

Sonnadara Lab Guide to Computer Facilities

November 2010

Contents

Basic Concepts	2
Prerequisites:	2
Limitations and Security:	2
Connection Instructions:.....	3
Modes of Operation.....	5
Mode 1:.....	5
Mode 2: Network Connect.....	7
Troubleshooting.....	9
Problem #1:.....	9
Solution #1:	9
Problem #2:.....	9
Solution #2:	9
Problem #3:.....	9
Solution #3:	9
Problem #4:.....	9
Solution #4:	9
Managing Data.....	10
Servers	11
Labdata5 Server	11
PMS-Lab Server	11
Dropbox	11
Remote Desktop Access.....	12
Data protection and Confidentiality	13
Support	13

Basic Concepts

A Virtual Private Network, or VPN is the term used to refer to any device that is capable of creating a semi-permanent encrypted tunnel over the public network *between two private machines or networks* to pass non-protocol specific, or arbitrary, traffic. One of the key elements of VPNs is encryption. To protect sensitive or non-routable data as it passes over the public Internet, we need to create a virtual private tunnel. This tunnel is built by encrypting the packets or frames of data and then encapsulating these in regular IP traffic between the two hosts or networks. At the end of this tunnel, the encapsulated encrypted data is decrypted and disassembled and sent on its merry way to the proper destination.

Typically, this requires the installation of specialized client software that routes network data to/from the remote site and the internal network. With SSL VPN, we are not dependent on specialized client software, but instead piggyback on top of an internet browser like Microsoft Internet Explorer/Netscape/Firefox and link with Java to implement the coding.

Prerequisites:

- Connection to the internet
- Windows 98,2000,XP, Vista, Windows 7, Mac OS X
- **Java** (get it from www.java.com)
- Administrator level access to the computer you are using to connect with (*only need this for the first time, subsequent connections do not need admin access*)

Untested operating systems, should work, but you'll have to fiddle with it on your own:

Linux, Palm Pilot, Windows CE, Windows Mobile, Mac OS 9

Limitations and Security:

While connecting via SSL VPN, you only have access to the lab servers and certain core services. This is needed in order to protect the hospital IT systems in case your computer has a virus or someone has stolen your password. If you find that you can't access a resource that you need, please talk to your supervisor.

On the subject of viruses, please make sure your computer has the most updated antivirus software installed. The IT folks are not concerned with viruses as much as "keystroke" recording software that records passwords and personal information as they're typed in. Antivirus software should catch most keystroke recording software out there.

Generally, try to avoid using internet cafes and public internet kiosks if you can, when using SSL VPN. The risk is that you never know if someone has installed a virus or recording software on those computers. That said, it's sometimes unavoidable, so when you do, please remember to close the browser window and log off the computer when you are done. This will prevent someone from getting into your files after

you've left the café. If you have accessed the network from an unsecure location, it is good practice to change your password as soon as possible once you get back to a more trusted environment.

Connection Instructions:

On the address bar of your internet browser, type in:

https://svpn.mshri.on.ca

You will then get a message looking like this:



Just click on **Yes**.

