER.LOG** that is created in the same directory as the **NTSERVE.EXE** program. This file can be examined to monitor the system operation. This file must not be opened

for write access while the NTSERVE program is running as it will cause the NTSERVE program to wait until exclusive write access is available.

This file is updated approximately every 10 minutes when the system is idle and more often during periods of heavy use.

It is not advisable to delete this file indiscriminately as it is often needed after a problem has been encountered and if it has been recently deleted it will not contain the information required to diagnose the problem. If problems are encountered with the operation of the CAN-8 server this file may be compressed using WinZIP or other programs and sent to Sounds Virtual for analysis.

Managing Video Resources

Video Formats

Both .avi and .mpg video files may be imported into lessons authored in EAASy II. Only .avi files display the sound file at the bottom of the student screen. The other choices, .mpg, and .mpeg, do not appear on the selection box but may be accessed by typing the file name and extension into the file selection box directly.

Video Codecs

In general, when video is digitized into .avi or .mpg formats, the video clip is compressed by a particular video compression codec that may be associated with the video driver of the video card in the computer. To play that video clip on a client workstation, the appropriate codec must reside on the client computer.

The easiest way to ensure compatibility is to digitize or recompress files using a codec that resides on the client computers.

To confirm which codecs reside on a computer, look under Settings/Multimedia/Devices/Video Compression Codecs. A list will appear including items such as "Indeo video R.32 by Intel". We cannot recommend particular codecs, although using ones produced by large companies such as Intel is probably safest.

The next step is to digitize or recompress the video clips to use a codec you have found to be available on all of the client machines. Each video digitizing software program is slightly different, so it is not possible to provide detailed instructions about how to digitize or recompress video clips. Consult the documentation for your digitizing software and determine how to set the format to match the codec which you know exists on client machines.

Video Storage

In CAN-8, sound, text and image files are part of the lessons in which they appear. The author simply imports these elements into the lesson while creating the lesson. These components of the lesson are then available to anyone accessing the lesson.

This is not the case for video. Video clips are only **linked** into lessons and not directly imported.

It is therefore important that the link to the video be true on all the client workstations that will try to access it.

There are 3 options to store videos:

- Link to a video placed on a network share.

Videos can be stored on a file server in a directory accessible by and streamed to the client workstations. It is not necessary that it be the same server where the CAN-8 system is located, but Microsoft File Sharing or other file sharing software such as Novell, must be installed on the machine that is to provide this shared resource.

For video files to be accessible on client machines, they must reside in a shared resource directory on a file server accessible from the client. Confirm that the shared resource is accessible from the workstation and place all video files into one shared directory with a suitable name (e.g., "video").

To make a directory shareable on a Microsoft-based server, right-click on the directory where the videos are stored. Choose Properties/Sharing. The default setting is "not sharing". Change this to "sharing". A little hand will appear under the folder indicating that this folder is now accessible from client stations on the network.

Care should be taken to ensure that access to this shared resource is read-only to prevent other users from erasing, modifying or adding their own files to the directory. On each client machine you must map a network drive to the shared resource by browsing the network neighbourhood and selecting the server and drive you wish to access. To do this, right-click on the desired resource and select "Map network drive" from the pop-up menu. Choose a drive letter that is the same as the one used by the authoring station as well as all the other workstations. If the drive letter is different, some stations will not be able to access the video. Select "Reconnect at Login" to make the connection permanent.

If in the lesson the link to the video is:

E:\Videos\video_name.avi

All workstations must have an E:\ mapped drive and the video folder must be shared.

- Link to a video placed locally on the client workstation.

If network bandwidth is an issue, the video can also be placed on the workstation instead of a network share. This however implies that the path to the video be the same one used by the authoring station as well as all the other workstations.

If in the lesson the link to the video is:

C:\VIDEOS\video_name.avi

All workstation **MUST** have a VIDEOS folder on their C drive, and the video file must be present on all the workstations.

- Link to a video placed on a webserver via URL.

A video placed on a webserver and linked to a lesson via a URL would allow all users (off and on campus) to access this video since the path would be valid from every station. The video is played within the CAN-8 interface but streamed via http. Make sure that your firewall rules and/or load shaper software do not prevent video downloads/streaming. In the case of a load shaper, the video may appear to load fast at first, then become increasingly slower.

Bandwidth requirements for video in CAN-8

Video compressed using MPEG 1 or 2 may have its compression rate adjusted such that the quality of the video is sacrificed to reduce the bandwidth required to transfer it. What follows is an analysis of bandwidth required based on our own experience with compressed video.

MPEG-1 was designed to use a standard frame size of 352x240 (SIF dimension) and in most cases delivers good quality video (and audio) at a rate of 64 KBytes/sec.

MPEG-1 may use other frame sizes, the data rate will vary when the frame size and also the frame rate is changed. The maximum "nominal" data rate for MPEG-1 is 115 KBytes/sec, this may be used to calculate maximum bandwidth requirements.

Calculating for the number of stations:

$30 \text{ Stations} * 115 \text{ KBytes/sec(peak)} = 3.4 \text{ MBytes/sec (peak)}$
For average video:
$30 \text{ Stations} * 64 \text{ KBytes/sec} = 1.9 \text{ MBytes/sec}$

This data rate is well within the limits of a network running at 100 Mbits/sec (10 MBytes/sec).

The MPEG-2 standard is in many ways similar to MPEG-1.

The primary motivation behind MPEG-2 was to have a standard that is more practical to edit in such systems as non-linear video editing. MPEG-2 also increases the quality of the video slightly by allowing a greater number of bits of quantization for DC components along with more flexibility in the encoding scheme.

