

# Creating a Custom mapr-admin Profile for PAM

*Describes how to install the packages and configure the Kerberos client to use PAM.*

If you wish to ensure that MapR uses a MapR-unique PAM configuration, you can:

- Leave the `/etc/pam.d/sudo` file as is - MapR strongly recommends against manually editing the `/etc/pam.d/sudo` file.
- Create your own PAM profile in `/etc/pam.d`, naming it `mapr-admin`.
- Manually edit `mapr.login.conf` and other ecosystem component configuration files to use `mapr-admin` only.

## Example /etc/pam.d/mapr-admin File

Below are some simple examples of what might work in the PAM profile you choose to edit in `mapr-admin`, or in another PAM profile, in close consultation with your Linux administrator.

```
account    required    pam_unix.so
account    sufficient  pam_succeed_if.so uid < 1000 quiet
account    [default=bad success=ok user_unknown=ignore] pam_ldap.so
account    required    pam_permit.so

auth       sufficient  pam_unix.so nullok_secure
auth       requisite   pam_succeed_if.so uid >= 1000 quiet
auth       sufficient  pam_ldap.so use_first_pass
auth       required    pam_deny.so

password   sufficient  pam_unix.so md5 obscure min=4 max=8 nullok
try_first_pass
password   sufficient  pam_ldap.so
password   required    pam_deny.so

session    required    pam_limits.so
session    required    pam_unix.so
session    optional    pam_ldap.so
```

**Note:**

The file `/etc/pam.d/sudo` should be modified only with care and only when absolutely necessary.