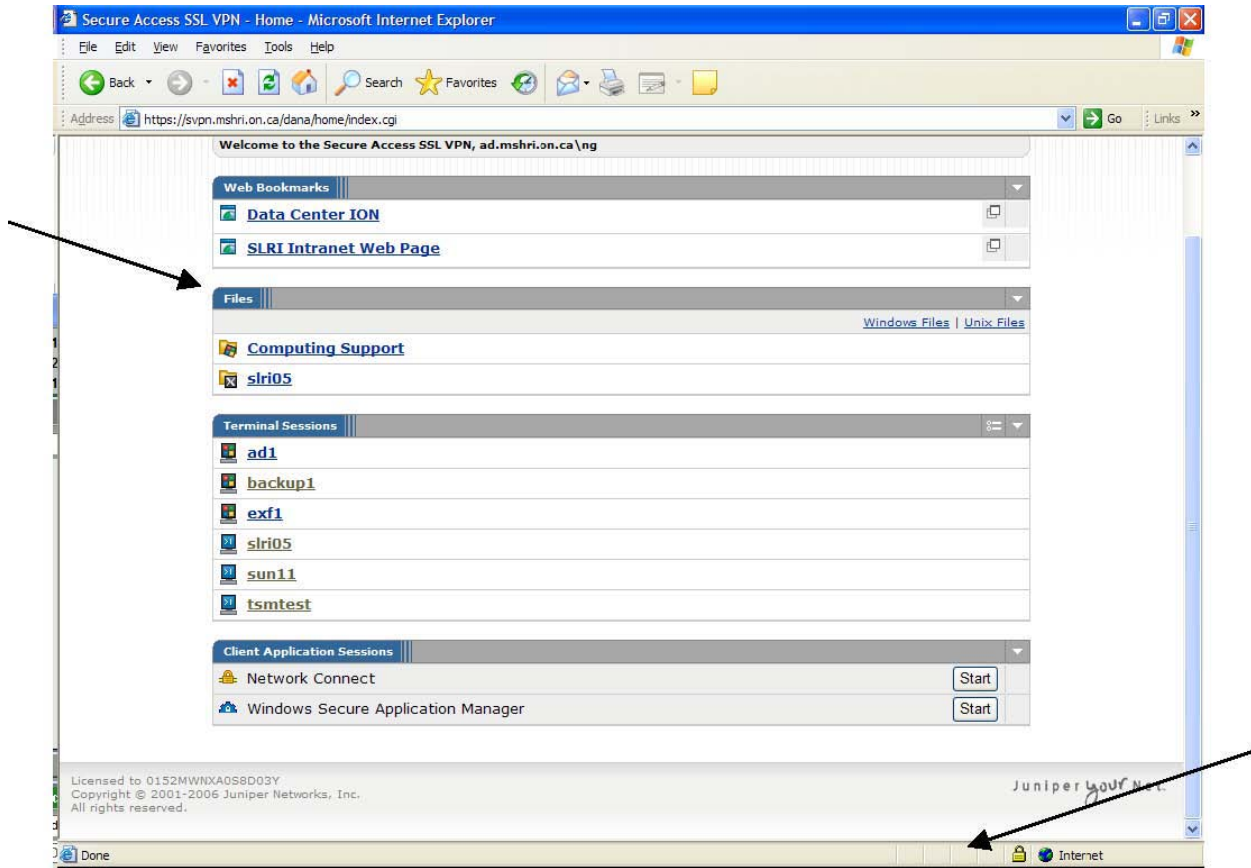
Next, the log on screen comes up, just type in your username. If you do not know your username, talk to your supervisor!

Then select the Sonnadara Lab realm and click on "Sign In".



You will now be presented with a basic menu that looks similar to the screenshot below.

Modes of Operation



There are 2 basic modes of operation:

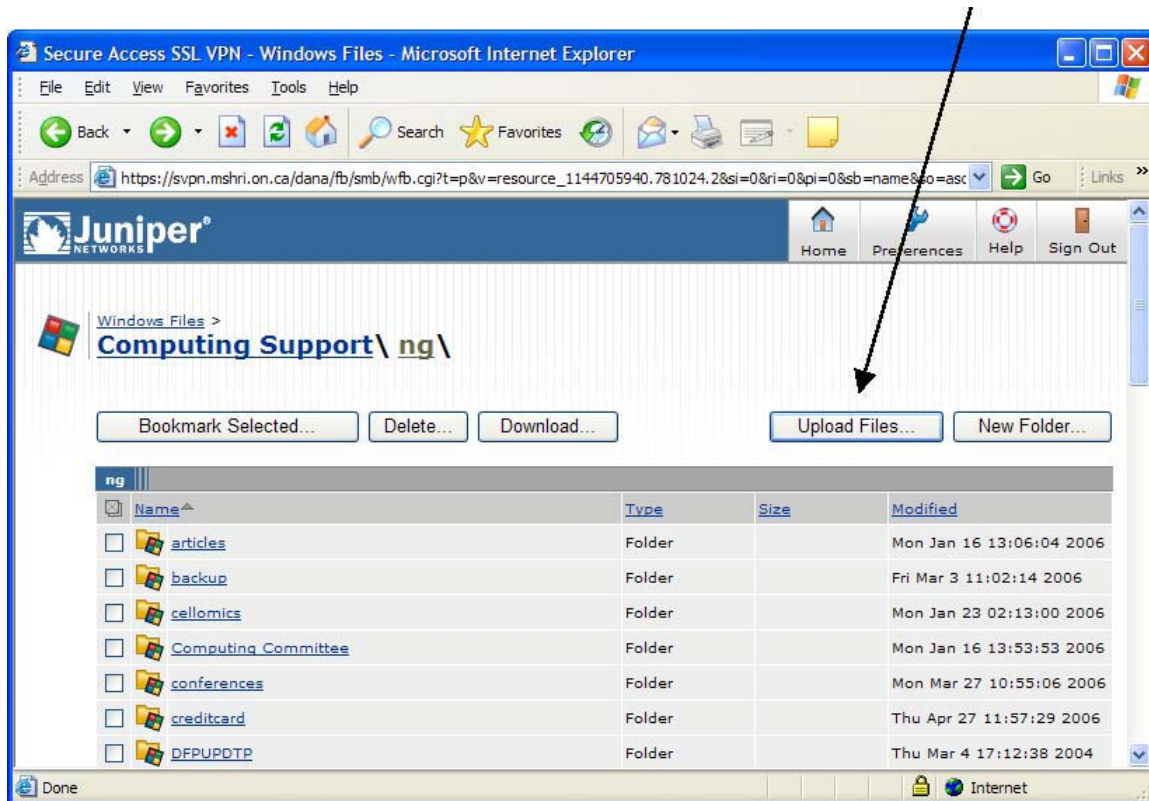
- 1 – Basic Web Browser menu mode
- 2 – Network Connect

Mode 1: If all you want to do is to retrieve a file from your network share, #1 is what you'll be using. The items just below the menu heading "Files" are links to your lab share folder. In the above picture, it's "Computing Support", but your screen will show "Labdata5" or something similar. Click onto the lab share folder and just click on the file you want, this will prompt you to save the file onto your local computer's hard drive.

***** WARNING WARNING WARNING!!!! ***** **When you click on save, YOU ARE NOT SAVING THE FILE BACK ONTO THE SERVER! You are in fact actually saving it onto the computer you are using.** For example, if you are sitting at an internet café and you download the PowerPoint file you needed, work on it for several hours and then click on save, you are saving the file onto the internet café's computer. When you go back to work, you'll realize that all the work you did at the café is not there and you've just wasted your money drinking all that overpriced coffee. What you must do is to

save the file, then UPLOAD it back into your folder. Please note the picture below. Click on the upload files and just follow the menu items.

We highly recommend that you do not overwrite your original files, and that instead you name your files incrementally, i.e. thesis1a.doc thesis1b.doc , etc etc. This will also let you visually verify that the new file has been successfully uploaded. Also remember **WHERE** you saved this file on the computer you are using. Do not just blindly click on “save”, make sure you specify which folder you are putting it in.



Also, be extremely careful what files you are downloading and where you are saving them. If they are confidential files, it is your responsibility to make sure they are deleted off of any place that may expose them to unauthorized access, i.e. an internet café. If you are unsure of how to do this, then do not use SSL VPN to access files in an unsecured place.

Mode 2: Network Connect: The #2 method of connecting – “Network Connect” – is the most flexible mode of connection. When connected, you will be able to access printers and also connect directly to your lab share. Conceptually, it will appear as if you are physically connected to our network. However, this mode requires that you have Administrator level access for the first time, in order to install the java modules that will handle the translations.

The first time you click on “Network Connect”, it will download and install a small java VPN module on your computer. You may need to click through some warning boxes that pop-up (like picture below). It is safe to agree to continue. The next time you use the SSL VPN from the same computer, the process will go much quicker since you won’t have to install anything and you won’t need to be at the Administrator level.

