KB0010539 - Latest Version

Using the Oracle Staff Student Interactive Database (SSID)

Revised by Ajay Simha

SSID is an Oracle database that eSolutions has created for students and staff to develop their IT skills in using and creating applications that use SQL and enterprise standards such as Oracle RDBMS. To request access to the Oracle database, please contact the IT Service Desk.

This helpful article explains the different ways to log in, give other users access to your data, and how to back up and restore your data. There are also tips included to optimise your use of the SSID and provide some help in handling the most common errors.

Table of Contents

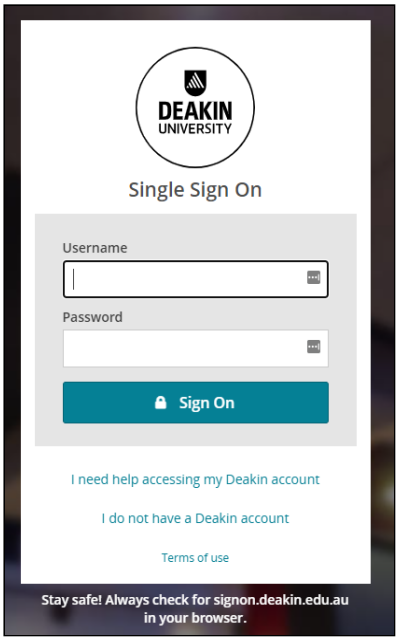
- Windows - Connecting to SSID for the first time
- Windows - Consecutive login to SSID
- Mac - Connecting to SSID for the first time
- Mac - Consecutive login to SSID
- Connecting via the web
- Giving other users access to data
- Backup data in SSID
- Restore data from a backup
- I get the following error: "ORA-01536: space quota exceeded for tablespace users"
- Settings for connecting to SSID via TeraTerm
- Other Tips

Windows - Connecting to SSID for the first time

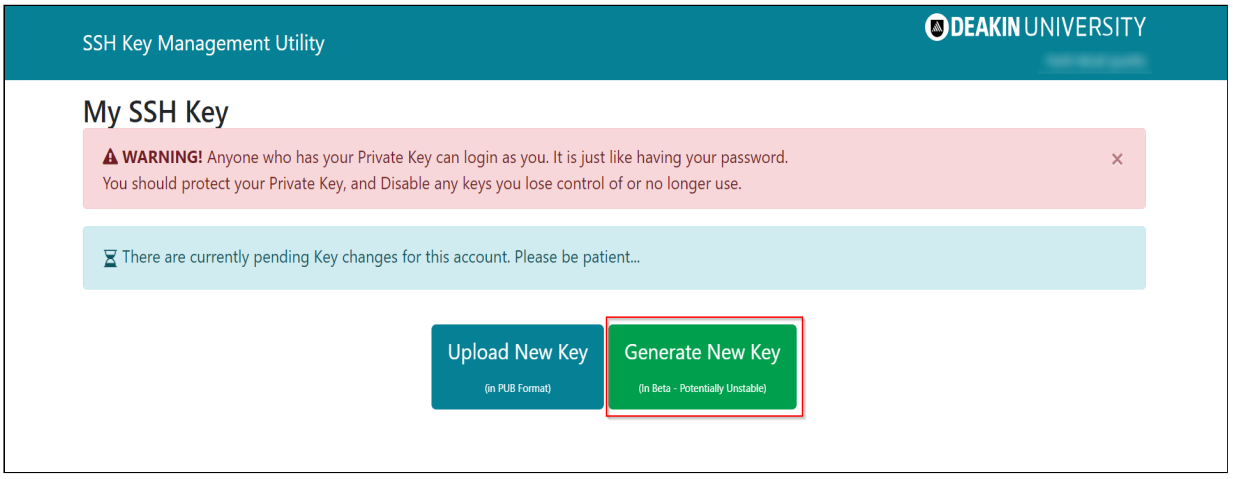
Please click on the relevant step number to expand the detailed instructions.

▼ **Step 1: Generate a New Key**

1. Login to the SSH Key Management Utility with your **Deakin Credentials**.

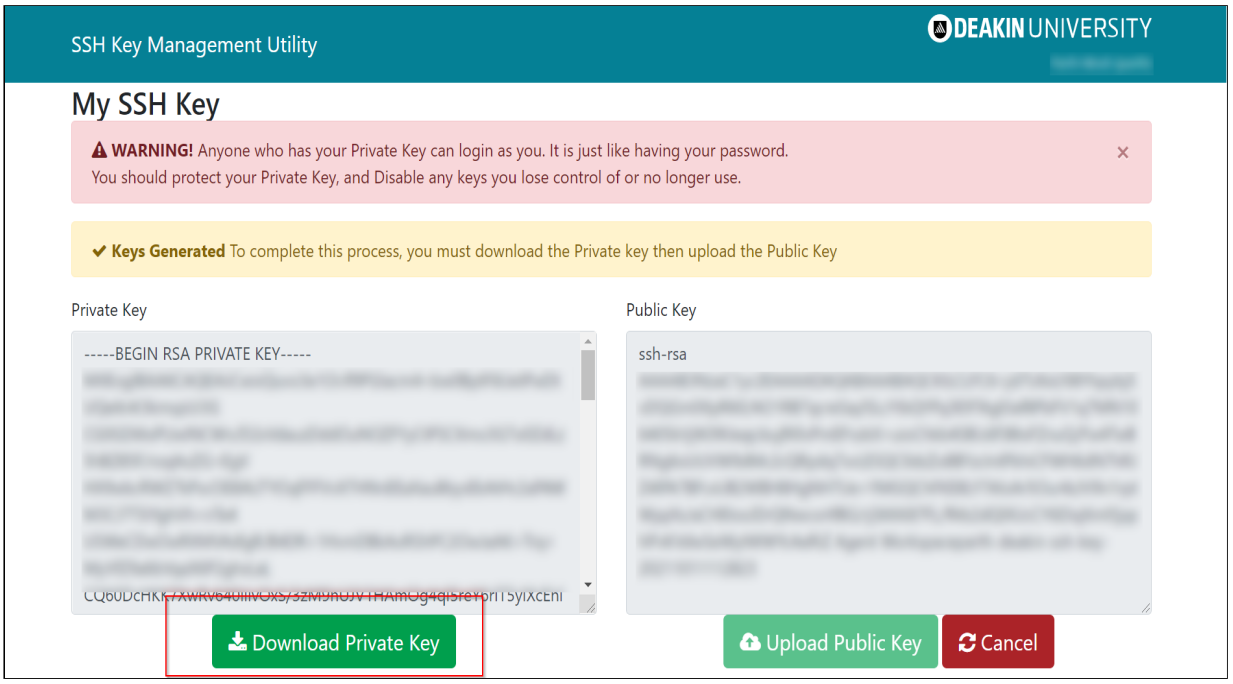


2. Once logged on, navigate to **Click Generate New Key,** this will generate the keys.

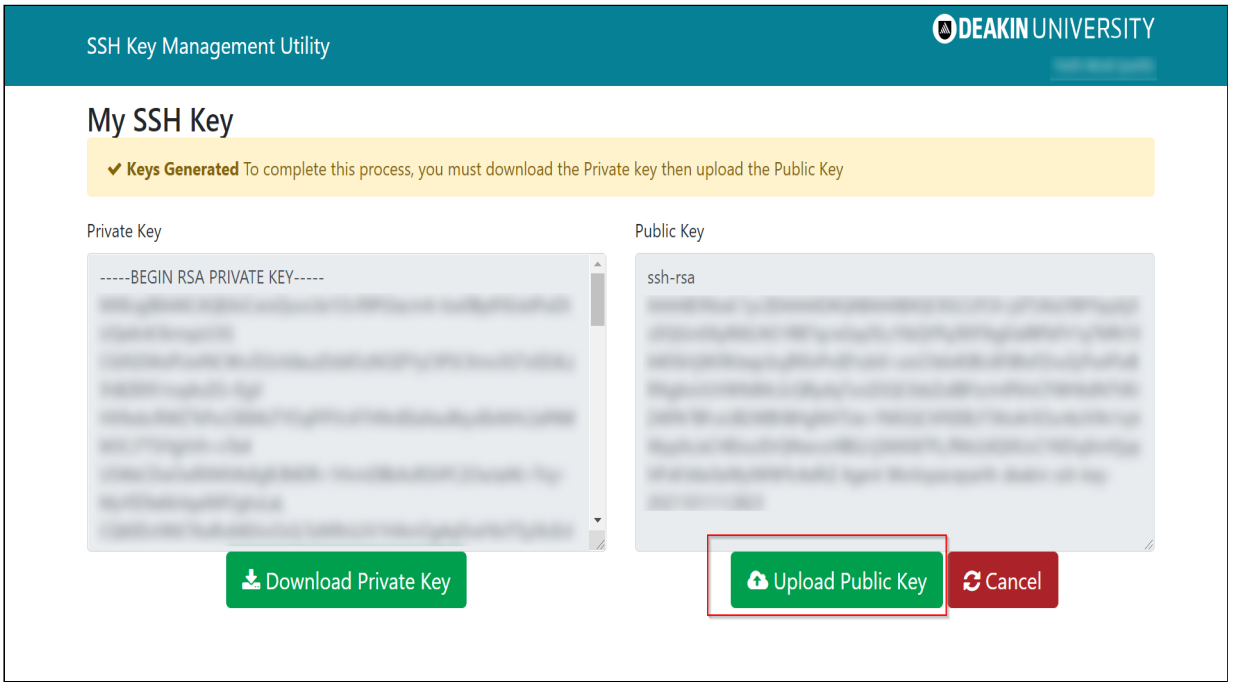


3. Once keys are generated to complete the process, you must **download Private Key** to a safe location within your computer.

The Private Key should be kept in a safe place within your computer, as anyone who has your private key can log in as you.