This said, the data rates for MPEG-2 tend to be higher for similar frame sizes and rates than for MPEG-1. The benefit in the lab situation is a slight increase in the quality of the video.

Some sample data rates for MPEG-2 are calculated below using a frame size of 352 X 480 (Half Horizontal CCIR 601 displays as 352 X 240) and frame rate of 24 fps.

The difference in video quality at the stations may not be noticed by most viewers, especially if the source material is a VHS tape.

Calculating for 30 stations:

$30 \text{ Stations} * 200 \text{ KBytes/sec(peak)} = 6 \text{ MBytes/sec (peak)}$
Average rate using 352 x 240 frame size:
$30 \text{ Stations} * 80 \text{ KBytes/sec} = 2.4 \text{ MBytes/sec}$

The average data rate is within the limits for 100 bits/sec ethernet but the peak rate may exceed it. Typical limits for ethernet are at approximately 30-40% of the bit rate (ie: 3-4 MBytes/sec).

Data Rates for Audio

In comparison, the data rates for the audio used by the CAN-8 system are very small. Our system uses our own format of compression that is done in real-time at the station when audio is recorded and is also decompressed when played back. The audio data transferred

by the CAN-8 system is always in compressed form on the network.

The average data rate for the audio in compressed form is 6 KBytes/sec.

Calculating for 30 Stations:

$$30 \text{ Stations} * 6 \text{ KBytes/sec} = 240 \text{ KBytes/sec}$$

Since each station may play and record at the same time, the peak rate would be double this number of 480 KBytes/sec. In most cases the students are not playing and recording at the same time.

System File Layout and Use

This Section is intended for any person responsible of maintaining the system hardware and installation. It describes various technical details of how the files for the CAN-8 system are organized on the server.

This description will assume that the system has been installed in the standard way and the drive and directory that contains the entire server based system is C:\SVSYS\ with the client side executables elsewhere.

There are two basic components to the directory structure of the system:

- the first is the registration and menu system components that effect the system in a global manner
- the second component pertains to directories and files that get created due to authoring lessons or students working with lessons.

Each will be described separately.

All system files are in **Binary** format and no attempt should be made to edit these files with any text based editor as it will corrupt them beyond repair.

Any of the files described could be in use by the server at any time. If files are being copied or moved around, it is **required** that the NTSERVE program be **stopped** before doing so.

Registration and Menu system files

The following files are in the root of the system install directory. These files will be present on all systems.

File or Directory name	Function
C:\SVSYS	Base System Directory
C:\SVSYS\NTSERVE.EXE	Server Executable
C:\SVSYS\NTSVTASK.EXE	Server Service Task (creates reports, etc)
C:\SVSYS\NTCHECK.EXE	Installation test file.
C:\SVSYS\SERVER.LOG	Server log (created by server, may not exist)
C:\SVSYS\ID\	Contains information about menu/registration
C:\SVSYS\SVI\	Default directory for creation of lessons
C:\SVSYS\DELETED\	Contains deleted data

The following is the contents of the ID subdirectory.

The files in the ID subdirectory contain all user registration information, the menu, classes, assignments, global keyboards, attributes, and temporary files used for reports. This section is for information purpose only. These files should **never** be **altered, edited** or **deleted**, unless instructed to do so by Sounds Virtual technicians.

File or Directory name	Function
USERS.DAT	System user database. Contains information about all users of the system.
MAIN.DAT	Menu file. Contains entire menu structure as seen by all users.
MAIN.1 MAIN.2 MAIN.5	Backup copy of MAIN.DAT as a result of editing the menus. There may be a total of 5 backups each in numeric order with the highest numbered one being the oldest one. These files may not all exist at any given time.
ATTRIB.DAT	System attributes. Maps attribute letters to names.
LOG.DAT	User activity log. All user activity regarding selections made from menus and the time spent are recorded in this file.
LICENSE.DAT	Connection License Information- Unique to your site
CHECK.DAT	May not be present in your system. Used to manage encrypted courseware or temporary licenses.

	This file should never be restored to an earlier date or to its original state, moved, edited in any way . This file should not be included in the system backup.
DELSNLOG.DAT	Record of users deleted from lesson trackers and placed in the ..\DELETED directory.
COURSES\ CLASS\ CLASS\1.DAT CLASS\2.DAT ... CLASS\1023.DAT	Location to store course authorization files provided by courseware vendors. Directory of information about classes. Each class created gets a file numbered from 1 to 1023. There may be any number of files in this directory. Files in the CLASS directory should not be modified or removed as they have linkages to the USERS.DAT file, and assignments.
ASSIGN\ ASSIGN\S2.DAT ASSIGN\C5.DAT	Directory of assignments. Assignment for Student number 2 Assignment for Class number 5 There may be as many files as there are assignments in this directory.
TMP\ TMP\S00001.DAT TMP\S03423.DAT	Directory contains temporary files. This directory does not have to be backed up Temp file for user number 1 Temp file for user number 3423 There may be any number of files in this directory.
GLOBAL\ GLOBAL\KBD001.DAT GLOBAL\KBD002.DAT	Directory contains default system keyboards for planner. Default keyboard 1 Default keyboard 2
images/ images/V001.DAT	Directory of background images used for the menu Images are stored in CAN-8 lesson format.

Lesson Directories

Unless specified by the MASTER when creating menus, the lesson directories are created by default in the **SVI** directory. Each lesson gets its own directory (including Babilon) and the following files are then created by either course authors or students using the lesson.

