**Linux and Unix Encryption at Rest**

Contents

[1. **LUKS** - https://access.redhat.com/solutions/100463 1](#_Toc72502540)

[**Environment** 1](#_Toc72502541)

[**Issue** 1](#_Toc72502542)

[**Resolution** 1](#_Toc72502543)

[2. Veracrypt 2](#_Toc72502544)

# **LUKS** - <https://access.redhat.com/solutions/100463>

**LUKS** (Linux Unified Key Setup) is a cross distribution, kernel based **disk encryption** standard. A central component of which is that all necessary setup information is stored within the format header; giving **full** decryption portability. ... This helps to keep things simple and in line with a 'single **disk** single use' remit.

## **Environment**

* **Red Hat Enterprise Linux (RHEL) 5, 6, 7, 8**

## **Issue**

* What is LUKS? cryptsetup? dm-crypt?
* What is the difference between cryptsetup plain and cryptsetup LUKS?
* What packages are required for LUKS in Red Hat Enterprise Linux?
* How can LUKS HDD-encryption be accomplished in Red Hat Enterprise Linux?
* What cipher does LUKS use to encrypt a disk?
* How big are the encryption keys LUKS uses? Can this be changed?
* Why do devices encrypted with cryptsetup use a different mode than devices encrypted at install-time?

## **Resolution**

* **Targeted solutions:**
  + [How to configure encrypted storage with LUKS using passphrases](https://access.redhat.com/solutions/447423)
  + [How to configure encrypted storage with LUKS using exportable keys instead of passphrases](https://access.redhat.com/solutions/1121163)
  + [How to add a passphrase, key, or keyfile to an existing LUKS device](https://access.redhat.com/solutions/230993)
  + [How to extend a LUKS encrypted volume](https://access.redhat.com/solutions/236543)
  + [How to extend a volgroup and filesystem backed by LUKS-formatted encrypted physical volumes](https://access.redhat.com/solutions/302923)
  + [How to change cipher, key-size, hash, master key of existing LUKS device](https://access.redhat.com/solutions/1162843)
  + [How can a specific directory on a filesystem be encrypted?](https://access.redhat.com/knowledge/solutions/202513)
  + [How to configure encrypted swap](https://access.redhat.com/solutions/1121603)
  + [How to recover lost LUKS key or passphrase](https://access.redhat.com/solutions/1543373)
  + [How to have a root LUKS partition decrypted without a password](https://access.redhat.com/solutions/256833)
  + [How to create LUKS-Encrypted image and mount it at boot](https://access.redhat.com/solutions/3440681)
  + [How to encrypt root volume group online using LUKS in RHEL?](https://access.redhat.com/solutions/2339691)
* **In-depth knowledge article for additional answers:**
  + [All about LUKS, cryptsetup, and dm-crypt](https://access.redhat.com/knowledge/articles/193443)
* **Product documentation references:**
  + [RHEL6 Installation Guide, Appendix C: Disk Encryption](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html-single/Installation_Guide/#Disk_Encryption_Guide)
  + [RHEL6 Security Guide: LUKS Disk Encryption](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/chap-Security_Guide-Encryption.html#sect-Security_Guide-LUKS_Disk_Encryption)
  + [RHEL7 Security Guide: Using LUKS Disk Encryption](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-Encryption.html#sec-Using_LUKS_Disk_Encryption)
  + [RHEL8 Security Hardening: Encrypting block devices using LUKS](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/encrypting-block-devices-using-luks_security-hardening)
* this is the article, we could test it on a non-prod first for testing

<https://unix.stackexchange.com/questions/444931/is-there-a-way-to-encrypt-disk-without-formatting-it#:~:text=The%20LUKS%20cryptsetup%20utility%20contains,should%20still%20backup%20your%20data>.

Is there a way to encrypt disk without formatting it?

When I was installing my OS, I didn't encrypt. Is there a way to encrypt it now without formatting and without losing any data? I read a few guides how to encrypt and everyone says that I need to ...

unix.stackexchange.com

* I found this related to LUKS without formatting  
    
  <https://unix.stackexchange.com/questions/444931/is-there-a-way-to-encrypt-disk-without-formatting-it#:~:text=The%20LUKS%20cryptsetup%20utility%20contains,should%20still%20backup%20your%20data>.

# Veracrypt

* The latest versions of VeraCrypt are available as pre-compiled libraries via the sourceforge, so we need to download the archive (i386 or i686 for **32 bit system**s and amd64 or x86\_64 for 64 bit systems), extract it and run the installation scrypt.

<http://linuxg.net/install-veracrypt-on-linux/>

* Should work on all the popular Linux systems, including Ubuntu, Linux Mint, Pinguy OS, Elementary OS, Deepin, Peppermint, LXLE, Linux Lite, Debian, Robolinux, SparkyLinux, Fedora, CentOS, OpenSUSE, Mageia, OpenMandriva, Arch Linux, Manjaro, ROSA Desktop etc.