

[How To] Full Install of Kali Linux on USB with LUKS Encryption and UEFI

Intro: This guide details a full install of Kali Linux on a USB or portable disk with Full Disk Encryption that is recognized as a UEFI device across multiple computers.

Note: By default, when Kali Linux is installed in UEFI mode, it records the boot configuration to the NVRAM of the host machine where it was installed; these boot instructions are lost once the disk is removed from the machine and the USB/disk will no longer be recognized as a UEFI disk. This guide will show you how to manually set up the encrypted partitions using Kali installer and install the grub configuration to the disk so as to make it portable and recognized as a UEFI disk across new PCs and Macs.

It will also show you how to install/reinstall grub to the USB/disk if no longer recognized as UEFI or removed from NVRAM (skip install and jump to ' [Fixing / Re-Installing GRUB to the Disk when not recognized as UEFI](#)').

1. Preparatory Steps:

Do a full backup of all your important files and the internal drives of the PC you will be using.

Format both USB/Disks you will be using with a GPT partition table.

Create a Kali Linux Live USB Install as described in the official documentation here:

<https://docs.kali.org/downloading/kali-linux-live-usb-install>

> download the iso from <https://www.kali.org/downloads/>
> verify iso with `sha256sum -b *.iso`
> write the image to disk with `dd if=kali-linux-2019.2-amd64.iso of=/dev/sd* bs=512k`

Enter Bios/UEFI firmware and disable 'fast boot' and 'secure boot' options; Make sure you will boot in UEFI mode.

> to access UEFI settings on new computers pre-installed with Windows 10 go to:

Settings > Update & Security > Recovery > Advanced start-up > Restart now

> On the next screen choose:

Troubleshoot > Advanced options > UEFI Firmware Settings

> the computer should restart in the BIOS/UEFI Menu; disable 'secure boot' and 'fast boot' options.

As the install will try to detect and write to an EFI partition, and will also mess with the boot entries in NVRAM, I strongly suggest removing any internal disk(s) with other Operating Systems installed before proceeding.

Note: If you have a bitlocker encrypted drive, make sure that you disable it or that you have the recovery key before changing the BIOS/UEFI settings and/or unplugging the internal disks!

2. Begin Installing Kali Linux

Note: Kali default installation settings for LUKS encrypted volume will partition the drive similar to the manual steps described bellow, but will format the boot partition with ext4 instead of ext2, and will create a swap partition twice the size of available RAM - which can end up being overkill in today's machines; You can even dispense with swap altogether but I find it useful to have it in a portable system; I allot 4GB of the disk to swap to reside alongside the root system on a LUKS encrypted volume.

Plug in both USB/Disks (one with the Kali Live system and the other with an empty GPT partition table); If no other disk is present it will automatically detect and boot into the Kali Live system - otherwise you will have to get into the Bios/UEFI settings and make the UEFI USB disk the default boot option.

> always use the USB ports directly connected to the motherboard (and not the ones on the PC case)!

On the Kali grub boot screen choose 'Start installer' - or you can use the Live System to format the USB/portable Disk if you haven't yet done so. Use the pre-installed 'Disks' or 'Gparted' program to create a new GPT partition table on the target device.

Note: On systems with Nvidia Graphics card, there will be several 'nouveau' errors on boot - if that is the case, restart the computer and on the grub boot screen, while highlighting the desired option (either 'Live system' or 'Start Installer'), press the keyboard 'e' and move down the cursor to the line starting with 'linux' and add the entry 'nouveau.modeset=0' (I usually add it after the 'splash' or 'quiet' arguments); press F10 to boot.

On the Installer go through the language and keyboard choices, the default network to be used, hostname and domain settings, and configure the root password.

I have found that the installer asks for confirmation if to install in UEFI mode, even on a machine where all systems have been installed in UEFI (contrary to what the installer thinks); choose 'yes' and continue.

3. Manual Partitioning the Disk

Note: You may use the option 'Guided - use entire disk and set up encrypted LVM' but be aware that you may end up with a swap partition of 16GB or 32GB, depending on the RAM detected; manual partition the disk to allocate your desired partition sizes.

At the partition disks screen choose 'Manual' option and continue.

You should see both your USB devices - the target device should only contain 'FREE SPACE'; Double click the target device and choose 'yes' to 'create a new empty partition table on this device'.

Create the EFI System Partition

> choose the FREE SPACE > create a new partition > 256 MB > Beginning > 'Use as' = EFI System Partition > (make sure bootable flag is **on**) > Done setting up the partition.