File or Directory name	Function
PLAN.DAT	The lesson plan, created by the planner.
LOG.DAT	Lesson user log, created by the planner, appended by the tracker and users.
V001.DAT	Recorded lesson item from planner. Each Vxxx.DAT file contains the contents of one lesson item from the planner. These files do NOT map to the numbers of the planner cells. The files may be numbered from V001.DAT to V255.DAT.
KBD001.DAT	Planner defined keyboard map.
PLAN.001	Backup PLAN.DAT file. Created when planner is edited.
USERS\	Directory for users responses.
USERS\S02345\	Directory containing responses for user number 2345. Each user that makes responses in the lesson gets a directory created. There may be any number of these directories.
USERS\S02345\R001.DAT	Response file number 1 for student 2345. There may be any number of response files.
USERS\S02345\I001.DAT	Instruction (message) file number 1 for student 2345. There may be any number of instruction files.
USERS\S02345\FILL.DAT	File containing information about fill in the blank questions. This file may be 0 byte in length.

Deleted Directory

The deleted directory contains a series of subdirectories that contain responses that were recorded for students that have been deleted from the tracker screens or from the system in general.

These files may be backed up for archival purposes if desired.

To free up disk space on the server, these files may be deleted at any time. The server does not have to be stopped to delete these files.

If tracker data is deleted by accident, user data may be recovered if the corresponding files are still present in the DELETED folder. The Deleted Data Recovery process requires a utility provided upon request by Sounds Virtual.

ACCESS CONTROL FOR USERS OF CAN-8 SERVERS

To provide control over where licensed connections to CAN-8 servers originate from, an access control system has been implemented.

The access controls allow the server administrator to allocate a specific **number of licenses** to a **range** of IP addresses. In this way, the server administrator may reserve a number of licenses for use in a classroom thus preventing others from outside the classroom from using them.

SETTING-UP THE ACCESS CONTROL

To setup the access controls, the server administrator must create a text file called **ACCESS.CFG** in the **SVSYS\ID** directory on the server. The contents of this file are as follows.

- The first line defines the number of licensed connections the server may support. This number must match exactly with the number of licenses that have been purchased from Sounds Virtual. If this number does not agree, the server will either allocate licenses that will not connect, or never connect licenses that do exist. The form of this line is below:

```
license 40
```

- In this case the server was licensed for 40 connections. There is one space between the word **license** and the number.
- The remaining lines all take the same form. There may be up to 200 such lines in the file.

The form is as follows:

[starting IP address][*whitespace*][ending IP address][*whitespace*][number]

The fields are as follows:

Field	Description
<i>whitespace</i>	One or more space characters
starting IP address	First IP address (inclusive) of the range
ending IP address	Last IP address (inclusive) of the range
number	Number of licenses to allocate to the range

A typical line would look like this:

10.0.0.1 10.0.0.250 10

The above line allocates 10 possible connections to the range of addresses starting at 10.0.0.1 and up to and including 10.0.0.250.

The access control list works on a "pool" basis. The starting pool is the number of licenses specified in the "license nn" line. Each allocation line reserves licenses from this pool. When all the allocation lines have been read, any remaining licenses may be used from any location.

Going back to our simple example file:

license 40
10.0.0.1 10.0.0.250 10

In this case, the server is capable of 40 licensed connections. Ten of those addresses are reserved for the range of IP address 10.0.0.1 to 10.0.0.250. You will note that there are a possible 250 IP addresses that may use up to 10 connections. This does not mean that only 10 users may sign on from those addresses, but that a **MINIMUM** of 10 users may **ALWAYS** sign on from those addresses. If users attempt to sign on from a reserved

range that has exceeded its allocation of addresses, then remaining licenses are allocated from the unreserved pool (in this case $40 - 10 = 30$ licenses). Thus, users are not prevented from signing on in the reserved range, only that a minimum are guaranteed to sign on.

Let's consider a more realistic and complex example:

```
license 35
10.0.0.1 10.0.0.250 10
10.0.1.0 10.0.1.250 10
172.16.32.1 172.16.32.250 10
```

In this case, three ranges are reserved, each having ten licenses allocated to them. So this means that a minimum of 10 users may sign on to the server from each of the ranges. The remaining number of licenses from the total is five. These five may be used from any IP address including addresses within the range of allocated addresses.

EXTENDED FORMAT

The extended form adds time and day restrictions so that the CAN-8 server may automatically create reservations depending on the day and during a defined time interval.

The form is as follows:

```
[first IP][WS][last IP][WS][# res][WS][day][WS][start time][WS][end time]
```

Where:

Field	Description
[WS]	- One or more space characters
[first IP]	- First IP address in range
[last IP]	- Last IP address in range
[# res]	- Number of licenses reserved for this range
[day]	- Day of week for this reservation where

	<ul style="list-style-type: none">• 0 = Sunday• 1 = Monday• 2 = Tuesday• ...etc.
[start time]	- Time (24 hr format) for this reservation to come into effect
[end time]	- Time (24 hr format) at which this reservation no longer applies

GENERAL NOTES

- The addresses must be specified with the lower numbered address first and the higher number second. If the order is reversed, the line will be ignored.
- Ranges may overlap with each other. In the case of the overlap, the first matching range has its allocated licenses assigned first, and then the next matching range in order as they appear in the file. When all overlapped ranges have their allocation exceeded, the remaining free pool will be used.
- Extended format: The start time must always be earlier (smaller) than the end time or the line will be considered containing an error. Therefore, any overnight reservation must be done in two lines as shown below:

```
10.0.0.10 10.0.0.50 10 0 1800 2400  
10.0.0.10 10.0.0.50 10 1 0001 0900
```

In the above example, 10 licenses are reserved for the specified IP range from Sunday 6PM to Monday 9AM

Lines with errors will be ignored by the server and a record of the error will be placed in the SERVER.LOG file at start up.

