How to log in to DSM with key pairs as admin or root permission via SSH on computers

https://www.synology.com/en-global/knowledgebase/DSM/tutorial/Management/How_to_log_in_to_DSM_with_key_pairs_as_admin_or_root_permission_via_SSH_on_computers?utm_source=account%20page&utm_medium=create%20ticket

Overview

With various file services, Synology NAS allows users to access shared folders and files over the Internet on their computers. By configuring key pairs access and root access, users can log in to DSM or even transfer file via SFTP without entering password from computers. For system security concerns, root access to Synology NAS via SSH is limited.

This article guides you through connecting to DSM with key pairs as admin and root permission via SSH from Windows and Mac computers.

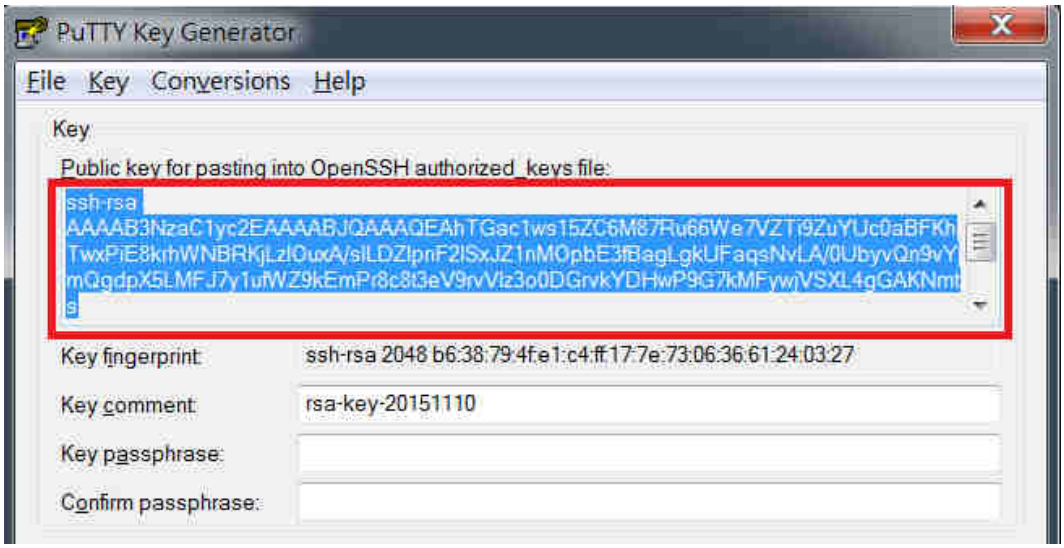
Note: Do not use Midnight Commander to create folders and files, as well as to assign access rights. Everything is done through the console. But you can insert a Public Key already using Midnight Commander
If you changed the host, but left the previous IP address, then do not forget to clear the cache of the old key `[HKEY_CURRENT_USER\SOFTWARE\SimonTatham\PuTTY\Ssh Host Keys]`

Contents

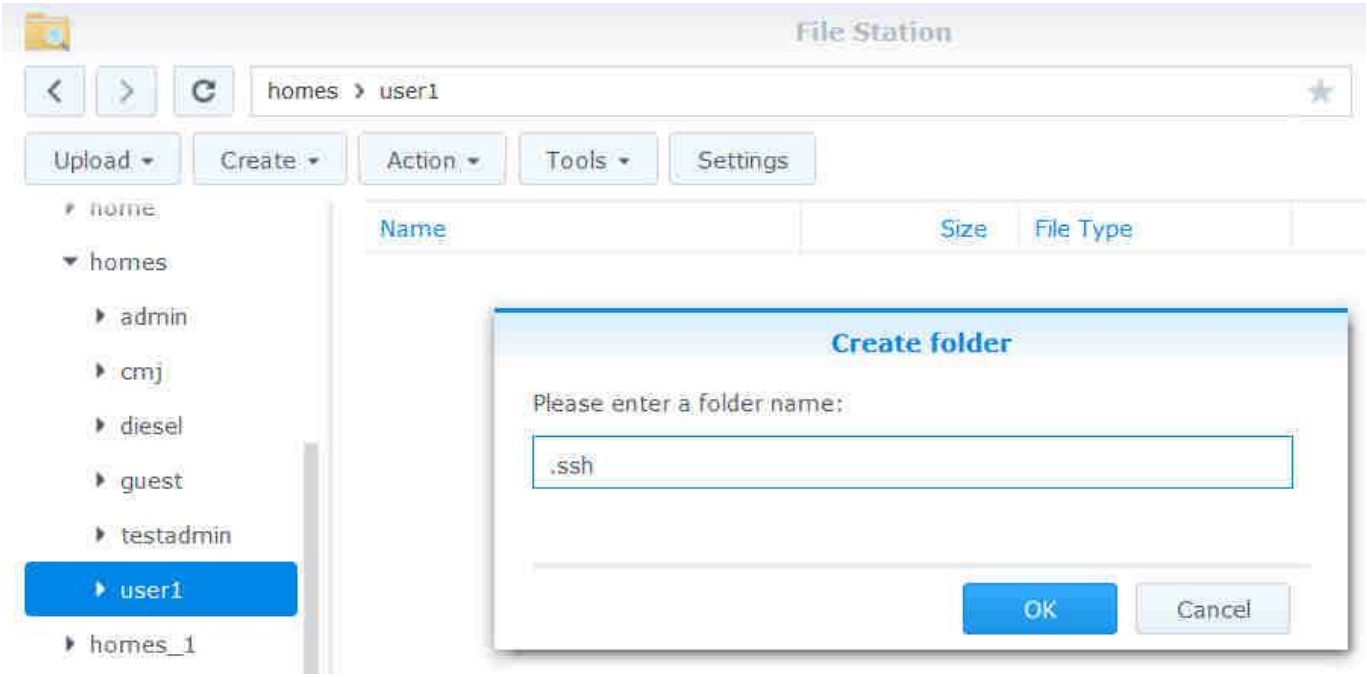
1. Login with key pairs as an administrator on Windows computer

