

[howto](#), [debian](#), [dropbear](#), [luks](#)

Install/Configure dropbear for remote unlocking encrypted root/swap-file systems functionality

- <https://www.hagen-bauer.de/2018/09/verschl%C3%BCsselt-es-debian-remote-starten.html>
- <https://www.arminpech.de/2019/12/23/debian-unlock-luks-root-partition-remotely-by-ssh-using-dropbear/>



This might be a further advancement. If I get it right - It's limiting the SSH key to one specific command and also automates execution of that command.

- <https://ctrlnotes.com/restrict-a-user-to-ssh-forced-command/#>

```
apt update && apt -y install busybox dropbear-initramfs
echo 'DROPBEAR=y' >> /etc/initramfs-tools/initramfs.conf
sed -i 's/DEVICE=/DEVICE=<YOURNETWORKDEVICE>/' /etc/initramfs-tools/initramfs.conf
echo 'IP:::::<YOURHOSTNAME>-luks:<YOURNETWORKDEVICE>:dhcp' >> /etc/initramfs-tools/initramfs.conf
echo "<YOURSSHPUBLICKEY>" >> /etc/dropbear-initramfs/authorized_keys
echo "<YOURBACKUPSSHPUBLICKEY>" >> /etc/dropbear-initramfs/authorized_keys
update-initramfs -u
```

If you have authenticated via your SSH-key and are logged on to dropbear's SSH server, use the following command to decrypt the LUKS partition and to get prompted for a password:



```
# connect to dropbear's SSH server on denker,
# you will get authenticated with your SSH key.
ssh <YOURHOSTNAME>-luks -l root
# then issue the following command:
cryptroot-unlock
# now enter the LUKS passphrase
```

~~DISCUSSION~~

From:
<https://wiki.nanoscopic.de/> - nanoscopic wiki

Permanent link:
<https://wiki.nanoscopic.de/doku.php/pages/howtos/debian/dropbear-luks?rev=1688387170>

Last update: 2023/07/03 12:26

