

## Table of Contents

<b>Setting Up an SSH Console</b> .....	1
<b>Configure SSH in FreeNAS</b> .....	1
<b>Specify SSH Public Key For a User</b> .....	3
<b>Setting up PuTTY in Windows</b> .....	5
<b>Public Key Authentication in PuTTY</b> .....	5
<b>Using SSH on a Mac</b> .....	5
<b>Using SSH on Linux</b> .....	8



# Setting Up an SSH Console

SSH stands for Secure SHell, and is a secure method to connect to a remote computer over a network. There are many advantages to using an SSH console rather than say the shell facility in the FreeNAS GUI.

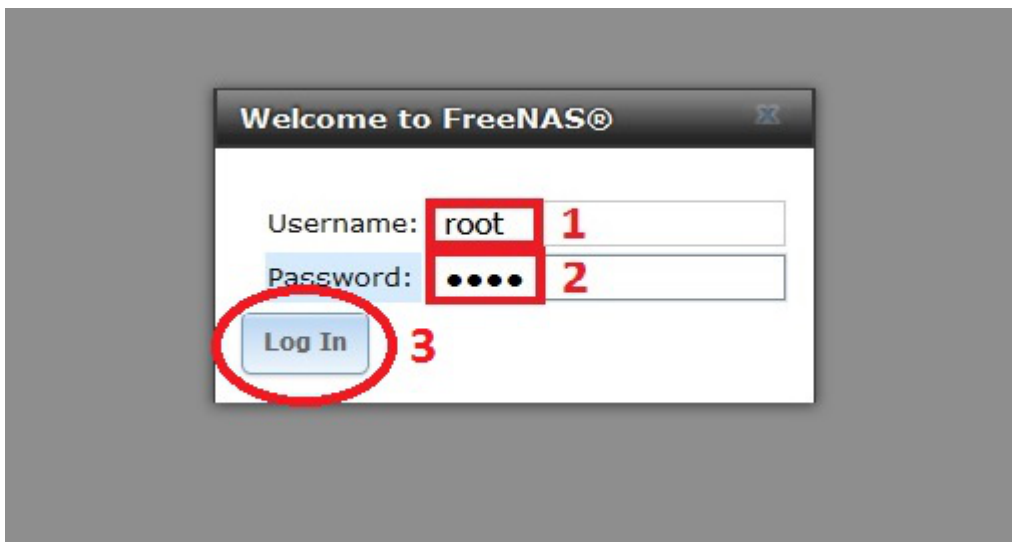
The SSH console is a window that has a scrolling function which means you can go back and view the output in the console. You can also select large bodies of text and copy and paste them. This can be particularly useful when trying to get help from someone as they need to see what you have done. It is also useful when compiling data (i.e. SMART test data).

An SSH console is also very secure in two ways. Firstly it can be configured to require a Public/Private key and a password before you can log in to the session and the server. Secondly the connection between the server and the client is encrypted. This means any information that goes between the two cannot be read directly.

## Configure SSH in FreeNAS

Open your web browser and type in the IP address of the FreeNAS web GUI that you noted down earlier (Fester used 192.168.0.58).

The web GUI will present itself and ask for the login details. Enter the username which is **root** (1) and your password (2) and click the “Log In” button (3).



Now you are logged into FreeNAS.

- Now navigate to the “Services” page (1).
- Click on the tiny spanner icon next to “SSH” (2).
- If you do not want the root user to be able to log in using only a password (i.e., if you want to require a public key, or if you don't want the root user to be able to log in remotely at all), uncheck the “Login as Root with password” tick box (3).

- If you want to require public key authentication, uncheck the “Allow password authentication” tick box (4).
- Make sure the remaining tick boxes are unchecked (5).
- Now click the “OK” button (6).

