

# Security

## Filesystem

- [3 Best Ways to Securely Wipe Disk in Linux](#): shred, wipe

```
sudo shred -v /dev/sda
# or (if too slow)
sudo shred -v -n 1 /dev/sda
```

## Users

- show all logged in users: `users`
- show user/groups assignments and identifiers: `id`

## Files

- `/etc/passwd`: defines users, their primary groups and login shell
- `/etc/shadow`: password (hash) database
- `/etc/groups`: defines all other groups a user is in

## Sudoers

File `/etc/sudoers` defines users (and options) related to command `sudo`. It might make sense to specify a varying `umask` in `~/ .bashrc`.

```
if [[ $(id -u) -eq 0 ]]; then
    umask 0022
else
    umask 0027
fi
```

## Firewall

- show `iptables` firewall rules: `iptables -L -n -v`
- show [Uncomplicated Firewall](#) (UFW) rules: `sudo ufw status verbose`
- show all predefined UFW application profiles: `sudo ufw app list`
- establish rules from predefined UFW application profile: `sudo ufw allow from 192.168.178.0/24 to any app samba4`
- delete `allow` rules from UFW application profile: `sudo ufw delete allow from 192.168.178.0/24 to any app samba4`

## Files

- `/etc/ufw/applications.d/*`: predefined UFW application profiles
- `/var/log/ufw.log`: UFW log (for example blocked packets)

From:

<https://wiki.rho62.de/> - rho62 Wiki

Permanent link:

<https://wiki.rho62.de/doku.php?id=linux:administration:security>

Last update: **2025/07/24 13:49**