4. The private key will be downloaded as a **privateKey.txt** file, once this is downloaded and **stored in a secure location on your computer. Click on Upload Public Key**



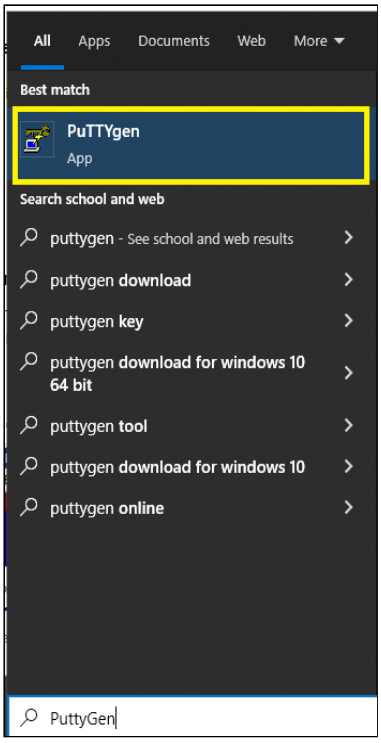
▼ Step 2: Convert your PrivateKey using PuTTYgen

If you intend to use PuTTY as an SSH Client, you will need to use PuTTYgen to convert your Private Key from PEM Format to PPK (PuTTY Private Key) format.

1. Install **PuTTY client (PuTTYgen and Pageant will be installed with PuTTY)**

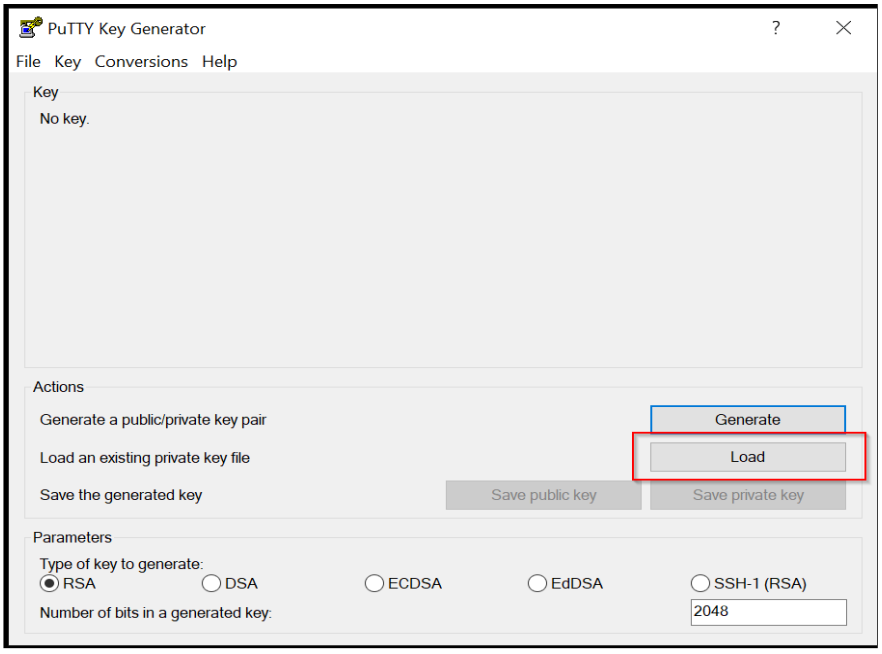
For Deakin Managed machines, install from **Software Center.** For Personal machines, download and install from the **following link.**

2. Once the software is installed, navigate to the **Start menu, search for PuTTYgen**

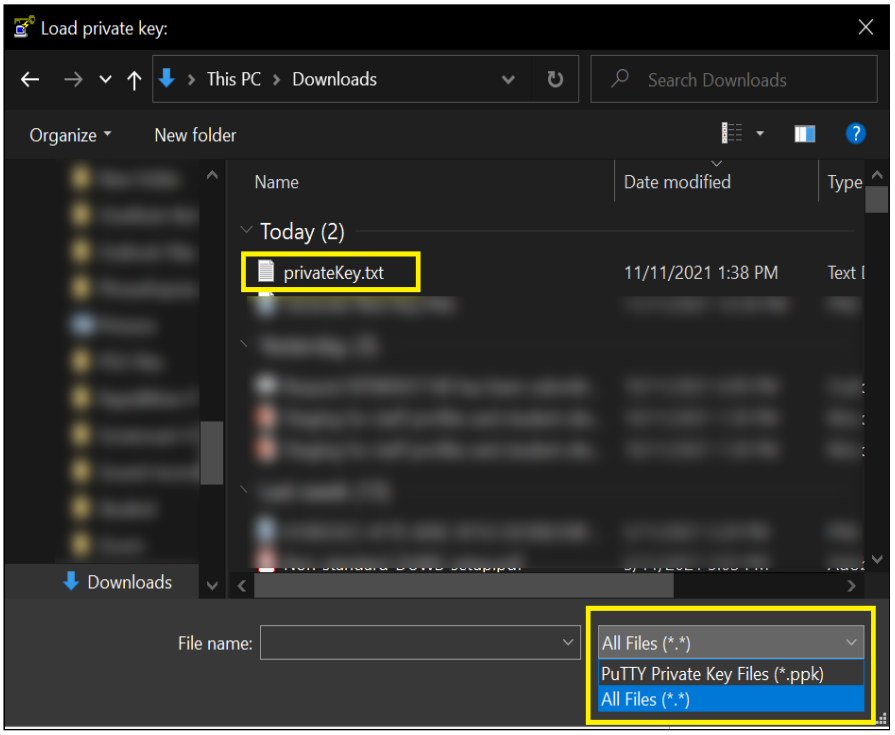


2. Launch **PuttyGen** App, navigate and click on **Load.**

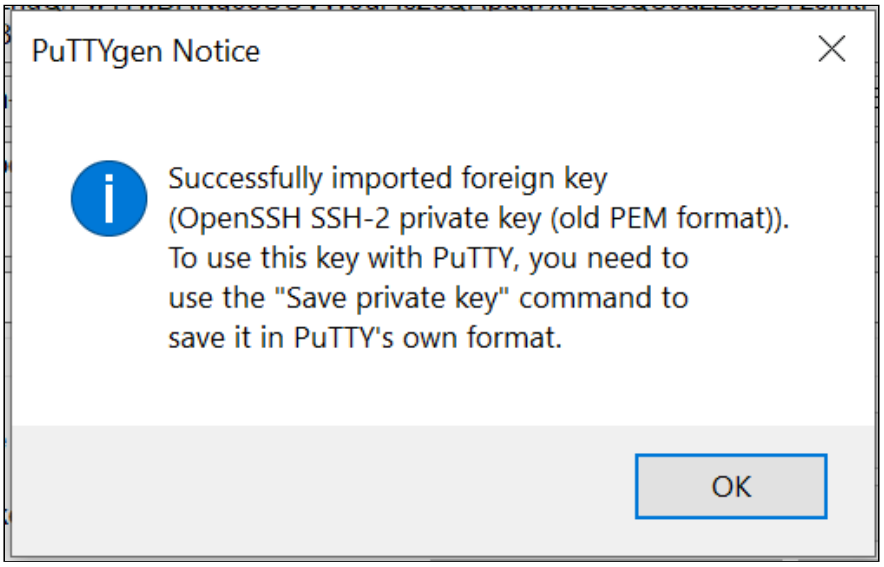
In PuTTYgen, set the following parameters:
Type of key to generate: **RSA** (NOT SSH-1 RSA)
Number of bits in a generated key: **2048** (or higher)



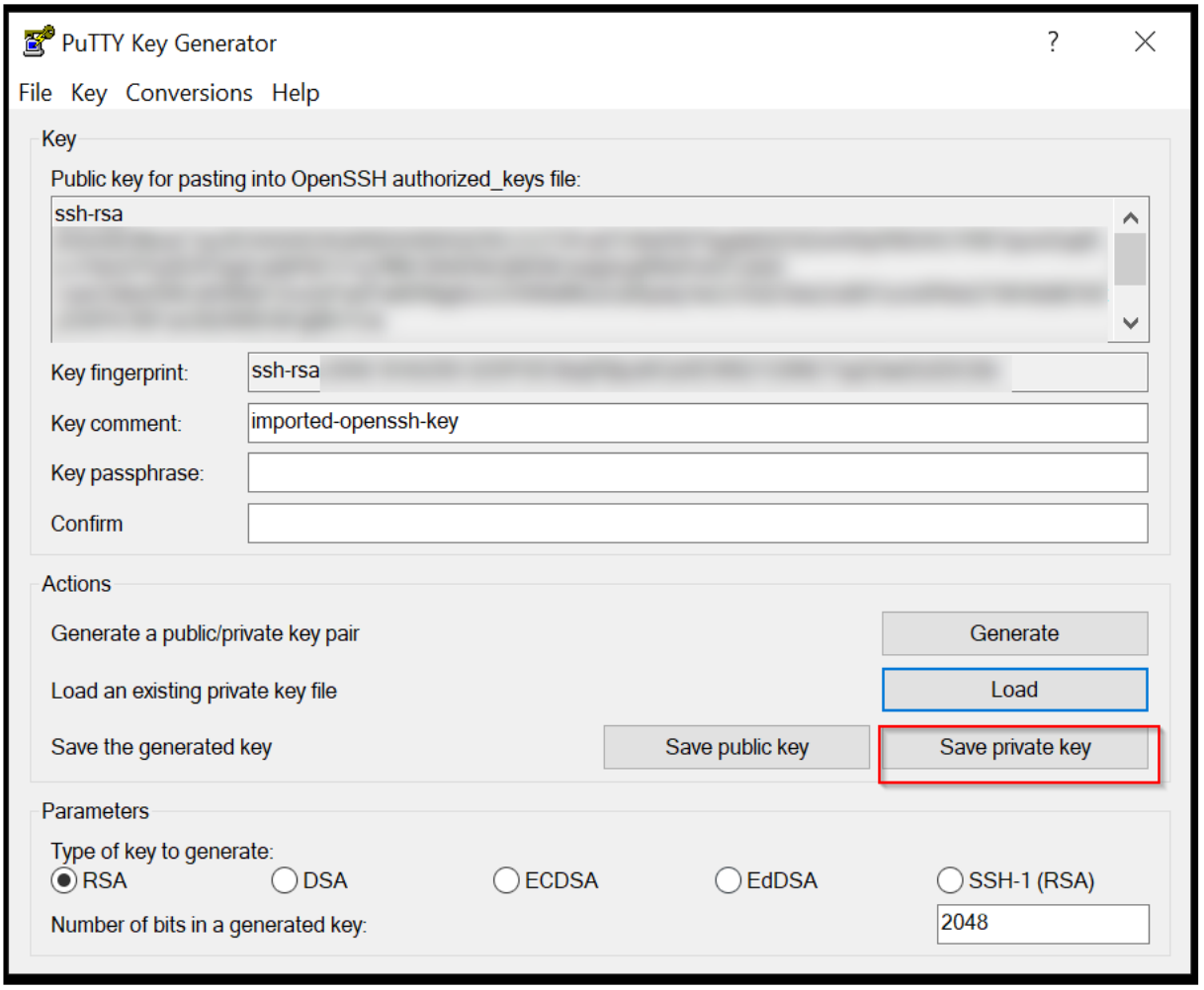
3. Locate the **privateKey.txt** file on your machine, change the **file type to All Files (*) to locate the .txt file.**