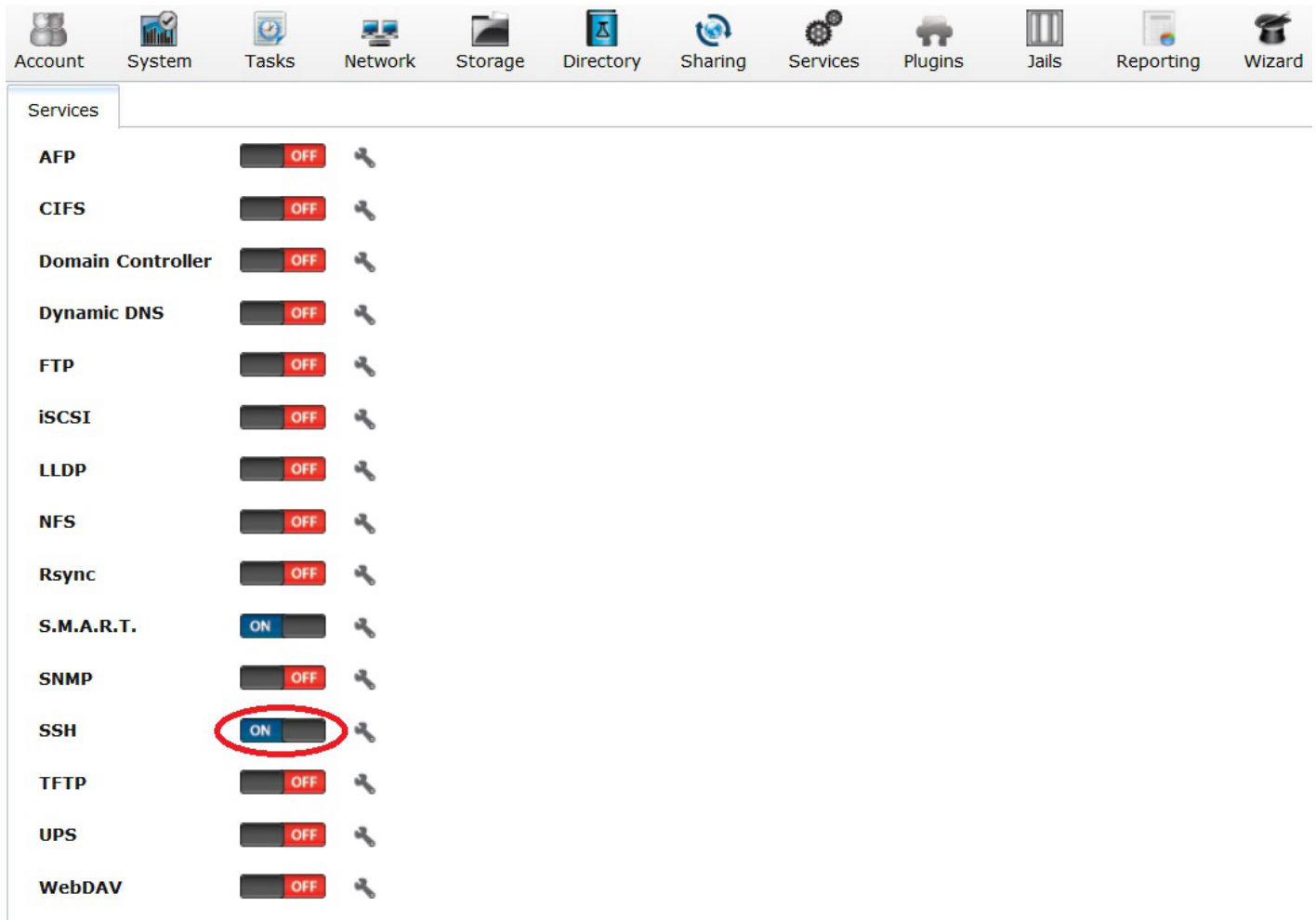
The screenshot shows the Services configuration window in a Linux desktop environment. The Services window is open, and the SSH service is selected. The SSH Settings dialog box is displayed, showing the following options:

- TCP Port: 22
- Login as Root with password:  (3)
- Allow Password Authentication:  (4)
- Allow TCP Port Forwarding:  (5)
- Compress Connections:  (6)

The OK button is circled in red. Red numbers 1 through 6 are overlaid on the image to indicate the steps:

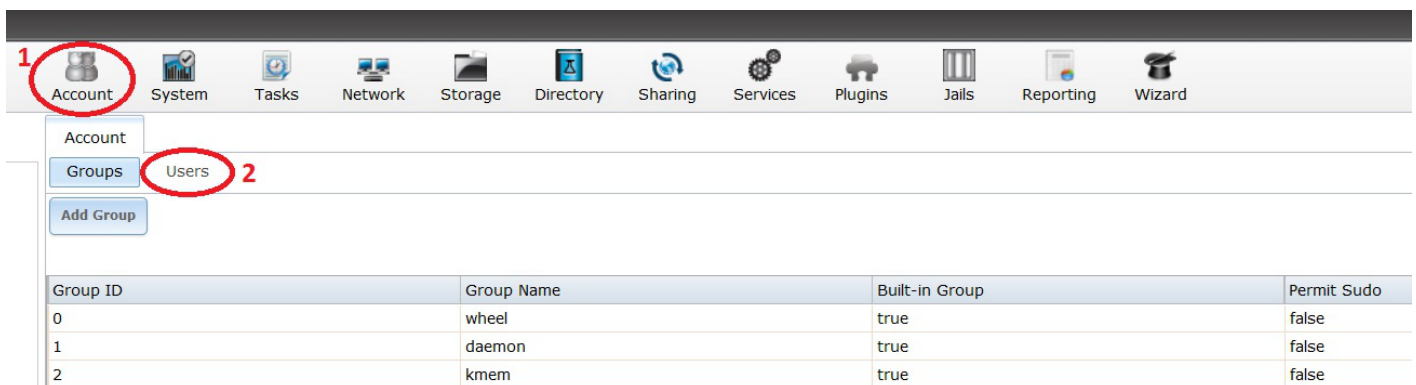
- 1: Services icon in the top bar
- 2: SSH service icon
- 3: Login as Root with password checkbox
- 4: Allow Password Authentication checkbox
- 5: Allow TCP Port Forwarding checkbox
- 6: OK button

Now turn on the SSH service.



## Specify SSH Public Key For a User

If you have required public key authentication in the SSH configuration, you'll need to tell FreeNAS what the public key is for each user who will be connecting via SSH. To do that, Navigate to the "Account" page by clicking on the Account icon (1). Now click on the "Users" button (2).



p { margin-bottom: 0.1in; direction: ltr; color: rgb(0, 0, 0); line-height: 120%; }p.western { font-family: "Times New Roman",serif; font-size: 12pt; }p.cjk { font-family: "Times New Roman",serif; font-size: 12pt; }p.ctl { font-family: "Times New Roman",serif; font-size: 12pt; }a:visited { color: rgb(128, 0, 128);

```
}a.western:visited { }a.cjk:visited { }a.ctl:visited { }a:link { color: rgb(0, 0, 255); }
```

Now select the “root” user account (1) (it will turn blue when selected) and click on the “Modify User” button (2).

The screenshot shows a web interface for user management. At the top, there are navigation icons for Account, System, Tasks, Network, Storage, Directory, Sharing, Services, Plugins, Jails, Reporting, and Wizard. Below these, there are tabs for Account, Groups, and Users. An 'Add User' button is visible. The main part of the interface is a table with the following columns: User ID, Username, Primary Group ID, Home Directory, Shell, Full Name, Built-in User, E-mail, and Disable password. The 'root' user (ID 0) is highlighted in blue. Below the table, there are two buttons: 'Modify User' (circled in red) and 'Change E-mail'.