Create the boot partition (boot partition does not contain any sensitive information and there is no need to encrypt it)

> choose the FREE SPACE > create a new partition > 768 MB > Beginning > 'Use as' = Ext2 file system > 'mount point' = /boot > (make sure bootable flag is **off**) > Done setting up the partition.

Create the encrypted Volume

> choose the FREE SPACE > create a new partition > (use remaining space or as much as you need) > Beginning > 'Use as' = physical volume for encryption > Done setting up the partition;

> Choose 'Configure encrypted Volumes' and confirm to 'write the changes to disk and configure encrypted volumes';

> Choose 'Create encrypted volumes' > selected partition to encrypt (should be the /dev/sd*3, identified by 'crypto') > Finish;

> Confirm to erase and overwrite with random data (you may want to cancel at the next screen if you do not require the full disk to be overwritten... it will save a lot of time and some wear on the USB);

> choose encrypted passphrase - use <https://www.useapassphrase.com/> to generate a strong and easy to remember passphrase.

Create Logical Volumes for root and swap

> choose 'Configure the Logical Volume Manager' and confirm to 'write changes to disks and configure LVM';

> choose 'Create volume group' and give it a name (for the purpose of this tutorial lets call it 'VGkali');

> choose the encrypted volume (that should be opened at /dev/mapper/sd*3_crypt) > confirm to 'write changes to disks and configure LVM';

> choose 'Create logical volume' > choose the Volume group (VGkali as per the earlier example) > give it a name (for the purpose of this tutorial lets call it 'lgswap') > choose your swap size (2048MB or 4096MB is enough);

> choose 'Create logical volume' > choose the Volume group (VGkali as per the earlier example) > give it a name (for the purpose of this tutorial lets call it 'lgroot') > use remaining space as suggested or customize to your preference;

> Finish.

Configure the Logical Volumes

> select the entry #1 under 'LVM VG VGkali, LV lgroot' > 'Use as' = Ext4 journaling file system > 'mount point' = / - the root file system > Done setting up the partition;

> select the entry #1 under 'LVM VG VGkali, LV lgswap' > 'Use as' = swap area > Done

setting up the partition;

- > Finish partitioning and write changes to disk;
- > Confirm to 'write the changes to disks' and proceed with the installation.

4. Finishing Installation

When asked if to 'Use a network mirror' make sure to answer **YES** so you have access to additional software; you can leave 'HTTP proxy information' blank and continue.

When you reach the 'Installation complete' screen you can remove the Kali Live USB Install and press continue; the installer will finish cleaning up and will reboot automatically.

Note: **DO NOT REMOVE THE USB/DISK WHERE THE SYSTEM WAS INSTALLED!** Just reboot into the newly installed Kali system while the boot configuration is still stored in the NVRAM; it should bring you straight into the Kali grub screen.

Note: If you have an Nvidia Graphics Card, make sure to press the 'e' key while highlighting the 'Kali GNU/Linux' option and add the 'nouveau.modeset=0' option as described earlier.

Boot into Kali Linux and input your Encryption passphrase to open the encrypted volumes when asked.

choose 'root' as the username and input your root password chosen at install.

5. Installing Grub to Disk and Making the System Portable

Once booted into the full install of Kali, edit the grub defaults file to allow installation on an encrypted drive:

> Open terminal and type:

```
nano /etc/default/grub
```

> add the following line below all the other GRUB options listed:
`GRUB_ENABLE_CRYPTODISK=y`

> NOTE: if you have an Nvidia Graphics Card you can also add the '`nouveau.modeset=0`' option after '`quiet`' under the '`GRUB_CMDLINE_LINUX_DEFAULT`' - be sure to install the nvidia drivers after.

> 'Ctrl + o' to save the file, 'Ctrl + x' to exit nano editor.

In the terminal run the following commands to install grub to the USB drive:

```
grub-install --target=x86_64-efi --efi-directory=/boot/efi --bootloader-id=kali-grub --boot-  
directory=/boot --removable --recheck --debug
```

```
update-grub
```

exit the terminal and reboot the system; It will ask you the encryption passphrase twice (once immediately after boot and again after the Kali grub menu); to change this behavior, edit again the `/etc/default/grub` and remove/comment out the '`GRUB_ENABLE_CRYPTODISK=y`' set earlier;
> Once it's done, run `update-grub` once again.

