

[Download](#)

---

The European framework for Quality and Self Regulation in Healthcare, of which has been downloaded by 31,000+€s rated, you will not see all the solutions provided in the. The most comprehensive pricing. Practical guidance and guidance on quality reporting, including. A free guide to training and development interventions for the resilience to change. a.Q: set all subdirectories of a specific folder to have Read-Only I was trying to set my.ssh folder to be read-only, however my question is that if i set the permissions of the folder to 777 it will be a disaster from what i have understood. I have some understanding of linux and i created a script with my idea as follows. `#!/bin/bash cd ~/.ssh setfacl -d -m d::rwx,d::g::rx,d::o::rx c:p:u setfacl -m u:user:rwx c:p:u #for duser:rwx c:p:d setfacl -d -m d::rwx,d::g::rx,d::o::rx c:p:u` How can I make a folder as read only for all its subdirectories? A: It's not the permissions per se that will cause problems with 777 permissions (actually I would generally consider those almost always a good idea, just putting that out there first), but the symlinks and links will cause the problems, as they will be able to overwrite data. The easiest way to avoid this would be to use setfacl to move all files and links that you don't want to be replaced under the.ssh directory. That means, moving all that into the.ssh directory will prevent them from being replaced. Another alternative would be to use acl commands, but I wouldn't do that. A: I assume you are speaking about the.ssh directory, and not about the.ssh folder itself. The way to do this is to make a file and execute it touch ~/.ssh/stopssh You then set your permissions so that the file has all the permissions you want, for example `sudo chmod 600 ~/.ssh/stopssh` Then, you can close your terminal and the changes should take effect. As a side note, you don't need to change permissions if you are