The file is only read once during server startup, so in order to have changes to the ACCESS.CFG file take effect, the NTSERVE program must be stopped and then re-started.

Client stations management

Generic Client installation

CAN-8 can be installed and run locally on the workstations, or installed and run from a network share.

The SVSETUP.EXE file delivered is meant for a generic installation of the CAN-8 32 bit client software. Default values are used and cannot be changed during the installation.

To create a pre-configured customized self-install file for your site, see the section [create a customized installation file](#).

Notes:

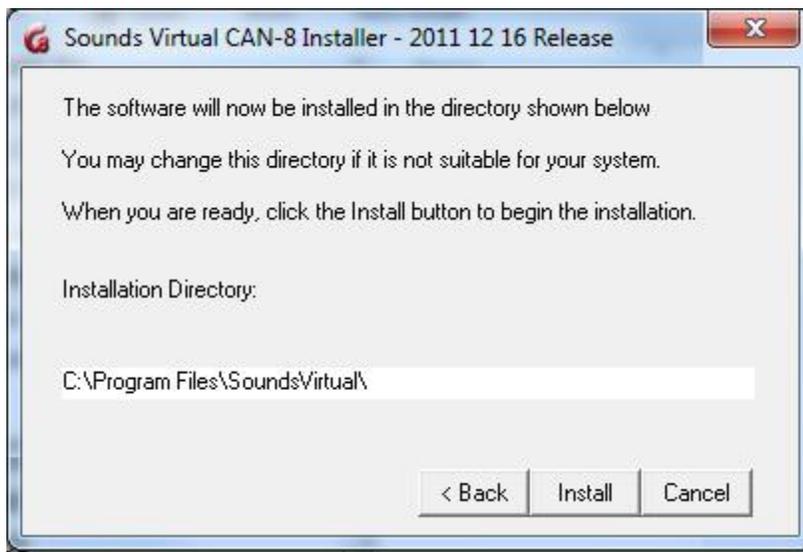
▶ Running the SVETUP.EXE file will uninstall all previous CAN-8 versions on that machine.

- Run the svsetup.exe provided to start the installation wizard.
- Once the License contract is read and accepted, click on the **Next** button.
-

Installation directory.

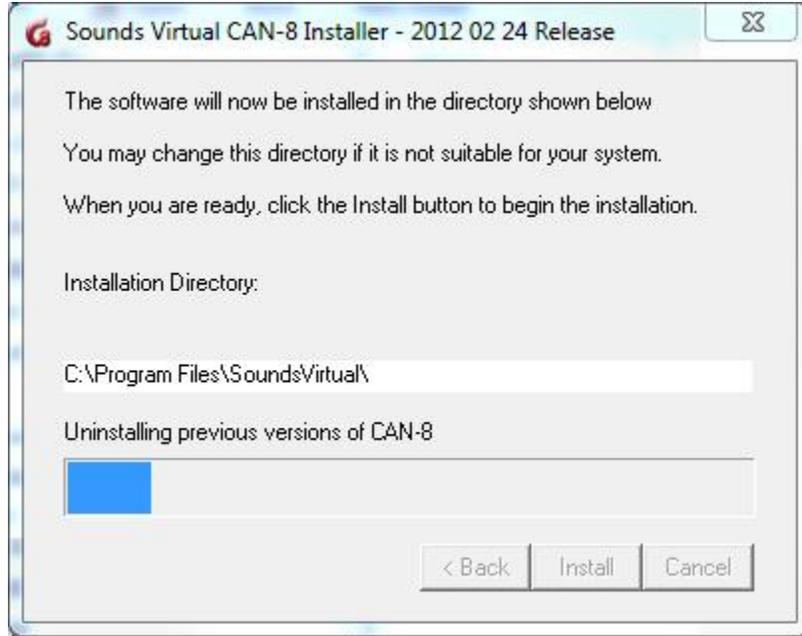
The default path is set to

C:\Program Files\SoundsVirtual\

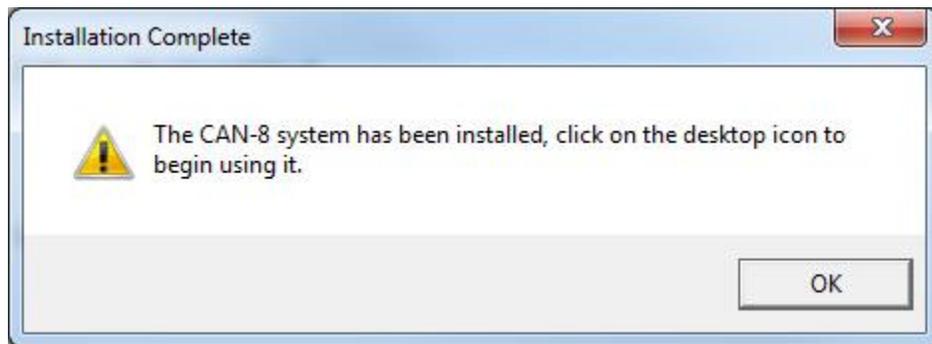


If you prefer to change the installation directory, change the path in this field, then select **Install**.

