**DShield Honeypot Setup**

1. Download and install Raspberry Pi Imager
2. Choose operating system
3. Customize installation
    a. Enable SSH
    b. Customize user account
    c. Set up public-key authentication
4. Write OS to micro SD card
5. Plug micro SD card and boot Raspberry Pi and run updates
6. Install DShield from GitHub
7. Expose honeypot to internet
8. Optional
    a. Set up additional logging
9. Appendix
    a. Additional setup screenshots

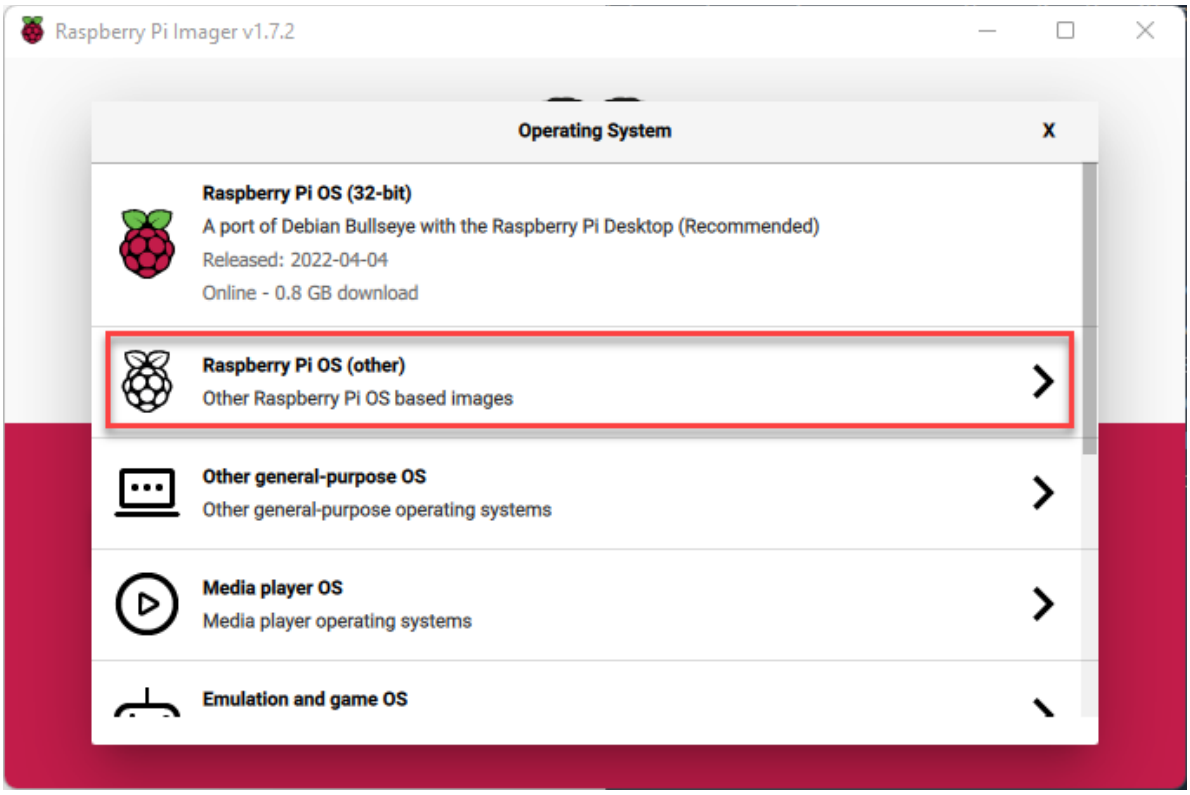
**Download and install Raspberry Pi Imager**

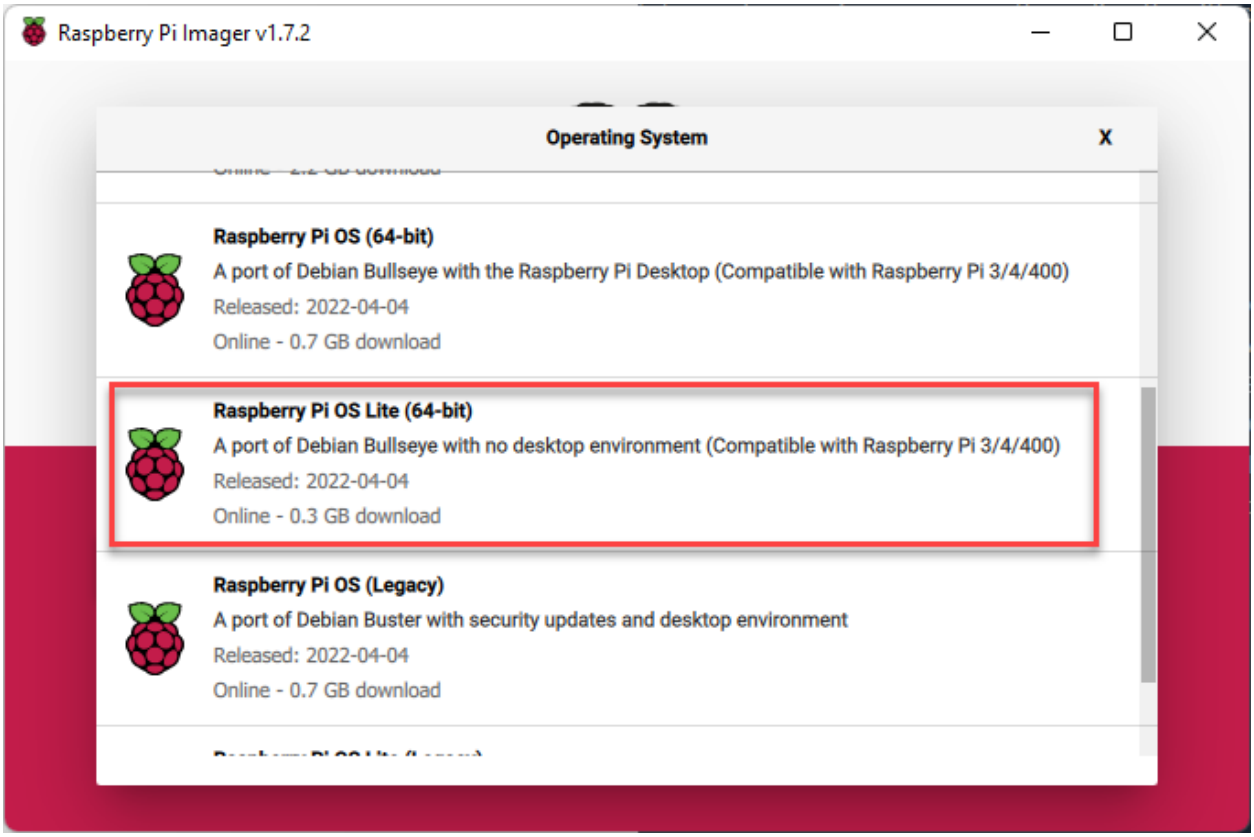
The Raspberry Pi Image software makes the installation of the Raspberry Pi software very easy. It can run on a variety of operating systems and will save time, especially if trying to configure multiple Rasberry Pis.

