SSH Checklist

# Linux

## 1) Version and Update

### a) How to tell what version of ssh is running

sshd -V

### b) Below is multiple ways of updated SSH

* pkg-add -r openssh-portable
* cd /usr/ports/security/openssh && make install clean
* portupgrade security/openssh-portable

## 2) Install Service (CentOS)

If only telnet is installed, SSH needs to be utilized since it’s more secure.

yum -y install openssh-clients

## 2) Configure Server Passwords Settings (CentOS)

The following changes need to be made in the following file:

vim /etc/ssh/sshd\_config

SSH allows for users to login as root, so it should be disabled. If you need access you can use the sudo command. The following is what needs to be changed in this file:

# line 48: uncomment and change(prohibit root login remotely)  
PermitRootLogin no

Ensure that there needs to be user authentication:

# line 77: uncomment  
PermitEmptyPasswords no  
PasswordAuthentication yes

If necessary, limit which users can use SSH. In this example Alice and Bob are the users:

AllowUsers alice bob

Ensure that SSH2 is being used and not SSH1, since SSH2 is the newer protocol. Meaning it is more secure:

#Uncomment Protocol 2,1 and change it to:  
Protocol 2

**IMPORTANT!**  Every time a change is made, you MUST restart the SSH service

systemctl restart sshd

## 3) Authenticate Keys (CentOS)

Having authorized key pairs will allow for more authentication throughout the network. The following is how to create and copy a key pair to the local SSH directory:

### Create Key Pair

ssh-keygen -t rsa

[mv](https://www.server-world.info/en/command/html/mv.html) ~/.ssh/id\_rsa.pub ~/.ssh/authorized\_keys

[chmod](https://www.server-world.info/en/command/html/chmod.html) 600 ~/.ssh/authorized\_keys

### Copy Secret Key to Local SSH Directory

[mkdir](https://www.server-world.info/en/command/html/mkdir.html) ~/.ssh

[chmod](https://www.server-world.info/en/command/html/chmod.html) 700 ~/.ssh

scp cent@10.0.0.30:/home/cent/.ssh/id\_rsa ~/.ssh/

ssh -i ~/.ssh/id\_rsa cent@10.0.0.30

### Restart Service

systemctl restart sshd

## 4) SCP

#### Copy the file "foobar.txt" from a remote host to the local host

$ scp your\_username@remotehost.edu:foobar.txt /some/local/directory

#### Copy the file "foobar.txt" from the local host to a remote host

$ scp foobar.txt your\_username@remotehost.edu:/some/remote/directory

#### Copy the directory "foo" from the local host to a remote host's directory "bar"

$ scp -r foo your\_username@remotehost.edu:/some/remote/directory/bar

#### Copy the file "foobar.txt" from remote host "rh1.edu" to remote host "rh2.edu"

#### Copying the files "foo.txt" and "bar.txt" from the local host to your home directory on the remote host

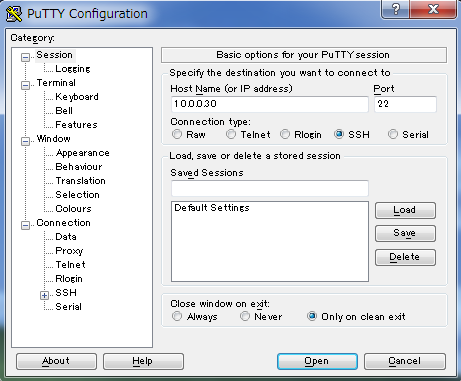
* $ scp your\_username@rh1.edu:/some/remote/directory/foobar.txt \
* your\_username@rh2.edu:/some/remote/directory/
* $ scp foo.txt bar.txt your\_username@remotehost.edu:~

Copy the file "foobar.txt" from the local host to a remote host using port 2264

$ scp -P 2264 foobar.txt your\_username@remotehost.edu:/some/remote/directory

## 4) Configure SSH Client (Windows)

An SSH client is need for windows, so for this example I will be using Putty (need a safe link to download). Below is how the window should look like. Ensure to put the correct host name (IP), and then select open. A command prompt should open asking for a password.



## 5) SSH File Transfer (Windows)

If the system we have uses Windows, we can us WinSCP. However, [WinSCP](https://winscp.net/eng/download.php) needs to be installed in order to be used. Once installed, here are the steps:

1. Select New
2. Input the correct information and file that is wanted to be transfered
3. Move to the 'Directory' section on the left menu and input remote server's directory and local client directory you want to login. Next, click login button.
4. Insert Password
5. Once logged in, you can upload or download files in WinSCP