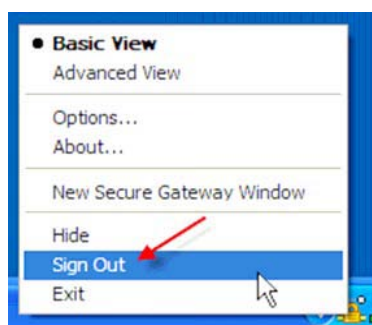


You should also see the following icon on the system tray in the lower right hand side of your screen. We refer to this as the “little alien” icon, since it looks like a little alien even though it is supposed to be a lock icon over a network cable. The two dots above the lock will blink when there is network traffic going over the SSL VPN.

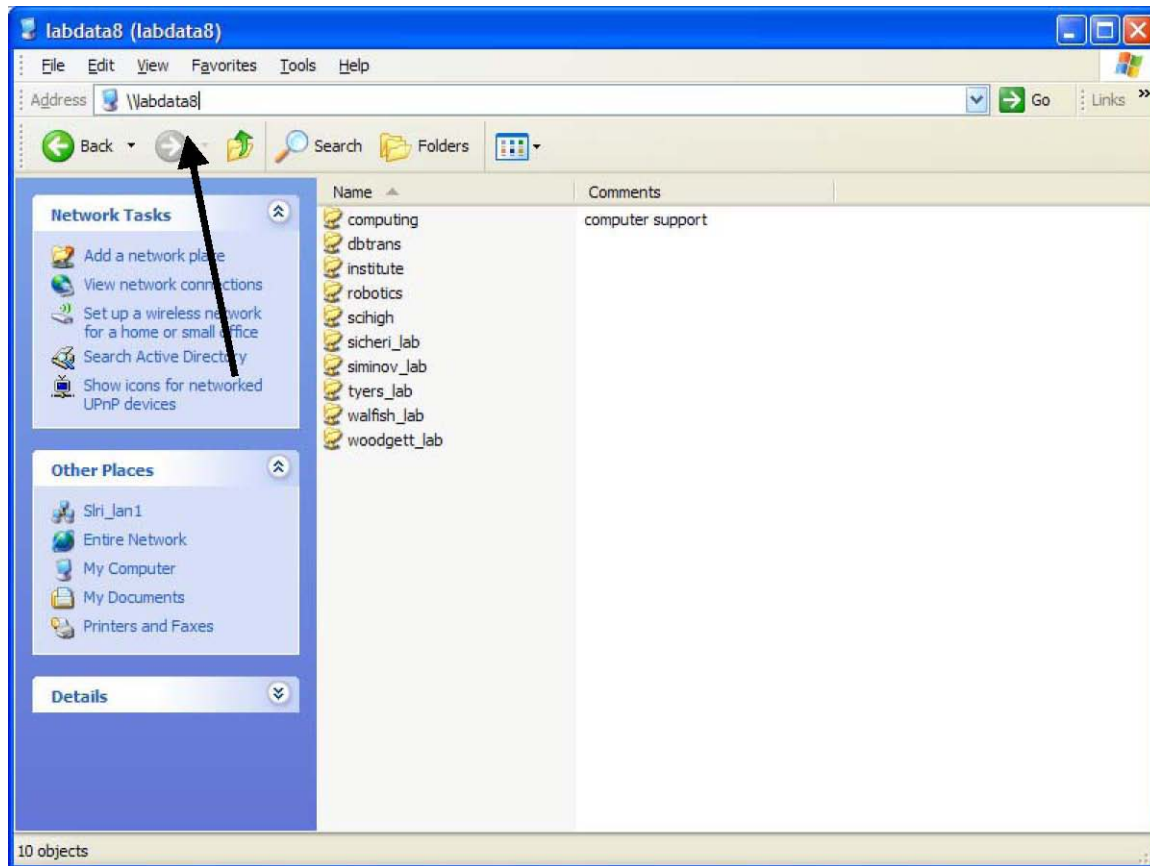


It should be noted that there are timeout values set for the SSL VPN. If no traffic passes over the SSL VPN for 60 minutes or more, the SSL VPN will automatically end your session (idle timeout).

When you are done using the SSL VPN, you **MUST** sign out. You can do this by right-clicking on the icon in the system tray and choosing “Sign Out” from the pop-up menu.



Now, to access the lab server folders , type in [\\labdata5.ad.mshri.on.ca](http://labdata5.ad.mshri.on.ca) and then navigate to the files you wish to access.