https://www.raspberrypi.com/software/

**Choose operating system**

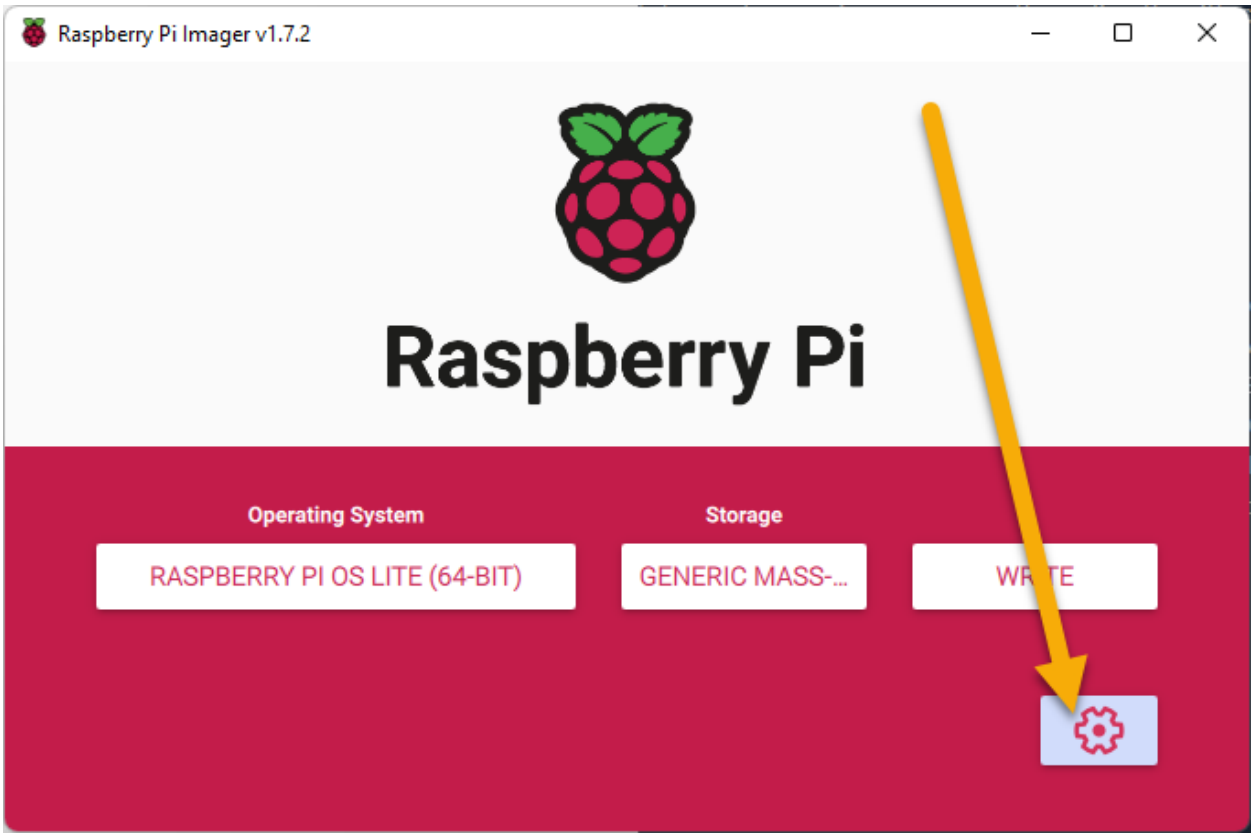
The Raspberry Pi Imager will let you choose your operating system and will download the necessary source files. In this case, one of the Lite options was chose to limit overhead and help keep space, storage and memory, for necessary applications. Choose what works for you and what is compatible with your Pi.


Raspberry Pi Imager v1.7.2
Operating System
Raspberry Pi OS (32-bit)
A port of Debian Bullseye with the Raspberry Pi Desktop (Recommended)
Released: 2022-04-04
Online - 0.8 GB download
Raspberry Pi OS (other)
Other Raspberry Pi OS based images
Other general-purpose OS
Other general-purpose operating systems
Media player OS
Media player operating systems
Emulation and game OS


Raspberry Pi Imager v1.7.2
Operating System
Raspberry Pi OS (64-bit)
A port of Debian Bullseye with the Raspberry Pi Desktop (Compatible with Raspberry Pi 3/4/400)
Released: 2022-04-04
Online - 0.7 GB download
Raspberry Pi OS Lite (64-bit)
A port of Debian Bullseye with no desktop environment (Compatible with Raspberry Pi 3/4/400)
Released: 2022-04-04
Online - 0.3 GB download
Raspberry Pi OS (Legacy)
A port of Debian Buster with security updates and desktop environment
Released: 2022-04-04
Online - 0.7 GB download

**Customize installation**

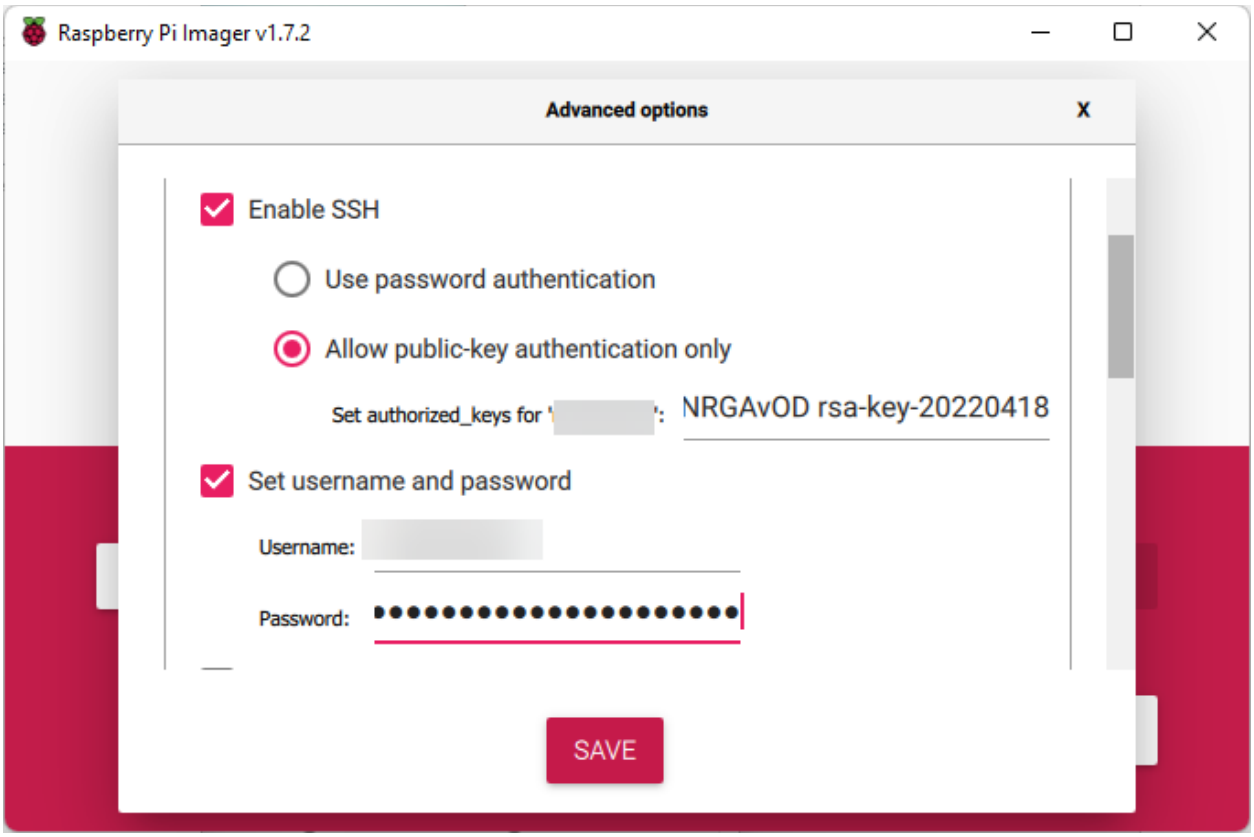
The customize installation option (the gear on the lower-right of the screen) can be a time-saver. It is an even more useful feature today since the built in “Pi” user is no longer being used to improve security [Ars Technica].




