CVS Client Setup Guide

Brad Touesnard

Table of Contents

Table of Figures

1.0 Introduction

The Concurrrent Versioning System (CVS) has become an integral tool in the development of many software applications. Although CVS clients are often setup on Unix and used as a command line application, there are several popular Windows GUI applications in use as well. This document details how to setup the CVS client known as WinCVS (http://www.wincvs.org) with SSH access to the CVS server.

2.0 Requirements

2.1 Client-Side Requirements

Table 2.1 lists the software packages required to successfully install WinCVS. If you do not have the packages installed, you should install them now.

Package	Download
OpenSSH (client only)	http://lexa.mckenna.edu/sshwindows/download/releases/
WinSCP	http://winscp.sourceforge.net/eng/download.php
Python	http://www.python.org/download/
WinCVS	http://www.wincvs.org/download.html#WINCVS

Figure 2.1: Required Software Packages

2.2 Server-Side Requirements

On the server, you must have a valid user setup with SSH access in order to access CVS via SSH. Please refer to the *CVS Server Setup Guide* for further details.

3.0 Configuring OpenSSH

3.1 Connecting to the Server via SSH

The OpenSSH for Windows client allows you to run SSH as a command line utility in Windows much like the utility bundled with Linux. To test it, do the following:

1. In Windows, click "Start" then "Run…"
2. Type "cmd" and click "Ok"
3. At the command prompt type "ssh <username>@<hostname>"

You should see something similar to the following:

```
The authenticity of host '<hostname>' can't be established.
RSA key fingerprint is ...
Are you sure you want to continue connecting (yes/no)?
```

4. Type "yes" after this prompt. You should see a warning message and a password prompt like the following:

```
Warning: Permanently added '<hostname>' (RSA) to the list of
known hosts.
<username>@<hostname>'s password:
```

5. Enter your SSH password. You should now be logged into the server via SSH.

3.2 Setting-Up Public-Key Authentication

Since every action on the CVS server will require authentication, we will use public key authentication to give us the convenience of not having to enter a password while maintaining security in the authentication and data exchange process.

3.2.1 Generating and Installing Keys

While still logged-in to the server via SSH, generate public and private SSH keys for your user:

```
$ ssh-keygen -t rsa -b 1024
```

The program will respond with some information and ask for which file to save the key. Simply press 'Enter' for the default.

```
Generating public/private rsa key pair.
Enter file in which to save the key (~/.ssh/id_rsa):
```

It will then ask for your passphrase, but since we want CVS to operate seamlessly through SSH, press the 'Enter' key twice to use no passphrase.

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:

Your identification has been saved in ~/.ssh/id_rsa.
Your public key has been saved in ~/.ssh/id_rsa.pub.
The key fingerprint is:
... <username>@<hostname>
```

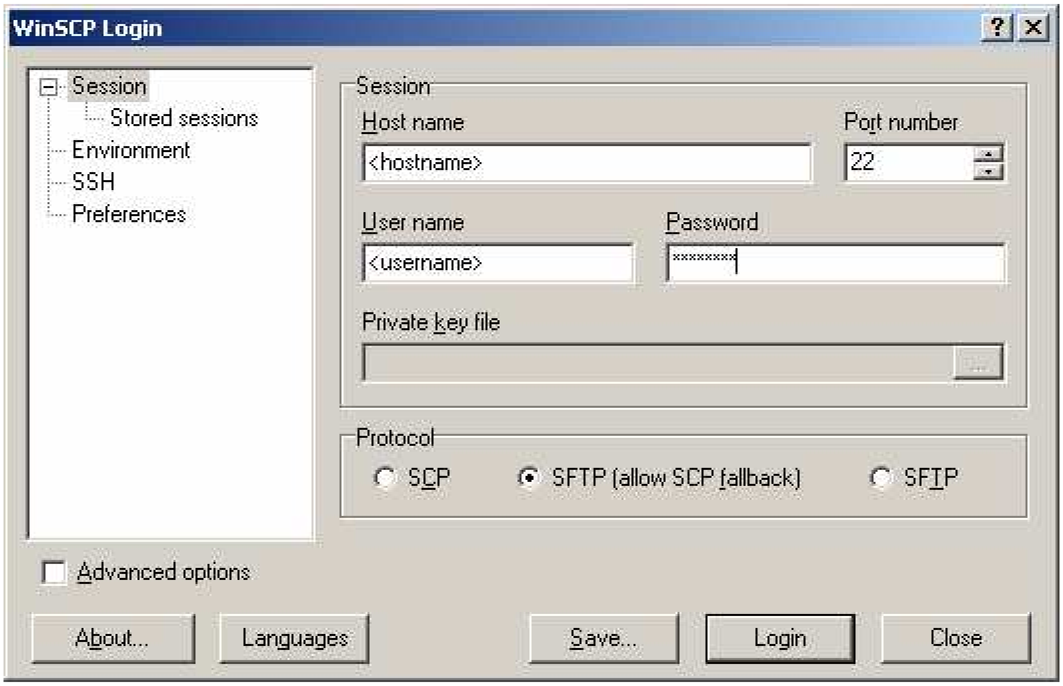
You should notice a new directory in your /home/username directory called ".ssh" and some files within it. The file "id_rsa" is the private key and the file "id_rsa.pub" is the public key. The public key is used on the server and the private key is used on the client. The next step is to install the keys on both the client and server.

Installing the public key on the server is easy:

```
$ cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
$ chmod 400 ~/.ssh/authorized_keys
```

Now to install the private key, you must copy it to your client machine. The best way to do this is by using an SCP client program to connect to the server via SSH and transfer the file. It is recommended to use WinSCP mentioned in Section 2.1 of this document.

To login with WinSCP, simply enter the same login credentials as you used to login with SSH. That is, the <hostname>, <username> and password for which you were prompted (Figure 3.1). The remaining options should be fine. Click the "Login" button.



Session

Host name: <hostname>

Port number: 22

User name: <username>

Password: ********

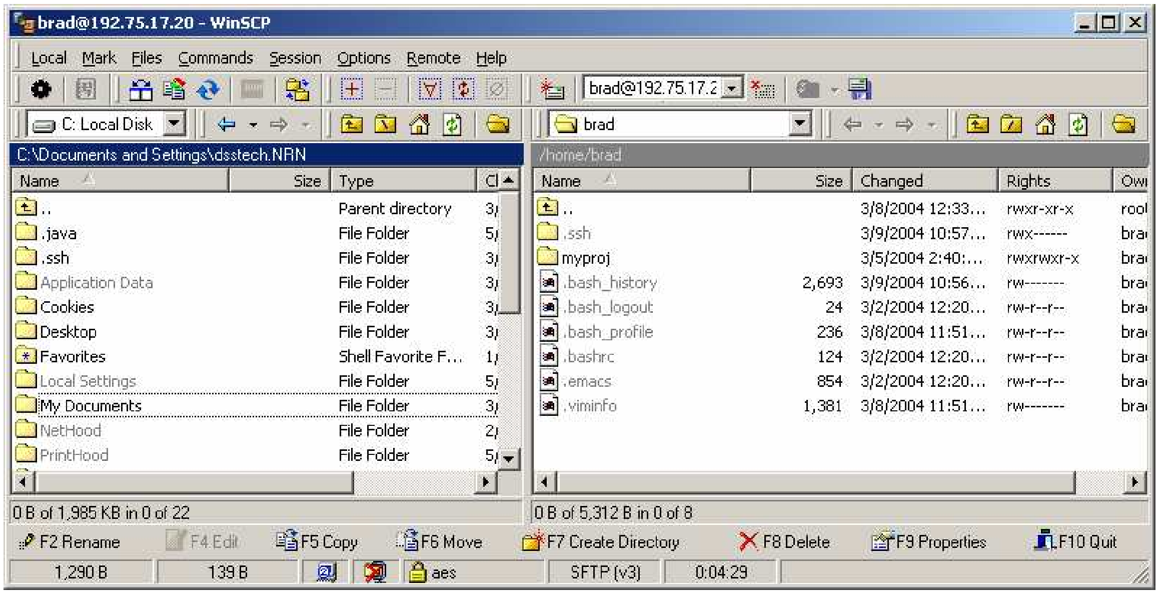
Private key file:

Protocol: ○ SCP ● SFTP (allow SCP fallback) ○ SFTP

□ Advanced options

Figure 3.1: WinSCP Login Information Screen

Once you are connected with WinSCP, you should see a display much like an FTP program (Figure 3.2). The right pane contains a list of the files in your home directory on the server and the left pane contains a local folder on your machine.



C:\Documents and Settings\dsstech.NRN

Name	Size	Type	C
..		Parent directory	3/
.java		File Folder	5/
.ssh		File Folder	3/
Application Data		File Folder	3/
Cookies		File Folder	3/
Desktop		File Folder	3/
Favorites		Shell Favorite F...	1/
Local Settings		File Folder	5/
My Documents		File Folder	3/
NetHood		File Folder	2/
PrintHood		File Folder	5/

0 B of 1,985 KB in 0 of 22

/home/brad

Name	Size	Changed	Rights	Ow
..		3/8/2004 12:33...	rwxr-xr-x	roo
.ssh		3/9/2004 10:57...	rwx------	bra
myproj		3/5/2004 2:40:...	rwxrwxr-x	bra
.bash_history	2,693	3/9/2004 10:56...	rw-------	bra
.bash_logout	24	3/2/2004 12:20...	rw-r--r--	bra
.bash_profile	236	3/8/2004 11:51...	rw-r--r--	bra
.bashrc	124	3/2/2004 12:20...	rw-r--r--	bra
.emacs	854	3/2/2004 12:20...	rw-r--r--	bra
.viminfo	1,381	3/8/2004 11:51...	rw-------	bra

0 B of 5,312 B in 0 of 8

1,290 B | 139 B | aes | SFTP (v3) | 0:04:29

Figure 3.2: WinSCP Main Screen

Now you must open the ".ssh" directory in the right pane (server) and copy the "id_rsa" file to the ".ssh" directory in your home directory on your machine. The home directory differs between versions of Windows:

For Windows 2000:

```
C:\Documents and Settings\<username>
```

For Windows NT 4.0

```
C:\WINNT\Profiles\<username>
```

For Windows 9x

```
C:\WINDOWS\Profiles\<username>
```

So in WinSCP on Windows 2000, you would change the directory in the left pane to "C:\Documents and Settings\<username>\.ssh" (creating the ".ssh" directory if it doesn't exist), then drag the "id_rsa" file from the right pane and drop it in the left pane.

3.2.2 Connecting with Private-Key Authentication

Now we can test to see if the Private and Public Keys are setup properly by establishing a new SSH connection.

1. In Windows, click "Start" then "Run…"
2. Type "cmd" and click "Ok"
3. At the command prompt, type "ssh <username>@<hostname>"

If you are not prompted for your password, then the authentication is working properly. You can now remove the "~/.ssh/id_rsa" file from the server to ensure no one else can use it to login to your account. Do not remove the "id_rsa" file from your local machine.

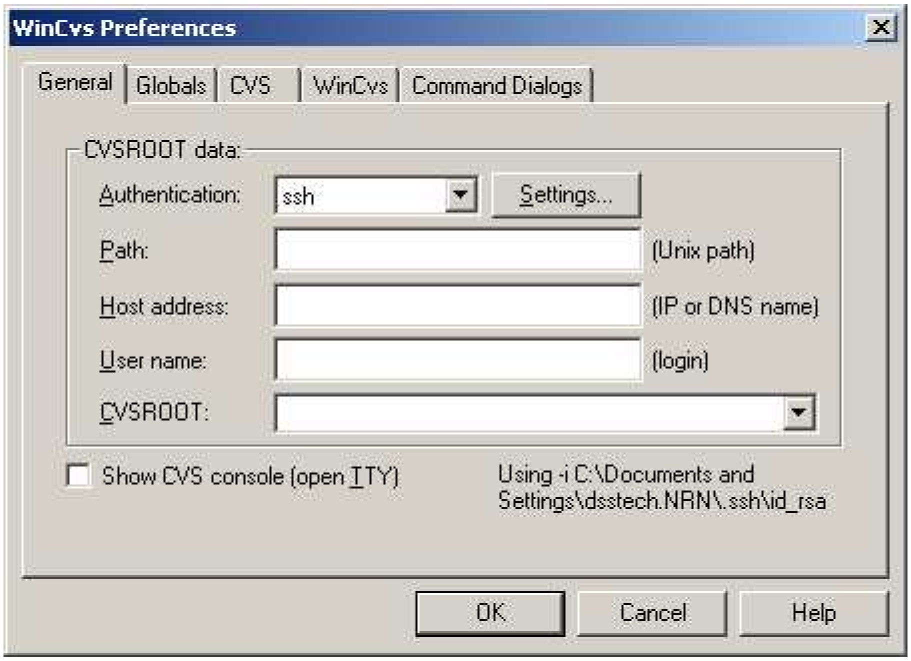
If you are prompted for your password, you should review the process to ensure you didn't miss anything or try again from the beginning. To ensure that your "id_rsa" file is being located by OpenSSH, run the ssh command with the path to the "id_rsa" file explicitly defined:

```
ssh –i C:\<home_dir>\.ssh\<private-key file> <username>@<hostname>
```

4.0 Configuring WinCVS

Now we must configure our WinCVS client to connect to the CVS server via SSH.

1. In Windows, start WinCVS from the "Start" menu or Desktop
2. Click "Admin" -> "Preferences" from the menu



Authentication: ssh

Path:

Host address:

User name:

CVSROOT:

☐ Show CVS console (open TTY)

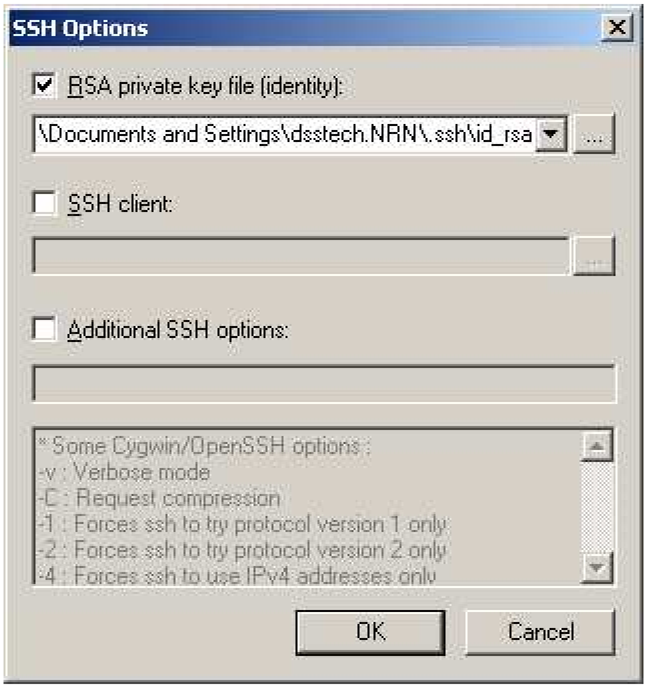
Using -i C:\Documents and Settings\dsstech.NRN\.ssh\id_rsa

Figure 4.1: WinCVS Preferences Dialog

3. Fill out the form (Figure 4.1) with the following values:

Authentication:	ssh
Path:	*Path to the CVS repository root* *(e.g. /home/cvs/cvsroot)*
Host address:	*Address of the CVS server* *(Same as <hostname>* used when setting up SSH*)*
User name:	SSH username to access the server (Same as <username> used when setting up SSH)

4. Click the "Settings…" button. A dialog will appear (Figure 4.2).
5. Select the "RSA private key file (identity)" checkbox
6. In the textbox, enter the path to you're the "id_rsa" file you copied from the server with WinSCP in the section Generating and Installing Keys.
7. Click "Ok".
8. Click the "Globals" tab
9. Adjust settings as shown in Figure 4.3
10. Click the "CVS" tab (Figure 4.4)
11. Enter the home directory of your local machine. You used this in the section Generating and Installing Keys.
12. Click "Ok"



☑ RSA private key file (identity):

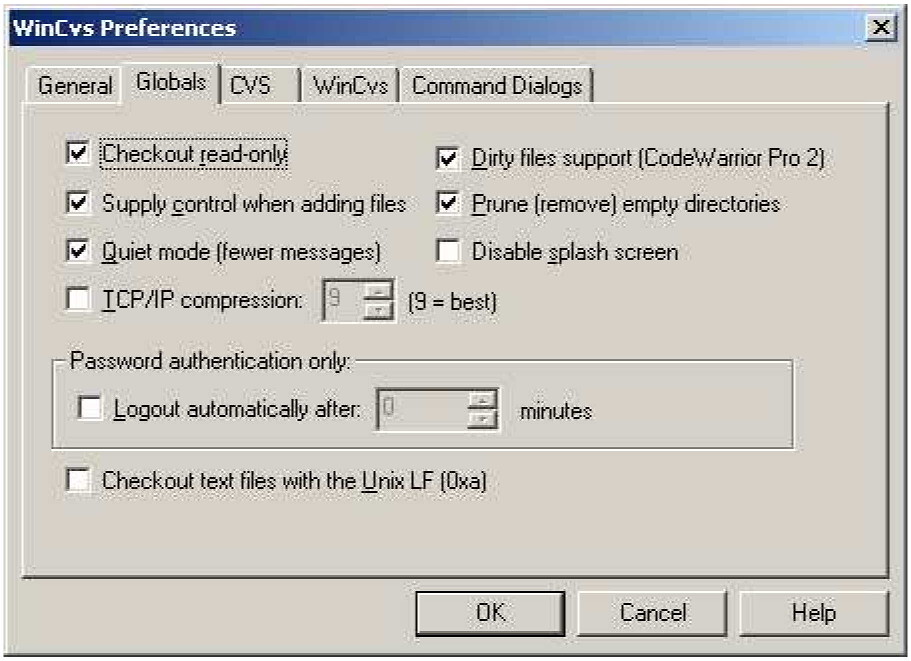
\Documents and Settings\dsstech.NRN\.ssh\id_rsa

☐ SSH client:

☐ Additional SSH options:

```
* Some Cygwin/OpenSSH options :
-v : Verbose mode
-C : Request compression
-1 : Forces ssh to try protocol version 1 only
-2 : Forces ssh to try protocol version 2 only
-4 : Forces ssh to use IPv4 addresses only
```

Figure 4.2: WinCVS SSH Options Dialog



☑ Checkout read-only

☑ Dirty files support (CodeWarrior Pro 2)

☑ Supply control when adding files

☑ Prune (remove) empty directories

☑ Quiet mode (fewer messages)

☐ Disable splash screen

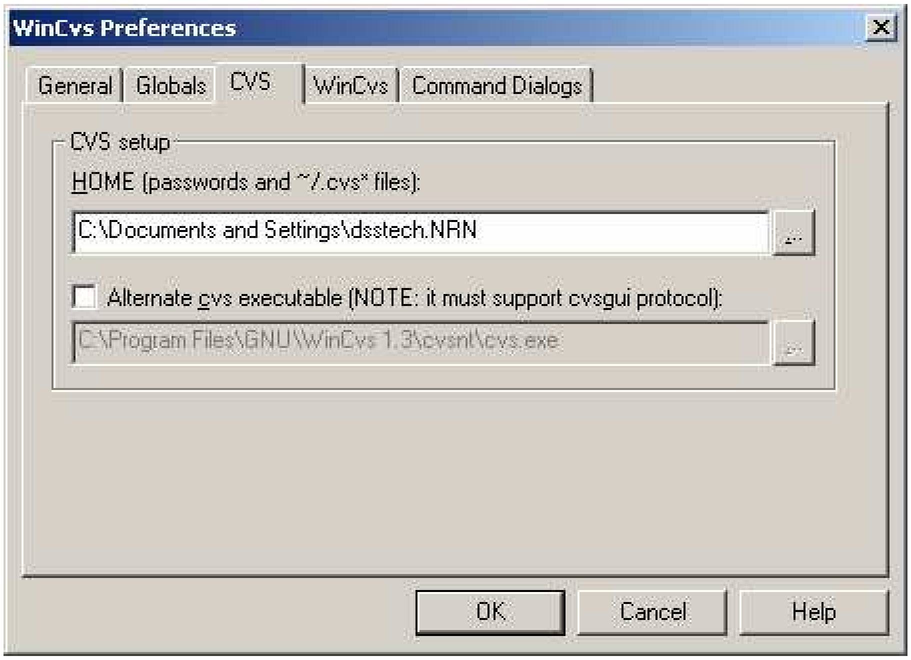
☐ TCP/IP compression: 9 (9 = best)

Password authentication only:

☐ Logout automatically after: 0 minutes

☐ Checkout text files with the Unix LF (0xa)

Figure 4.3: WinCVS Globals Preferences Dialog



WinCvs Preferences

CVS setup

HOME (passwords and ~/.cvs* files):

C:\Documents and Settings\dsstech.NRN

☐ Alternate cvs executable (NOTE: it must support cvsgui protocol):

C:\Program Files\GNU\WinCvs 1.3\cvsnt\cvs.exe

Figure 4.4: WinCVS CVS Preferences Dialog

Now WinCVS should be ready to go!

Sources

Reagan, Patrick. “A Practical Guide to WinCVS and SSH”. http://www.wincvs.org/ssh.html. [Accessed 2004-03-09]