Troubleshooting

While testing the SSL VPN, the testers ran into a few issues. If you run into problems getting the SSL VPN to work, one of these solutions may solve your problem.

Problem #1: Your browser hangs after logging in, but before or while the SSL VPN client is being installed.

Solution #1: Quit the browser and go into your Start > Control Panel > Add/Remove Programs section. Look for “Juniper Network Network Connect” and remove it if it exists. Also, remove any “Java 2 Runtime Environment” or “J2SE Runtime Environment” items. Now go to <http://www.java.com/> and click on the “Download Now” icon. After you install the latest Java Runtime, restart your browser and try the SSL VPN again.

Problem #2: I still can't seem to get the SSL VPN client to automatically download and install.

Solution #2: You can try manually downloading and installing the client. Go back to the SSL VPN web page and click on the “Manual SSL VPN Client Install” download link. Select the Network Connect client appropriate for your operating system.

Problem #3: You were able to login to the SSL VPN and the SSL VPN client seemed to install okay, but it just doesn't work.

Solution #3: Make sure the SSL VPN icon is in the system tray and is not greyed-out. If it isn't in the system tray, try clicking the “Start” button on the Network Connect web page. If that doesn't work, check to make sure you don't have any other VPN clients installed such as CheckPoint VPN client, Cisco VPN client or Netscreen VPN client. Other VPN clients may interfere with the SSL VPN client operations. Either disable them or use the Add/Remove Program option in the Control Panel to delete the other VPN clients.

Problem #4: I keep getting disconnected from the SSL VPN after leaving my machine for a while.

Solution #4: There are two timeout values for the SSL VPN. One is an “idle timeout” which is set for 60 minutes. If no traffic passes over the SSL VPN for 60 minutes, it will end your session. You should get a pop-up about 5 minutes prior to warn you. The other timeout value is a “max session length.” This is the maximum amount of time you can be signed onto the SSL VPN for a given session. This is set to 24 hours. After 24 hours, the SSL VPN will end your session, and you will need to login again. It should also warn you about 5 minutes prior.

Managing Data

Data is the lifeblood of our lab, and so it should always be treated with diligence and care. In our lab, we often deal with sensitive information, so please be mindful of this both when you are working on data (i.e. don't leave things lying around), and also when talking about data with collaborators (i.e. do not discuss sensitive information in a public place).

The majority of our data is electronic in nature. The basic organisational principles for managing data in our lab are thus:

- 1) Raw data is sacrosanct. One copy of any collected data should be kept in its original state, and any manipulations or analysis should be done on a copy. This allows us to always go back to the data that was collected in case we need to analyse it in a different way, and to check for mistakes.
- 2) Keep careful records of everything that you do to a datasheet, either in a lab journal, or in a text file that gets stored with the data. This is crucial for validating our analyses.
- 3) Use a sensible file naming system that makes it clear what has been done to a file. In other words, rather than just naming files data1, data2 and so forth, a naming system such as 'EVAR_questionnaire_averaged_filtered' makes it easy to know exactly what you are looking at, and reduces the chances of mistakes being made. Also, DO NOT USE SPACES in file names as they sometimes cause problems over remote access. Rather, use a '_' or '-' to delineate words.
- 4) Confidentiality must be respected. Data files which contain sensitive information must always be password protected, and data should never be stored on unprotected machines. Email is not secure.
- 5) Be diligent about backups. We have two servers in the lab that you can use for backing up your data so there is no excuse! Also, please make sure that master copies of data live on the servers. If you want to work on your local computer, that is fine, but be sure to upload files to the server each day.

Servers

The Sonnadara Lab uses two servers. The primary server is [\\labdata5.ad.mshri.on.ca](http://labdata5.ad.mshri.on.ca), and this is the server on which most of your work will be saved. We also have a secondary server (pmslab-server [\\10.197.116.40](http://10.197.116.40)) which is used for storing large files such as video files, and for backups.

Note that neither server is backed up on a regular basis, so you are responsible for keeping regular backups of your work. It is a good idea to use the pmslab server to back up data stored on the labdata5 server. Most computers in the lab have large hard drives, and can be used to make extra safety copies of data. Laptops often get wiped, so do not store anything important on any of the SSC laptops.