Enabling SSH is great option to customize right away to allow access to the device remotely without any display. This is especially helpful for headless setups where additional hardware to interact with the device may not be readily available. Customizing the user account and using public-key authentication is also recommended to improve authentication security and limit effectiveness of attacks that may exist with using the “Pi” account.

To enable public-key authentication and customize the user account, the following options need to be selected. In order to set a custom user account with public-key authentication a public-key and password must be specified.

- Check “Enable SSH”
- Select “Allow public-key authentication only”
- Enter authorized_keys value (look below for generating using PuTTY Key Generator)
- Check “Set username and password”
- Set “Username”
- Set “Password”

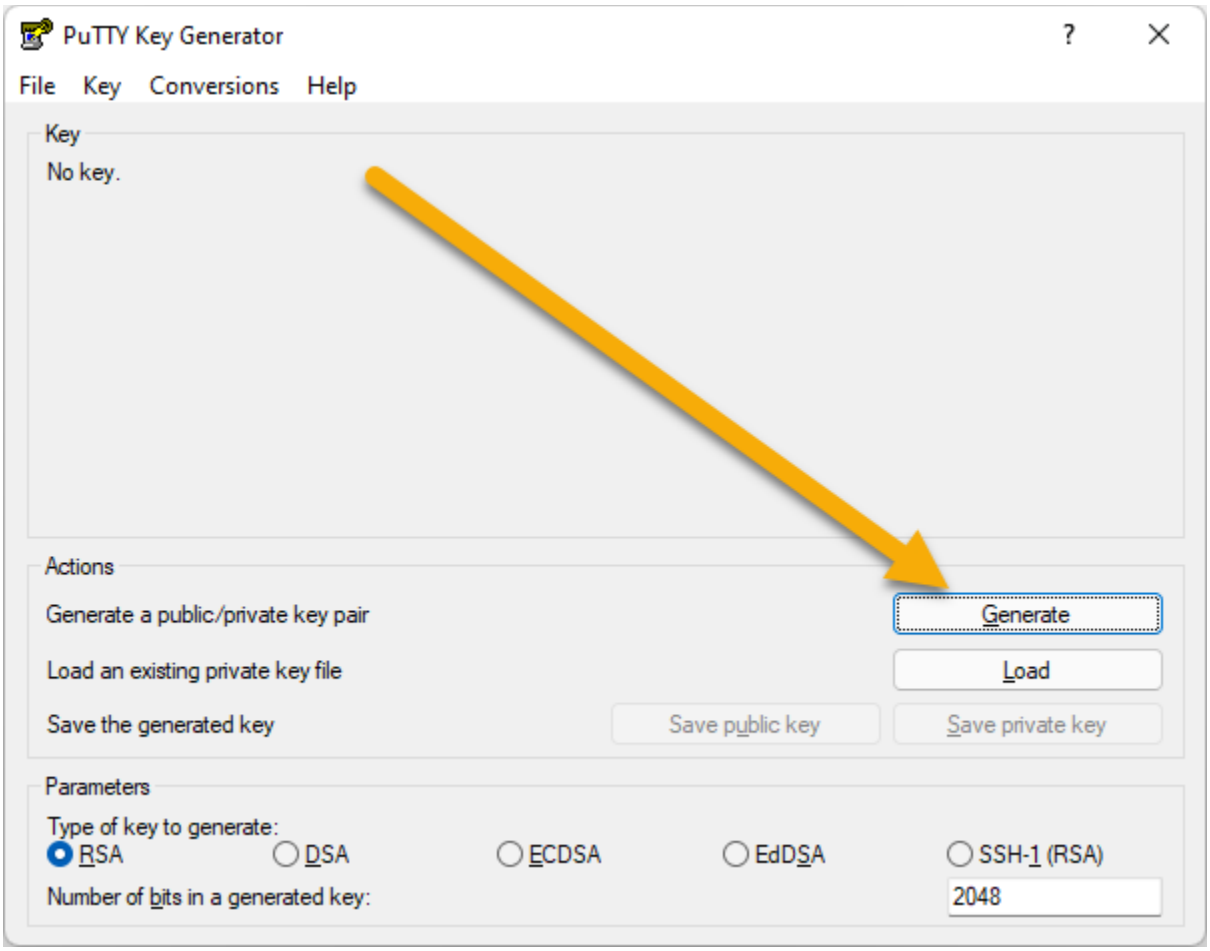


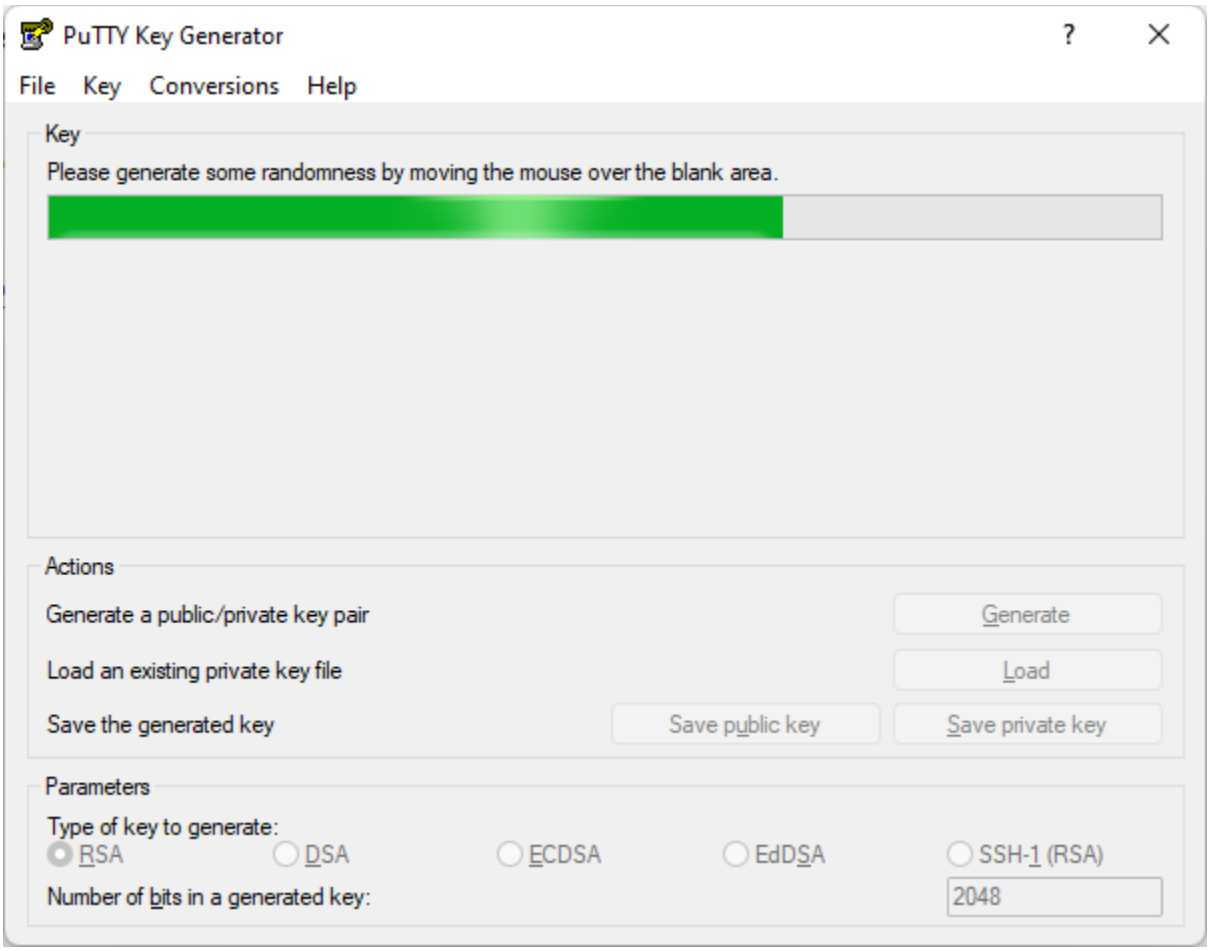

The user account password will only be used for physical console access to the device. Use a password that is complex and very long. In most cases, the device will usually only be accessed using SSH and public-key authentication. The password supplied cannot be used to authenticate using SSH with these options. Only public-key authentication will be capable of authenticating with SSH.

A variety of tools can be used to create a key to authenticate with a device. In this case PuttyGen was used [SSH Academy].

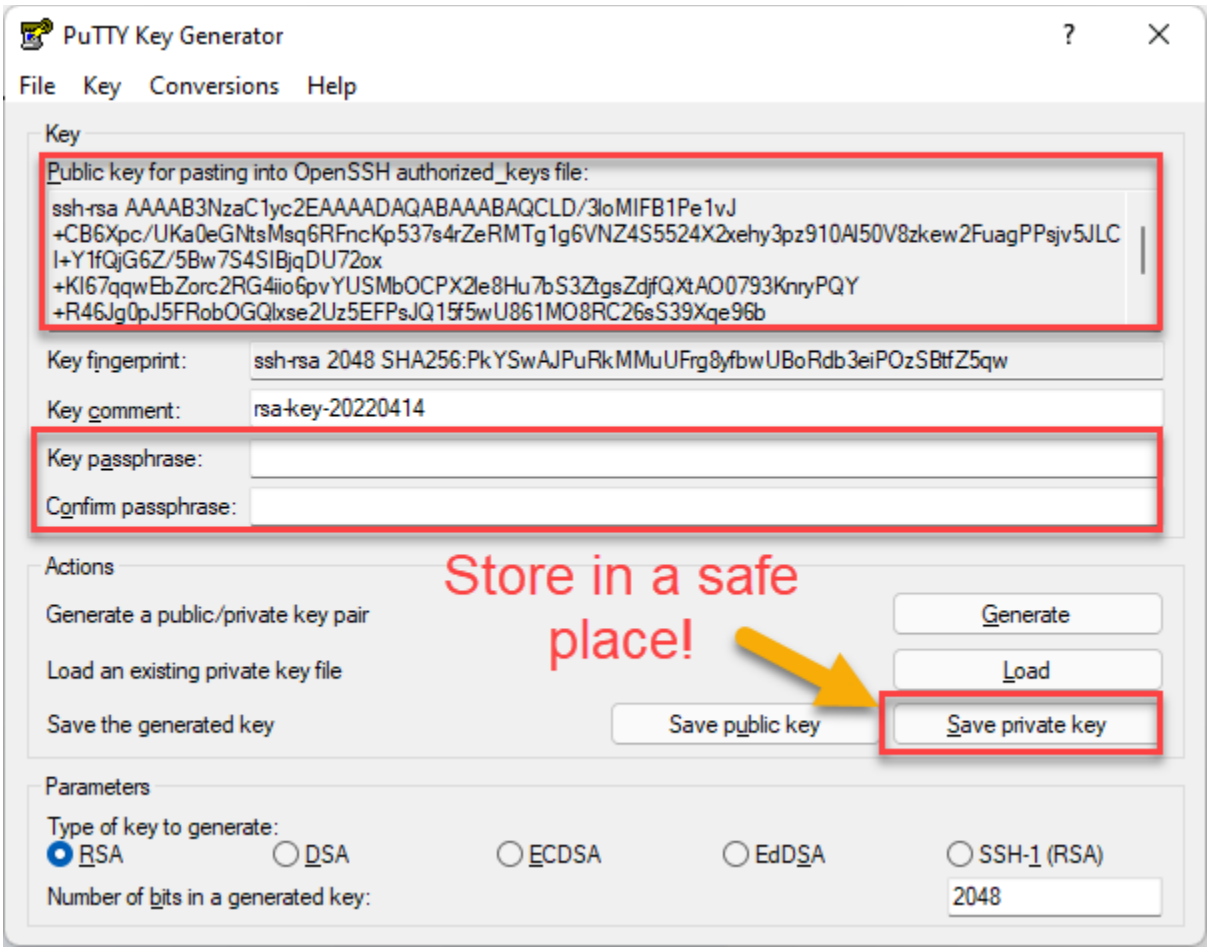
Through this process, two keys will be created:

- Public key → stored on device hosting SSH services (your honeypot in this case)
- Private key → used by device to access honeypot over SSH public-key authentication