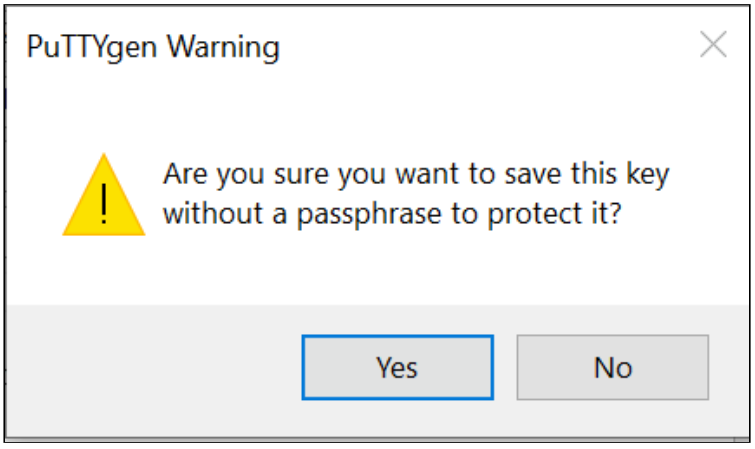
4. Once the key is loaded you will get the following notification.



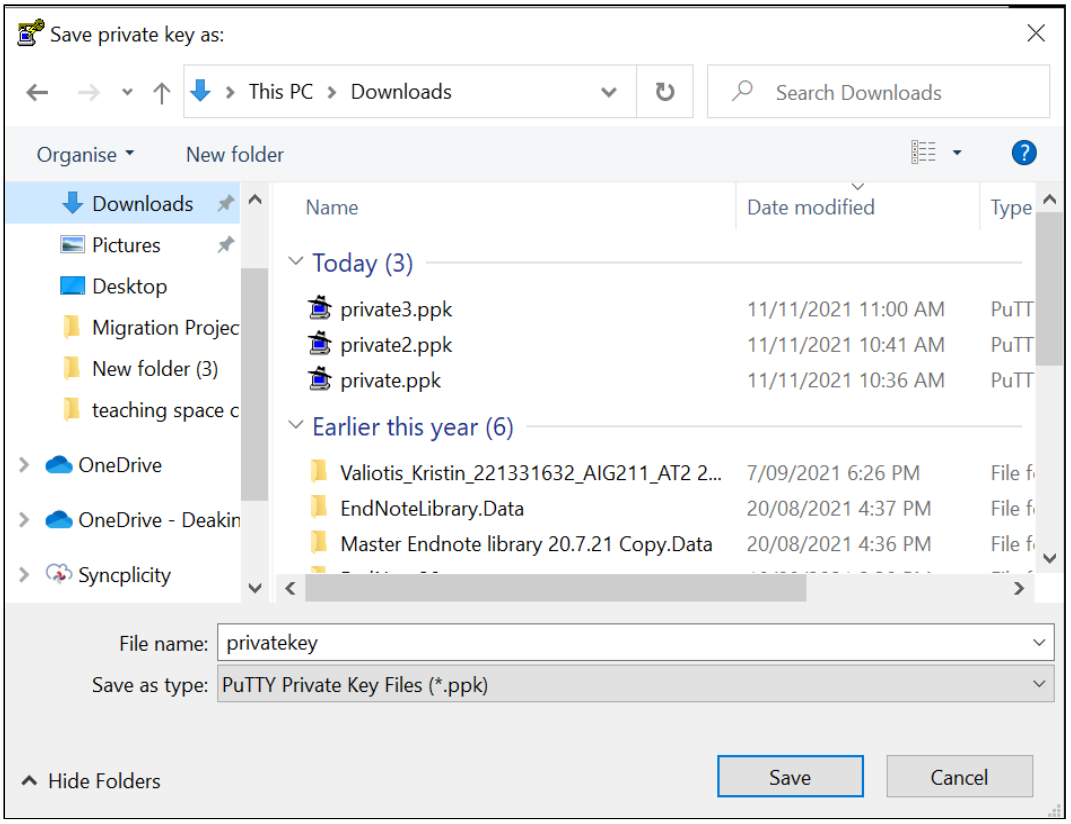
5. Now **save the Private Key in the.PPK format.**



6. You will get a warning message when saving the Private Key. Select **Yes** to save the private key.



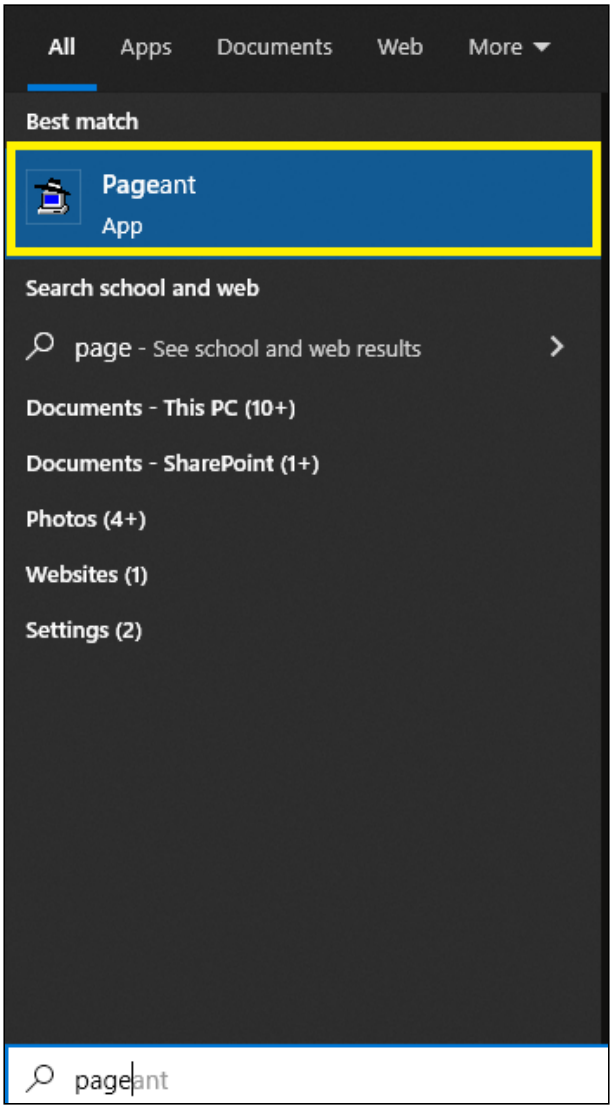
7. Please **save the Private Key in the.PPK format into a location you can remember.**



▼ **Step 3: Add your converted ppk key to Pageant**

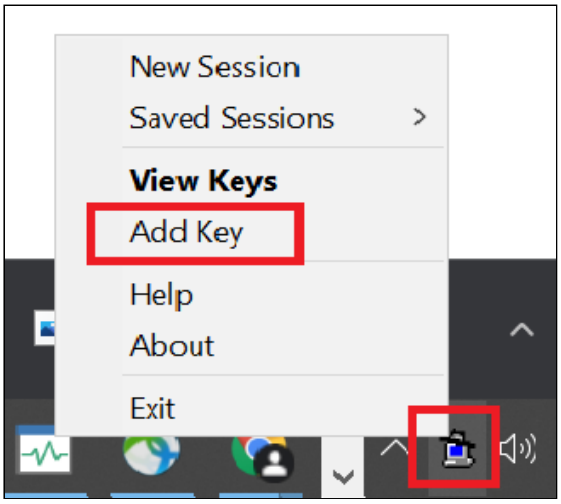
Before your private key can be used for authentication with PuTTY, it must be converted to a format PuTTY can open.