This section explains how to log in DSM with key pairs as an administrator on your Windows computer.

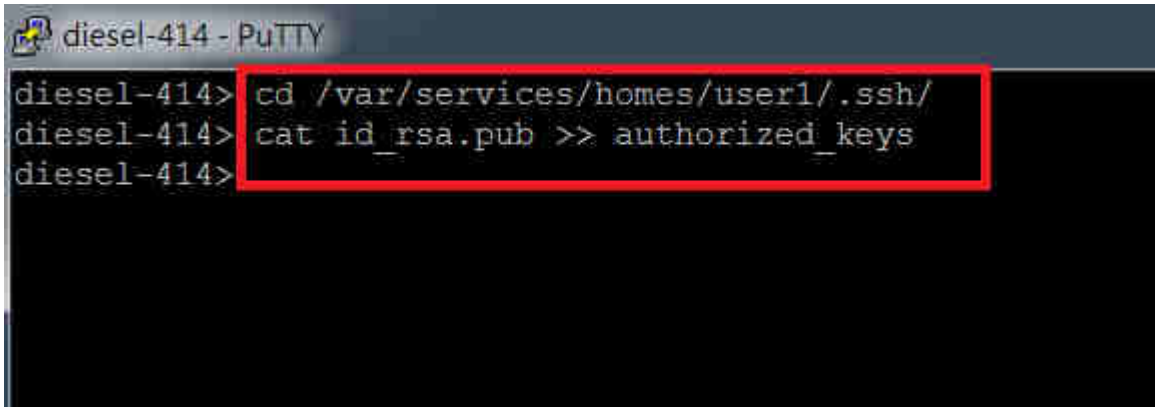
1. Log in to DSM using an account belonging to the **`Local Administrators`** group.
2. Go to **`Control Panel`** > **`Terminal & SNMP`** > **`Terminal`**, and check the box next to **`Enable SSH Service`** to allows your Synology NAS to support SSH command-line interface services.
3. Go to **`Control Panel`** > **`User`** > **`Advanced`** > **`User Home`**, and check the box next to **`Enable user home service`**.
4. Generate the private and public keys via PuTTYgen. Copy and save the text displayed in the enclosed window as a .txt file, and name it as **`id_rsa.pub`**.



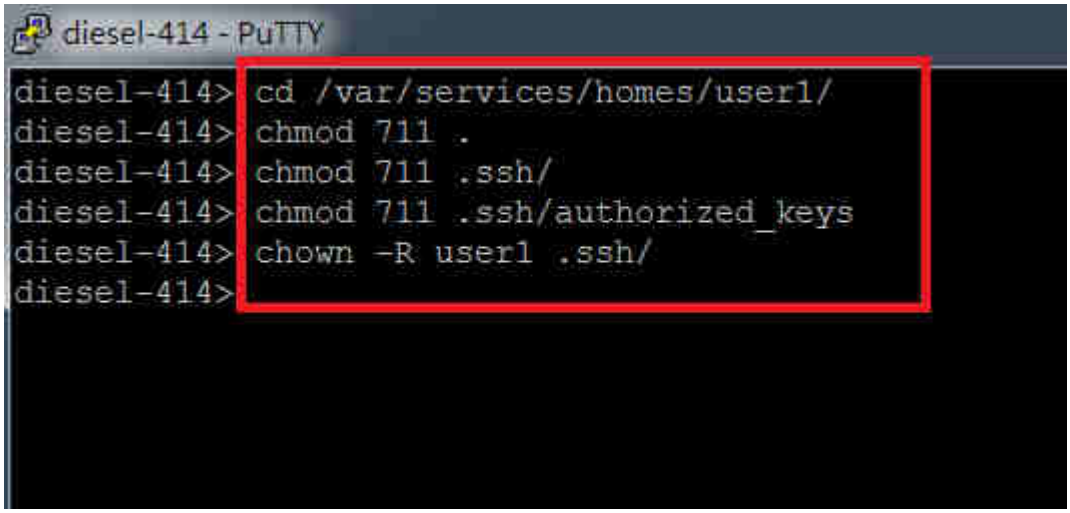
5. Create a ".ssh" folder in File Station, and upload the public key **`id_rsa.pub`** from the PC to the created folder (Path: home/.ssh/id_rsa.pub).