Note: At this point, you should have a fully installed and encrypted Kali system to a portable USB disk that is recognized as a UEFI device across computers, including Macs. I would suggest running the first updates batch on the computer where you've installed the system (without any other OS installed) as the update will automatically run an `update-grub` and this will detect any other OS present and show the options in the grub menu next time booting (if you are moving the disk across devices you will be picking up a few 'ghost entries' each time `update-grub` is run; You can boot and run the command on a PC/laptop in which you removed the internal disk to rebuild the grub menu without any other options or you can manually edit them).

6. Fixing / Re-Installing GRUB to the Disk when not recognized as UEFI

If your device stops being recognised as an UEFI drive, or if your EFI partition gets corrupted, or if you've installed the system but removed it from the PC before installing the grub to the drive, you can always reinstall grub and fix most boot issues; You will need to boot into a Kali Live USB System to do this:

Plug both USB disks to the computer and boot - if there isn't any other disk/OS installed it should boot into the grub screen of the Kali Live USB; choose to boot the 'Live System'.

Note: If you have a Nvidia Graphics Card follow the steps described earlier to add the 'nouveau.modeset=0' option to boot.

Open the terminal and find your disk structure with the following command:

```
fdisk -l
```

> make a note which one is the encrypted drive - if you followed the partition scheme above should be /dev/sd*3

Issue the following command to unlock your encrypted Volume

(for the sake of this tutorial we are assuming that your USB disk is partitioned as described earlier and that your Volume Group is named VGkali and your Logical Volumes within it are named lgroot and lgswap)

```
cryptsetup open /dev/sd*3 cryptkali
```

> enter your passphrase when asked

Scan for logical volumes and make sure they are active

```
lvscan
```

Make sure the logical volumes are mapped:

```
ls /dev/mapper
```

Mount all necessary folders as needed:

```
mount /dev/mapper/VGkali-lgroot /mnt
```

```
mount --bind /dev /mnt/dev
```

```
mount --bind /proc /mnt/proc
```

```
mount --bind /sys /mnt/sys
```

```
mount --bind /sys/firmware/efi/efivars /mnt/sys/firmware/efi/efivars
```

```
mount /dev/sd*2 /mnt/boot
```

```
mount -o remount,rw /dev/sd*1 /mnt/boot/efi
```

```
mkdir /mnt/hostrun
```

```
mount --bind /run /mnt/hostrun
```

Chroot into your mounted system:

```
chroot /mnt
```

run the following commands:

```
mkdir /run/lvm
```

```
mount --bind /hostrun/lvm /run/lvm
```

Edit the grub defaults file to allow installation on an encrypted drive if you haven't yet done so:

```
nano /etc/default/grub
```

> add the following line below all the other GRUB options listed:

```
GRUB_ENABLE_CRYPTODISK=y
```

> Note: if you have an Nvidia Graphics Card you can also add the 'nouveau.modeset=0' option after 'quiet' under the 'GRUB_CMDLINE_LINUX_DEFAULT' - be sure to install the nvidia drivers after.

> 'Ctrl + o' to save the file, 'Ctrl + x' to exit nano editor.

Install grub to the disk with:

```
grub-install --target=x86_64-efi --efi-directory=/boot/efi --bootloader-id=kali-grub --boot-directory=/boot --removable --recheck --debug
```

Update grub to generate the boot configuration files:

```
update-grub
```

Note: at this point the command seems to hang - in all the times I've tried it, it takes about 10 minutes until the terminal returns 'Generating grub configuration file' and another 10 minutes until it starts outpouring warnings regarding the devices not being 'initialized in udev database'; At this time I just interrupt the command with 'Ctrl + c' and continue;

Exit chroot and proceed to unmount the drives:

```
exit
```

```
umount /mnt/dev
```

```
umount /mnt/proc
```

```
umount /mnt/sys/firmware/efi/efivars
```

```
umount /mnt/sys
```

```
umount /mnt/boot/efi
```

```
umount /mnt/boot
```

```
umount /mnt/hostrun
```

```
umount /mnt/run/lvm
```

```
umount /mnt
```


Power-off, remove the Kali Live Install USB drive and restart the system - it should boot into the default Kali grub screen and the usb drive should be recognized as a UEFI disk across PCs and Macs.

To disable having the system ask for the encryption passphrase twice at boot, edit again the `/etc/default/grub` on the installed system and remove/comment out the 'GRUB_ENABLE_CRYPTODISK=y' set earlier;
> Once it's done, run `update-grub` once again.

You should now have a fully installed and portable version of Kali Linux.

The quieter you become, the more you are able to hear.

Revision #10

Created Sat, Jun 1, 2019 12:00 PM by [Editor](#)

Updated Fri, Jun 12, 2020 1:03 PM by [Editor](#)