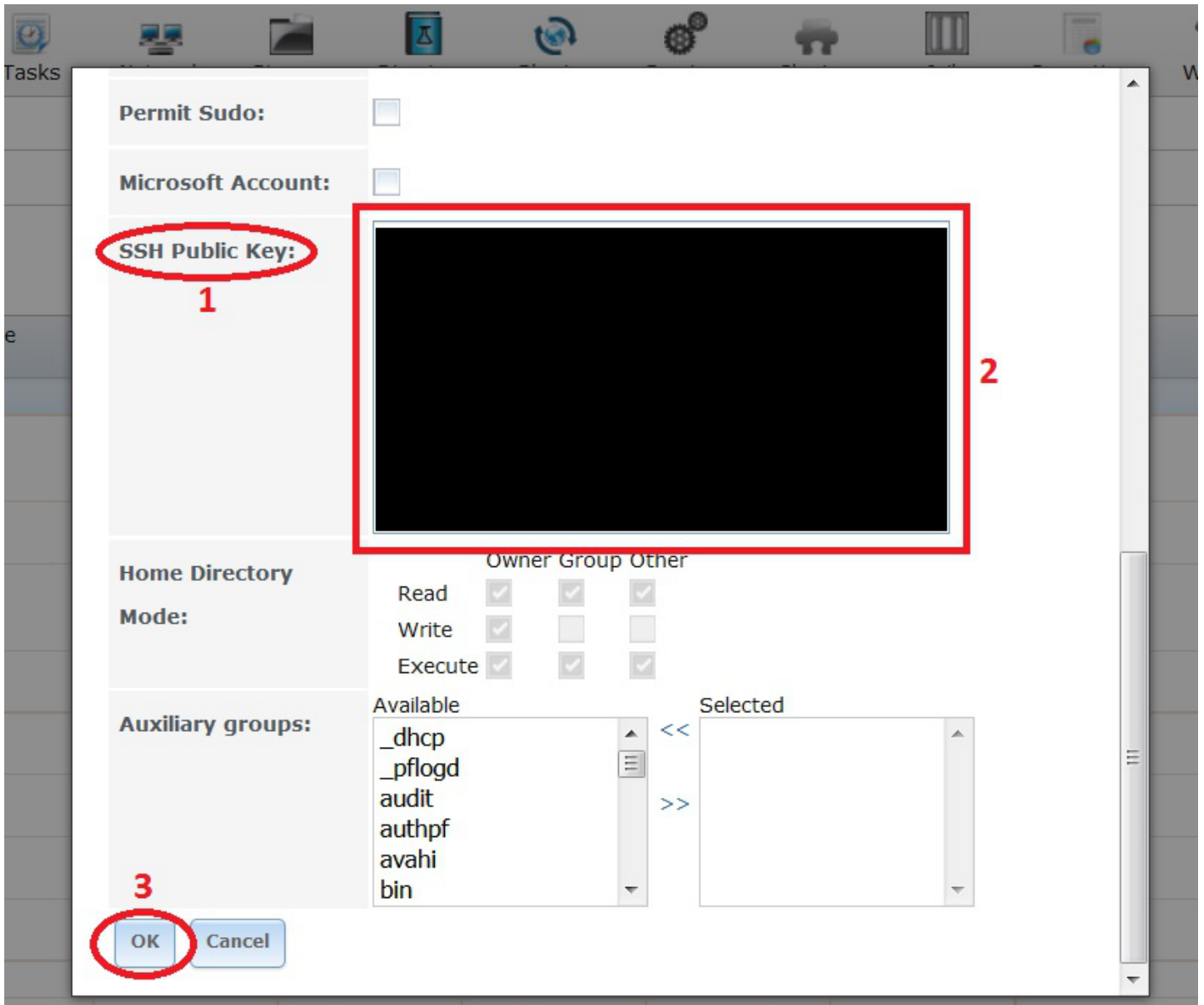
User ID	Username	Primary Group ID	Home Directory	Shell	Full Name	Built-in User	E-mail	Disable password
0	root	0	/root	/bin/csh	root	true		false
1	daemon	1	/root	/usr/sbin/nologin	Owner of many system processes	true		false
2	operator	5	/	/usr/sbin/nologin	System &	true		false
3	bin	7	/	/usr/sbin/nologin	Binaries Commands and Source	true		false
4	tty	65533	/	/usr/sbin/nologin	Tty Sandbox	true		false
5	kmem	2	/	/usr/sbin/nologin	KMem Sandbox	true		false
7	games	13	/	/usr/sbin/nologin	Games pseudo-user	true		false
8	news	8	/	/usr/sbin/nologin	News Subsystem	true		false
9	man	9	/usr/share/man	/usr/sbin/nologin	Mister Man Pages	true		false
14	ftp	14	/nonexistent	/bin/csh		true		false
22	sshd	22	/var/empty	/usr/sbin	Secure Shell	true		false

```
p { margin-bottom: 0.1in; direction: ltr; color: rgb(0, 0, 0); line-height: 120%; }p.western { font-family: "Times New Roman",serif; font-size: 12pt; }p.cjk { font-family: "Times New Roman",serif; font-size: 12pt; }p.ctl { font-family: "Times New Roman",serif; font-size: 12pt; }a:visited { color: rgb(128, 0, 128); }a.western:visited { }a.cjk:visited { }a.ctl:visited { }a:link { color: rgb(0, 0, 255); }
```