1. Click on **Start Menu, search** for **Pageant**



2. Click on **Pageant**

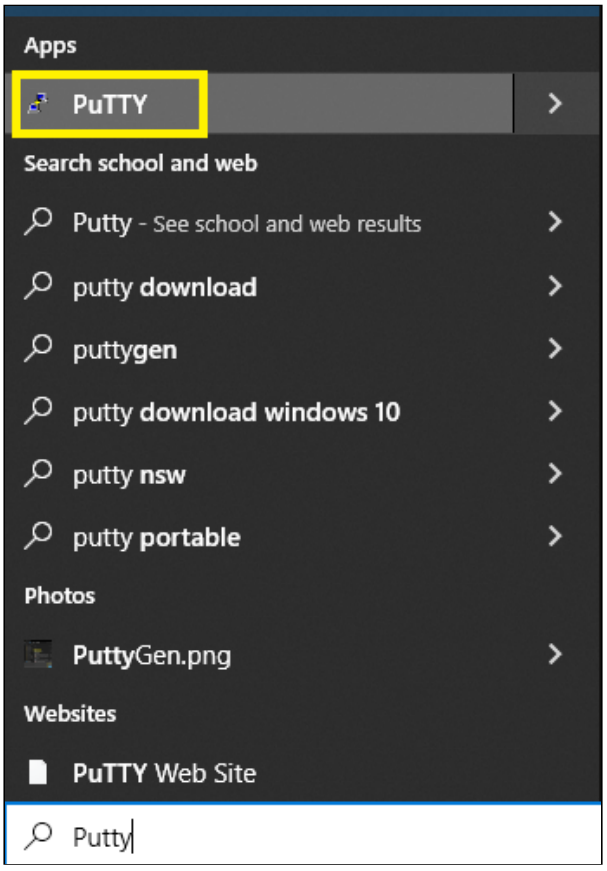
The app will launch in the background, please navigate to Taskbar and right-click on the Pageant app icon and click on Add Key



3. A pop window will open, now locate and add Private Key in the.PPK format which was previously saved.

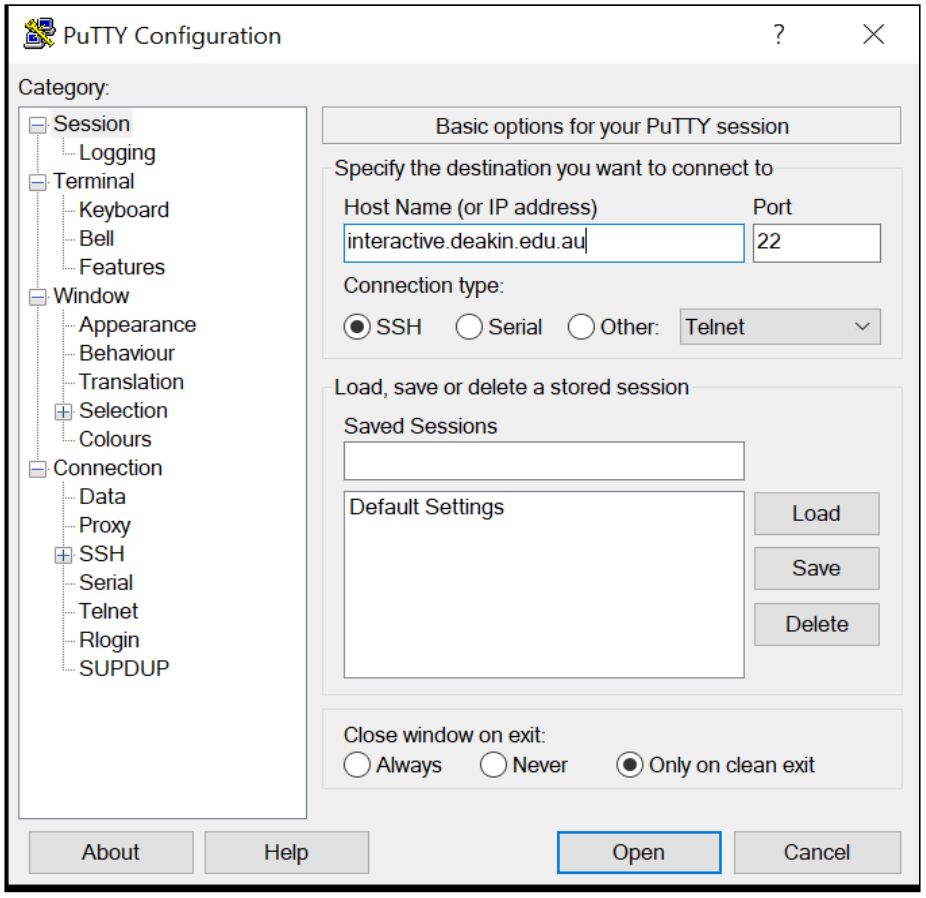
▼ **Step 4: Connecting to the SSID using PuTTY**

1. Click on Start Menu, search for **PuTTY**

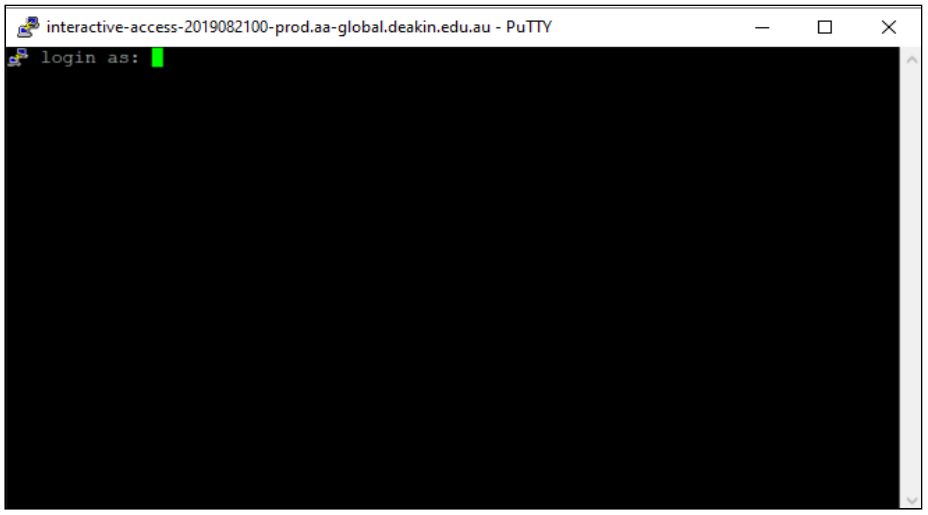


2. Open **PuTTY.**

3. Enter the host (**interactive.deakin.edu.au**) and port (**22**) and click on **open.**

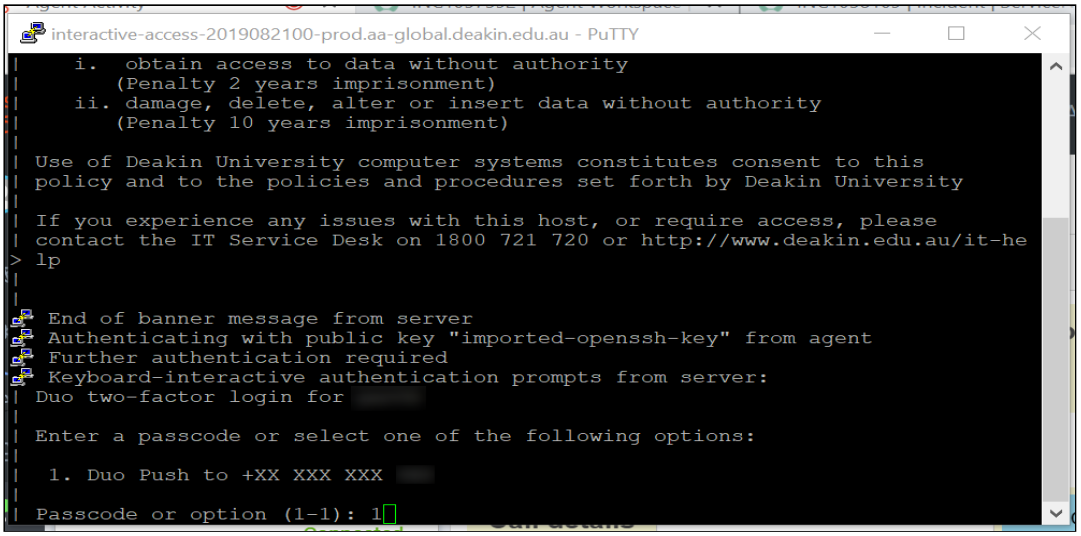


4. You may see a warning, click on **Yes** and the **login window will now open**

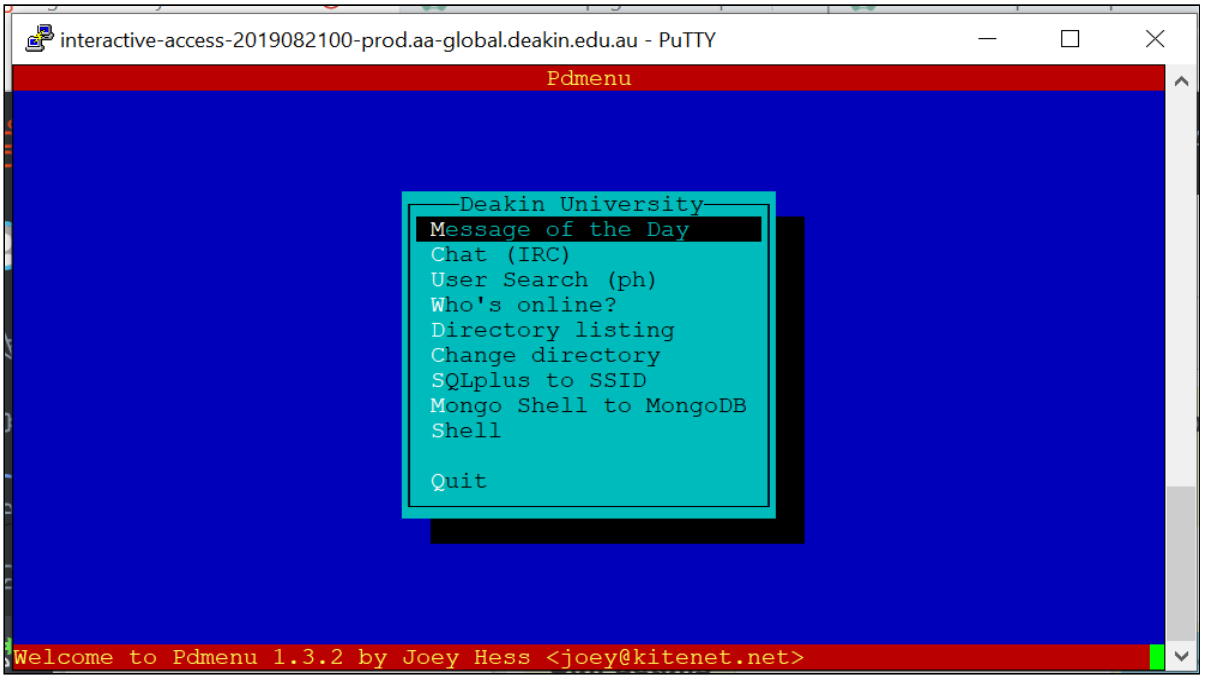


5. Enter your **Deakin username and press enter.**

6. You will be prompted authentication method for DUO**. Enter 1 to send the Duo Push request for the Multi-factor Authentication or enter the PIN from the DUO app.**



7. Once Approved or PIN is entered from the DUO app, you will be connected to SSID successfully.



If you connect to the interactive host and the menu does not appear, it is most likely that you have a corrupt **.bashrc** file.