6. Login to DSM with root permission via SSH. Please refer to this article for more information.
7. Append the public key content to the existing **`authorized_keys`** file by executing the enclosed commands below.



8. Execute the enclosed commands below to ensure the permissions of the user home folder, ".ssh", and file "authorized_keys" are 711.

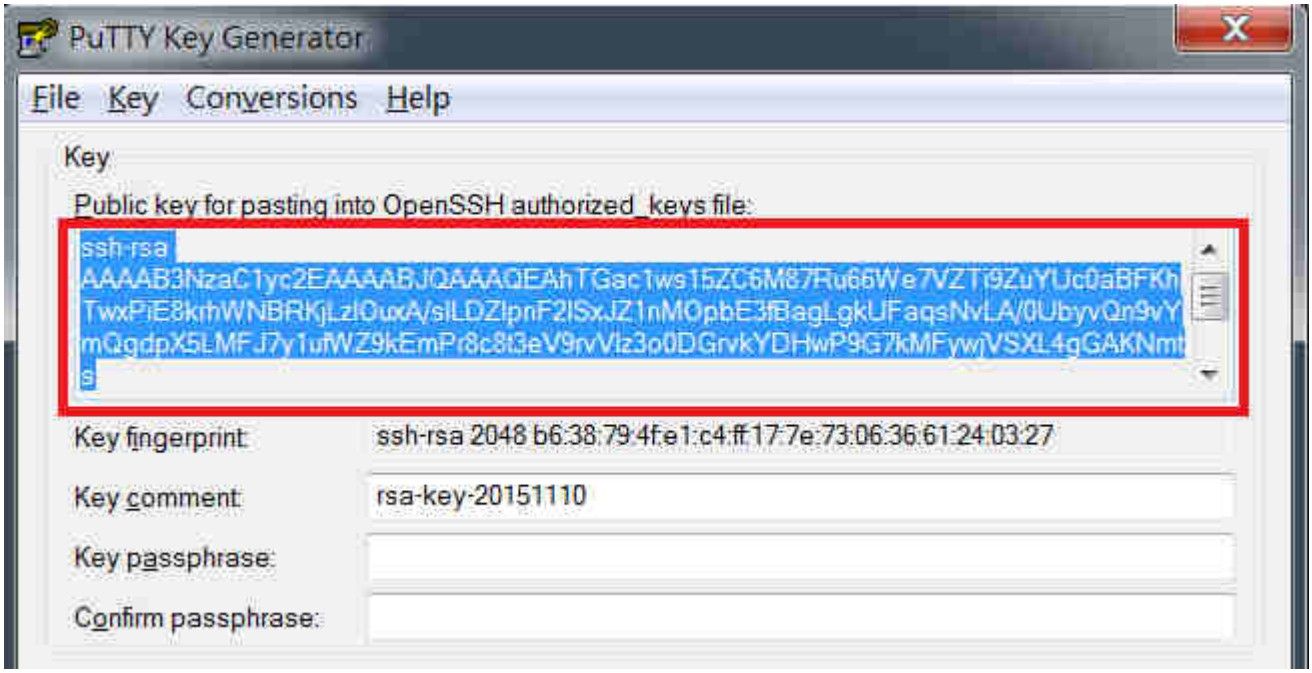