The modify user window should now pop up. Scroll down till you come across the “SSH Public Key:” entry (1).

Now right click in the blank box next to it and paste in the previously copied public key (2).

Now click the “OK” button (3).



## Setting up PuTTY in Windows

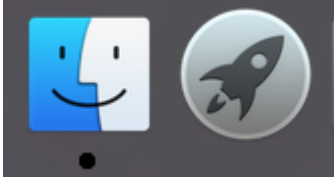
Modern operating systems ship with an SSH client installed. Unfortunately, Windows is still not a modern operating system in this regard, so a third-party client will need to be used. Popular clients include [Bitvise](#) and [PuTTY](#).

## Public Key Authentication in PuTTY

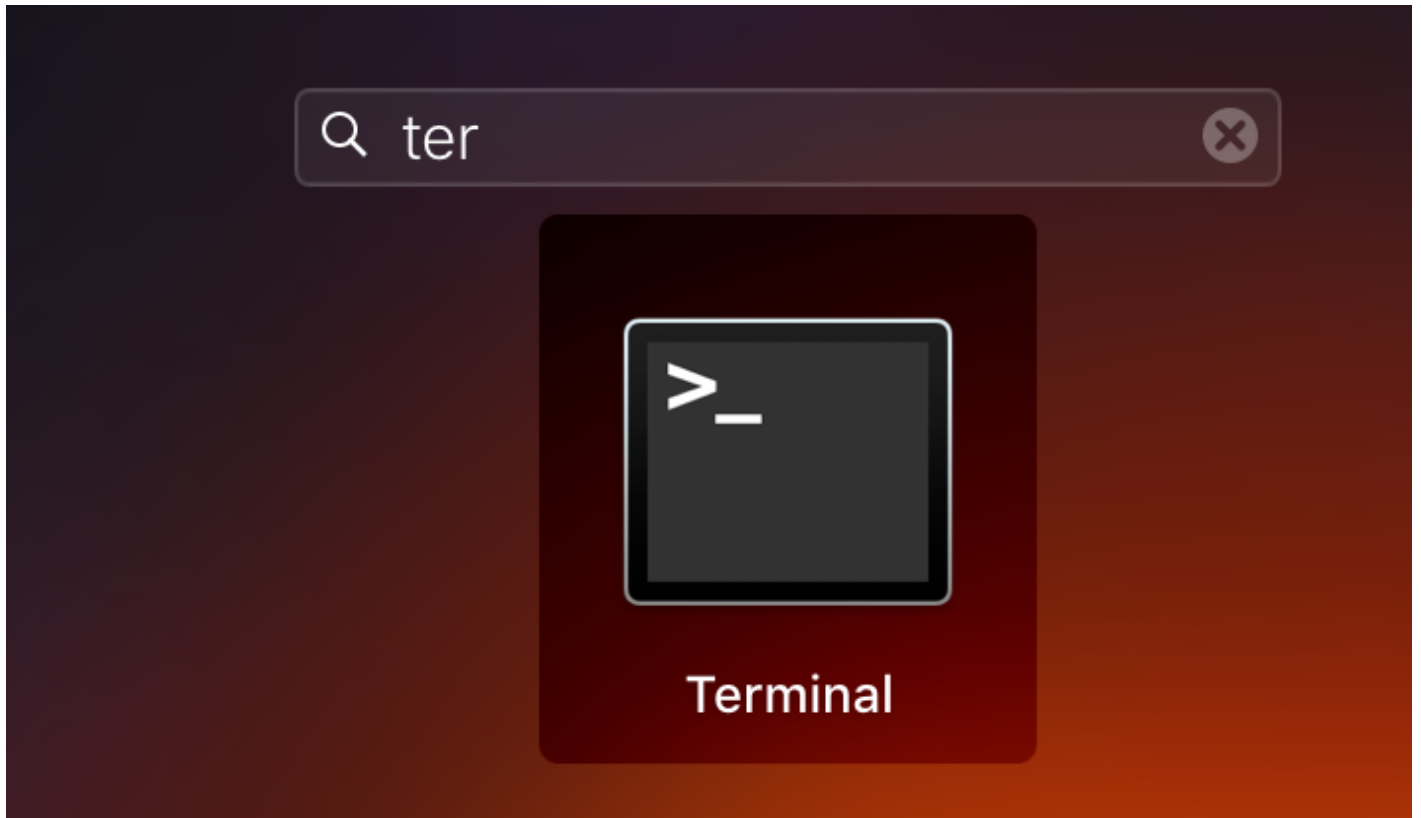
## Using SSH on a Mac

Mac OS X includes an SSH client, but it must be used from the command line. To use it, you'll need to

open a terminal window. Start by clicking the launchpad button in your dock (it looks like a rocket):