To fix this:

1. Delete .bashrc
   - **If on-campus:** Delete the file from your home directory using **rm ~/.bashrc**.
   - **If off-campus:** Use the command **rm .bashrc**.

2. Re-login to **interactive.deakin.edu.au**.

The file will be recreated with the correct contents.

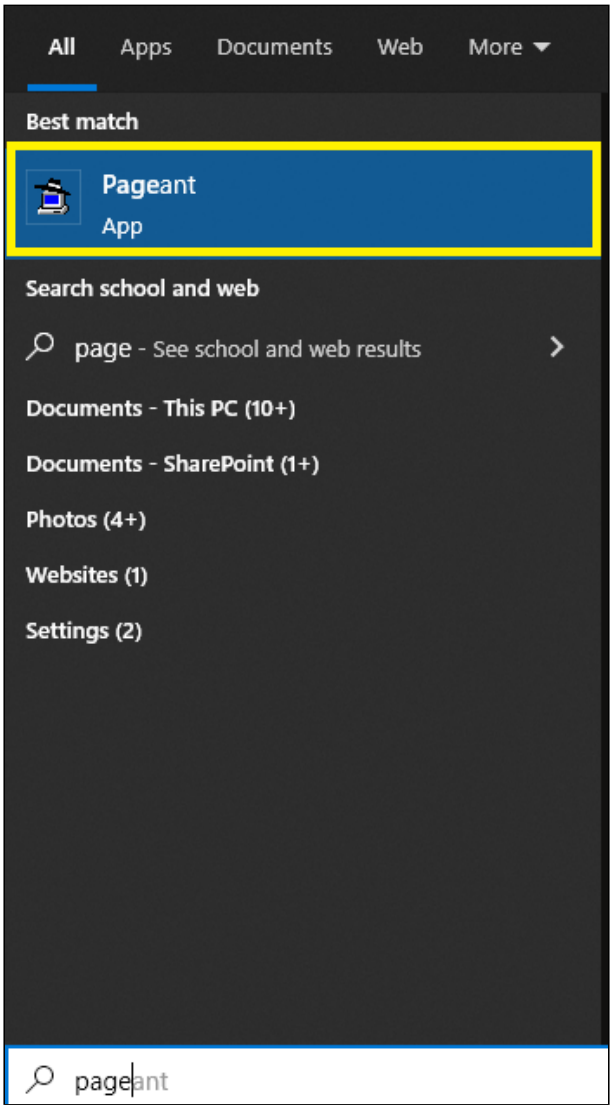
Windows - Consecutive login to SSID

If you have already completed the initial setup or if you restart your computer, please follow the steps below.

Please click on the relevant step number to expand the detailed instructions.

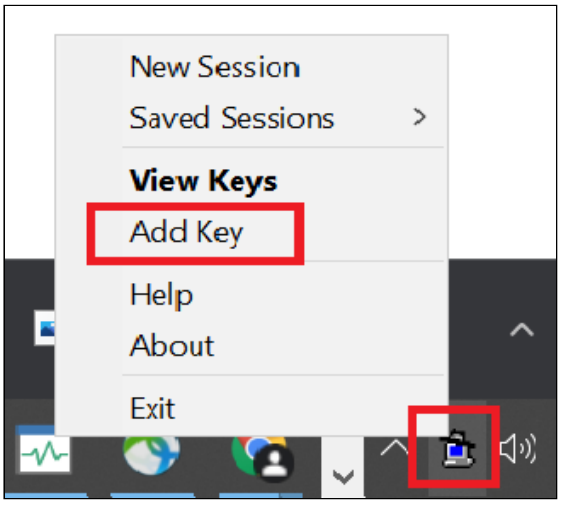
▼ **Step 1: Opening Pagent and adding the Key**

1. Click on **Start Menu, search** for **Pageant**



2. Click on **Pageant**

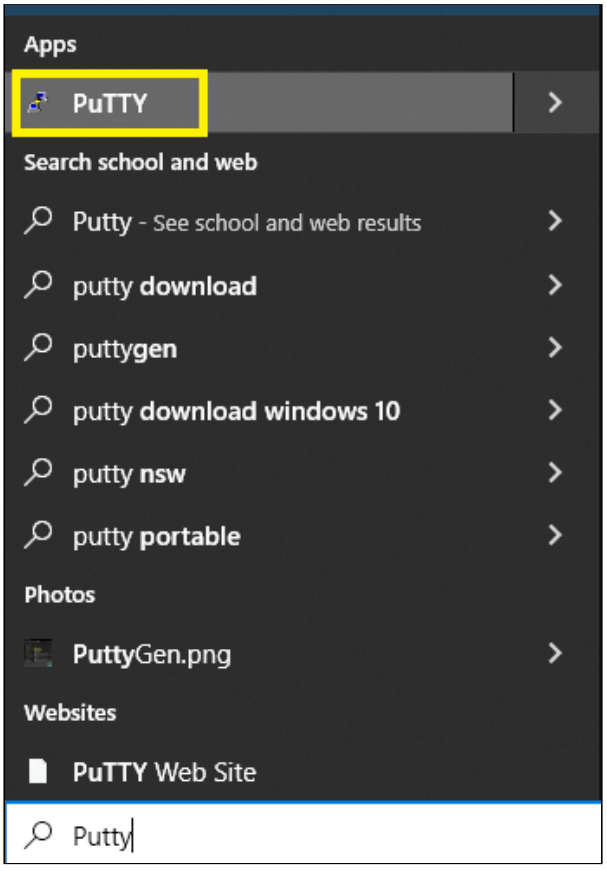
The app will launch in the background, please navigate to Taskbar and right-click on the Pageant app icon and click on Add Key



3. A pop window will open, now locate and add Private Key in the.PPK format which was previously saved.

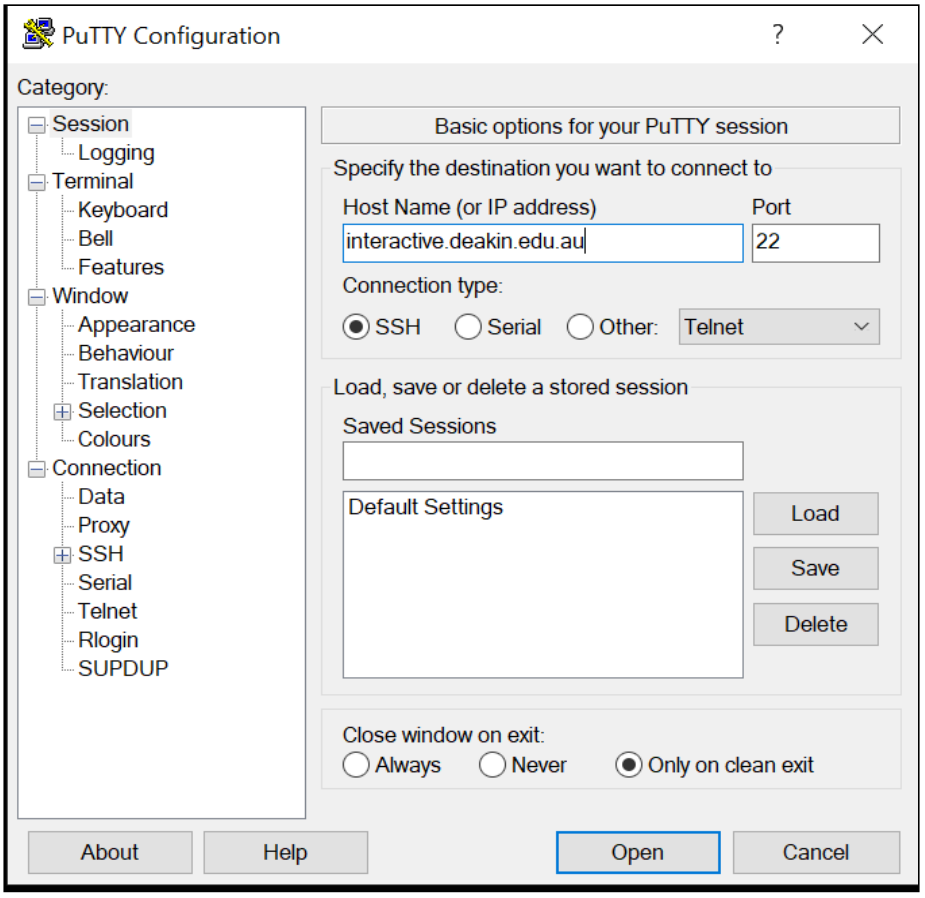
▼ **Step 2: Opening PuTTY and accessing SSID**