9. The specified DSM user can now connect to the Synology NAS via SSH without entering the password (in PuTTY).

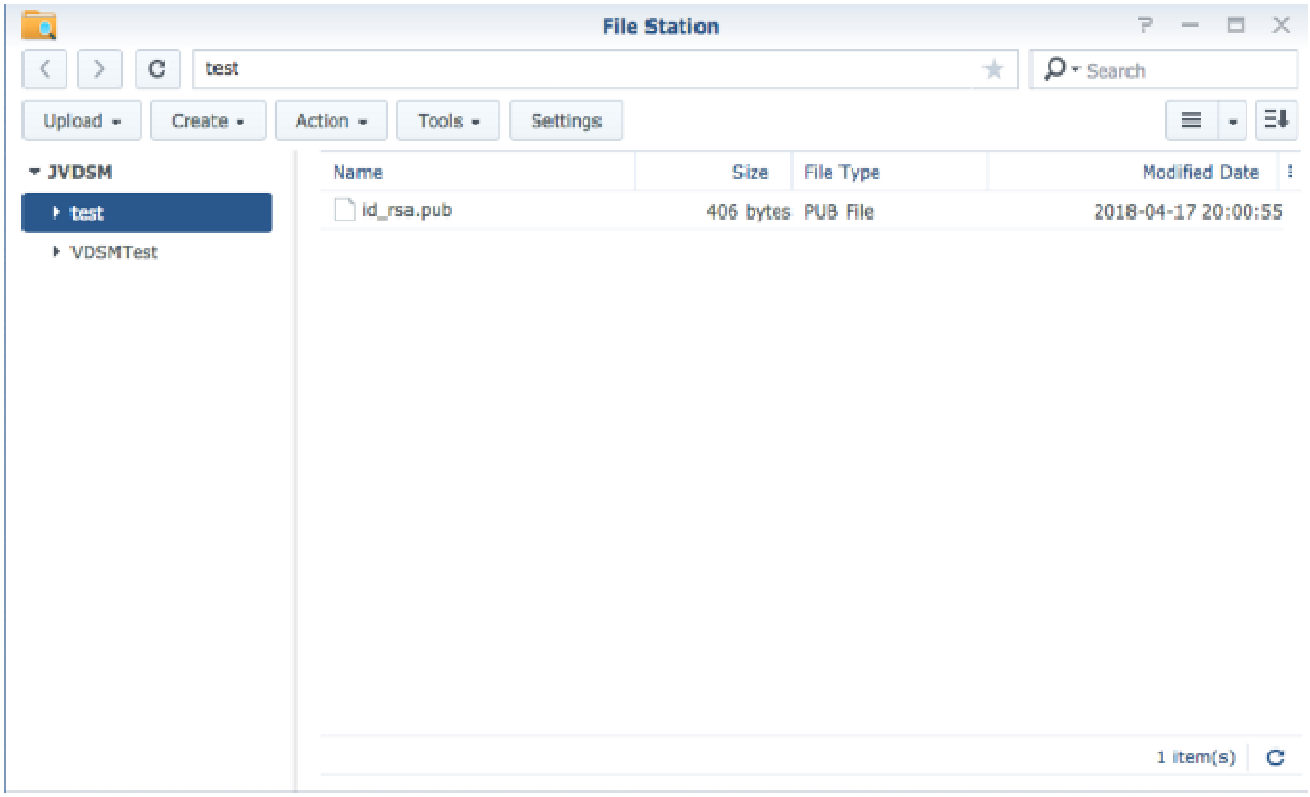
2. Login with root permission on Windows computer

This section explains how to log in DSM with root permission on your Windows computer.

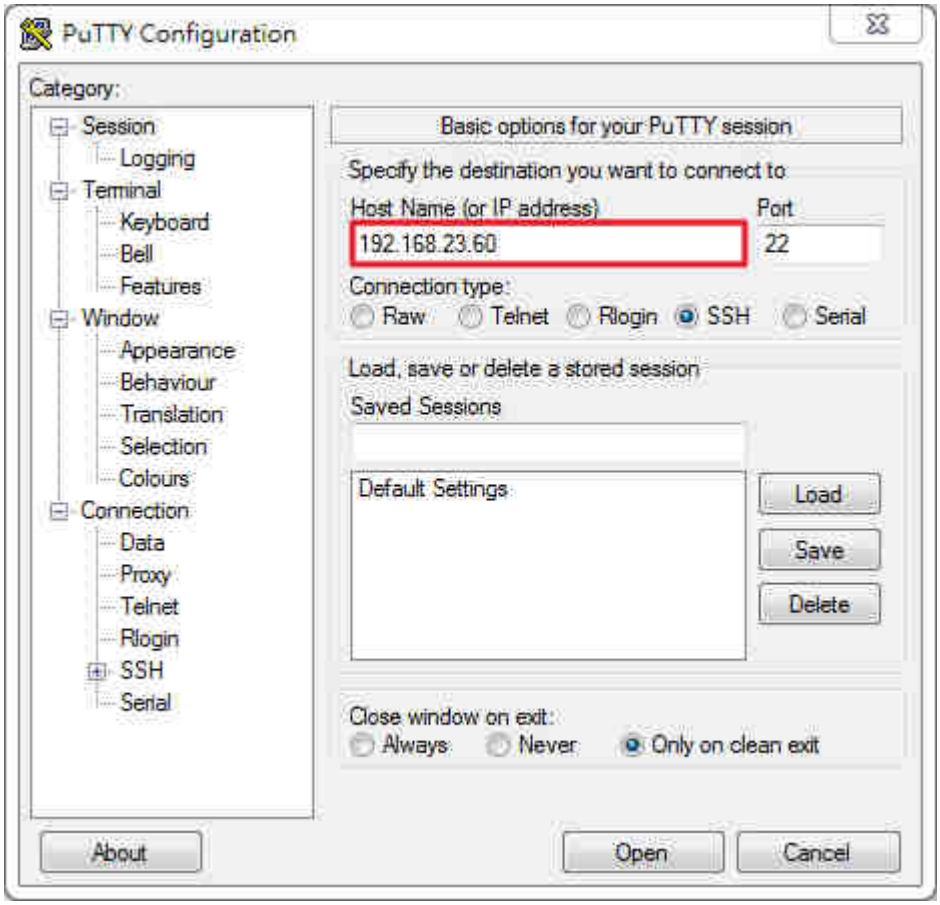
1. Generate the private and public keys via PuTTYgen. Copy and save the text displayed in the enclosed window as a .txt file, and name it as **`id_rsa.pub`**.



