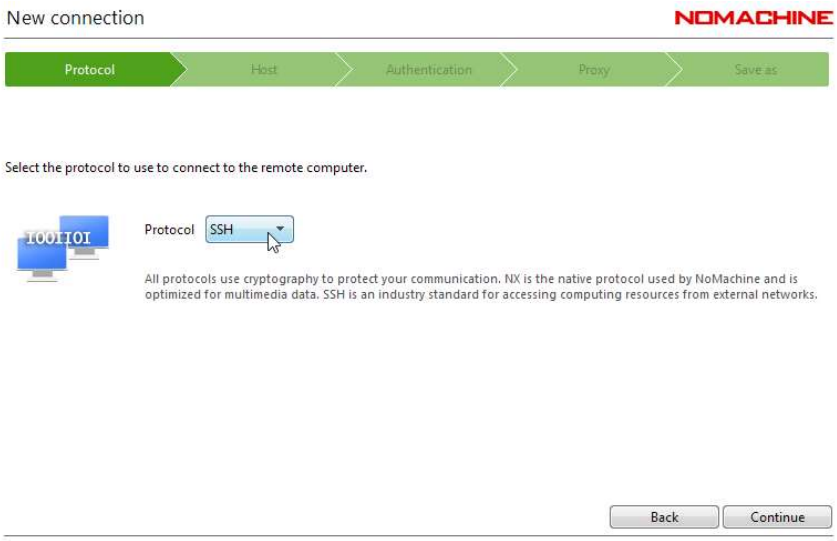
Installing, configuring and Using NX NoMachine to connect to the Redhawk3 Cluster

NoMachine (also called NX) is a tool that can be used to connect to Miami's Redhawk3 cluster when a graphical desktop interface is needed. This document outlines how to install and use NX NoMachine.
NoMachine is available for Windows, Mac and Linux platforms.

Download the required file

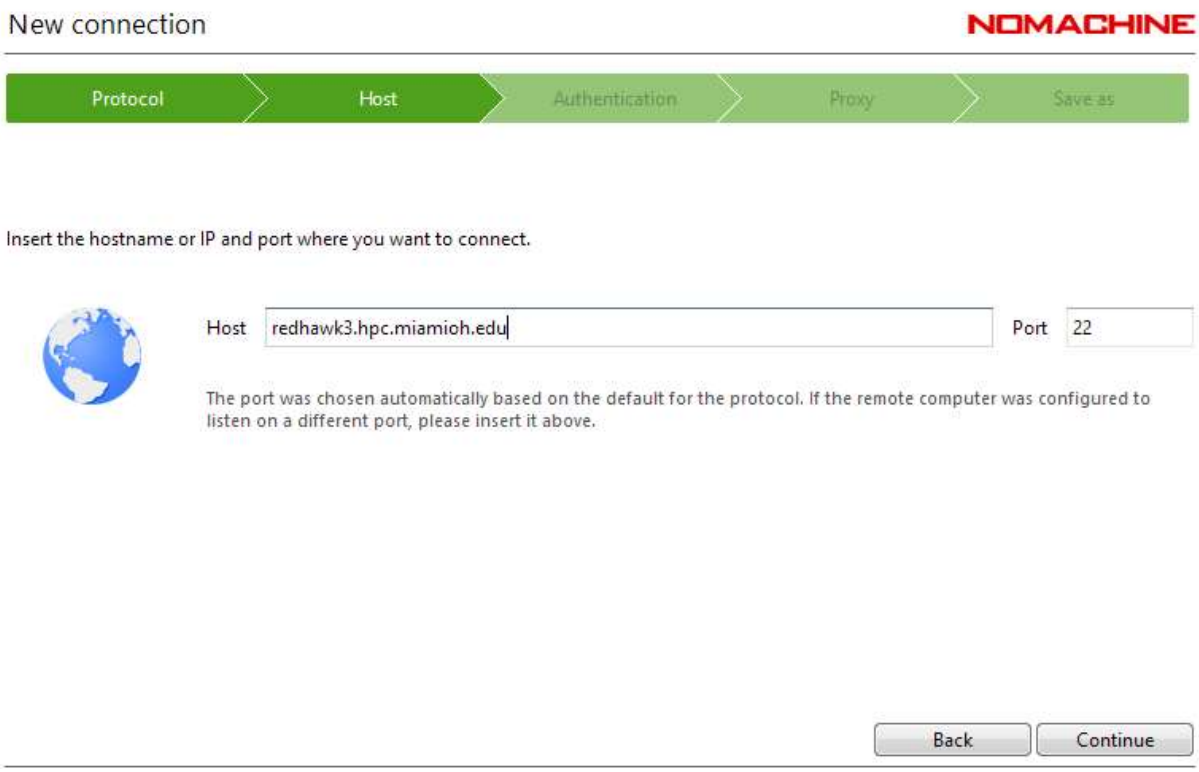
Visit https://www.nomachine.com/ and download the installer by clicking the suggested link.
Once the download has completed, double-click the installer and install the software.
Navigate to the start menu and launch NX. This brings up the Welcome screen and the interface to configure the tool.
Create a "New" connection.

Select "SSH" as the required protocol.



Hit “Continue”.

The hostname is “redhawk3.hpc.miamioh.edu”. Alternatively, the traditional “redhawk.hpc.miamioh.edu” can be used in the near future.



Miami is implementing a new universal authentication policy in the fall of 2018 which will apply to the Redhawk3 cluster as well.

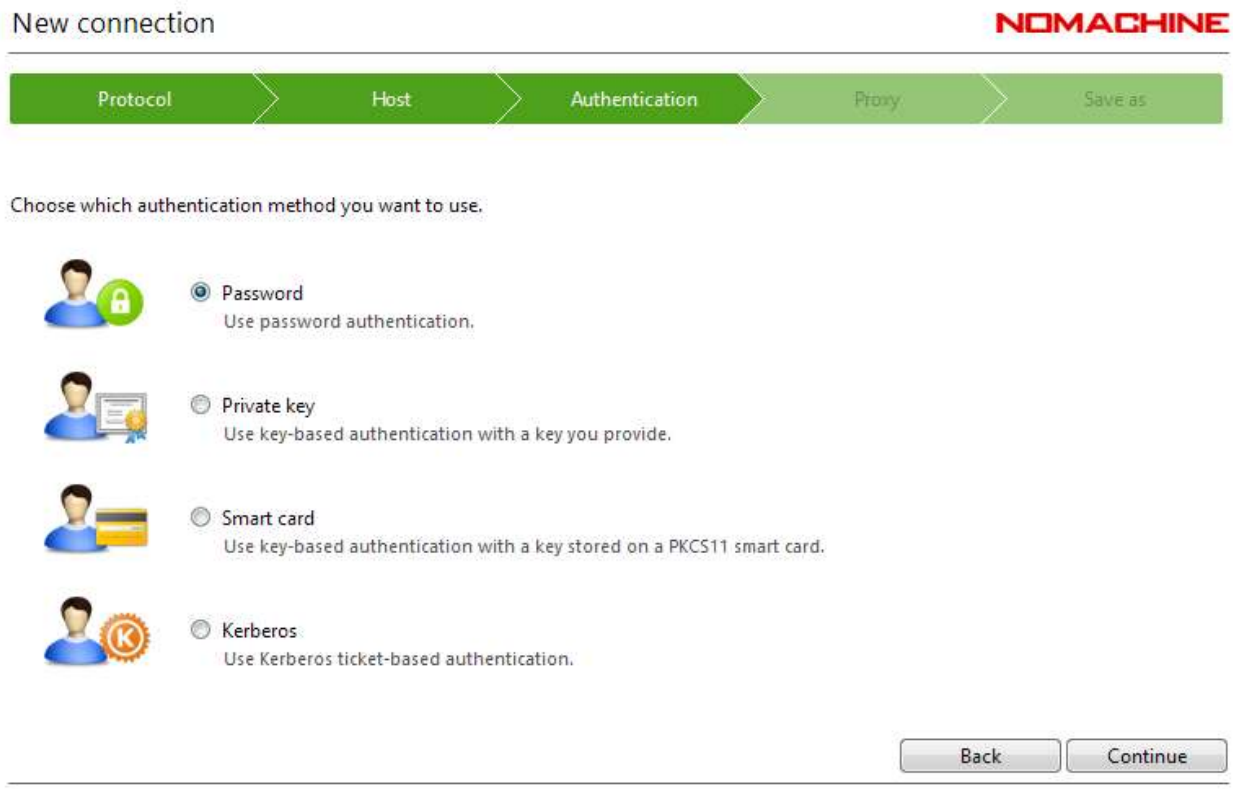
There will be two alternative methods to authenticate that are both in compliance with the new security policy. The first one uses the conventional uniqueID with password along with a two-factor authentication code. Information on how to obtain these codes can be found at http://miamioh.edu/twofactor.

The second one is based on ssh key pairs. Once a pair of keys is present on the client (e.g. office) machine and the cluster, entering a password or two-factor code is no longer required, thus making access to the cluster more convenient.

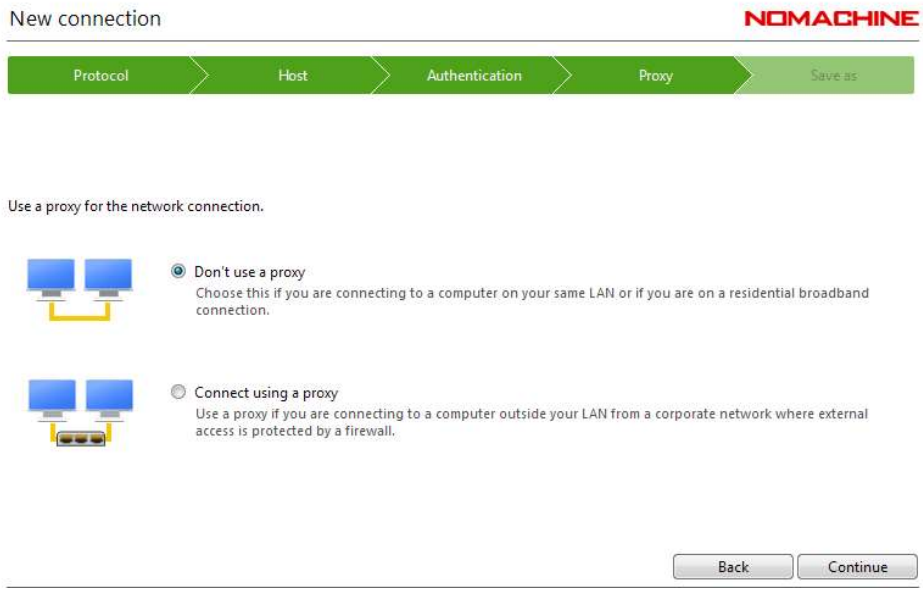
Below we provide information for the configuration of both methods. The first, password and two-factor code method, is required in order to be able to configure the second method.

