# Setting up Public/Private Keys for Ab Inition GDE SSH.

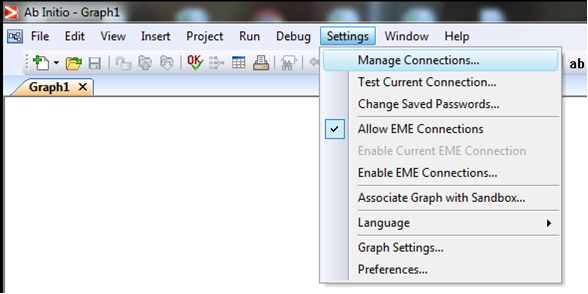
If you have not yet done the [Host-to-host (EME) SSH ppk setup](https://eda.wellsfargo.com/collab/home/dc/wiki2/Pages/Troubleshooting-GDE-EME-connection-issues.aspx), do that first, because when you test your GDE connection setup, it’s going to try to talk to the EME, which is on a different server. If you haven’t done that first, your GDE connection will fail talking to the EME and will eventually lock your account for number of failed attempts.

This procedure will generate a public key for your Linux $OLD\_HOME/.ssh/authorized\_keys file, and a private key for your desktop or other local folder, plus capture a password for those keys that you can save (encrypted) in the GDE to make a secure connection.

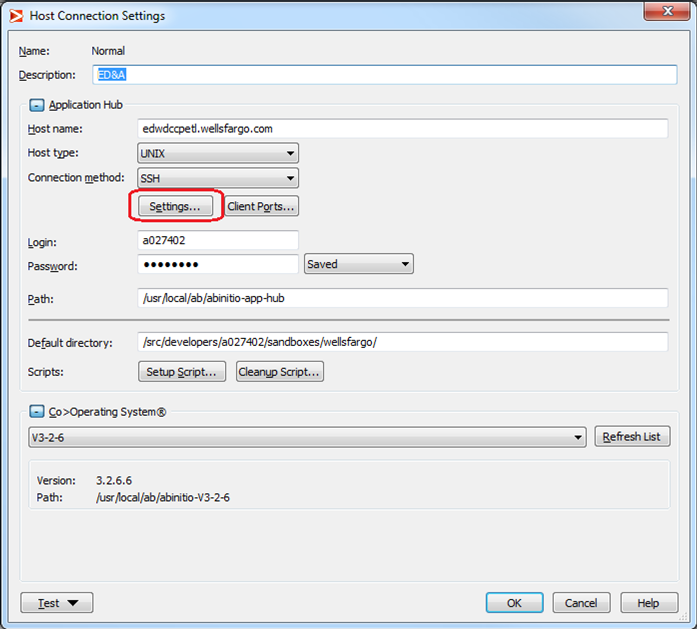
This can be done prior to your ad-ent ID being converted to 2FA for Linux.

If you do it after being converted to 2FA, then most likely you will need to set password to always prompt in your host connection before generating keys, and use your 2FA fob login when prompted.

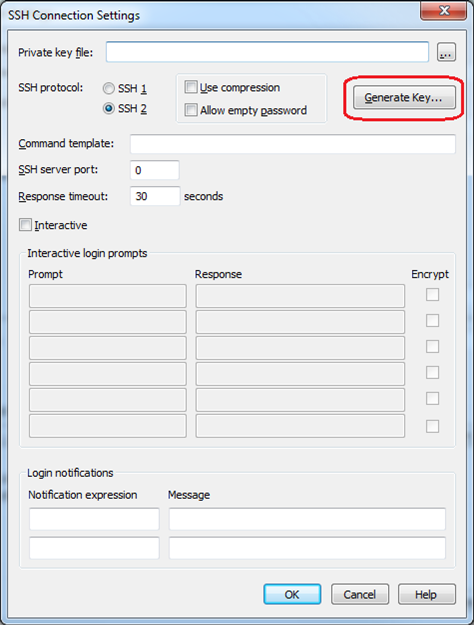
1. Start GDE. Go to Settings -> Manage Connections



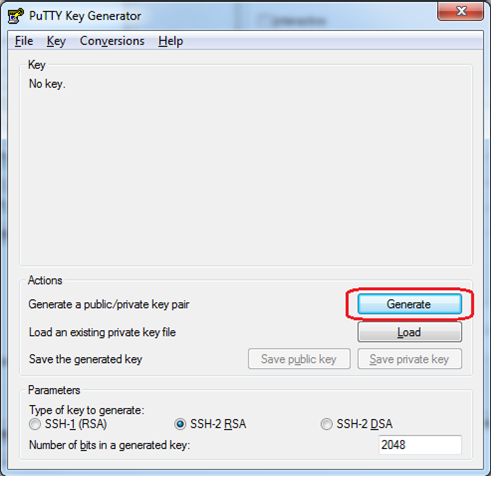
1. Open up the “Normal” connection (or whichever connection you normally use).
2. Click on the settings button underneath the connection method = SSH