- The file then searches for previous CAN-8 32-bit client that may be present on the station:

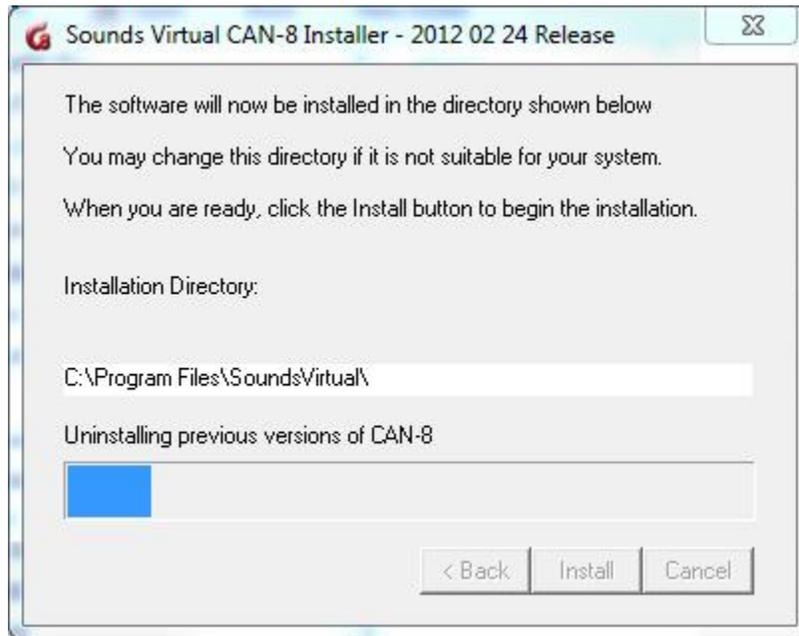


If none is found, or if the CAN-8 files found are less recent the version you are installing, they are uninstalled

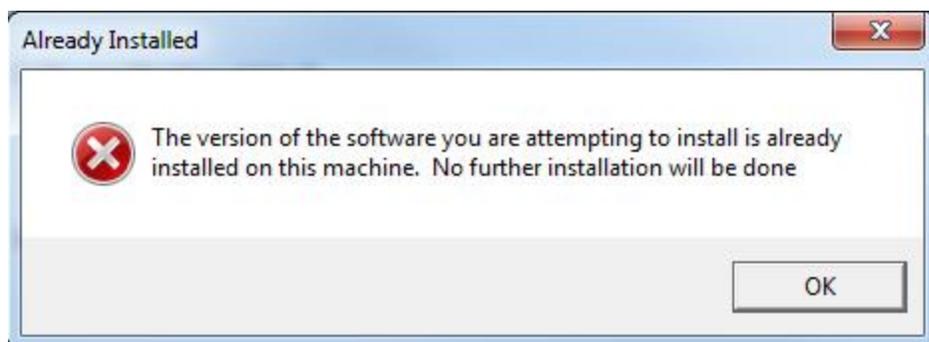


and the installation concludes.

- If the version you are attempted to install is identical to the version identified on your machine, this message shows, and the installation is terminated.



- If the version you are currently installing is less recent than the one identified on your machine, the installation is terminated with this message.



- The Reference Manual is installed in the same directory than the software. This is the default path to access it from the CAN-8 interface. If you need to place the manual in a shared folder, you must create a customized installation file.

Create a customized Installation file

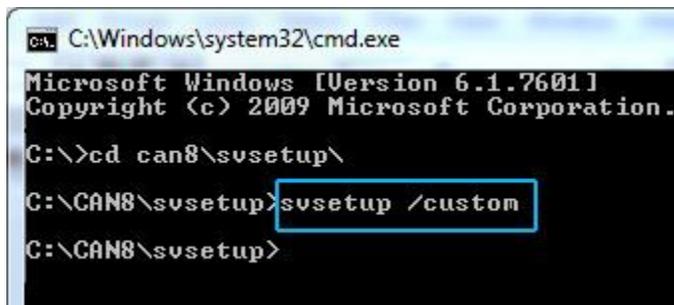
Your site may need to distribute the CAN-8 client to remote users, or may want to set the server information (locked or hidden), without having to edit the registry manually.

The same SVSETUP.EXE file can be run with the /CUSTOM parameter to create a new customized self-install file, which can then be distributed or installed locally.

- Open a command prompt (you cannot run the /custom parameter from the Windows interface)
- Change to the directory where the SVSETUP.EXE file is located

then type the following command:

svsetup /custom

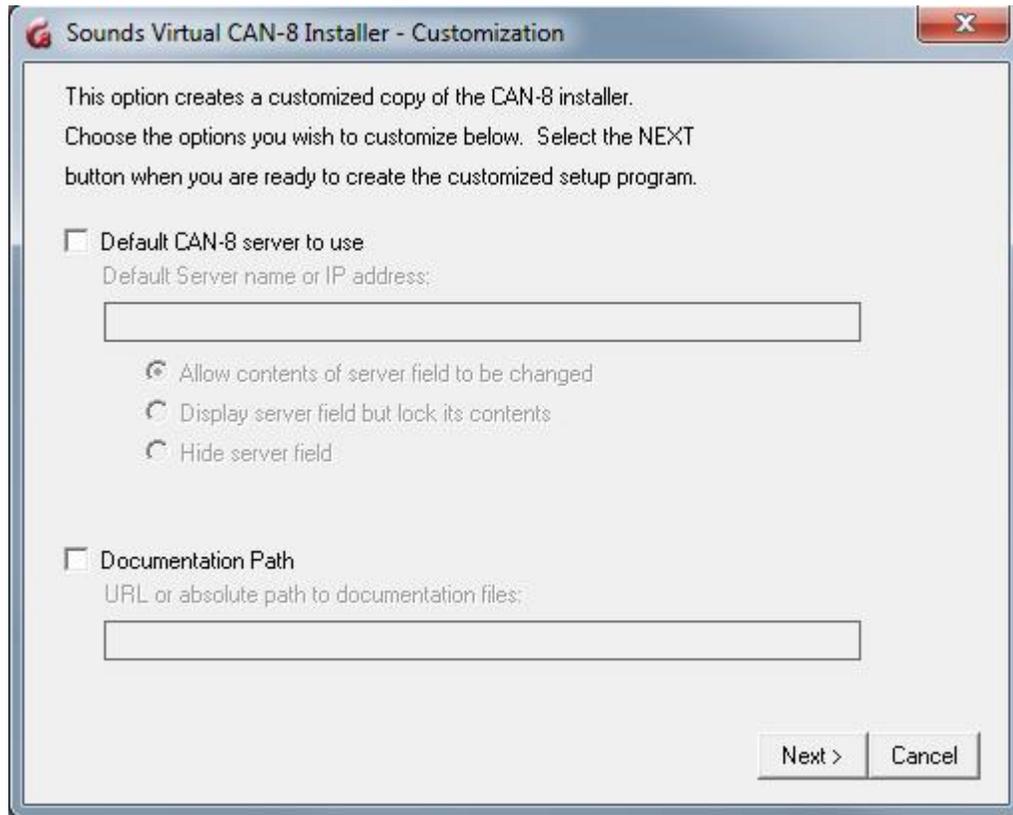


```
ca. C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.

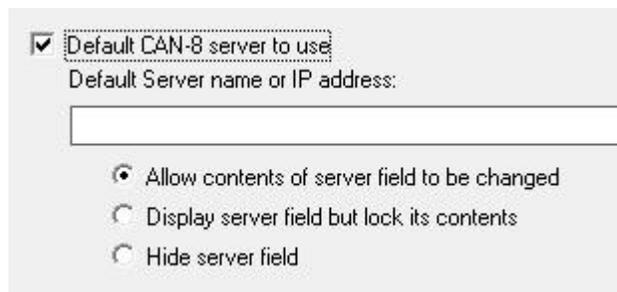
C:\>cd can8\svsetup\
C:\CAN8\svsetup>svsetup /custom
C:\CAN8\svsetup>
```

(space between svsetup and /custom)

- The customization console comes up.



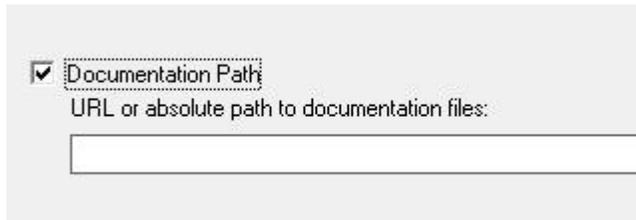
- To customize the **Server** field, select *Default CAN-8 server to use*, and type the DNS name or IP address of the CAN-8 server.



Next select on of the 3 options:

- **Allow contents of server field to be changed:** The server name or IP address will show by default when a user opens the login screen; the user can however change it.
- **Display server field but lock its contents:** The server name or IP address shows when the user opens the login screen; It is however greyed out and locked. The user cannot change it.

- **Hide server field:** The **Server** field is hidden from the login interface. The user cannot see nor change the server name.
- If you want to change the default path for the reference manual for a network share, select **Documentation path** and type the URL or absolute path to the documentation.

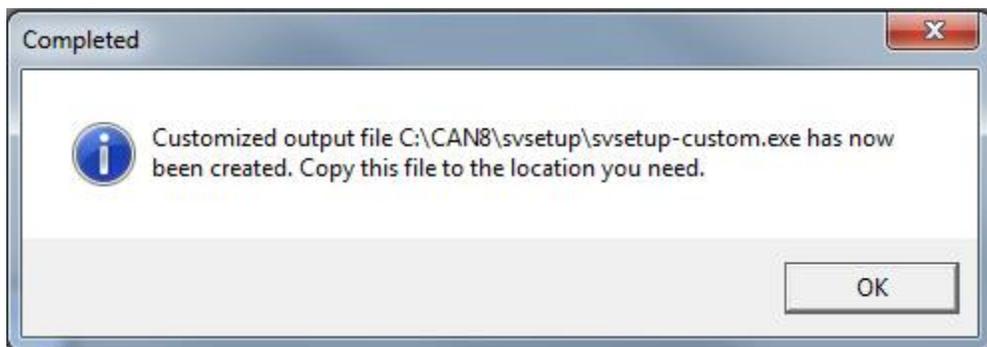


A screenshot of a software configuration window. It features a checkbox labeled 'Documentation Path' which is checked. Below the checkbox is a text input field with the placeholder text 'URL or absolute path to documentation files:'. The input field is currently empty.

NOTE:

- ▶ When customizing the svsetup, you only change the registry keys created during the installation from their default value to the one you specified.
- ▶ The *Document Docpath* value **does not change the installation path of the manual**. Instead, it creates a registry key that indicates to the CAN-8 client that the online manual should be accessed not from its default path but from the specified one. The manual is **always** installed in the same folder as the software.
- ▶ If you change the default documentation path, you will have to manually place a copy of the manual in the path you specified in the *Docpath Documentation* field.