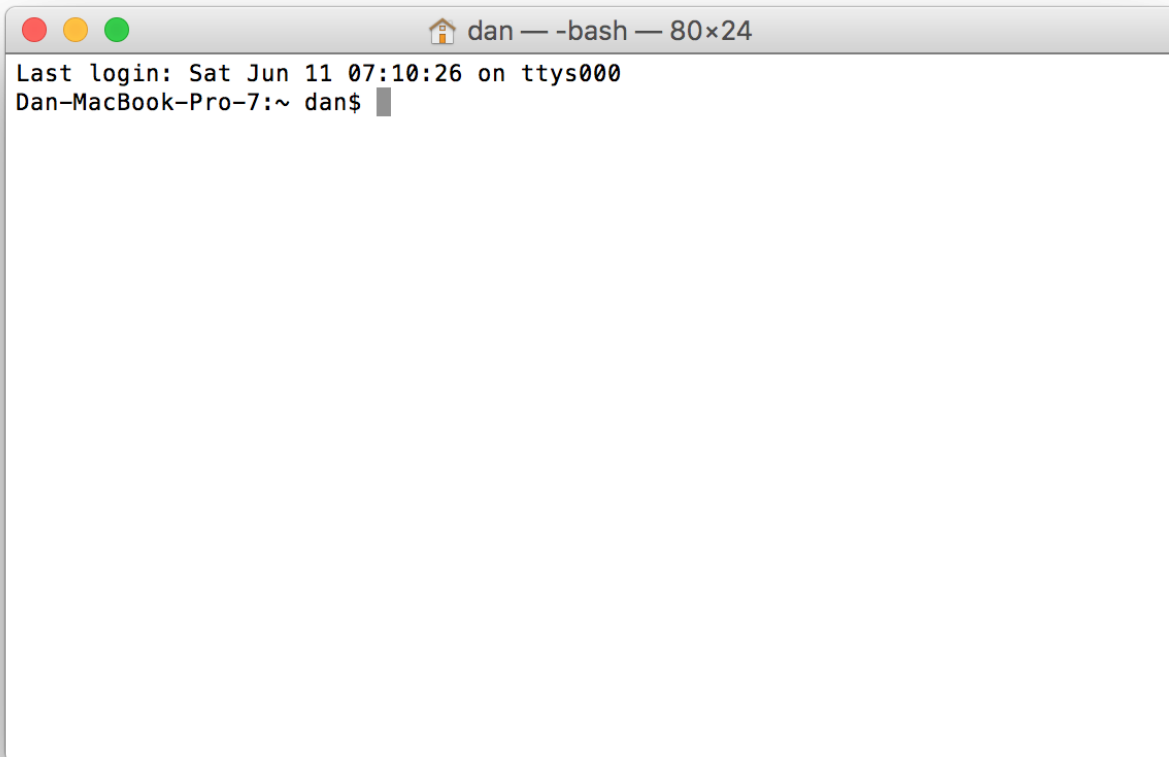


Begin typing “Terminal” into the search bar at the top, until you see the Terminal icon below:



Then click on the Terminal icon. You'll see a window like this:



A screenshot of a macOS terminal window. The title bar shows a home icon, the name 'dan', and the shell '-bash' with a window size of '80x24'. The terminal content shows a login message: 'Last login: Sat Jun 11 07:10:26 on ttys000' followed by the prompt 'Dan-MacBook-Pro-7:~ dan\$' and a cursor.

To connect to a server using SSH, you can simply type

```
ssh user@host
```

Where “user” and “host” are the username and hostname, respectively, that you want to connect to. For example,

```
ssh root@freenas
```

Or you can use an IP address:

```
ssh root@192.168.0.5
```

If you have required public key authentication on your FreeNAS server, you'll need to generate a keypair. To do this, type

```
ssh-keygen -t rsa
```

...and simply accept the defaults. The result will look like this:

```
Dan-MacBook-Pro-7:~ dan$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/dan/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/dan/.ssh/id_rsa.
Your public key has been saved in /Users/dan/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:ZB0ZFqEWWJuCgEWIyFd/Thk5K0uncH8LT06w0CSdRdk dan@Dan-MacBook-Pro-7.local
The key's randomart image is:
+---[RSA 2048]-----+
|+=+ .. +*.B=      |
|=. o o+o E+.     |
|  . . +oB+o      |
|    ..o=+        |
|   ..+ .S.       |
|  .oo..o         |
