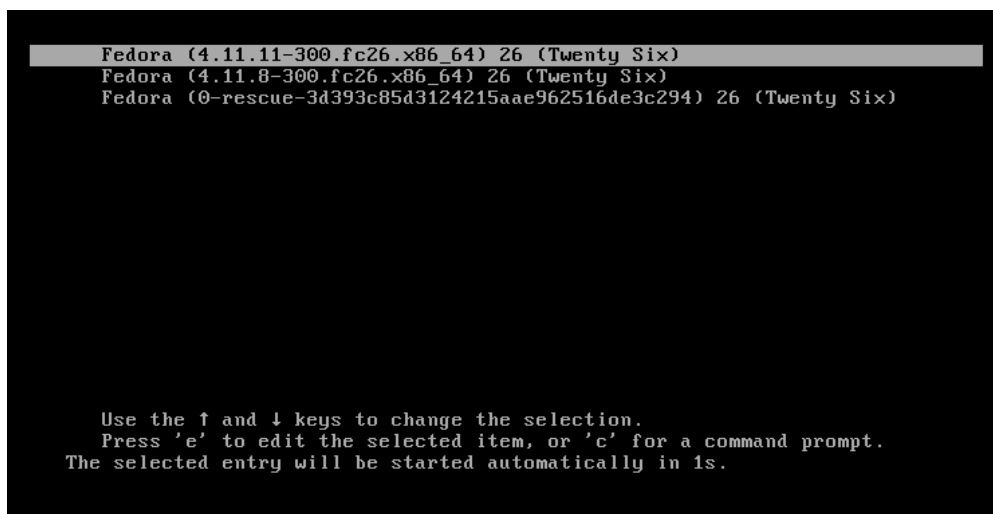# How to reset root password on Fedora

A system administrator can easily reset a password for a user that has forgotten their password. But what happens if the system administrator forgets the root password? This guide will show you how to reset a lost or forgotten root password. Note that to reset the root password, you need to have physical access to the machine in order to reboot and to access GRUB settings. Additionally, if the system is encrypted, you will also need to know the LUKS passphrase.

Edit the GRUB settings

First you need to interrupt the boot process. So you'll need to turn on the system or restart, if it's already powered on. The first step is tricky because the grub menu tends to flash by very quickly on the screen.
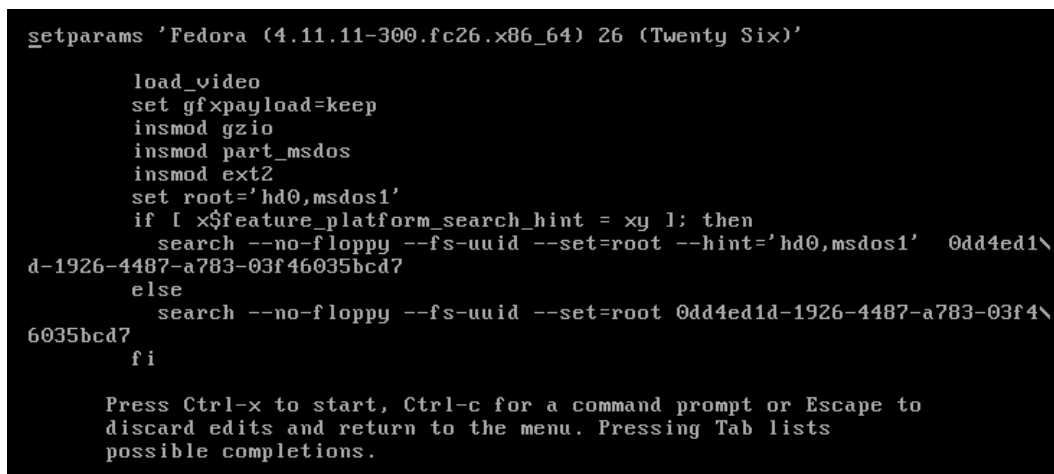
Press *E* on your keyboard when you see the GRUB menu:

After pressing 'e' the following screen is shown:

Use your arrow keys to move the the *linux16* line.

```
       linux16 /vmlinuz-4.11.11-300.fc26.x86_64 root=/dev/mapper/fedora-root \
ro rd.lvm.lv=fedora/root rd.lvm.lv=fedora/swap rhgb quiet LANG=en_US.UTF-8
       initrd16 /initramfs-4.11.11-300.fc26.x86_64.img


       Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
       discard edits and return to the menu. Pressing Tab lists
       possible completions.
```

Using your *del* key or *backspace* key, remove *rhgb quiet* and replace with the following.

rd.break enforcing=0

```
          search --no-floppy --fs-uuid --set=root 0dd4ed1d-1926-4487-a783-03f4\
   6035bcd7
          fi
          linux16 /vmlinuz-4.11.11-300.fc26.x86_64 root=/dev/mapper/fedora-root \
   ro rd.lvm.lv=fedora/root rd.lvm.lv=fedora/swap rd.break enforcing=0 LANG=en_US\
   .UTF-8
          initrd16 /initramfs-4.11.11-300.fc26.x86_64.img                        ↓


       Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
       discard edits and return to the menu. Pressing Tab lists
       possible completions.
```

After editing the lines, Press *Ctrl-x* to start the system. If the system is encrypted, you will be prompted for the LUKS passphase here.

Note: Setting enforcing=0, avoids performing a complete system SELinux relabeling. Once the system is rebooted, restore the correct SELinux context for the /etc/shadow file. (this is explained a little further in this process)

Mounting the filesystem

The system will now be in emergency mode. Remount the hard drive with read-write access:

 # mount –o remount,rw /sysroot

Password Change

Run chroot to access the system.

```
# chroot /sysroot
```

You can now change the root password.

```
# passwd
```

Type the new root password twice when prompted. If you are successful, you should see a message that *all authentication tokens updated successfully.*

Type *exit*, twice to reboot the system.

Log in as root and restore the SELinux label to the /etc/shadow file.

```
# restorecon -v /etc/shadow
```

Turn SELinux back to enforcing mode.

```
# setenforce 1
```