1. Click on Start Menu, search for **PuTTY**

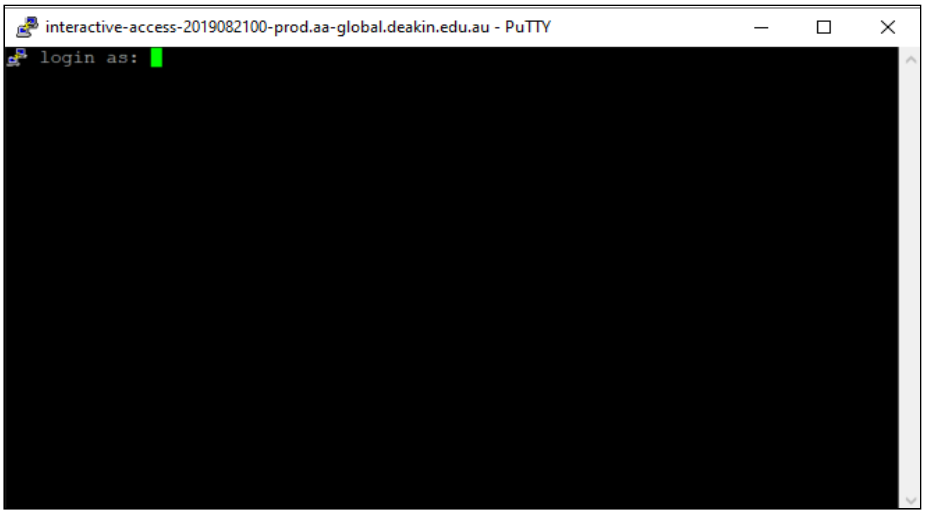


2. Open **PuTTY.**

3. Enter the host (**interactive.deakin.edu.au**) and port (**22**) and click on **open.**

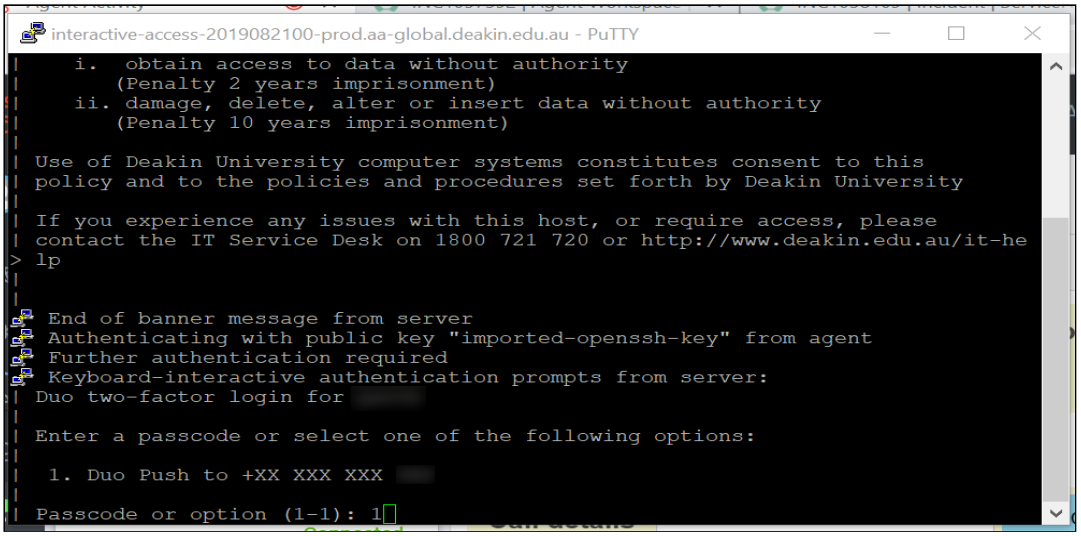


4. You may see a warning, click on **Yes** and the **login window will now open**

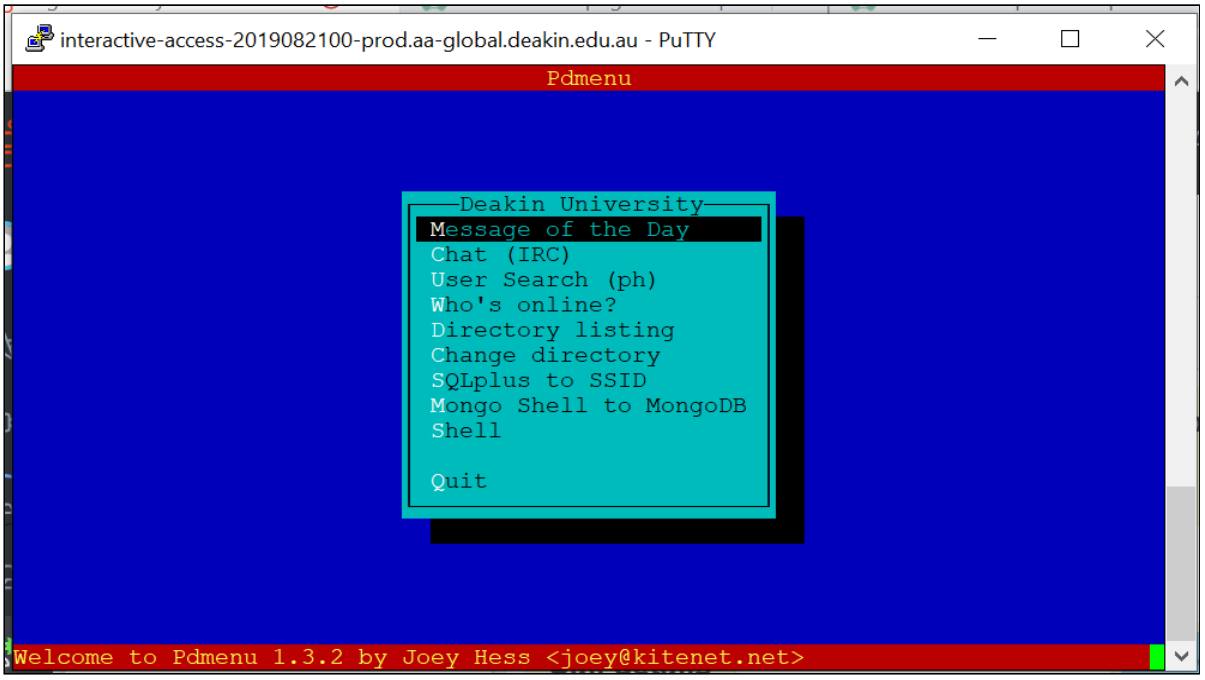


5. Enter your **Deakin username and press enter.**

6. You will be prompted authentication method for DUO**. Enter 1 to send the Duo Push request for the Multi-factor Authentication or enter the PIN from the DUO app.**



7. Once Approved or PIN is entered from the DUO app, you will be connected to SSID successfully.



Mac - Connecting to SSID for the first time

Please ensure that you are connected to the Cisco Anyconnect VPN: Cisco AnyConnect (VPN) – Installation & Usage Instructions (macOS).

For macOS and Linux platforms, SSH keys are generated via Terminal command and saved locally.

Please click on the relevant step number to expand the detailed instructions.

▼ Step 1: Generating a Public Key

1. Open Terminal and enter the following command:

ssh-keygen -t rsa -b 2048

```
— -bash — 80×24
Last login: Thu Nov 11 13:20:42 on ttys000

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
s-MacBook-Pro:~ $ ssh-keygen -t rsa -b 2048
```

2. Enter a location to save the Public and Private Keys. The default path is the '.ssh' folder in your Home Directory.

Please enter the following path: **/Users/username/.ssh/id_rsa**

```
— ssh-keygen -t rsa -b 2048 — 80×24
Last login: Thu Nov 11 13:20:42 on ttys000

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
-MacBook-Pro:~ $ ssh-keygen -t rsa -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/ /.ssh/id_rsa): /Users/ /.ss
h/id_rsa
/Users/ /.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
```

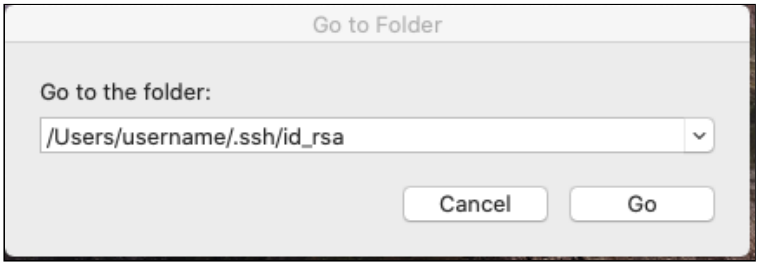
3. If the file already exists then type **Y** to go on to the next step.

4. A passphrase is highly recommended, but not mandatory. Please type the password if you want to continue with the passphrase, otherwise simply press enter to continue.

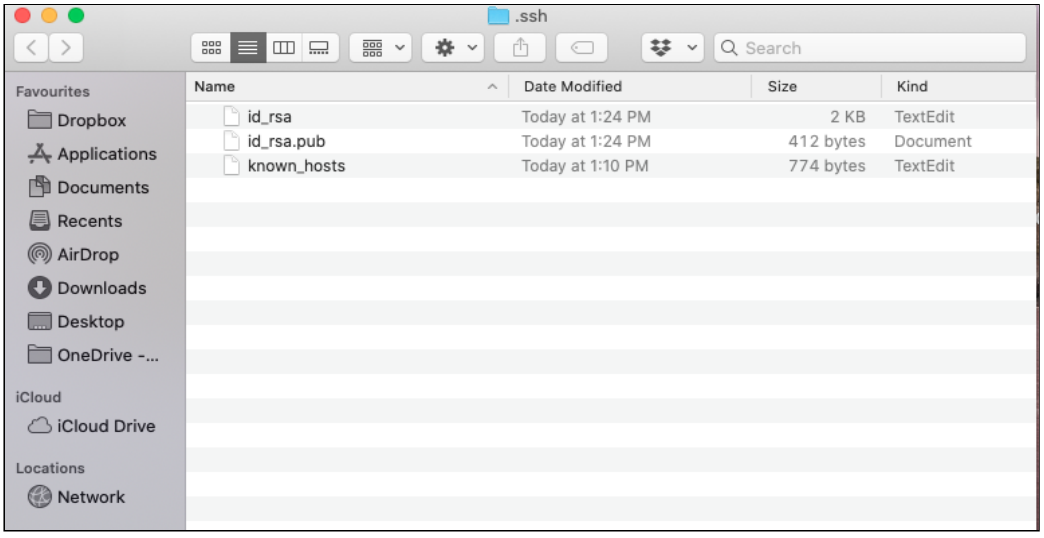
```
— -bash — 80×24
Enter file in which to save the key (/Users/[redacted]/.ssh/id_rsa): /Users/[redacted]/.ss
h/id_rsa
/Users/[redacted]/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/[redacted]/.ssh/id_rsa.
Your public key has been saved in /Users/[redacted]/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:Xs7i9P1Xf/J0SGBaL09h1xITPH+Wpcmb8fKIHVgSbiE [redacted]@[redacted]s-MacBook-Pro.loca
l
The key's randomart image is:
+---[RSA 2048]----+
|              .+. |
|           E o ooo|
|            o+++==|
|            +++*=+|
|         S o..+++.|
|        . +  .==.o|
|         + o  oo==|
|        o o .. +.*|
|         . . ...+o|
+----[SHA256]-----+
[redacted]s-MacBook-Pro:~ [redacted]$
```