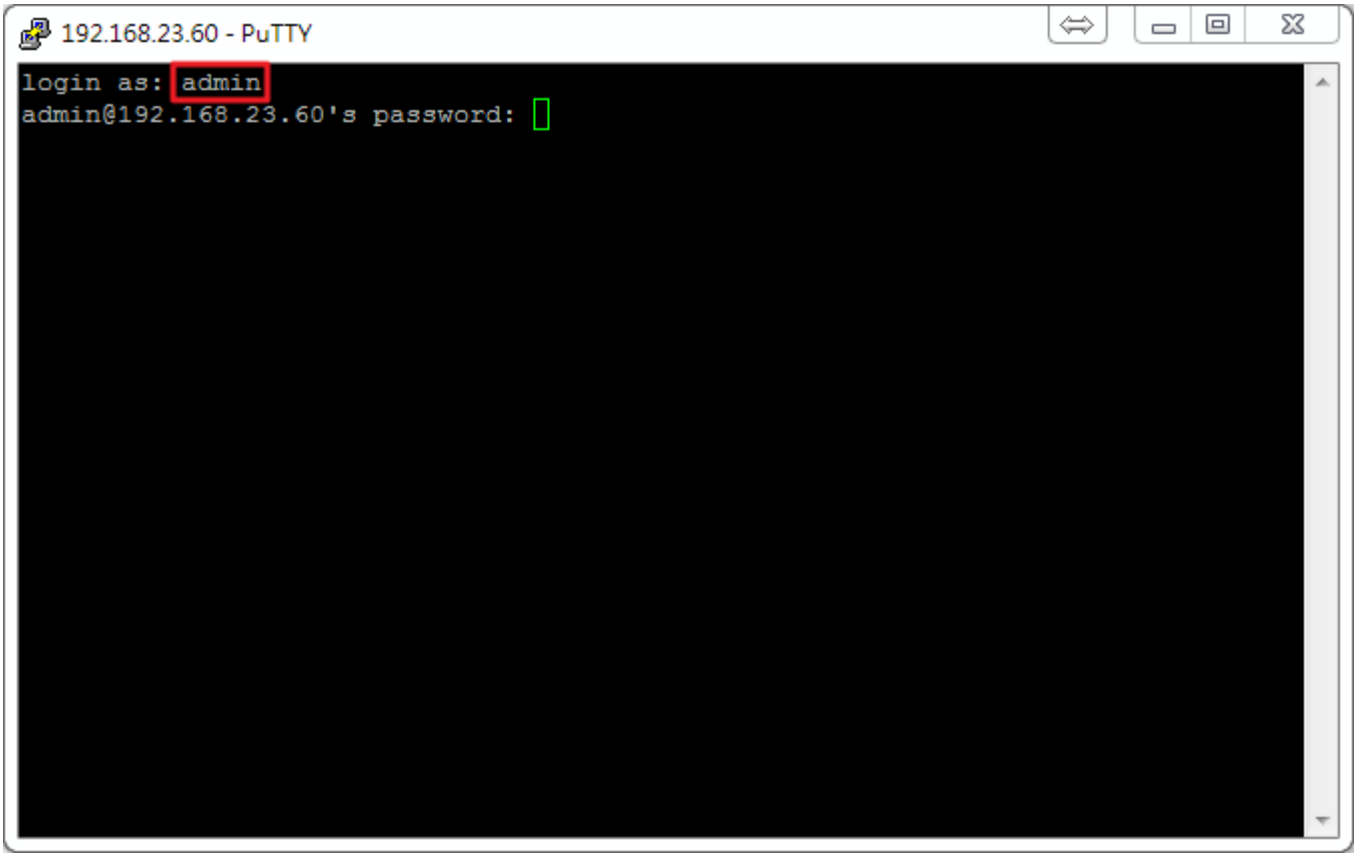
2. Upload the public key **`id_rsa.pub`** from the PC to a temporary folder in File Station on your DSM. For example, place it under the shared folder "**`test`**".