Password and two-factor code configuration

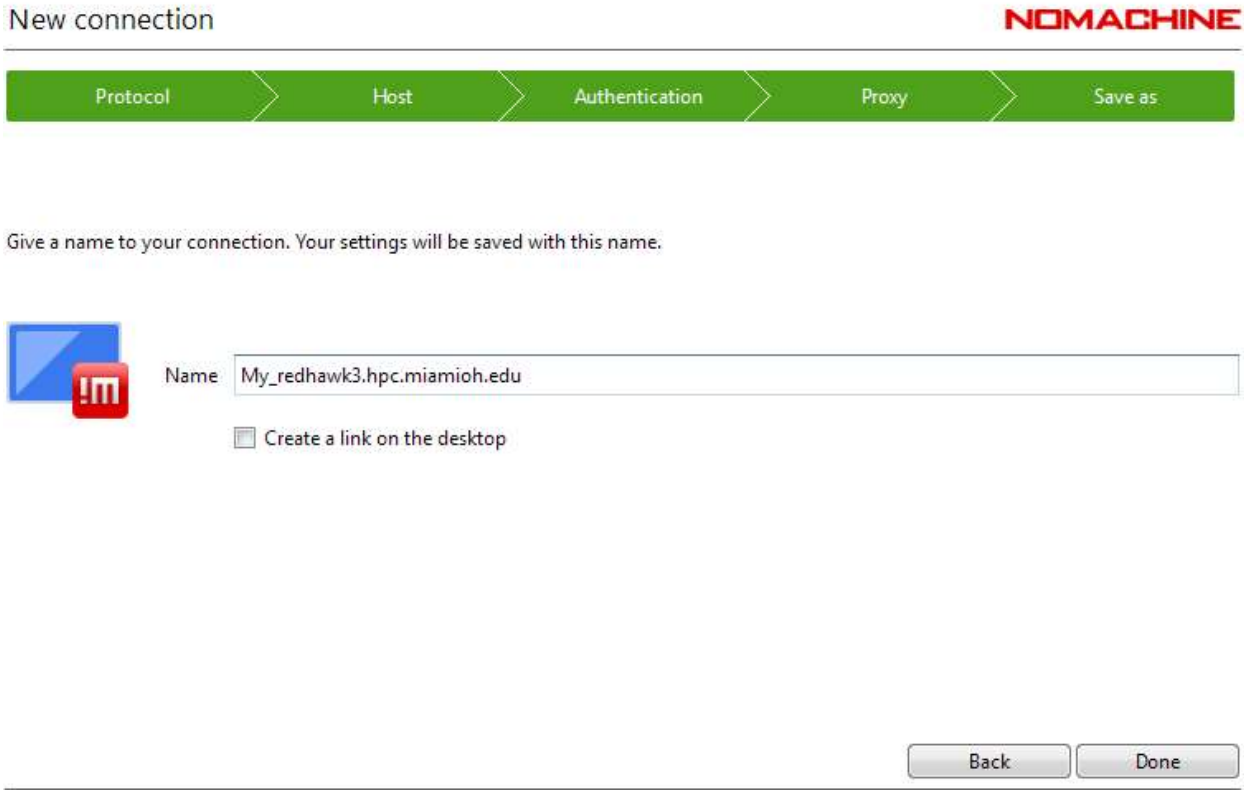
Select “Password”, hit “Continue”.



On the following screen, accept the defaults, as indicated in the screen shot.

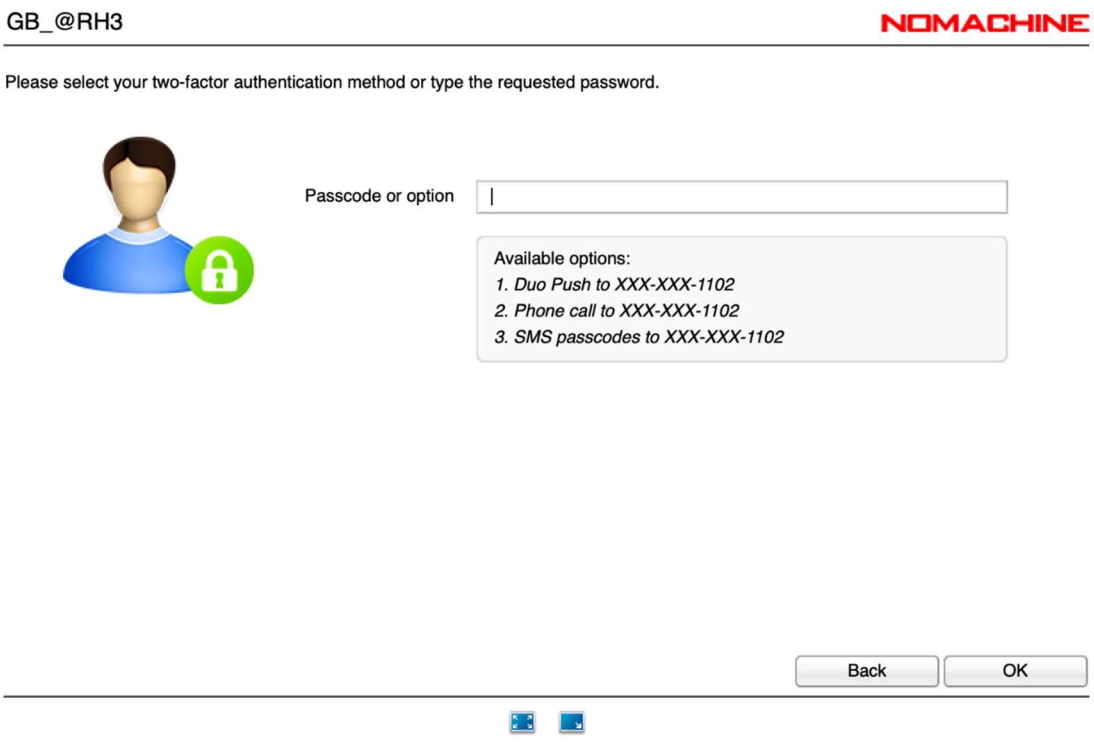


Give the new connection a proper name, it will be re-used each time you connect to the cluster, unless it gets deleted at some point.

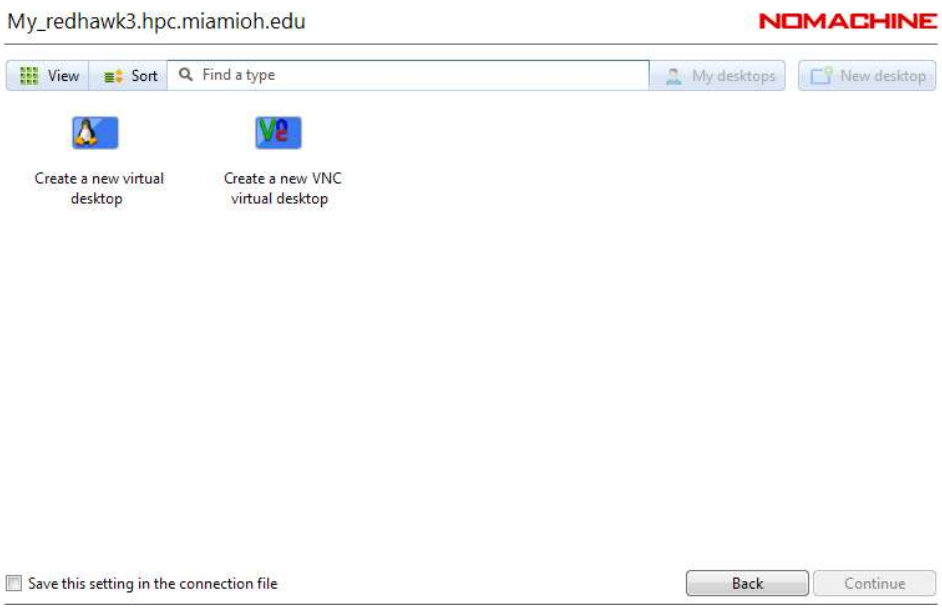


The newly created connection will be saved to the NX screen of existing connections.