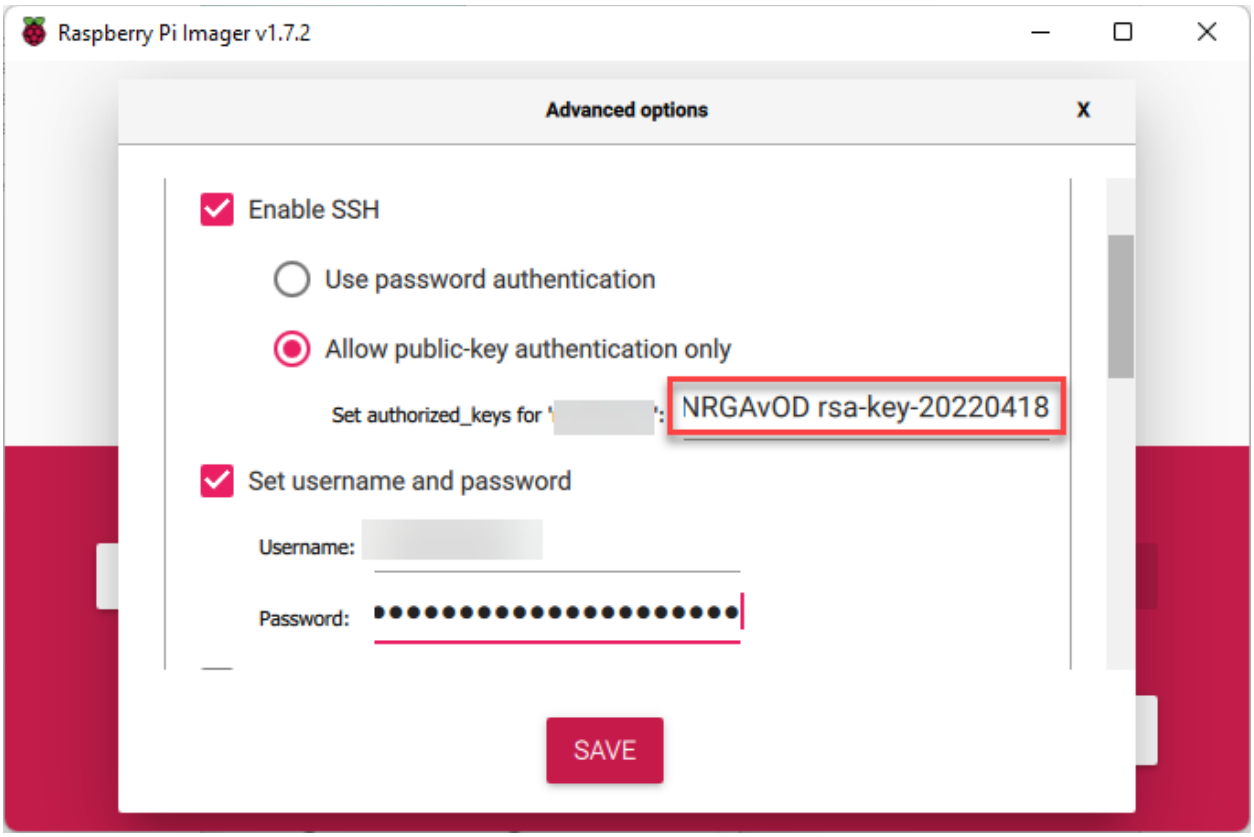

PuTTY Key Generator
File
Key
Conversions
Help
Key
No key.
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA
DSA
ECDSA
EdDSA
SSH-1 (RSA)
Number of bits in a generated key:
2048




For extra protection of your key, enter and confirm a passphrase to be used. You will need to save the public and private keys so that you can use them for further steps. The private key is very important to protect since this is what will be used to authenticate to whatever service you're using. This is where a passphrase can help to protect that data, or it can be stored in another fashion to limit its access, such as offline or in a password manager protected by multi-factor authentication.

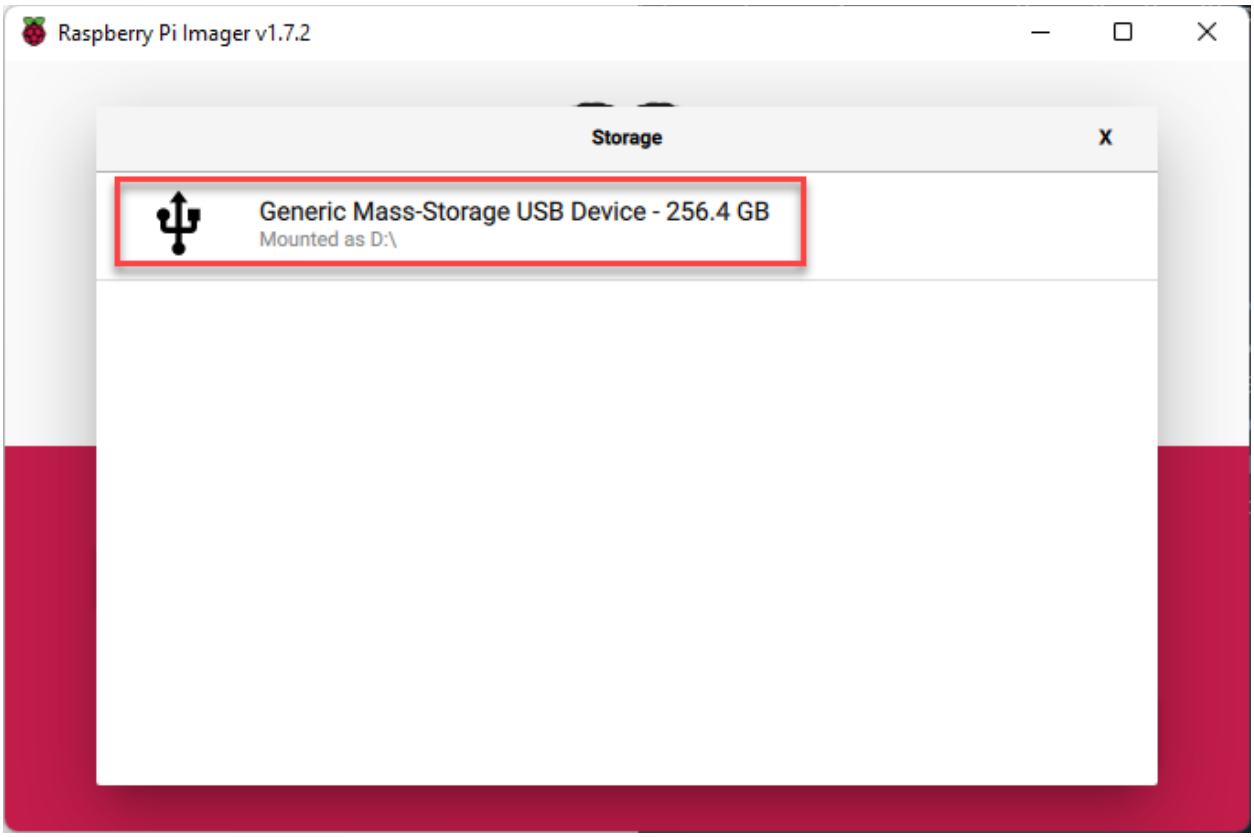



The public key will be entered into the last field of the Raspberry Pi Imager software.




**Write OS to micro SD card**

If you haven't already, you will need to choose your media by using the "Storage" button. It will likely only display your micro SD card media. If nothing is showing, try reconnecting your micro SD card media and check you system to see that it is properly detected.




Choose the gear in the lower-right to customize your settings.

Other options can be customized as desired. Choose the “WRITE” option to deploy the image to the micro SD card.

**Plug micro SD card and boot Raspberry Pi and run updates**

You’ll notice that very quickly you’ll be up and running at a terminal prompt (or GUI) if you used the automated option. Make sure to run updates!

```
sudo apt-get update; sudo apt-get full-upgrade -y
```

In our case, everything was already fully updated.

```
[  OK  ] Reached target Multi-User System.
         Starting Update UTMP about System Runlevel Changes...
[  OK  ] Started LSB: Resize the root filesystem to fill partition.
[  OK  ] Finished Update UTMP about System Runlevel Changes.

                    :~ $ sudo apt-get update; sudo apt-get full-upgrade
Get:1 http://archive.raspberrypi.org/debian bullseye InRelease [23.7 kB]
Get:2 http://archive.raspberrypi.org/debian bullseye/main arm64 Packages [272 kB]
Get:3 http://archive.raspberrypi.org/debian bullseye/main armhf Packages [278 kB]
Hit:4 http://deb.debian.org/debian bullseye InRelease
Get:5 http://security.debian.org/debian-security bullseye-security InRelease [44.1 kB]
Get:6 http://deb.debian.org/debian bullseye-updates InRelease [39.4 kB]
Get:7 http://security.debian.org/debian-security bullseye-security/main arm64 Packages [124 kB]
Get:8 http://security.debian.org/debian-security bullseye-security/main armhf Packages [127 kB]
Get:9 http://security.debian.org/debian-security bullseye-security/main Translation-en [80.6 kB]
Fetched 988 kB in 7s (144 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
                    :~ $
```