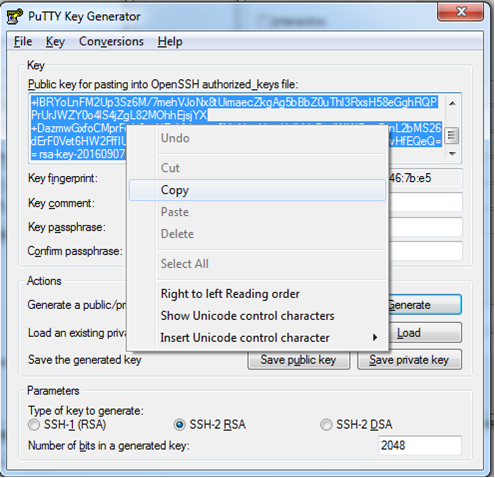
1. Glick the “Generate Key…” button



1. In the window that comes up, click on Generate, then complete the process by which it asks you for random input



1. Copy the public-key section, then add it to $OLD\_HOME/.ssh/authorized\_keys



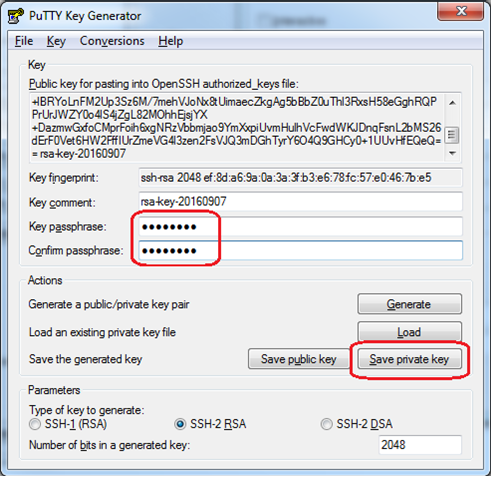
After adding the key to the authorized\_keys file:

[cdpra04a0400] a434989 /home/a434989/.ssh

> tail -1 authorized\_keys

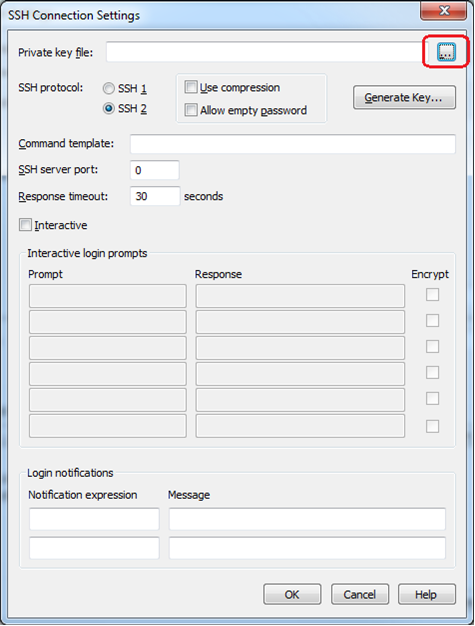
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAg3JSrNIioFi94lNSl8k1olJCnSTgfrUWE2HFIifvo2+goir3h3rbpi9s;sDSSGSAGUghwgpoaishgASGEs/KKN/ZDN/Fb59WpcZ7XIcSHEDe+KiOoxXNBfJtC1DGVT/0HxAfJLpmm1DwgxpIxaW0YLLOcVeOomgXTJ03Fu0v6aMG3TX34gowDj8J7ahuiagiufGaseFESEsgfe06Z/2ldYP495q0vcoyVJUAQukQAhax42FtYNQG+Ja+5+2vE/oylTxqjfbernquHCusd8lIzcDu/RMxbBwOKv6Daetjaglh$WERGww96zIl8D0e0wUhe8sA4rKTs+eezAktr9lusouAX8or+Q7YYHFTdNw== rsa-key-20160907

1. Add a key passphrase, then click “Save private key”



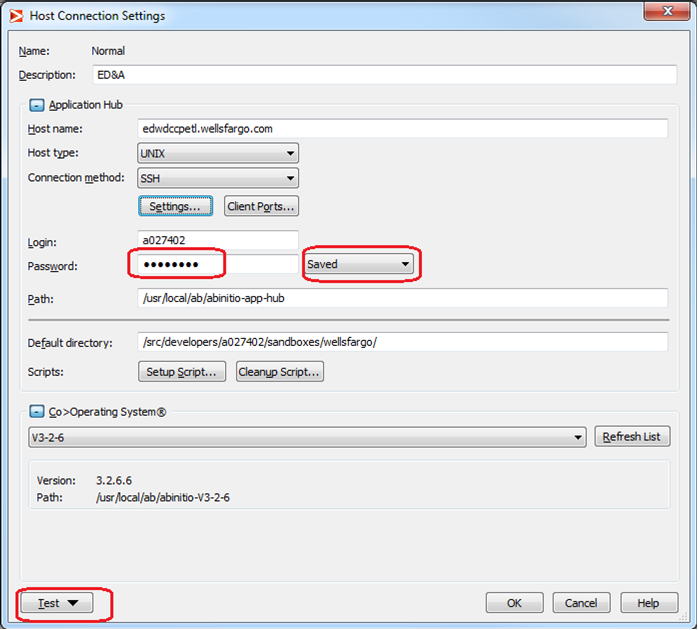
* 1. save to a location where GDE can read, and remember the path to that key
  2. NOTE: I found that my GDE can’t read from “My Documents”. It resulted in a permission denied error. I believe this needs to be local, so I saved it to a folder in “My Desktop”, which worked.
  3. Exit the key generation screen

1. In GDE SSH connections settings window, click on the “…” next to “Private key file:” and choose the key you saved in Step 7.



* 1. Click OK in GDE SSH connections settings window

1. In Host Connection Settings window, enter the passphrase of the key into the password box, then test the connection.



10. If you have multiple Dev cluster app hosts that you want to connect to, then you can take the private key generated in steps 5 & 6, add it to your authorized\_keys file on the hosts as well, and use the same desktop private key for that connection (steps 8 & 9).

Remember to always use the app host alias or at least the VIP alias, rather than the hostname, for the connection.

PS : Make sure that config file is present in all host at /src/developers/user\_id/home/sshwork

*[This procedure contributed by Mark Horn.]*