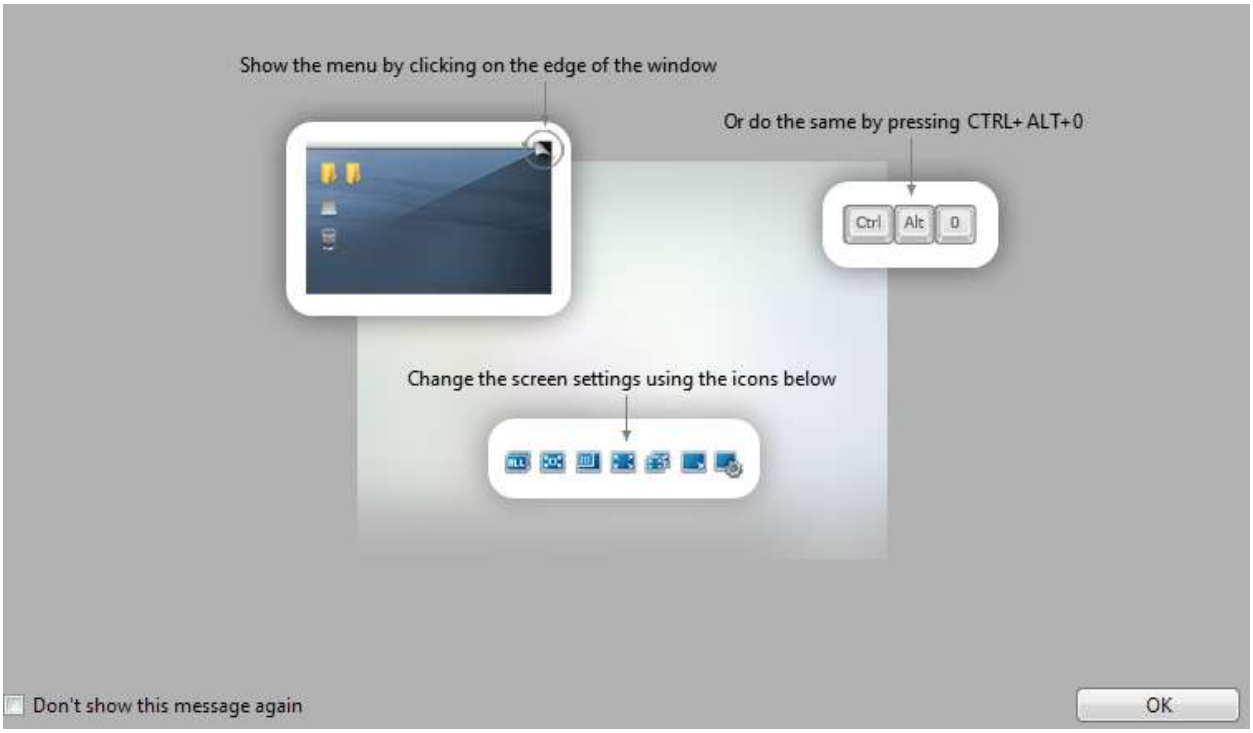
Double-clicking this connection will take you to a screen that asks you to authenticate with password (make sure the user name is your UniqueID) and then enter one of the numbers 1, 2 or 3, depending on your two-factor preference option. For a DUO push, you would be entering 1 and hit OK.



You can then create a new virtual desktop.

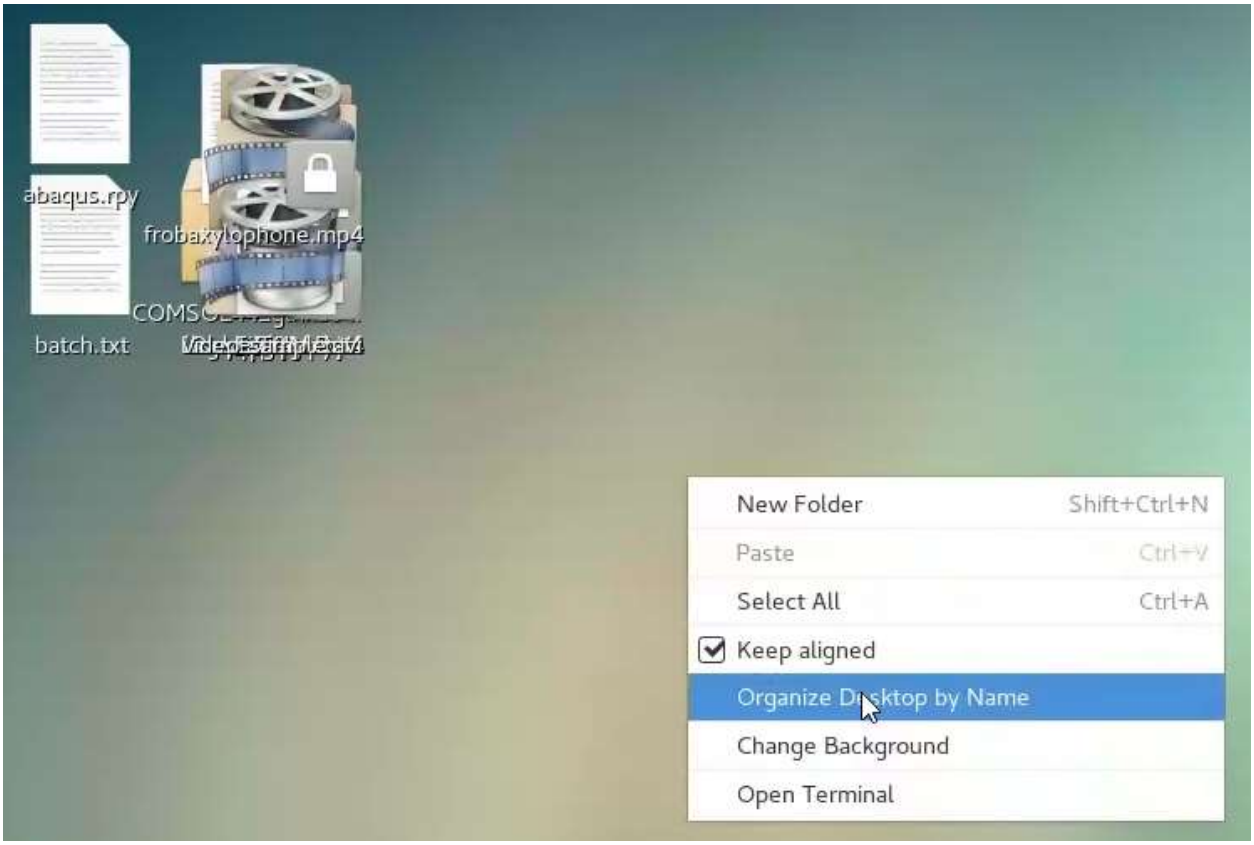


After this has been created, there will be a few informational screens whose appearance can be suppressed once the user is familiar with the operational details of the NX connection tool.



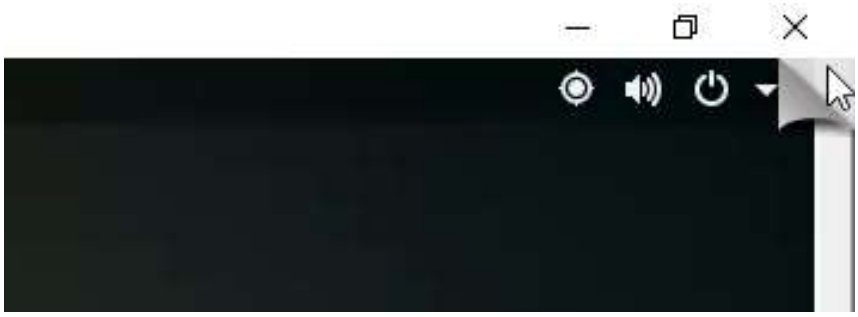
The new NX desktop's layout will be slightly different from what users are used to on the old Redhawk cluster. In case the desktop is not occupying the full space of the window at login time, a dog-ear near the top right corner can be brought up by scrolling over with the mouse pointer. Then proceed as indicated on the next page.

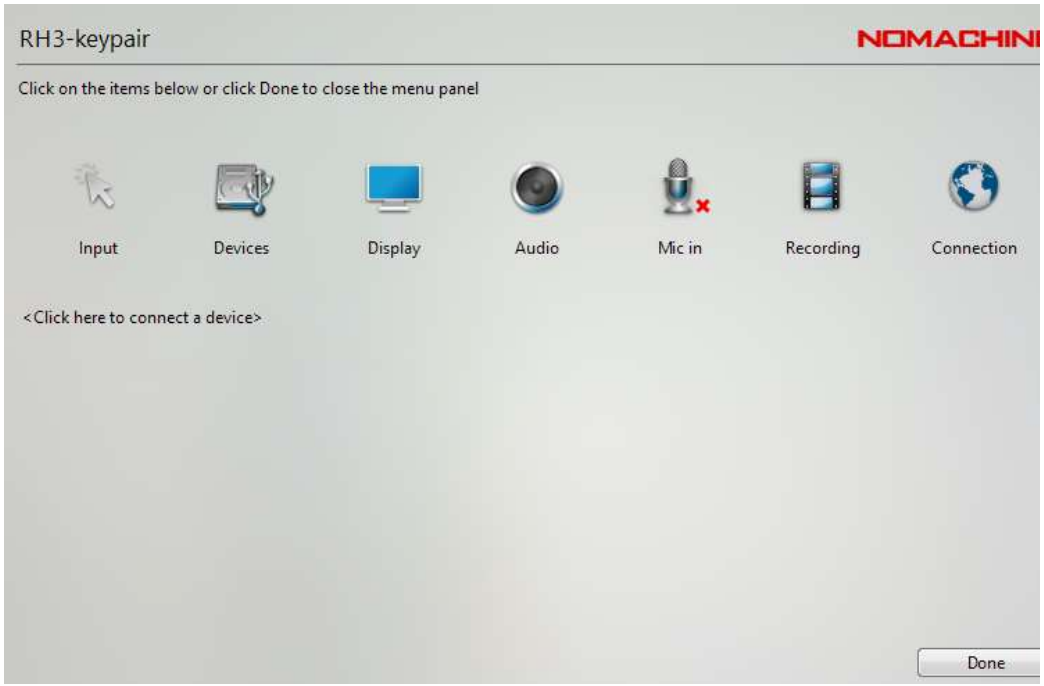
Many users will also need to organize the desktop by right-clicking on it and chose the option as indicated in the snap-shot.