**Install DShield from GitHub**

Get the DShield source from GitHub and start the install! There are also instructions available at this site as well. No additional instructions will be reviewed, but some screenshots have been included in the appendix of this write-up to show you what the full process may look like.

https://github.com/DShield-ISC/dshield

```
POSTINSTALL OPTION

In case you need to do something extra after an installation, especially when you do an automatic
update, in which case you may loose changes made after the initial installation.
For this situation you can have a post-installation script in /root/bin/postinstall.sh, which
will be called at the end of processing the install.sh script, also called in the automatic update.


Done.

Please reboot your Pi now.

For feedback, please e-mail jullrich@sans.edu or file a bug report on github
Please include a sanitized version of /etc/dshield.ini in bug reports
as well as a very carefully sanitized version of the installation log
  (/srv/log/install_2022-04-13_220221.log).

IMPORTANT: after rebooting, the Pi's ssh server will listen on port 12222
           connect using ssh -p 12222

### Thank you for supporting the ISC and dshield! ###

To check if all is working right:
   Run the script 'status.sh' (but reboot first!)
   or check https://isc.sans.edu/myreports.html (after logging in)

 for help, check our slack channel: https://isc.sans.edu/slack

 In case you are low in disk space, run /srv/dshield/cleanup.sh
 This will delete some backups and logs
Log: /srv/log/install_2022-04-13_220221.log
                    :~/dshield/bin $
```

After the setup is completed, restart your Honeypot and you should be all set!

**Expose honeypot to internet**

To start getting logs, you will need to expose your honeypot to start collecting data. Check with the manufacturer for your own router settings. In many cases this may be using the DMZ function to exposed this device to the internet using it's internal IP address.

```
ls /srv/cowrie/var/lib/cowrie/tty/
ls /srv/cowrie/var/lib/cowrie/downloads/
```

TTY will show logged command interactions with the honeypot and downloads will be a repository for any requested download or upload from an attack.

**Optional – Configure additional local honeypot logging**

Get a more interesting experience by adding more logging so that you can review even more data directly on your honeypot.

To enable more logging, edit the following files (you have to edit them as root):

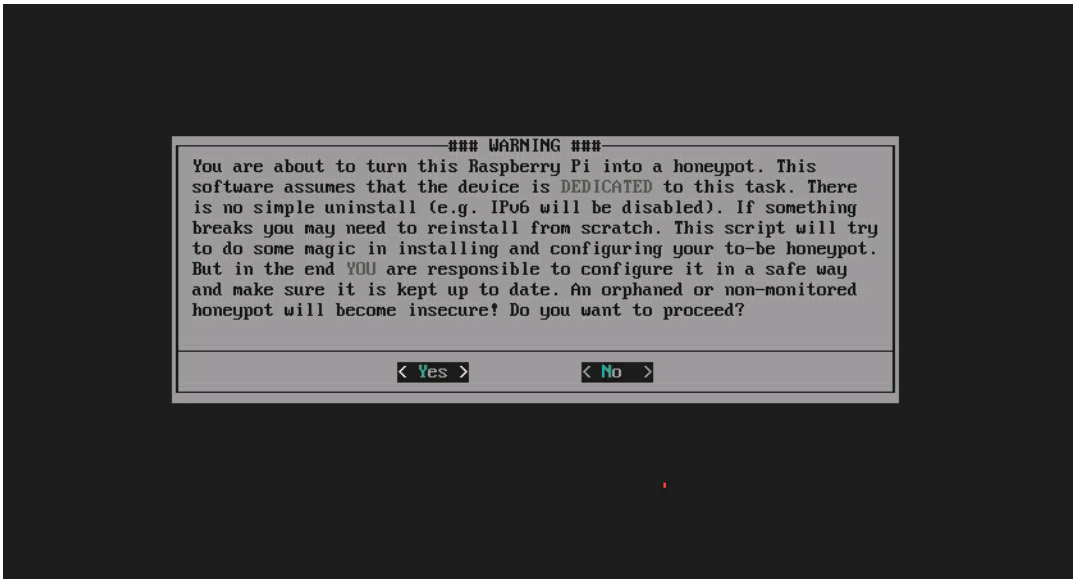
/etc/dshield.ini : add the line "localcopy=/tmp/local.log"

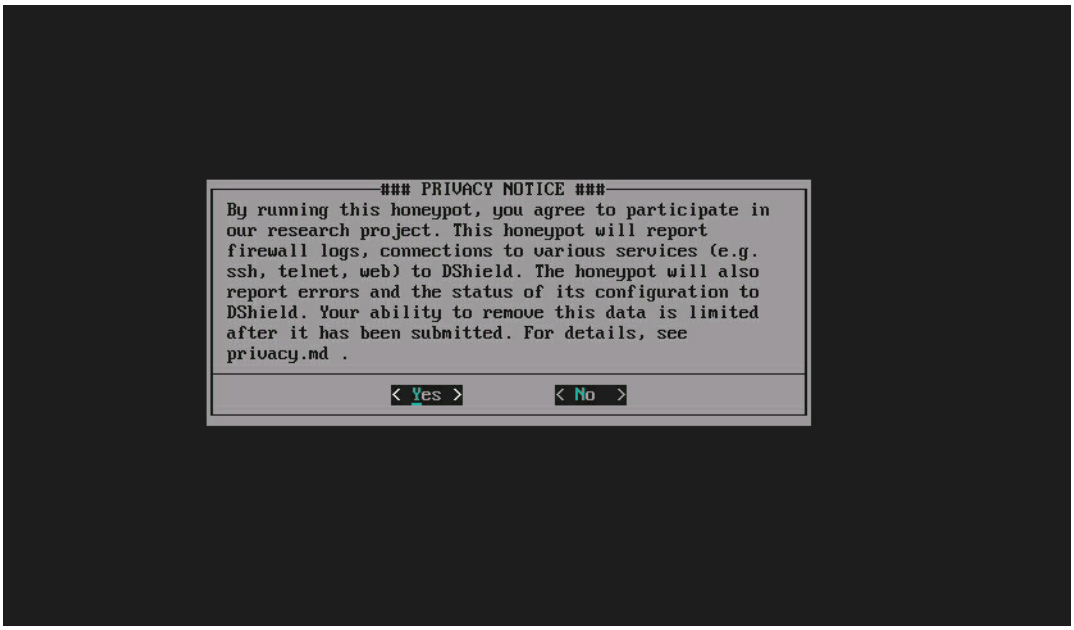
/srv/cowrie/cowrie.cfg: change the line "ttylog = false" to "ttylog = true"

[Ars Technica] https://arstechnica.com/gadgets/2022/04/raspberry-pi-os-axes-longstanding-default-user-account-in-the-name-of-security/

