

---

# pam\_listfile

Autorise ou refuse les services basé sur un fichier arbitraire

le module récupère l'item du type spécifié :

**user** spécifie le username, PAM\_USER  
**tty** spécifie le nom du terminal, PAM\_TTY  
**rhost** spécifie le nom de l'hôte distant, PAM\_RHOST  
**ruser** spécifie l'utilisateur distante, PAM\_TUSER

et cherche une instance de cet item dans **file=filename**. **filename** contient une ligne par item listé. Si l'item est trouvé, alors si **sense=allow**, retourne **PAM\_SUCCESS** sinon si **sense=deny**, retourne **PAM\_AUTH\_ERR**.

Si une erreur est rencontrée (par exemple si **filename** n'existe pas ou un argument mal construit est trouvé), alors si **onerr=succeed**, retourne **PAM\_SUCCESS**, sinon si **onerr=fail**, retourne **PAM\_AUTH\_ERR** ou **PAM\_SERVICE\_ERR**.

**apply=** peut être utilisé pour restreindre l'application à un utilisateur spécifique (**apply=username**) ou un groupe (**apply=@groupname**). Utile seulement avec tty, rhost et shell

## OPTIONS

**item= [tty|user|rhost|ruser|group|shell]** Ce qui est listé dans le fichier et doit être vérifié  
**sense=allow** Action à prendre si trouvé dans le fichier.  
**file=/path/filename** Fichier contenant un item par ligne  
**onerr=succeed** quoi faire si quelque chose se produit comme l'impossibilité d'ouvrir le fichier  
**apply=user** restreint à l'utilisateur ou le groupe spécifié  
**quiet** ne log par les erreurs

fournis tous les types de module

## Valeurs retournées

**PAM\_SUCCESS** en cas de succès  
**PAM\_AUTH\_ERR** en cas d'échec  
**PAM\_BUFF\_ERR, PAM\_SERVICE\_ERR** en cas d'erreur interne  
**PAM\_IGNORE** si aucune règle ne s'applique

## Exemples

L'authentification classique ftpusers peut être implémenté avec cette entrée dans /etc/pam.d/ftpd

```
auth required pam_listfile.so onerr=succeed item=user sense=deny file=/etc/ftpusers
```

note que les utilisateurs listés dans /etc/ftpusers ne sont pas autorisés pour accéder au service ftp

**Pour autoriser le login pour certains utilisateurs, vous pouvez utiliser une entrée dans /etc/pam.d/login**

```
auth required pam_listfile.so onerr=fail item=user sense=allow file=/etc/loginusers
```