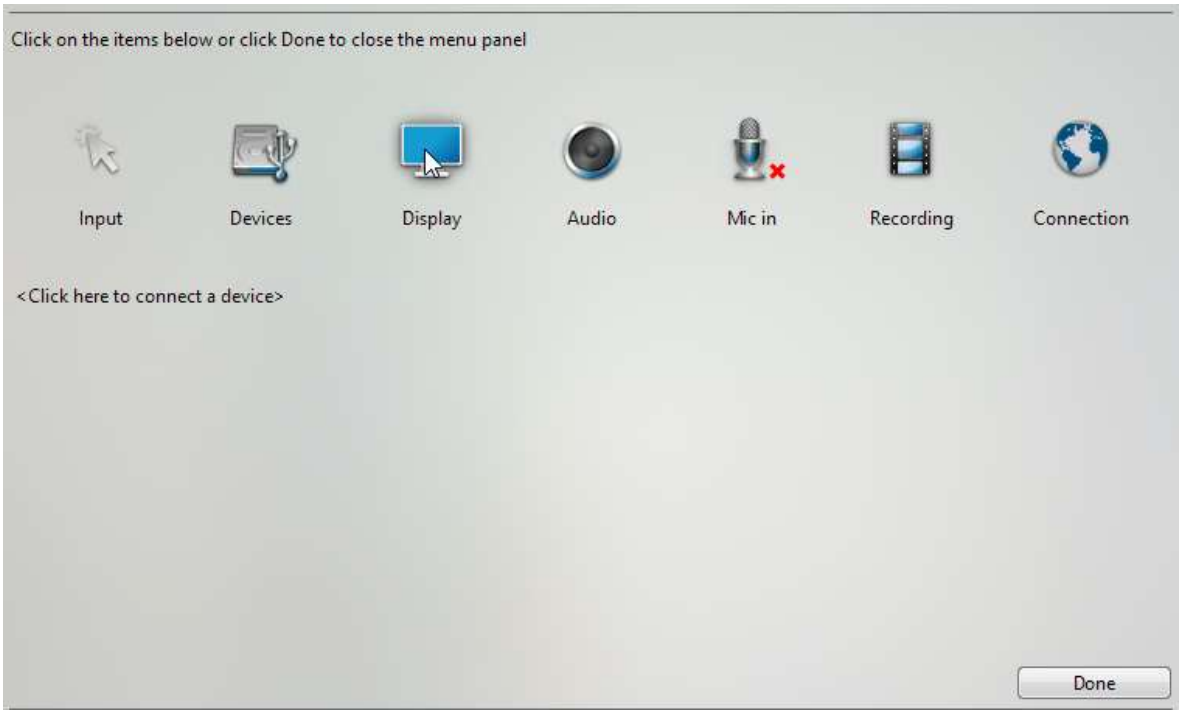


The main menu is condensed into what is called “Activities” and by clicking it, access to the most frequently used tools, such as an x-terminal, can be gained. Right-clicking on any of the symbols will allow to launch the tools.

A dog-ear appears when scrolling over the region of the upper right corner of the NX desktop window and by clicking into that space, the menu panel can be accessed.

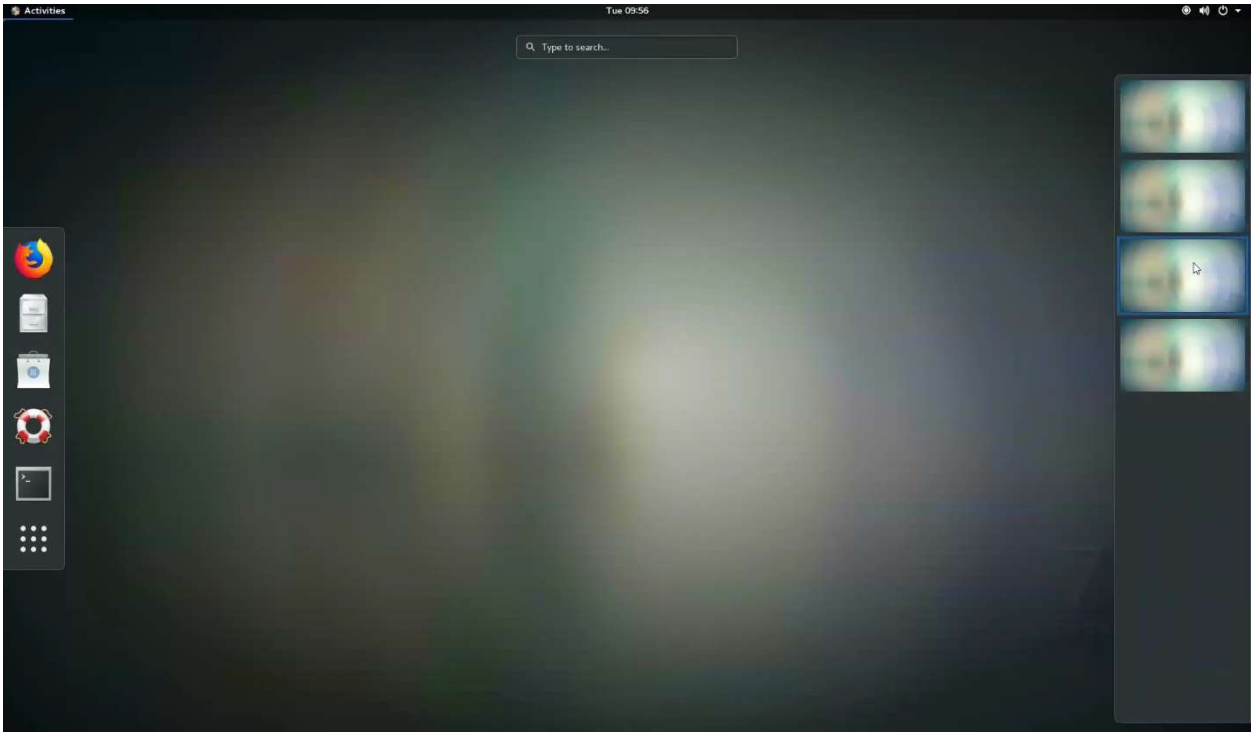




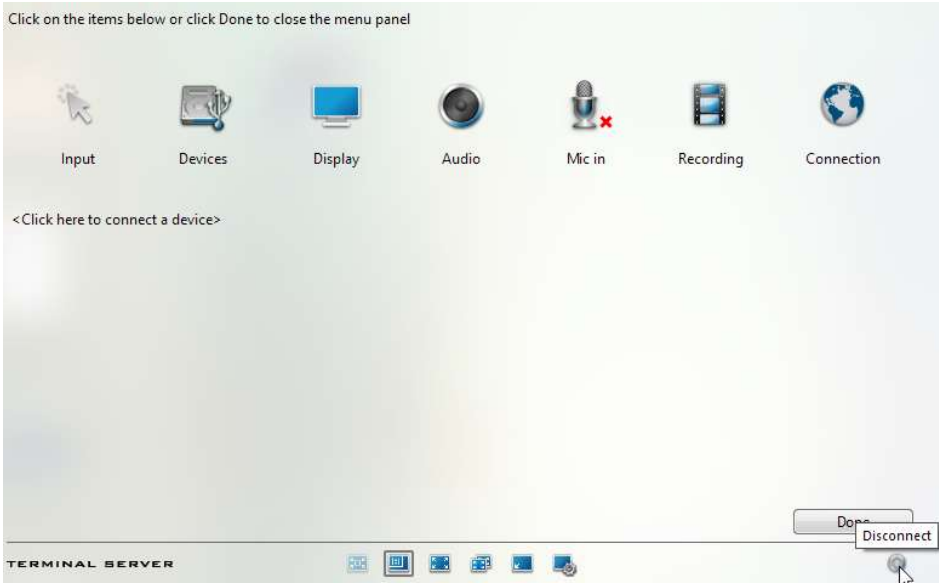


To fit the NX desktop nicely on your monitor select “Display” and then “Resize remote screen”.

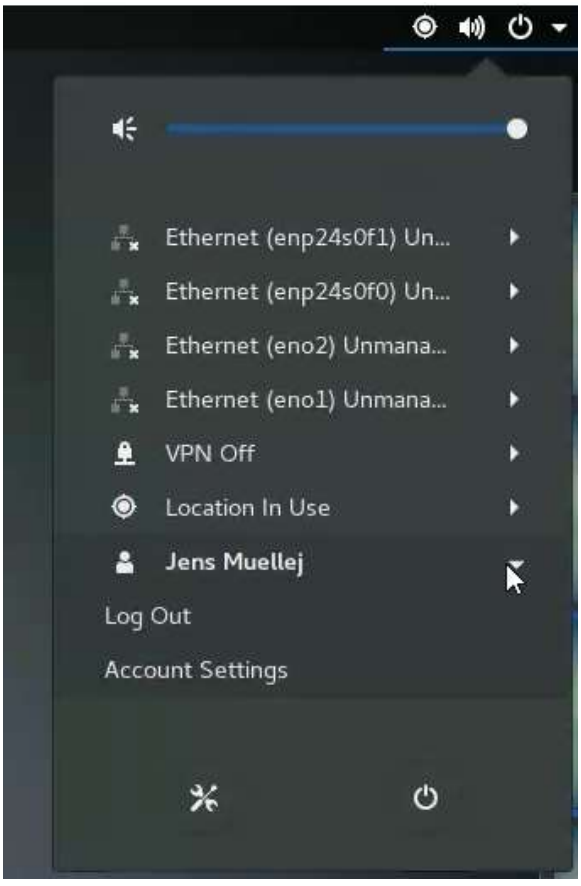
If you plan to work on different work spaces simultaneously, the switch panel can be accessed by clicking “Activities” and then navigate to the right side of your desktop.



To disconnect from a session you can grab the dog-ear at the top right, click into the space and hit the disconnect button on the menu panel.



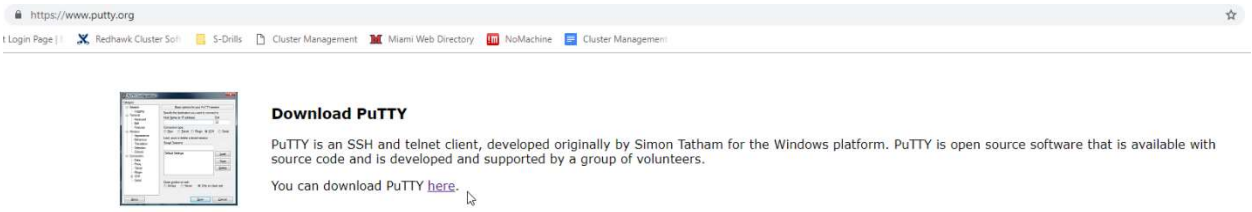
Once a connection to the cluster is not needed any more for an extended period of time it may be a good idea to just log out of the system.