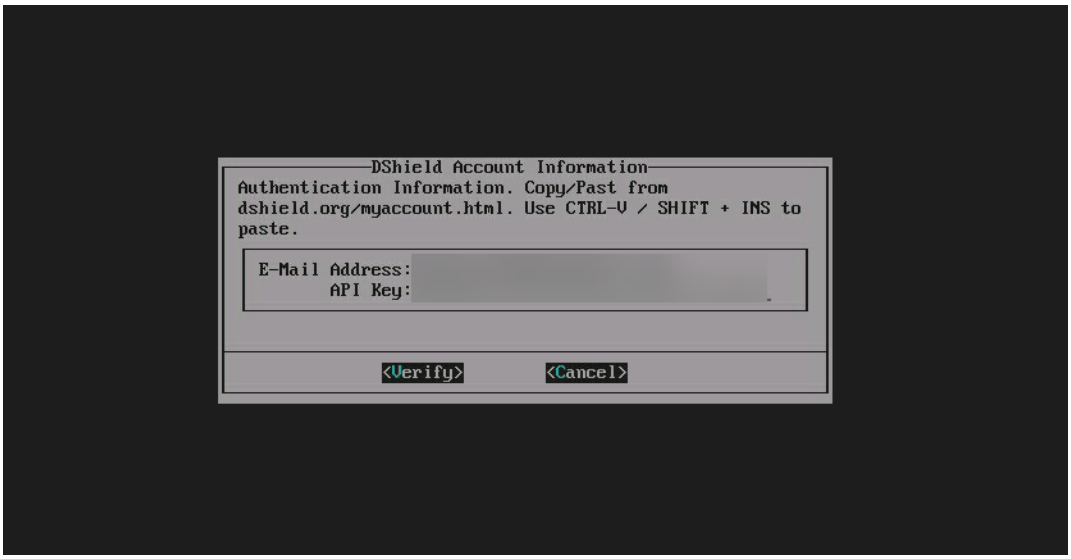
[SSH Academy] https://www.ssh.com/academy/ssh/putty/windows/puttygen

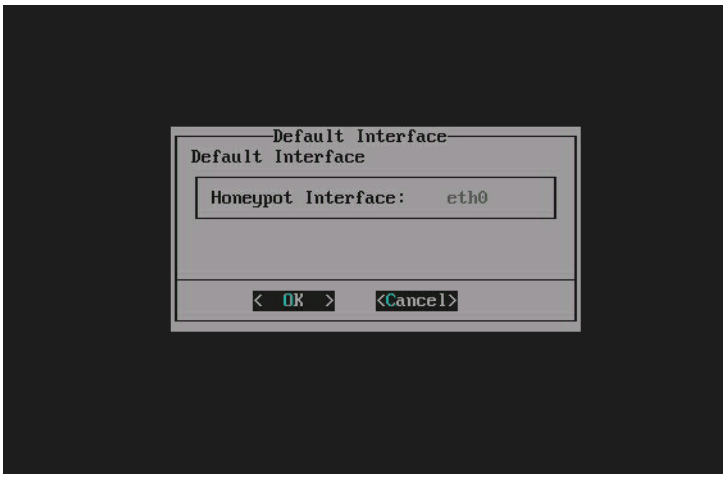
**Appendix – Additional setup screenshots**

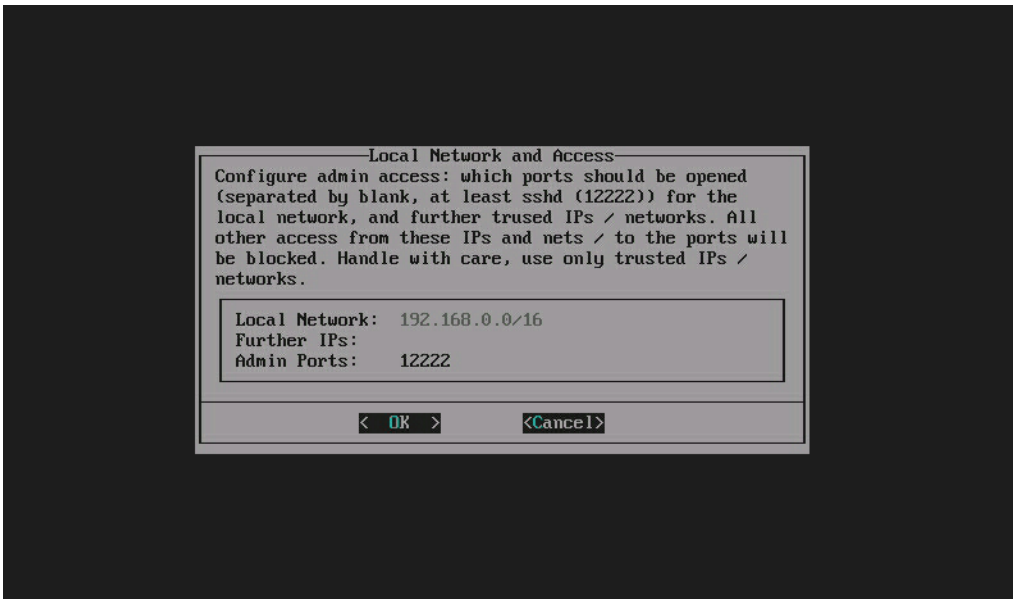


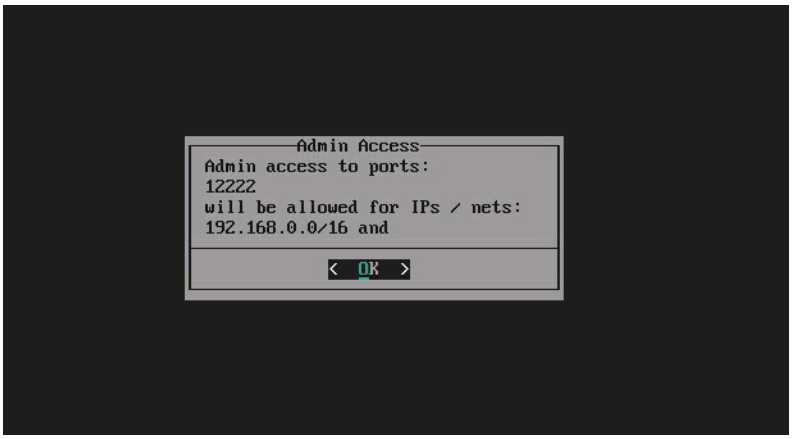

### PRIVACY NOTICE ###
By running this honeypot, you agree to participate in our research project. This honeypot will report firewall logs, connections to various services (e.g. ssh, telnet, web) to DShield. The honeypot will also report errors and the status of its configuration to DShield. Your ability to remove this data is limited after it has been submitted. For details, see privacy.md .
< Yes >
< No >

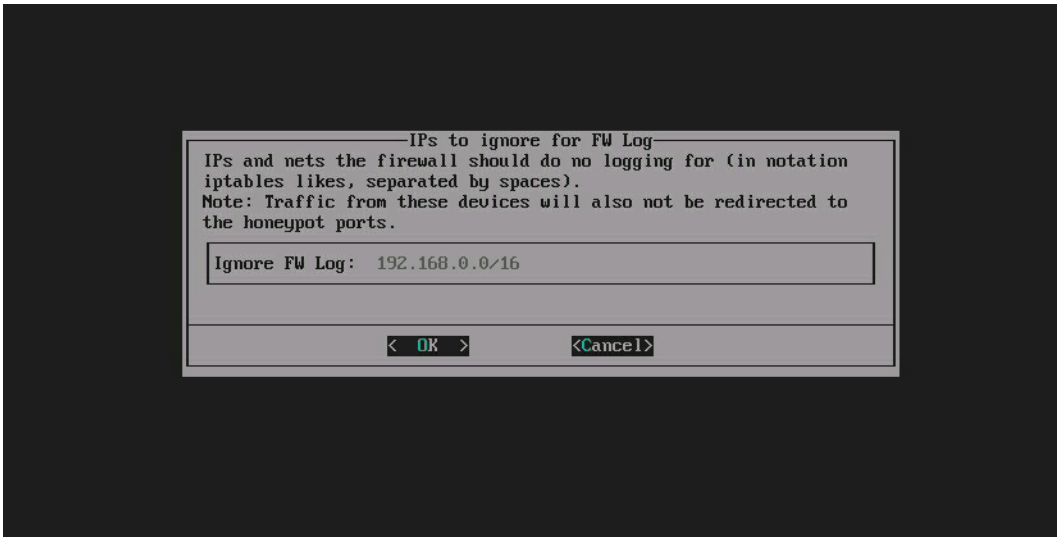

Automatic Updates
We do release updates periodically, and recommend you apply them automatically. Please choose if you want them or if you want to keep up your dshield stuff up-to-date manually.
( ) manual
(*) automatic
< OK >
<Cancel>