|   oo+o o        |
|    ...*         |
|     .+          |
+-----[SHA256]-----+
Dan-MacBook-Pro-7:~ dan$ █
```

The system will prompt you for a passphrase; this is optional. If you enter a passphrase, you will need to enter it every time you use this keypair (i.e., every time you use ssh). If you leave the passphrase blank, you won't need to enter it when you connect to a remote server, but neither will a thief who manages to steal your computer. You'll now need to view your public key, to enter it in the FreeNAS configuration. To do that, type

```
cat .ssh/id_rsa.pub
```

The result will look like this:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQACxoFuJ2Px8sIA0zla1FXjnG+af2kRNhj/FcQ5nh0n6F2LepgX
f/4SQFjx5BwAD88H6/06lTaUAqprxKS4m33SKN7poH6RaeIfbJXwjJ/o0Cx0QbugGAeMKjHOBg4fsHw
vqGLT7o0lcQ0ubmGBZlSx9R9IFNmnDLAru+Z5gjuAwKCXGw2dxVqbq2IwB3jEoA3bbo8gy6Dso5wV75
0EC+dYlB/lQrxW/uscgPjpi1XCFVuWtajyz9jujakR1uHuRRphsp56GXVTovwM3P6h52ADDhr5vkfsk
GKgMETj940x5+MFbmBvC9iIMIErGLfWIAQY+8NjosQYfieU5U48oDmDb dan@Dan-MacBook-
Pro-7.local
```

Copy this, all on line line, and paste it into your FreeNAS configuration.

## Using SSH on Linux

SSH on Linux works just like SSH on a Mac. Follow the instructions above.

From:

<https://familybrown.org/dokuwiki/> - **danb35's Wiki**

Permanent link:

[https://familybrown.org/dokuwiki/doku.php?id=fester:ssh\\_setup&rev=1465662362](https://familybrown.org/dokuwiki/doku.php?id=fester:ssh_setup&rev=1465662362)

Last update: **2016/06/11 16:26**