Labdata5 Server

Each user in our group has their own home directory on the labdata5 server. This is a private folder to which only you (and in special circumstances, your supervisor) will have access.

We also have a 'shared' folder, which is visible to all members of the lab and it is in this folder that any data which is part of a collaborative project should be stored. If you are working remotely with a slow network connection, you may find that the most efficient workflow is to save a file to your local drive, work on it, and then upload it to the server when you are done. **If you do this, make sure you upload your file to the server!** It is a good idea, as outlined above, to use an incremental file naming system so that you can make sure your file did upload to the server. Also, please be sure to delete any confidential information from the local computer you are using. **It is your responsibility to make sure that data confidentiality is respected at all times.**

PMS-Lab Server

Not every user in our group has an account on the PMS-Lab server, but each project does. Please talk to Dr. Sonnadara if you do not know your login details. Files on this server should be stored in the appropriate project folder within the \data folder for shared data, or in your home directory for private files.

Dropbox

We are experimenting with a lab dropbox account which we use for working on collaborative projects *involving non-confidential data*. For more information on dropbox, please visit <http://www.dropbox.com>. In short, dropbox is a utility that enables changes to files made on one of the lab computers to automatically propagate to all of our other computers, so it's a great way to keep files in sync. However, we are limited to under 2G of storage, so please do not store large files in the dropbox folder.

The shared account username is sscpmslab@gmail.com. Please ask someone in the lab for the password.

Please note that Dropbox should only be used for non-confidential data as it is a public resource.

Remote Desktop Access

Given the number of people in the lab who are working remotely, at least at times, we have configured several computers for off-site access using the Windows Remote Desktop Client. To access these machines, you first need to be connected to the Lunenfeld VPN.

You then need to run the remote desktop client (this will work both on PCs or Macs), and connect to the machine by IP address as follows:

Bach: 10.197.116.93 (*Ranil's PC*)

Byrd 10.197.116.20 (*Monitor Room PC*)

Monteverdi: 10.197.116.121 (*PMS-Lab PC*)

Cortex: 10.197.116.30 (*Data Acquisition PC*)

If you are not sure which machine you need to connect with, please try Byrd or Monteverdi first. You should use the same credentials that you would use if you were logging into these machines in the lab.

Data protection and Confidentiality

You have been told this many times, but for completeness, here it is again. The lab servers should not, under any circumstances, be used to store illegal or pirated software, music or videos. Lab computers and printers should similarly not be used for improper activities.

Passwords and logins should never be shared. If someone needs access to your files, please talk to your supervisor.

Many projects within the lab involve the use of data which contains patient or participant information. This data is highly confidential, and should it be leaked, could cause many problems for you, your supervisor, the hospital and the university. Therefore, please treat data with appropriate respect, and never, ever cut corners for convenience. This means that all files should be password protected, and data should never be stored on unprotected machines. Files which are downloaded to local computers must be deleted and purged from any recycle bins at the end of each working session. Hard copies of data must be kept under lock and key, and shredded when no longer required. Data which is copied to portable media must always be stripped of confidential information, or appropriate precautions taken (i.e. data must be encrypted, and only secure portable media [such as these](#) should be used). If you are unsure of appropriate procedures and protocols, please talk to your supervisor.

If you wish to use your personal laptops for work and are dealing with any confidential or patient data, the hard drives must be encrypted. You may find out about how to get your hard drive encrypted by contacting Tony or Maria at the addresses below (there is no charge for doing this). It is your responsibility to inform your supervisor of your intention to use your personal computer for any confidential work with sufficient notice that appropriate steps can be taken to ensure complete security of confidential data.

Also, please note that Mount Sinai Hospital regularly monitors network traffic, and any activity such as downloading illegal files or file sharing will set off more alarms than you want to think about.

Support

If you need help, please talk to someone else in the lab in the first instance, or email tony@lunenfeld.ca or maria@lunenfeld.ca. Shunne Leung (<mailto:shunne.leung@utoronto.ca>) is also a valuable resource within the Surgical Skills Centre.