# Aucun GPO restreignant l’authentification des administrateurs

ID METSYS : 34  
ID PingCastle : [P-LogonDenied](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)

Charge de travail : 3 jours  
Difficulté : 3 - Requière des connaissances avancées sur l'anomalie

****Description****

Si un administrateur ouvre une session sur une machine compromise, ses identifiants peuvent être volés (keylogger, capture du hash du mot de passe, ou autre).

****Recommandation****

Il est recommandé d’utiliser des comptes dédiés à l’administration AD et de limiter l’usage de ces comptes à quelques machines identifiées comme sûres (postes ou serveurs d’administration dédiés). Il est recommandé d’empêcher l’ouverture de session sur les autres machines du domaine pour limiter les risques.

Ceci peut être fait dès maintenant par GPO (configurer « Deny log on locally » sur toutes les machines du domaine sauf les DC et machines d’administration).