3. Use command line interface (e.g. PuTTY) to connect to DSM via SSH.



4. *login as: admin*: "admin" account belongs to the Local Administrators group on the NAS.



5. Append the public key content to a new **authorized_keys** file by executing the command below. (**/volumeX/test/id_rsa.pub**, **X** means the volume in which "**test**" shared folder is. Please replace it with your volume where the **id_rsa.pub** is.)

```
root@SUP-Jayw:~# cp /volumeX/test/id_rsa.pub /root/.ssh/authorized
```

6. Execute the enclosed commands below to ensure the permissions of the ".ssh" folder and the file "**authorized_keys**" are 700 which is equivalent to rwx.

```
root@SUP-Jayw:/# ll /root | grep ssh
drwx------  2 root root  4096 May 30 18:29 .ssh
```

Please also make sure the owner and group of "**authorized_keys**" is "root". If not, enter the command "chown root:root /root/.ssh/authorized_keys" to edit the permission.

```
root@SUP-Jayw:/# cd /root/.ssh/
root@SUP-Jayw:~/.ssh# ll
total 20
drwx------  2 root root 4096 May 30 18:29 .
drwx------ 10 root root 4096 Sep 20 17:40 ..
-rwx------  1 root root  406 Apr 17 20:00 authorized_keys
-rw-r--r--  1 root root 5845 Sep 27 11:20 known_hosts
```

7. The specified DSM user can now connect to the Synology NAS via SSH without entering the password.

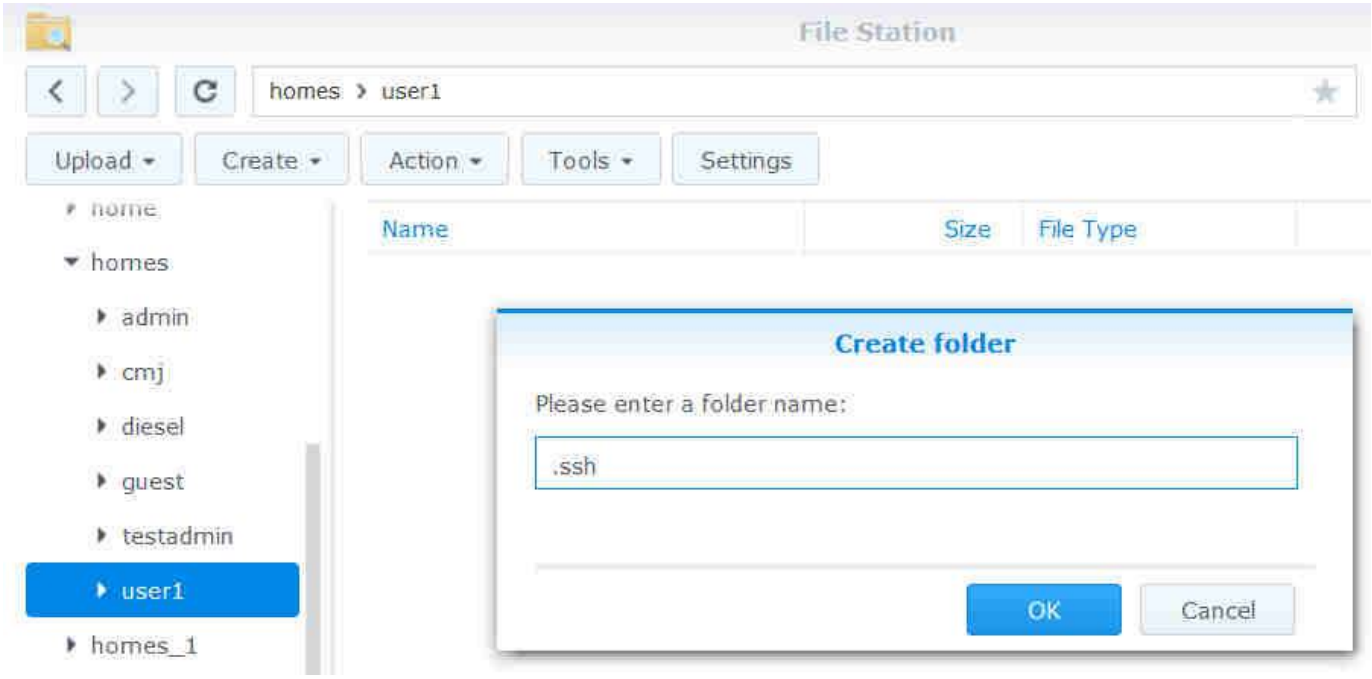
3. Login with key pairs as an administrator on Mac computer