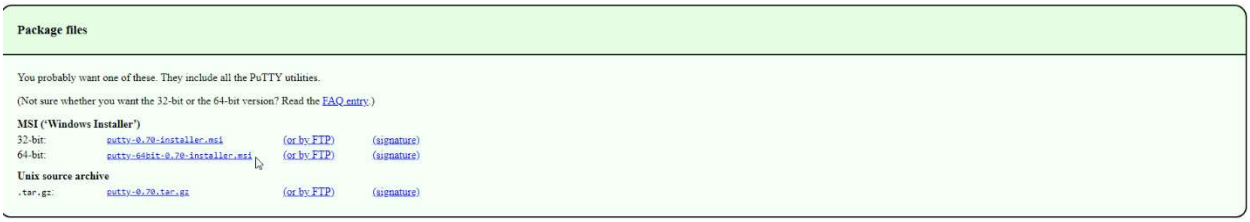
Key pair configuration

An additional tool is required to create key pairs. For this tutorial we choose PuTTY, but other ssh client tools can be used as well.

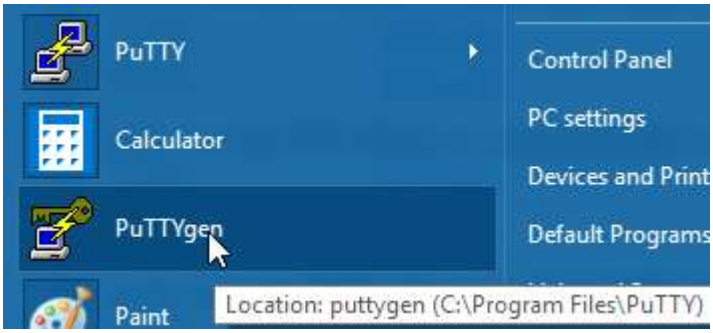
Get the installer from www.putty.org.



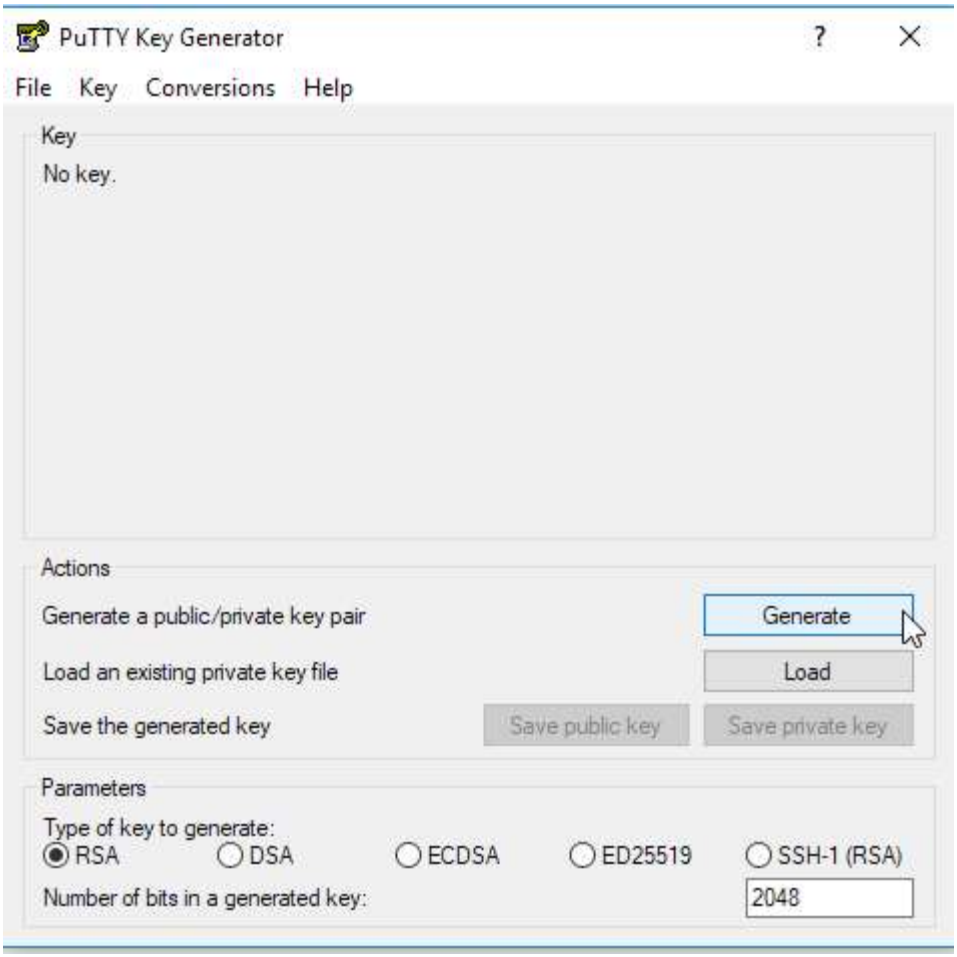
The proper installer for a specific platform is located here:



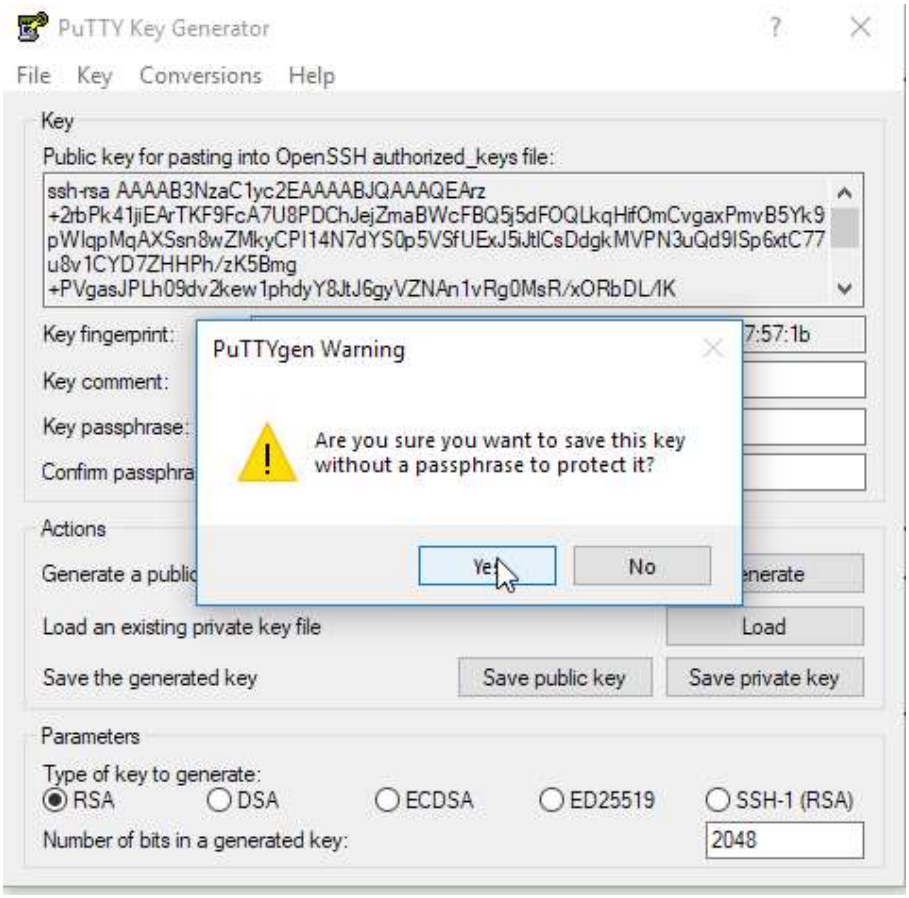
Once downloaded and installed, launch PuTTYgen, the tool's key pair generation feature.



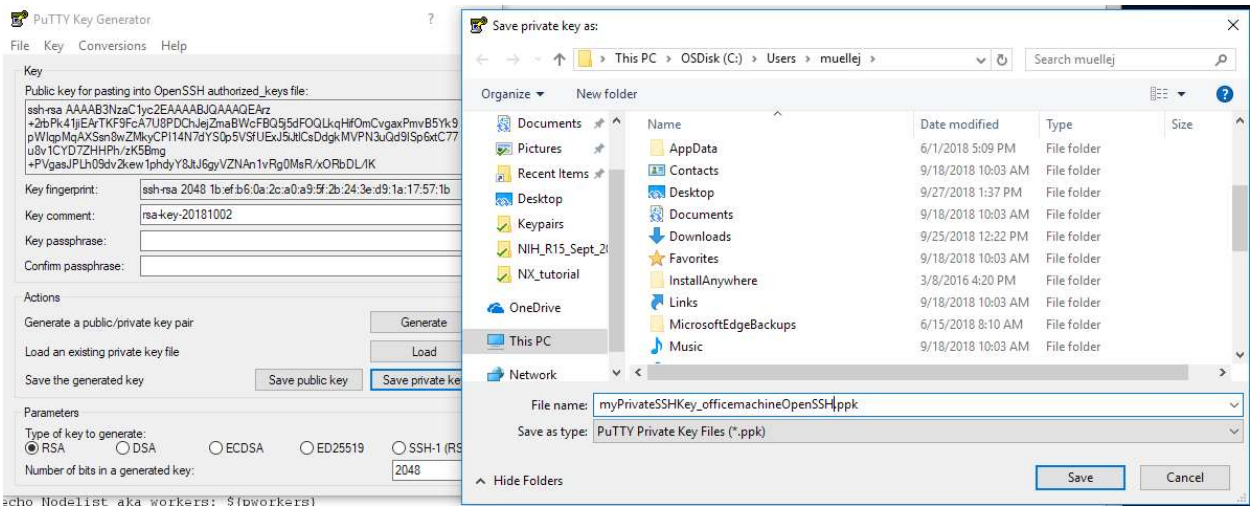
Click “Generate” and move the mouse around in the empty area to generate the key pair.



