# Ordinateurs actifs sans changement de mot-de-passe tous les 30 jours

ID METSYS : 11  
ID PingCastle : [S-PwdNeverExpires](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html), [P-AdminPwdTooOld](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html), [S-PwdLastSet-90](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)  
ID PurplKnight : [Admins with old passwords](https://www.purple-knight.com/fr/security-indicators/), [Users with Password Never Expires flag set](https://www.purple-knight.com/fr/security-indicators/), [Computers with password last set over 90 days ago](https://www.purple-knight.com/fr/security-indicators/), [Users with old passwords](https://www.purple-knight.com/fr/security-indicators/), [Built-in domain Administrator account with old password (180 days)](https://www.purple-knight.com/fr/security-indicators/)  
ID ANSSI : [vuln2\_dont\_expire](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#dont_expire), [vuln1\_password\_change\_priv](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#password_change_priv), [vuln2\_password\_change\_server\_no\_change\_90](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#password_change_server_no_change_90)

Charge de travail : 3 jours  
Difficulté : 2 - Requière quelques connaissances sur l'infrastructure et l'anomalie qu'elle contient

****Description****

La vulnérabilité d'un mot de passe augmente avec le temps, en même temps que le risque de compromission par une attaque de type « brute force », par un attaquant acquérant des renseignements sur l'utilisateur ou par l'utilisateur lui-même partageant son mot de passe. Dans le cadre d'un compte privilégié, les conséquences d'une compromission du mot de passe sont décuplées par le pouvoir octroyés à ces comptes dans le domaine et la forêt.

****Recommandation****

Il est recommandé d'évaluer la liste des comptes privilégiés n'ayant pas changé de mot depuis plus de 90 jours et considérer la possibilité de changer celui-ci. Ce changement ne doit pas intervenir sporadiquement mais faisant partie d'une procédure régulière, automatisée ou manuelle, documentée et supervisée.

Aucun compte avec l’option « le mot de passe n’expire jamais » ne devrait être membre du groupe Domain Admins. Soit il faut retirer le compte du groupe, soit mettre en place un mécanisme de changement de mot de passe.