DShield Account Information
Authentication Information. Copy/Past from dshield.org/myaccount.html. Use CTRL-V / SHIFT + INS to paste.
E-Mail Address:
API Key:
<Verify>
<Cancel>

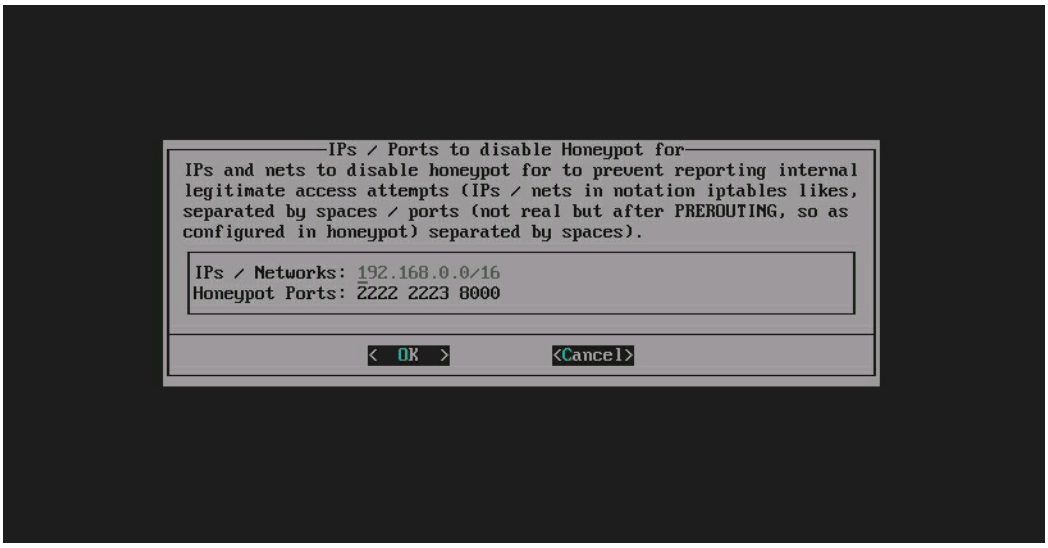

Default Interface
Default Interface
Honeypot Interface: eth0
< OK >
<Cancel>

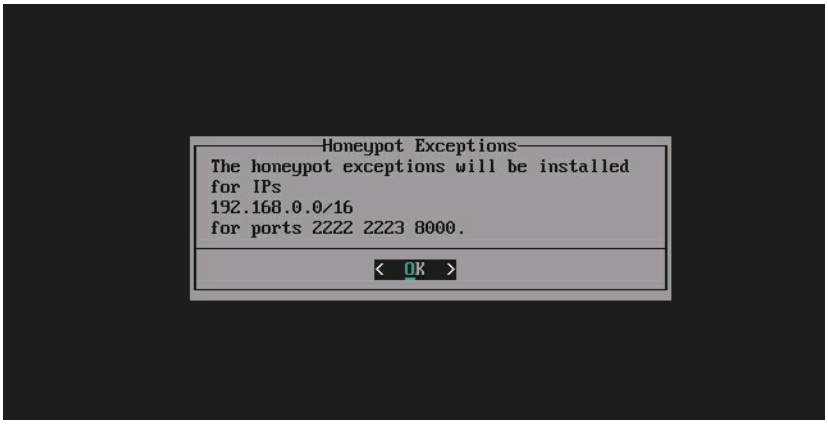

Local Network and Access
Configure admin access: which ports should be opened (separated by blank, at least sshd (12222)) for the local network, and further trused IPs / networks. All other access from these IPs and nets / to the ports will be blocked. Handle with care, use only trusted IPs / networks.
Local Network: 192.168.0.0/16
Further IPs:
Admin Ports: 12222
< OK >
<Cancel>


Admin Access
Admin access to ports:
12222
will be allowed for IPs / nets:
192.168.0.0/16 and
< OK >


IPs to ignore for FW Log
IPs and nets the firewall should do no logging for (in notation
iptables likes, separated by spaces).
Note: Traffic from these devices will also not be redirected to
the honeypot ports.
Ignore FW Log: 192.168.0.0/16
< OK >
<Cancel>

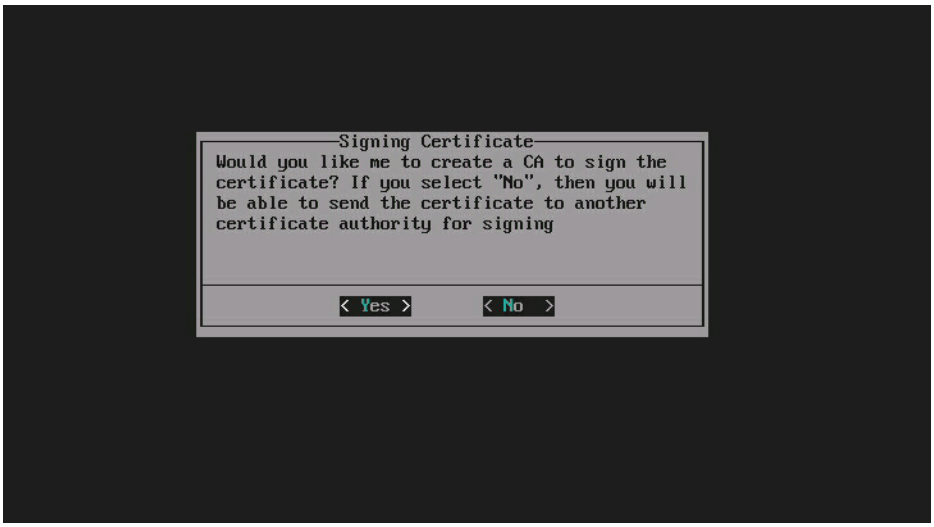

Firewall Logging Exceptions
The firewall logging exceptions
will be installed for IPs
192.168.0.0/16
< OK >




```
Doing further configuration
Added user 'cowrie'
Installing Python packages with PIP. This will take a LOOONG time.
Doing further cowrie configuration.
Installing and configuring postfix.
package configuration for postfix
```


Creating SSL Certificate
Enter the details for your SSL Certificate
Country: US
State: Florida
City: Jacksonville
Company: DShield
Depart.: Decoy
Hostname :
< OK >
<Cancel>


Signing Certificate
Would you like me to create a CA to sign the certificate? If you select "No", then you will be able to send the certificate to another certificate authority for signing
< Yes >
< No >