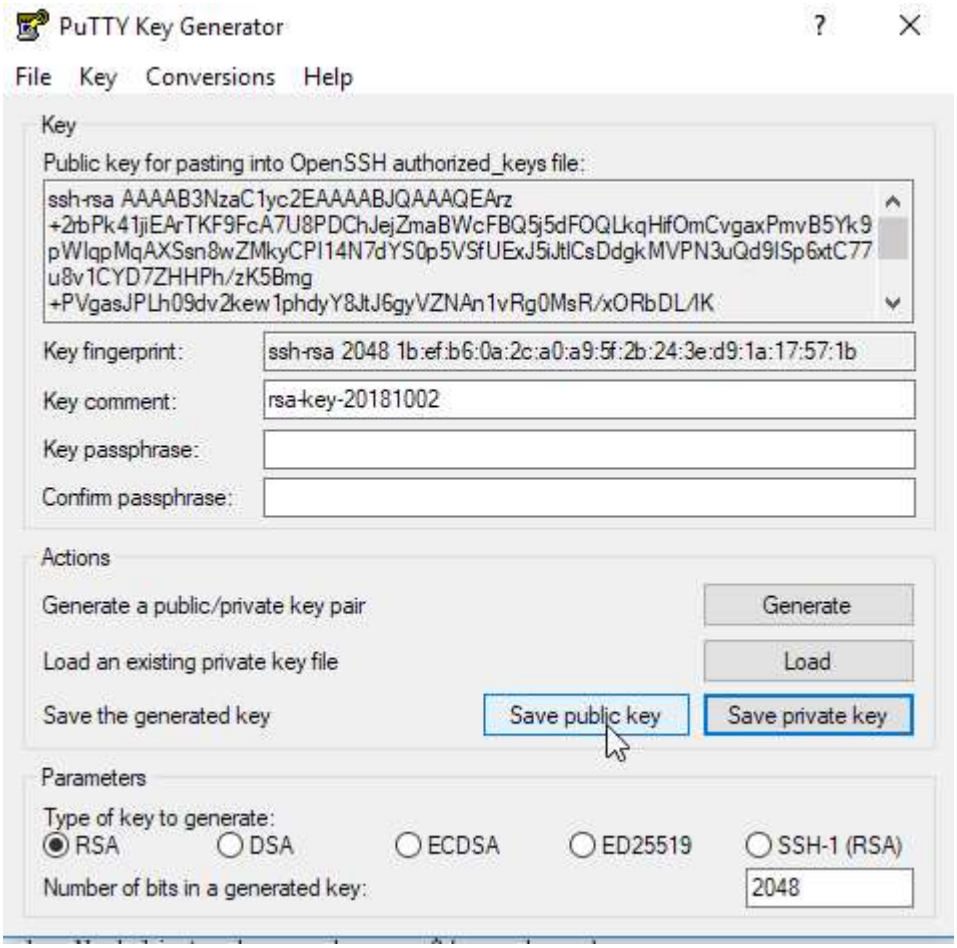
Once completed, select “Conversions->Export OpenSSH key”. You can skip the passphrase, it is not a requirement.

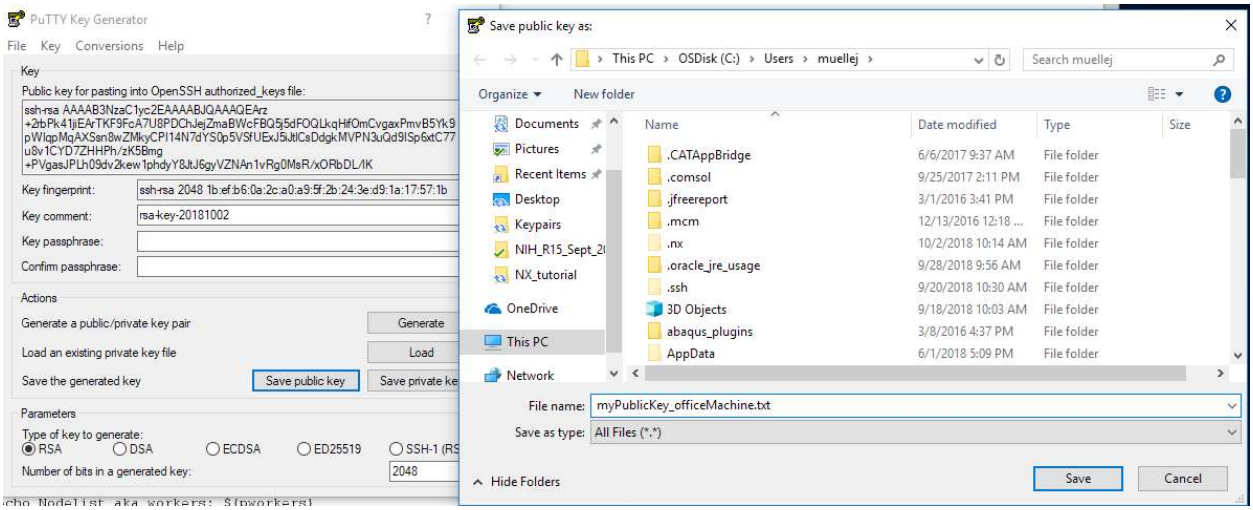


Save the private key in a preferred location.



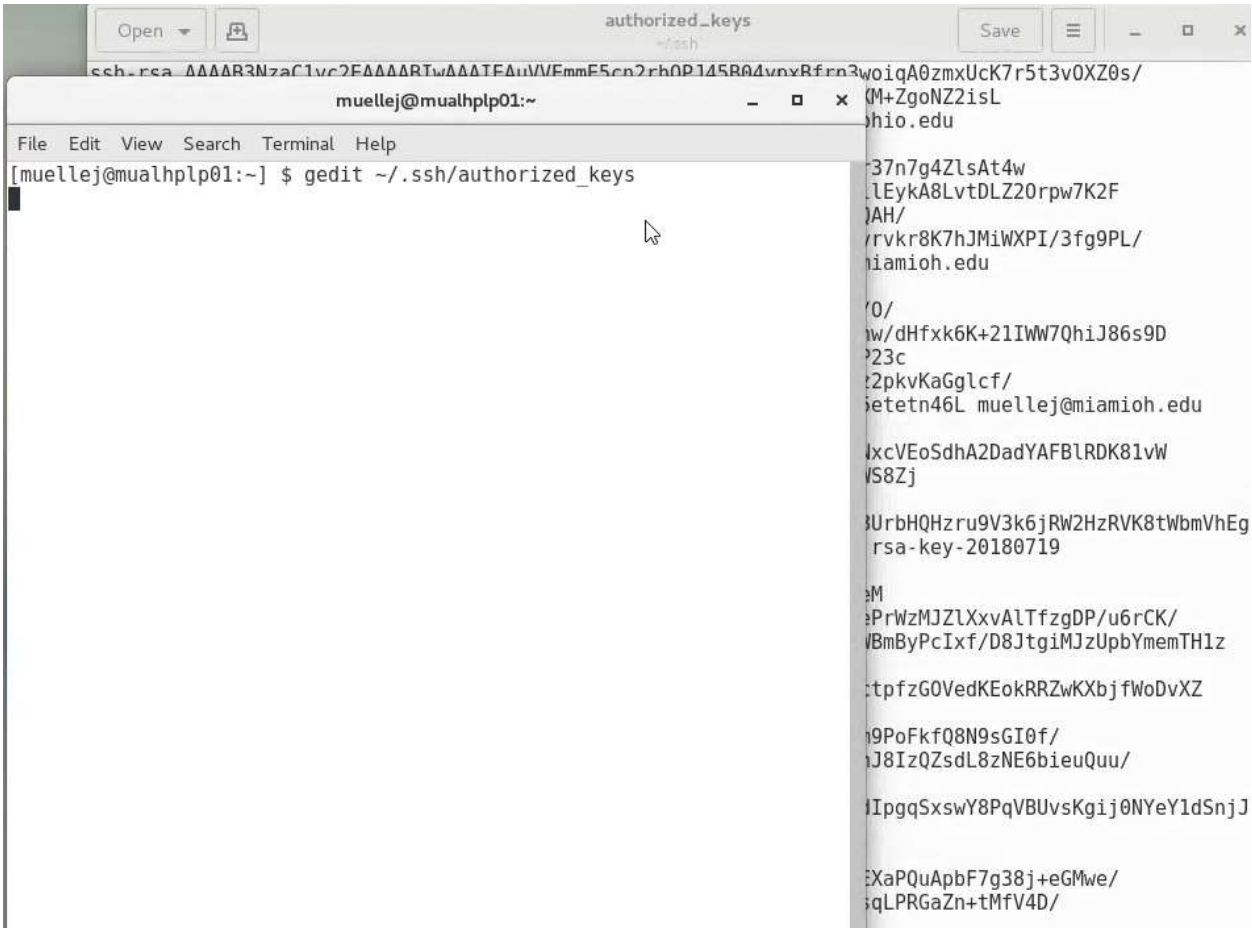
Save the public key in a preferred location.