5. Enter the **same passphrase** again and it will create the Public and Private key successfully.

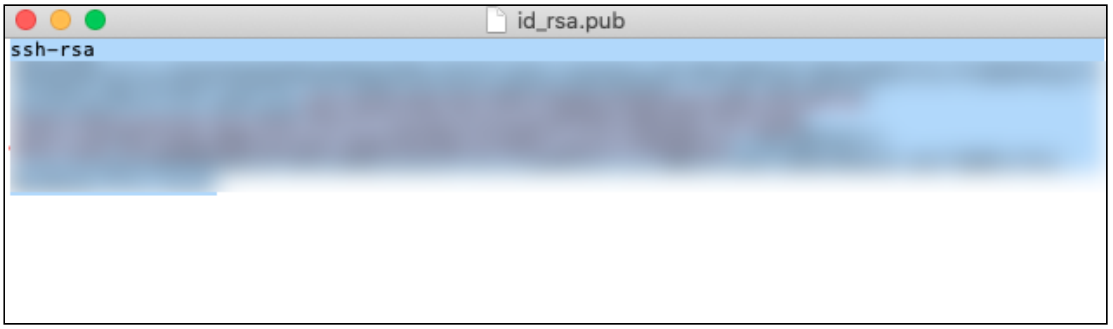
6. Go to the following folder from the Finder: **/Users/username/.ssh/id_rsa**



7. Two files should be created there. **id_rsa (Private key) and id_rsa.pub (Publick key)**

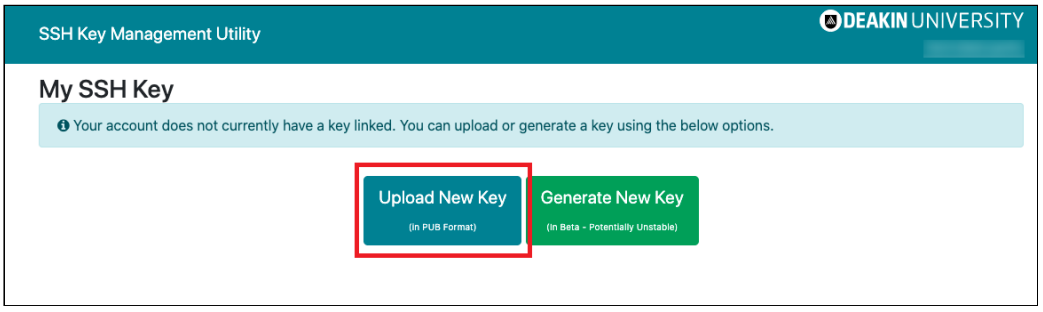


8. Open the id_rsa.pub file using any of the text editors software.

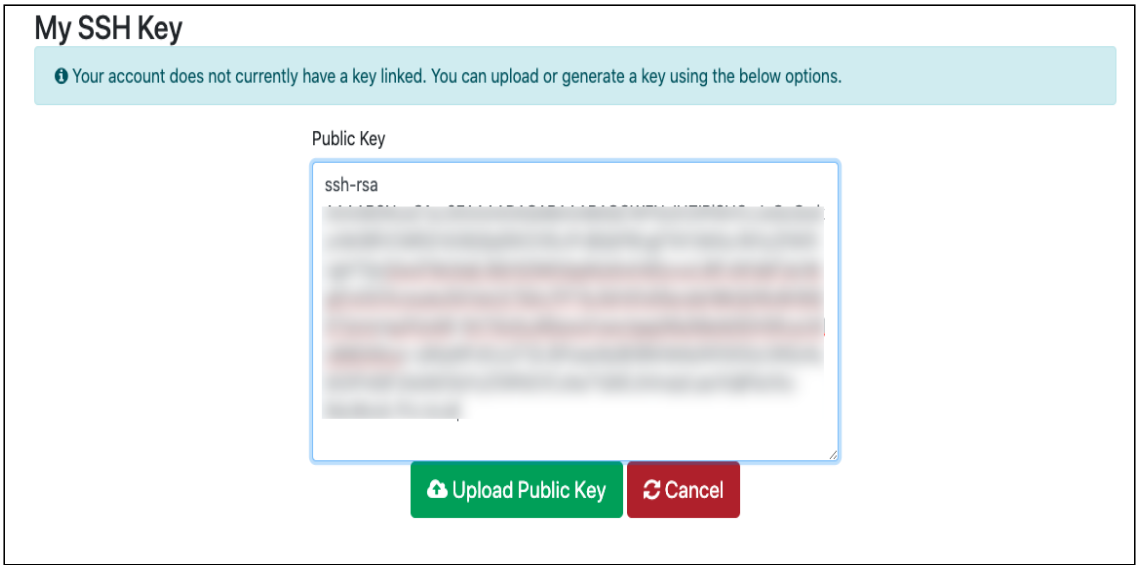


9. Copy the content of the file and Login to the SSH Key Management Utility

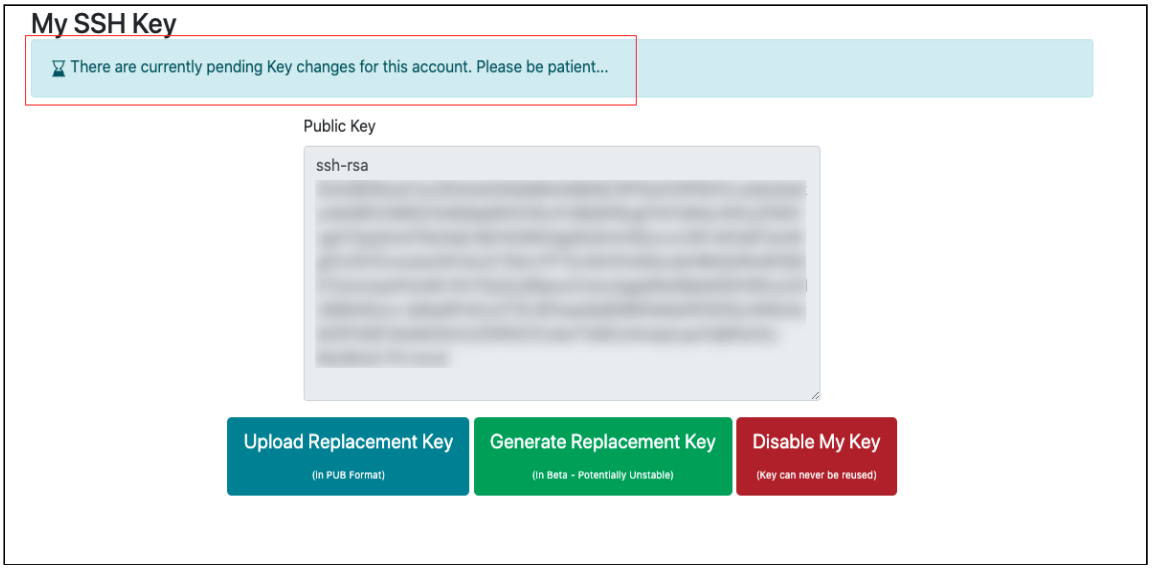
10. Click on the Upload New Key to upload the Public key



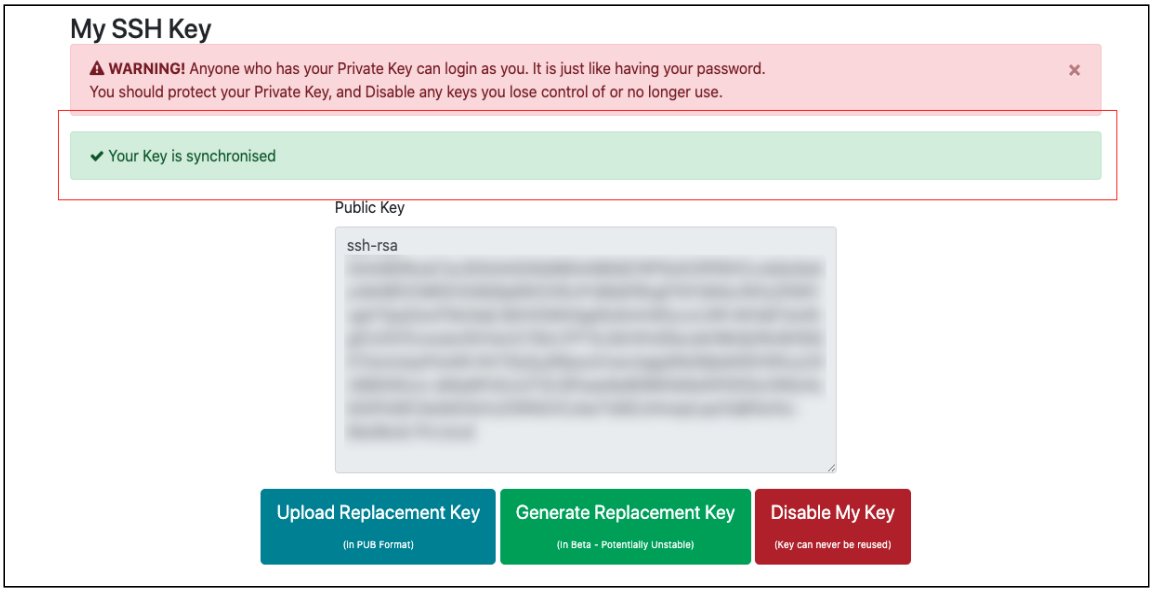
11. Paste the content of the id_rsa.pub file and select **Upload Public Key**



12. You will see a message advising, "There are currently pending key changes for this account. Please be Patient". Please wait until the changes are synchronised.