- Click on the **Next** button.



- The customized self-install file is created in the same directory the SVSETUP.EXE was run from. It is named SVSETUP-CUSTOM.EXE.

Notes:

- ▶ You may need to create several customized self-install files (to distribute on your LAN

or remotely for example). Before creating a second Custom file, rename the first one or move it to a different directory to prevent it from being replaced by the newer one, then start the above procedure again.

▶ You CANNOT create a self-install file from a SVSETUP-CUSTOM.EXE. You must use the original SVSETUP.EXE provided.

▶ The SVSETUP-CUSTOM.EXE file cannot be edited. If the information included has changed, you must create a new /CUSTOM file.

Silent Installation of the client

To perform a silent install:

- Open a command prompt.
- Change to the directory where the SVSETUP.EXE file is located then type the following command:

```
svsetup /q  
or  
svsteup /quiet
```

- The icon will appear on the workstation's desktop.

Deploying CAN-8 VirtuaLab via Windows Group Policy Objects (GPO)

The installation / Upgrade of the system and of the needed registry keys can also be done via Microsoft Group Policy Objects

Although the steps required will be different for each site depending on what other GPO tasks have been established, the rough outline is as follows:

- On a test machine with the same existing pre-update configuration, run the CAN8 client installation program (as administrator) and isolate the newly created registry keys for use in the GPO.
- Create a GPO task to update the existing executable (SVMGR.EXE) with the newly installed one from the test machine.
- Add any additional tasks such as creating a desktop shortcut to point to the CAN-8 executable. The .ico file is available from our download page.

You may now deploy this to all users with the same GPO.

Notes:

During a local installation of an updated CAN-8 client, CAN-8 is required to be run once with administrative privileges to create the registry keys under HKEY_LOCAL_MACHINE instead of the HKEY_CURRENT_USER. Microsoft Group

Policy Objects however will let you update the needed registry entries at the same time than the software, thus preventing this step.

Uninstall CAN-8

To uninstall the client software

- Go to *Start > Control Panel*.
- **Add/Remove Program** or **Programs > Uninstall a program**
- In the software list, select CAN-8 and click on the **Remove** button or right click on CAN-8 and select **Uninstall/Change**.

This process will uninstall the software, the desktop icon and the registry keys created during the installation.

Registry Keys and Values

The first time the client is run on a workstation, a *registry key structure* that includes several subkeys is created.

These keys and subkeys dictate the behaviour of the system and should never be edited nor deleted, (unless advised by a Sounds Virtual technician) as doing so will result in software misbehaviour.

NOTE:

- Manual installation/update on each station.
 - ▶ When installing CAN-8 locally on each station, Windows group policy settings may prevent regular users from writing to the registry. Therefore it is necessary that the software be initially installed by a user with the appropriate rights on the machine for the Registry key structure to be created.
 - ▶ However, This is not sufficient. The software also has to be **run as administrator** at installation time. (right click on the icon, and then select **run as administrator**. This will create the appropriate key in **HKEY_LOCAL_MACHINE**.
 - ▶ If the software is run by someone with administrative rights but is not **run as administrator**, the Reg key will instead be

created in **HKEY_CURRENT_USER** and will therefore not be accessible to other users.

▶ The software will have to be run once with full **Write** privileges (administrator or other) on each workstation.

- Installation/update via an image:

▶ If the lab stations are being imaged, the software will have to be run once with full **Write** privileges on the original disk before the image is created. This will allow the reg key to be created before the image is pushed.

- Installation/update via a GPO:

▶ If the software is installed via a GPO, there is no need to run the software once with admin privileges.

The structure of the CAN-8 registry keys is as follows:

All

Windows

32 bit

Operating Systems : HKEY_LOCAL_MACHINE\Software\SoundsVirtual\VirtualLab\2.0\[date]\

ng

System

s :

All

Windows

64

bit HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SoundsVirtual\VirtualLab\2.0\[date]\

Operating Systems :

ng

System

s:



Where **[date]** is the version date of the client installed. A new [date] key is automatically created every time a more recent version is run.

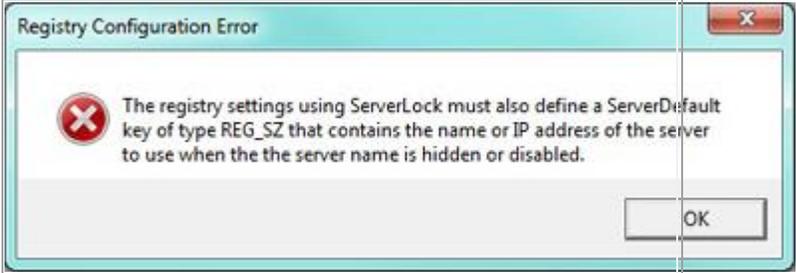
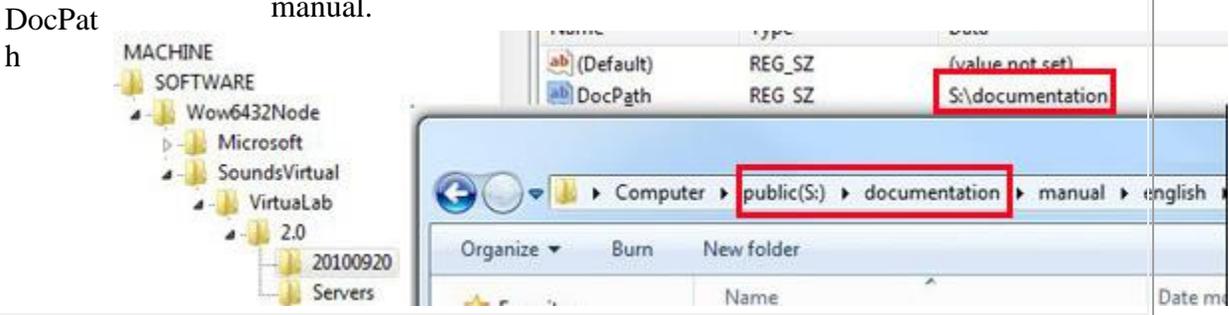
Several registry values can be added to this **[date]** key to modify the system's default behaviour.