This section explains how to log in DSM with key pairs as an administrator on your Mac computer.

1. Log in to DSM using an account belonging to the **Local Administrators** group.
2. Go to **Control Panel** > **Terminal & SNMP** > **Terminal**, and check the box next to **Enable SSH Service** to allows your Synology NAS to support SSH command-line interface services.
3. Go to **Control Panel** > **User** > **Advanced** > **User Home**, and check the box next to **Enable user home service**.
4. Generate the private and public keys via command lines:
    a. Launch the built-in Terminal app on Mac computer to generate key pairs.
    b. Execute the command "ssh-keygen" on the console. The public key **id_rsa.pub** and the private key **id_rsa** will be generated in the specified path. When migrating the private key to another device, make sure to use encrypted transfer via HTTPS, FTPS, or SFTP to prevent key leakage.

```
[redacted]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/jay/.ssh/id_rsa):
/Users/jay/.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/jay/.ssh/id_rsa.
Your public key has been saved in /Users/jay/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:7RwSUOTf7zABAZCrnLSY1MT0dap2QA02V5YB5rrG2Vw jay@jayde-Mac-mini.local
The key's randomart image is:
+---[RSA 2048]----+
|    o. BBO+*o    |
|     o+.O.+..    |
|    o  o.= .     |
|   . o .+ + o    |
|  . = ++ S E o   |
|   o =o * = . o  |
|       = o o o . |
|      .      +   |
|             .   |
+----[SHA256]-----+
```

5. Create a ".ssh" folder in File Station, and upload the public key **id_rsa.pub** from the PC to the created folder (Path: home/.ssh/id_rsa.pub).



6. Login to DSM with root permission via SSH. Please refer to this article for more information.
7. Append the public key content to a new **authorized_keys** file by executing the command below. There will be two files, **authorized_keys** and **id_rsa.pub**, in the **.ssh** folder.

```
root@SUP-Jayw:/var/services/homes/jay/.ssh# cat id_rsa.pub >> authorized_keys
root@SUP-Jayw:/var/services/homes/jay/.ssh# ll
total 8
drwx--x--x+ 1 root  root   50 Sep 27 13:45 .
drwx--x--x+ 1 jay   users  24 Sep 27 13:35 ..
-rwx--x--x+ 1 root  root  406 Sep 27 13:45 authorized_keys
-rwx--x--x+ 1 admin users 406 Sep 27 13:42 id_rsa.pub
```

8. Execute the commands below to ensure the permissions of the user home folder, ".ssh", and file "authorized_keys" are 711.

```
root@SUP-Jayw:/var/services/homes/jay/.ssh# cd /var/services/homes/jay/
root@SUP-Jayw:/var/services/homes/jay# chmod 711 .
root@SUP-Jayw:/var/services/homes/jay# chmod 711 .ssh/
root@SUP-Jayw:/var/services/homes/jay# chmod 711 .ssh/authorized_keys
root@SUP-Jayw:/var/services/homes/jay# chown -R jay .ssh/
root@SUP-Jayw:/var/services/homes/jay# exit
logout
Connection to 10.12.3.23 closed.
[redacted]:~ jay$ ssh jay@10.12.3.23
jay@SUP-Jayw:~$
```