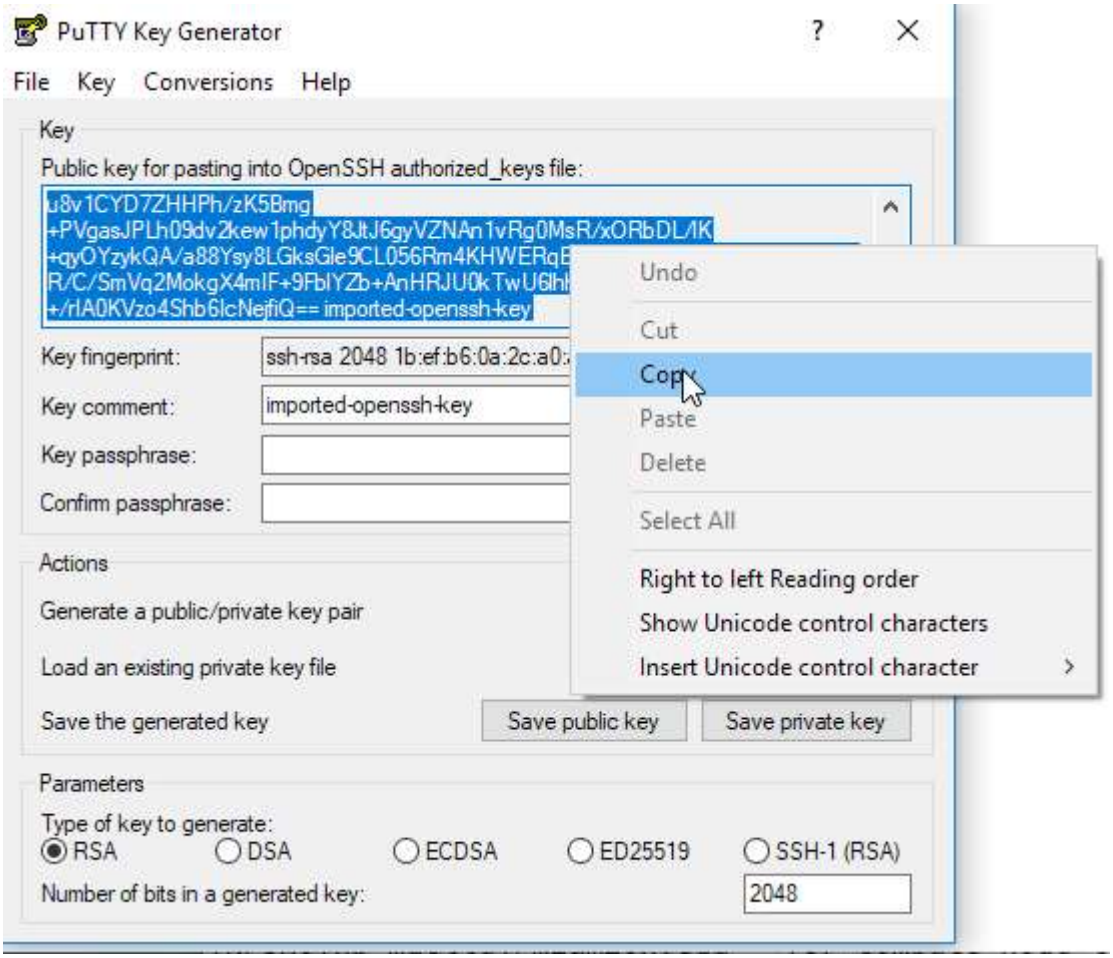


The public key needs to be copied to the cluster. Open a terminal on the NX desktop and launch the text editor gedit according to the snap shot.

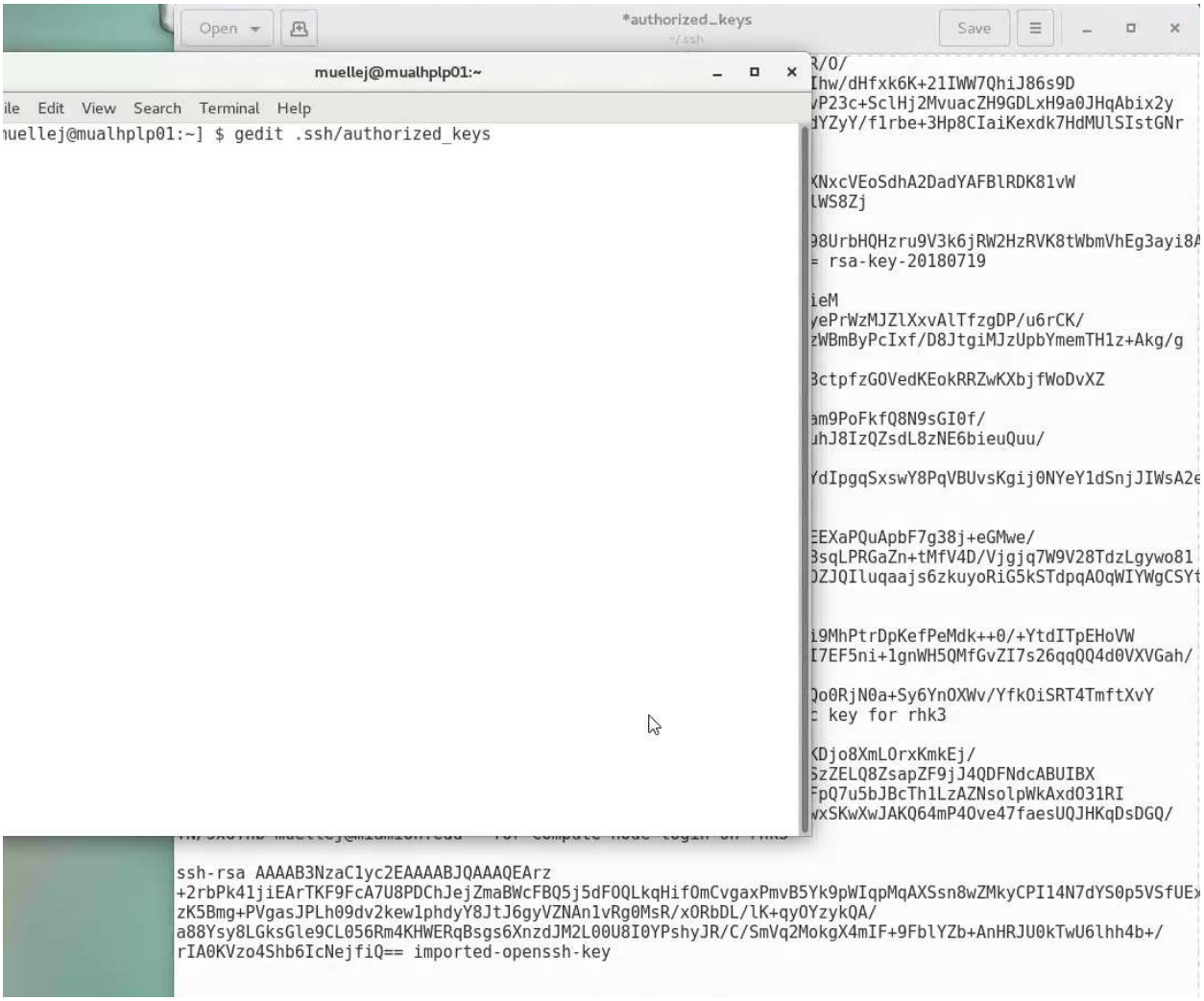
Specifically type and enter: gedit ~/.ssh/authorized_keys



Copy the public key in the PuTTYgen window into the mouse buffer (right-click).


PuTTY Key Generator
File Key Conversions Help
Key
Public key for pasting into OpenSSH authorized_keys file:
u8v1CYD7ZHHPh/zK5Bmg
+PVgasJPLh09dv2kew1phdyY8JtJ6gyVZNAn1vRg0MsR/xORbDL/lK
+qyOYzykQA/a88Ysy8LGksGle9CL056Rm4KHWERqE
R/C/SmVq2MokgX4mIF+9FblYZb+AnHRJU0kTwU6lhl
+/rlA0KVzo4Shb6lcNejfiQ== imported-openssh-key
Key fingerprint:
ssh-rsa 2048 1b:ef:b6:0a:2c:a0:
Key comment:
imported-openssh-key
Key passphrase:
Confirm passphrase:
Undo
Cut
Copy
Paste
Delete
Select All
Right to left Reading order
Show Unicode control characters
Insert Unicode control character
Actions
Generate a public/private key pair
Load an existing private key file
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA
DSA
ECDSA
ED25519
SSH-1 (RSA)
Number of bits in a generated key:
2048

Navigate back to the gedit editor that is open with the authorized_keys file on the cluster NX desktop. Paste the public key into the file, or below any keys that may already exist in the file.



Save the file and exit the editor.

The file authorized_keys needs to have proper permissions. Type:

ls -l .ssh/authorized_keys

You will see an output similar to this:

-rwx------. 1 muellej muellej 2265 Oct 18 08:19 .ssh/authorized_keys*

The highlighted part is important. If yours does not match the above you can adjust that by typing:

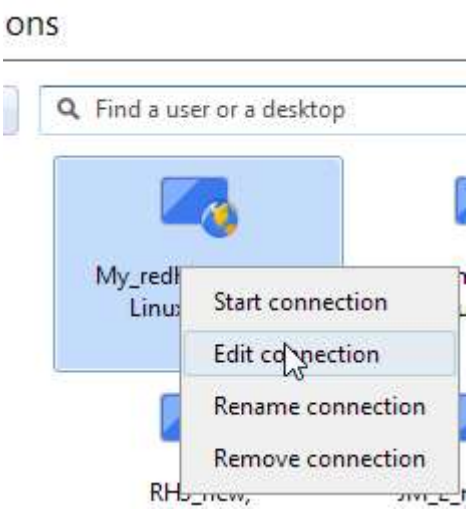
chmod go-rwx .ssh/authorized_keys

and

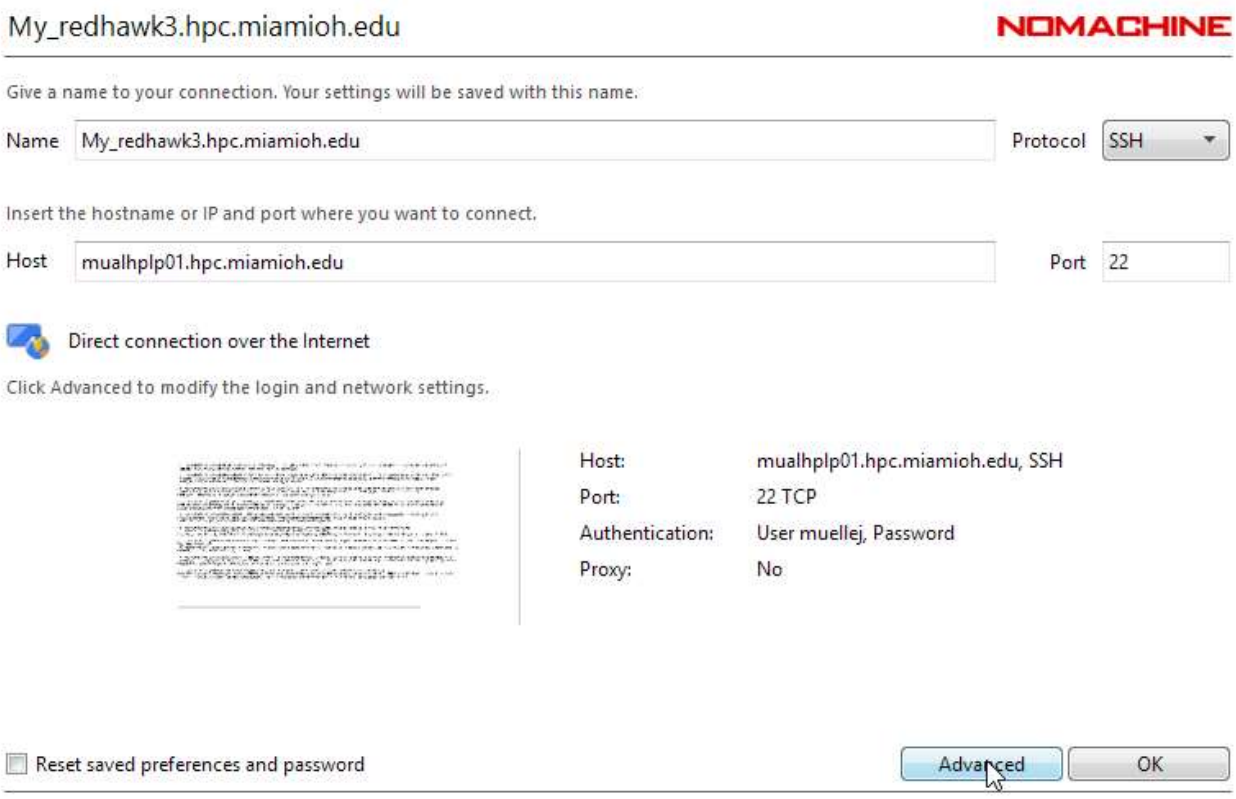
chmod u+rwx .ssh/authorized_keys

Log out from the NX session.

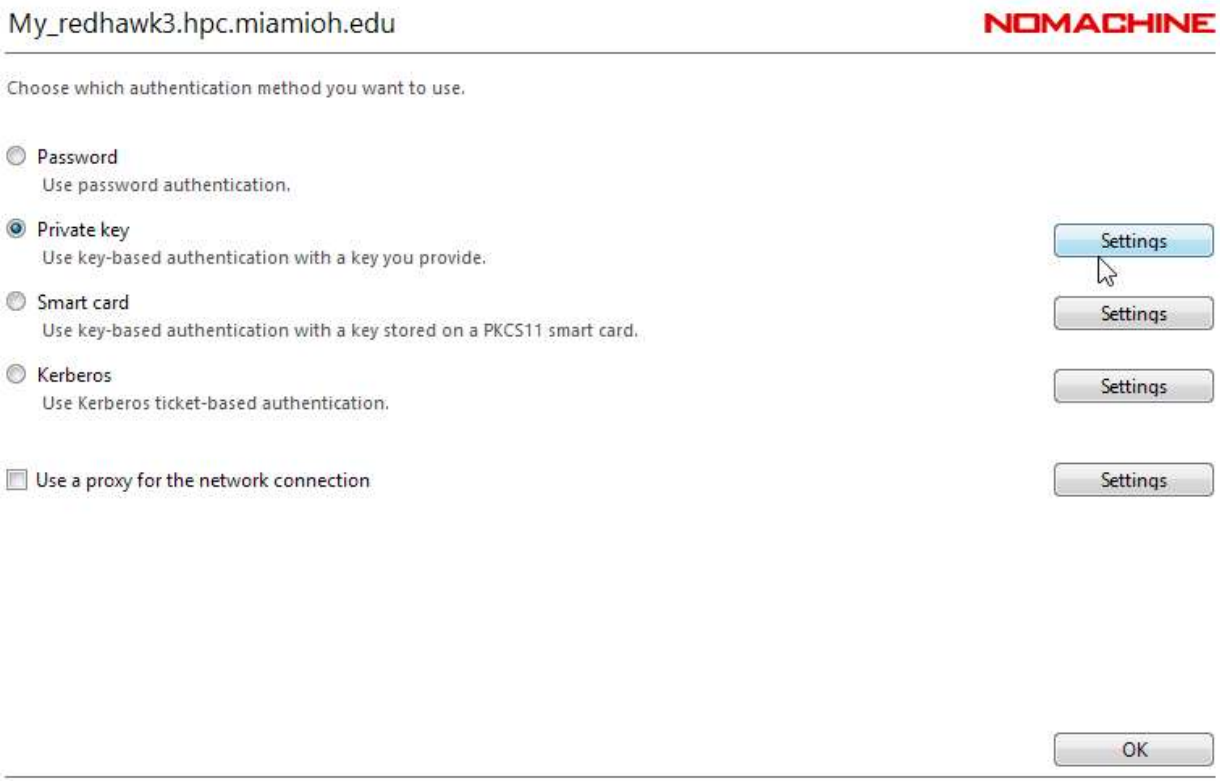
Launch NX again and navigate to the “Recent connections” pane and right-click on your NX connection to edit it.

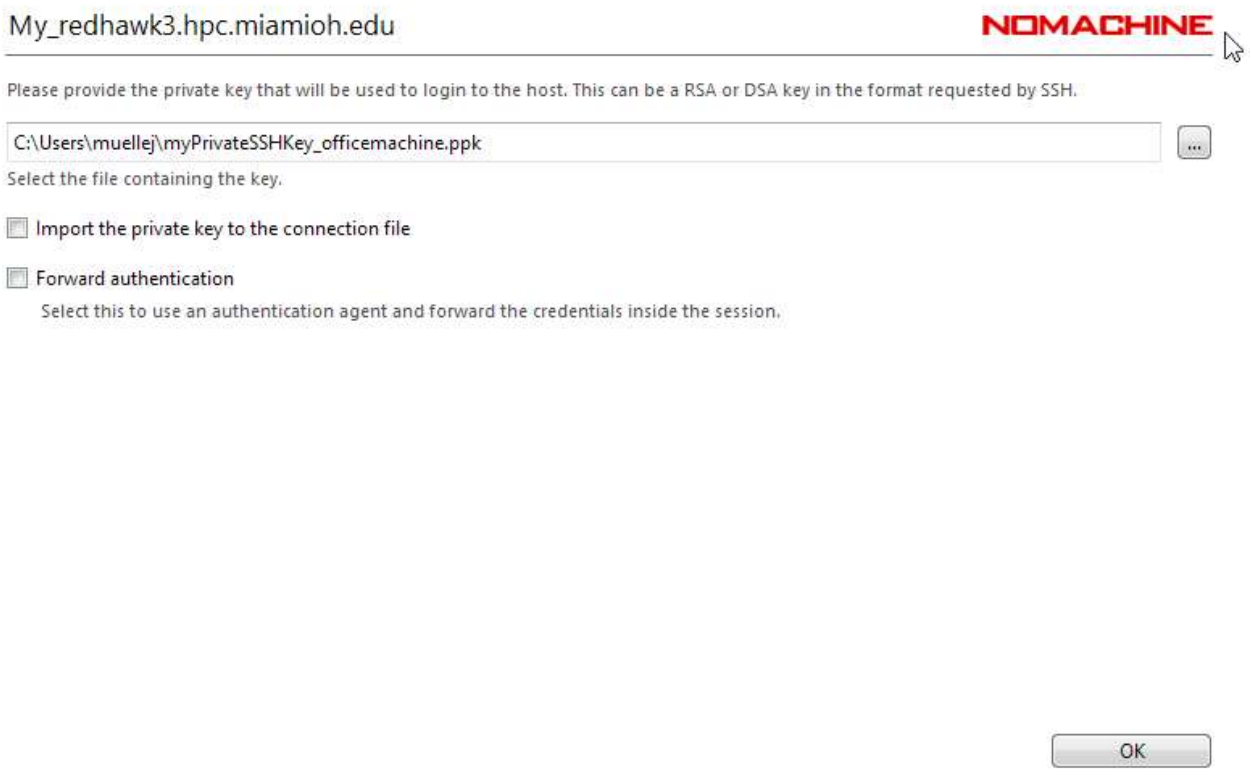


Select “Advanced”.



Select “Private key”. Hit “Settings” and navigate to the location where you saved your private key.


My_redhawk3.hpc.miamioh.edu
NOMACHINE
Choose which authentication method you want to use.
Password
Use password authentication.
Private key
Use key-based authentication with a key you provide.
Settings
Smart card
Use key-based authentication with a key stored on a PKCS11 smart card.
Settings
Kerberos
Use Kerberos ticket-based authentication.
Settings
Use a proxy for the network connection
Settings
OK


My_redhawk3.hpc.miamioh.edu
NOMACHINE
Please provide the private key that will be used to login to the host. This can be a RSA or DSA key in the format requested by SSH.
C:\Users\muellej\myPrivateSSHKey_officemachine.ppk
...
Select the file containing the key.
Import the private key to the connection file
Forward authentication
Select this to use an authentication agent and forward the credentials inside the session.
OK

Hit “OK” and reconnect with your username. You will not get prompted for a password or two-factor code from now on. You can apply the same procedure for other client machines that you use to connect to the cluster.

Each machine will need to have its own private key and the corresponding public key copied to the authorized_keys file on the cluster.