These values should be entered in the folder with the most recent date. (or currently installed version). When a newer version is installed, the system will automatically copy the registry values from the previous version's [date] key. It will not copy any value from any other key than the LAST [date].

NOTE:

- ▶ **Extreme care should be taken when editing the System Registry**
- ▶ The values below are the same for 32 bit and 64 bit OS.

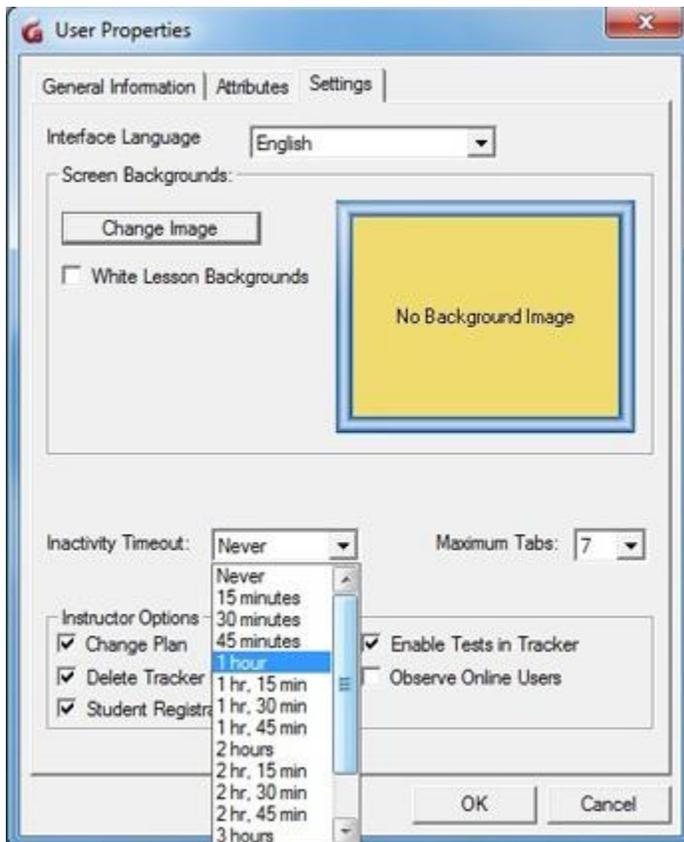
Value name	Value type	Value data	Description
KeepAlive	REG_DWORD	Number between 4 and 45	Represents the time interval in seconds in which the CAN-8 client sends Keepalive packets to the CAN-8 server to keep firewall ports opened. Firewalls settings can close the UDP ports if it detects inactivity on the UDP ports for a set number of seconds (i.e.: 30s), thus disconnecting the client station from the server. Setting this value to a lesser number than the firewall timeout settings will keep the ports open
ServerDefault	REG_SZ	Server's IP address or DNS name	Sets the default server name that will always appear in the server field of the login screen when the CAN-8 program is started. If this value is not set, the server field will by default show the name or IP of the last server accessed . This value still allows the user to change the server's info in the login screen.
ServerLock	REG_DWORD	0, 1 or 2	NOTE: The ServerDefault Value must be created before this value otherwise the following message will appear when signing on:

			 <p>The registry settings using ServerLock must also define a ServerDefault key of type REG_SZ that contains the name or IP address of the server to use when the the server name is hidden or disabled.</p>
			<ul style="list-style-type: none"> • 0: The server name is not locked. Users can change the server IP address or DNS name in the server field of the login screen. • 1: The Server name is visible but locked (greyed out). The information in the server field cannot be changed. • 2: The Server name is locked and the server field is hidden in the login screen.
Admin	REG_DWORD	1	allows the use of ADMIN in place of MASTER to login.
DocPath	REG_SZ	Directory path (UNC or normal) to location of the online manual.	<p>Default is to look in the directory svmgr.exe was run from. If the manual is not in its default path, this value must be set to point to its new location.</p>  <p>The screenshot shows the registry value for DocPath set to S:\documentation and a file explorer window showing the path Computer > public(S:) > documentation > manual > english.</p>
MediaPlayer	REG_SZ	File path of executable to use as the media player.	If not set, the system default media player is used to render any media files accessed by the CAN-8 menu.
Browser	REG_SZ	File path	If not set, the system default browser is used.

		of executab le to use as the browser.	
--	--	---------------------------------------------------	--

Client Inactivity Timeout

To help manage the licenses used and avoid wasting some in workstations left unattended, an Inactivity Timeout period can be set in the user profile. This will automatically free the license after a period ranging from 15 mn to 3hours and 45 mn:



Licenses liberated via Inactivity Timeout are placed back in the license pool they belong to.

Sounds Virtual Inc
920 Yonge Street , suite 801
M4W 3C7 Toronto
www.can8.com

[Back to top of page](#)