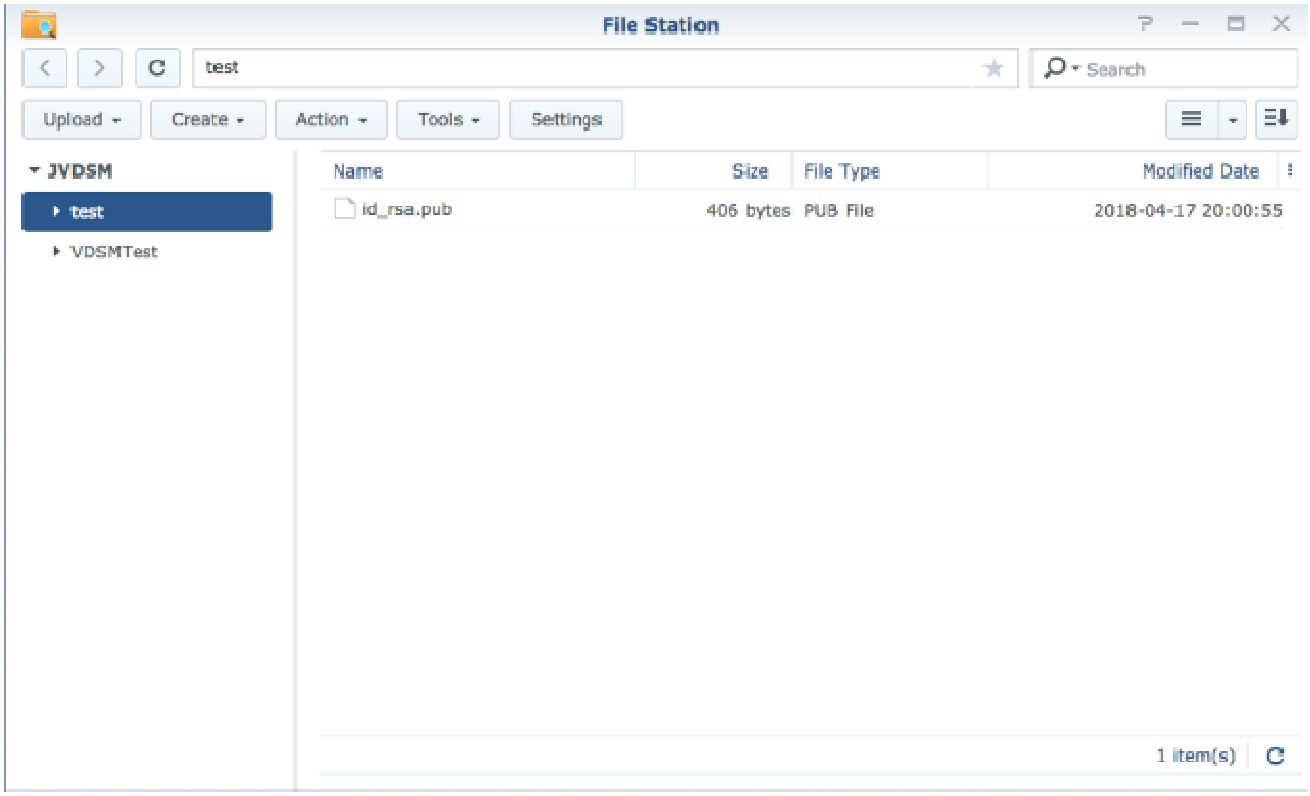
9. The specified DSM user can now connect to the Synology NAS via SSH without entering the password.

4. Login with root permission on Mac computer

This section explains how to log in DSM with root permission on your Mac computer.

1. Log in to DSM using an account belonging to the **Local Administrators** group.
2. Go to **Control Panel** > **Terminal & SNMP** > **Terminal**, and check the box next to **Enable SSH Service** to allows your Synology NAS to support SSH command-line interface services.

3. Please follow the instructions of step 4 in the previous section to generate the private and public keys via command lines.
4. Upload the public key **id_rsa.pub** from the PC to a temporary folder in File Station on your DSM. For example, place it under the shared folder "**test**".



5. Log in to DSM with root permission via SSH/Telnet. Please refer to this article for more information.
6. Append the public key content to a new **authorized_keys** file by executing the command below. (**/volumeX/test/id_rsa.pub**, **X** means the volume in which "**test**" shared folder is. Please replace it with your volume where the **id_rsa.pub** is.)

```
root@SUP-Jayw:~# cp /volumeX/test/id_rsa.pub /root/.ssh/authorized_keys
```

7. Execute the enclosed commands below to ensure the permissions of the ".ssh" folder and the file "**authorized_keys**" are 700 which is equivalent to rwx.

```
root@SUP-Jayw:/# ll /root | grep ssh
drwx------  2 root root  4096 May 30 18:29 .ssh
```

Please also make sure the owner and group of "**authorized_keys**" is "root". If not, enter the command "chown root:root /root/.ssh/authorized_keys" to edit the permission.

```
root@SUP-Jayw:/# cd /root/.ssh/
root@SUP-Jayw:~/.ssh# ll
total 20
drwx------  2 root root 4096 May 30 18:29 .
drwx------ 10 root root 4096 Sep 20 17:40 ..
-rwx------  1 root root  406 Apr 17 20:00 authorized_keys
-rw-r--r--  1 root root 5845 Sep 27 11:20 known_hosts
```

8. The specified DSM user can now connect to the Synology NAS via SSH without entering the password.