13. Once the changes will be synchronized, you will see the following message.



▶ **Step 2: Accessing your SSID**

Mac - Consecutive login to SSID

If you have already completed the initial setup or if you restart your computer, please follow the following steps.

1. Open **Terminal** and enter the **command ssh username@interactive.deakin.edu.au**. **Please replace the username with your Deakin username.**

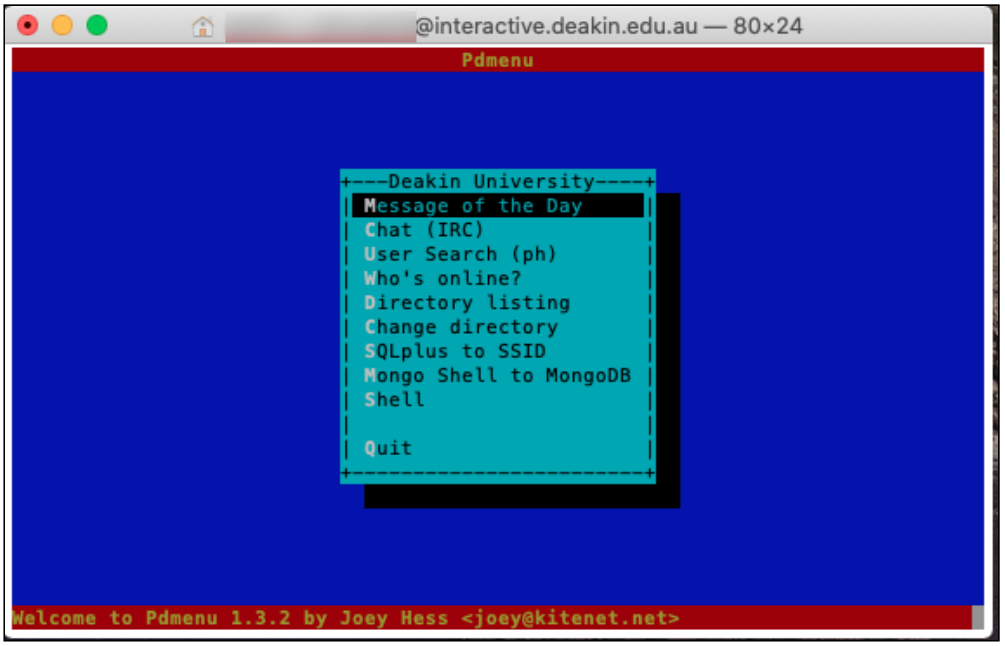
```
— -bash — 80×24
Last login: Thu Nov 11 13:21:42 on ttys000

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
s-MacBook-Pro:~ $ ssh username@interactive.deakin.edu.au
```

2. If you have set the password for a passphrase, then you will need to type the password to go on to the next step.

3. You will be prompted authentication method for DUO**. Enter 1 to send the Duo Push request for the Multi-factor Authentication or enter the PIN from the DUO app.**

```
.deakin.edu.au — 80×24
for authorised purposes. Evidence of unauthorised use may be used for
criminal prosecution by University staff, legal counsel and law
enforcement agencies.

It is a criminal offense to:
   i.  obtain access to data without authority
      (Penalty 2 years imprisonment)
   ii. damage, delete, alter or insert data without authority
      (Penalty 10 years imprisonment)

Use of Deakin University computer systems constitutes consent to this
policy and to the policies and procedures set forth by Deakin University

If you experience any issues with this host, or require access, please
contact the IT Service Desk on 1800 721 720 or http://www.deakin.edu.au/it-help


Duo two-factor login for

Enter a passcode or select one of the following options:

 1. Duo Push to +XX XXX XXX

Passcode or option (1-1): 1
```

4. Once Approved or PIN is entered from the DUO app, you will be connected to SSID successfully.



Connecting via the web

You can access your SSID database from the web in many different ways. One of the most popular ways to access databases from the web is using PHP.

Here is a small example of what you will need to connect to SSID from the web using PHP.

```
<?
$dbuser = "gary"; // Your user name here
$dbpass = "garyspassword"; // Your password here
$db = "SSID";
$connect = OCILogon($dbuser, $dbpass, $db);
$query = "grant select on phnum to barry";
$command = ociparse($connect, $query);
ociexecute($command);
ocilogoff();
?>
```

This example will connect to SSID as the user 'gary' and execute the query 'grant select on phnum to barry'.

eSolutions are not able to assist students with connecting to the database in this manner.

This example is here simply as a guide.

Giving other users access to data

To grant other users access to data in your database, you will need to perform one of the following commands:

- This example will give the user 'barry' access to view the data within a table called 'phnum'
  SQL> grant select on phnum to barry;
- This will give 'barry' access to insert data into the table 'phnum'
  SQL> grant insert on phnum to barry;
- This will allow 'barry' to update/change data that is in the table 'phnum'
  SQL> grant update on phnum to barry;
- This will allow 'barry' to delete data from the table 'phnum':
  SQL> grant delete on phnum to barry;

To remove access, follow the examples below:

- This will stop 'barry' from viewing data in the table 'phnum'
  SQL> revoke select on phnum from barry;

- This will prevent 'barry' from doing anything with the table 'phnum'
  SQL> revoke update, insert, delete on phnum from barry;

Backup data in SSID

Each night eSolutions automatically backs up data within the database. However, it is a good idea to create a backup of your data yourself.

Here is an example of how to do it:

```
bash$ export ORACLE_HOME=/opt/oracle/product/client/12.1.0.2

bash$ export TWO_TASK=SSID

bash$ $ORACLE_HOME/bin/exp file=~/mybackup.dmp
```

You will be prompted for your username and password. Once this is completed all your data will now be backed up in the file **mybackup.dmp**.

Please note that if you do not **commit** changes to your data, it will not be saved, neither will it be backed up.

Restore data from a backup

To restore your data from a backup to the database you will need to do the following:

Ensure the tables you want to recover are not in the database
SQL> select table_name from user_tables;

If the table is in there you will need to drop it before you replace the table from your backup
SQL> drop table phnum;

Insert your table with the following commands

```
bash$ export ORACLE_HOME=/opt/oracle/product/client/12.1.0.2

bash$ export TWO_TASK=SSID

bash$ $ORACLE_HOME/bin/imp file=mybackup.dmp tables=phnum
```

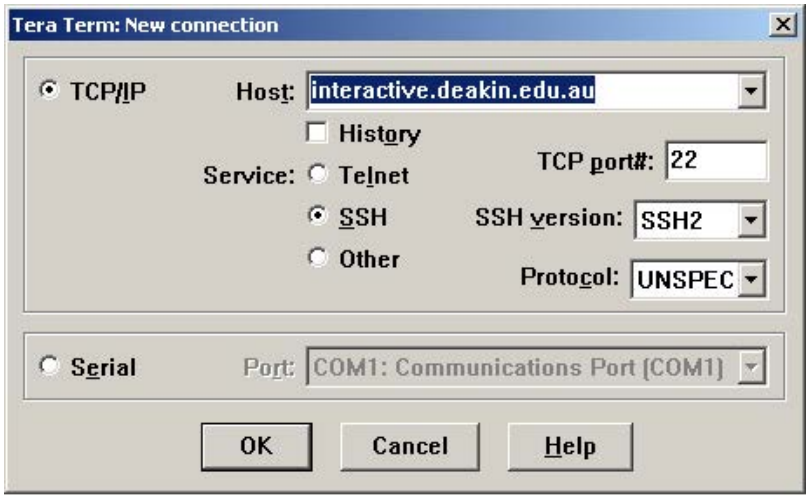
This command will replace the table phnum and all the data that was in it from the time you performed a backup (as above)

I get the following error: "ORA-01536: space quota exceeded for tablespace users"

This means that your database quota is full. Each user within SSID has been given 10MB of storage inside the database.

Settings for connecting to SSID via TeraTerm

- The TeraTerm connection settings should look like this:



Other Tips

- Ensure you log in with just your username and not your email address
- A good size to set the terminal window on a Deakin computer is 132 x 50. The Oracle command *set linesize 132* is also needed to take advantage of the resized window
- You can paste to Oracle, however, if the command is multi-line Oracle may echo back the line numbers after you paste in the command. This is not a problem. Copying out of Oracle will not work without editing, because you also get Oracle's line numbers and any other prompts mixed in with it
- While students cannot take Oracle home, they can Download TeraTerm

Copy Permalink

Helpful? Yes No

100% found this useful

Rate this article ☆☆☆☆☆

Most Useful

How to activate your Deakin IT account
Dan Perdrisat • 3686 Views • 4mo ago • ★★★☆☆

How do I clear my web history (Cookies & Cache)?
Matt Johansson • 457 Views • 12mo ago • ★★★★☆

Duo Mobile (MFA) – Install Duo Mobile on your new device
Aiden Walridge-Finlayson • 1043 Views • 4mo ago • ★★★★☆

Accessing your files in Apps and Desktops Anywhere
Jennifer Baker • 129 Views • 4mo ago • ★★★★☆

Microsoft Outlook – Forwarding Deakin Emails to Other Email Addresses
John Smart • 947 Views • 8mo ago • ★★★★★