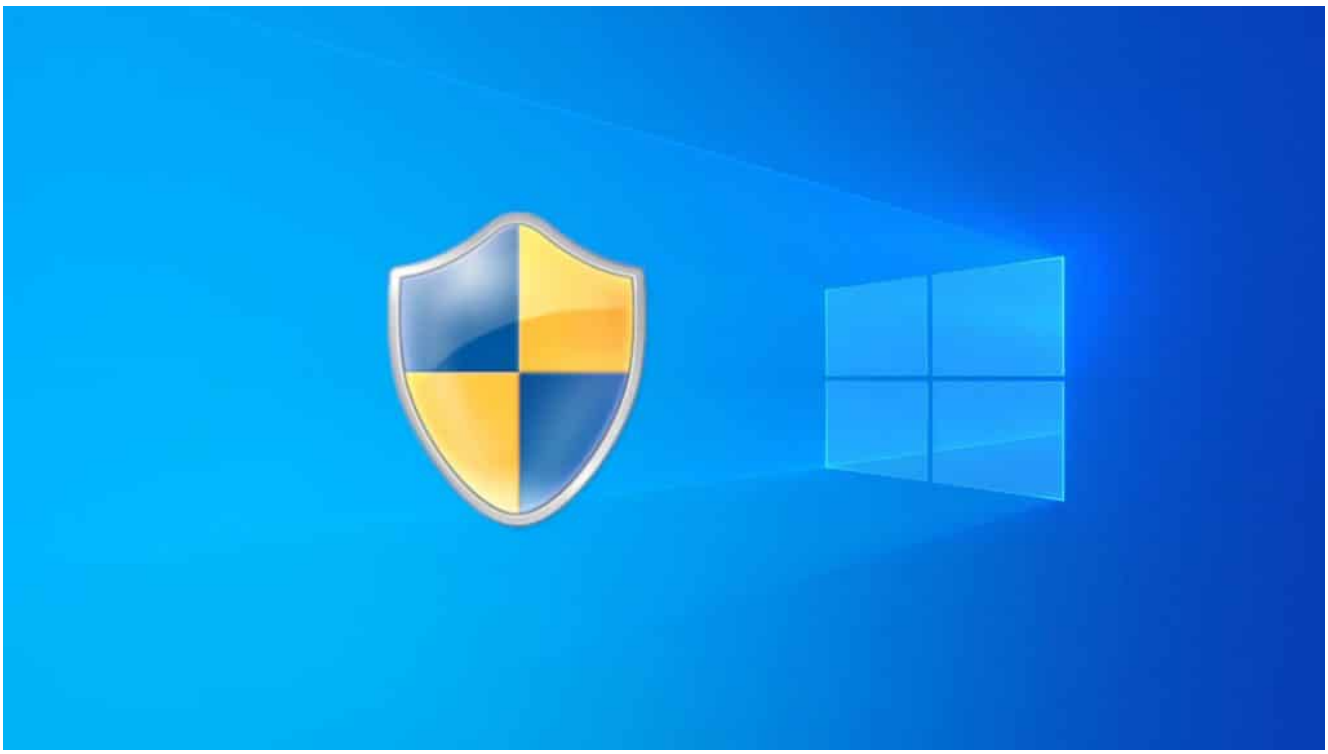
Le contrôle des comptes utilisateurs (UAC) de Windows

Le contrôle des comptes utilisateurs (UAC) est un mécanisme de sécurité, apparu depuis Windows Vista.
L'UAC virtualise les accès utilisateurs afin de sécuriser Windows.
Le contrôle des comptes utilisateurs est une barrière afin de lancer les applications sans les droits administrateurs même depuis une session administrateur.
Ainsi l'utilisateur doit donner son autorisation dans le but de lancer son application en administrateur.

Ce mécanisme se nomme aussi **UAC** pour **User Account Control**.
En français on traduit cela par le contrôle des comptes utilisateurs.

Cet article vous explique comment fonctionne l'UAC et comment le configurer.



Le contrôle des comptes utilisateurs (UAC) de Windows

La page suivante donne les explications afin de bien comprendre le fonctionnement des utilisateurs sur Windows : [FAQ – compte utilisateur administrateur et standard sur Windows 7 et Windows 10]

Comprendre les droits administrateurs

Lorsque vous lance une application, celle-ci hérité des permissions issues de l'utilisateur.

Si vous lancez une application avec un utilisateur administrateur, l'application possède les droits administrateur.
Enfin si vous lancez une application avec le compte invité, qui est un compte restreint, l'application ne possède pas de permissions élevées.

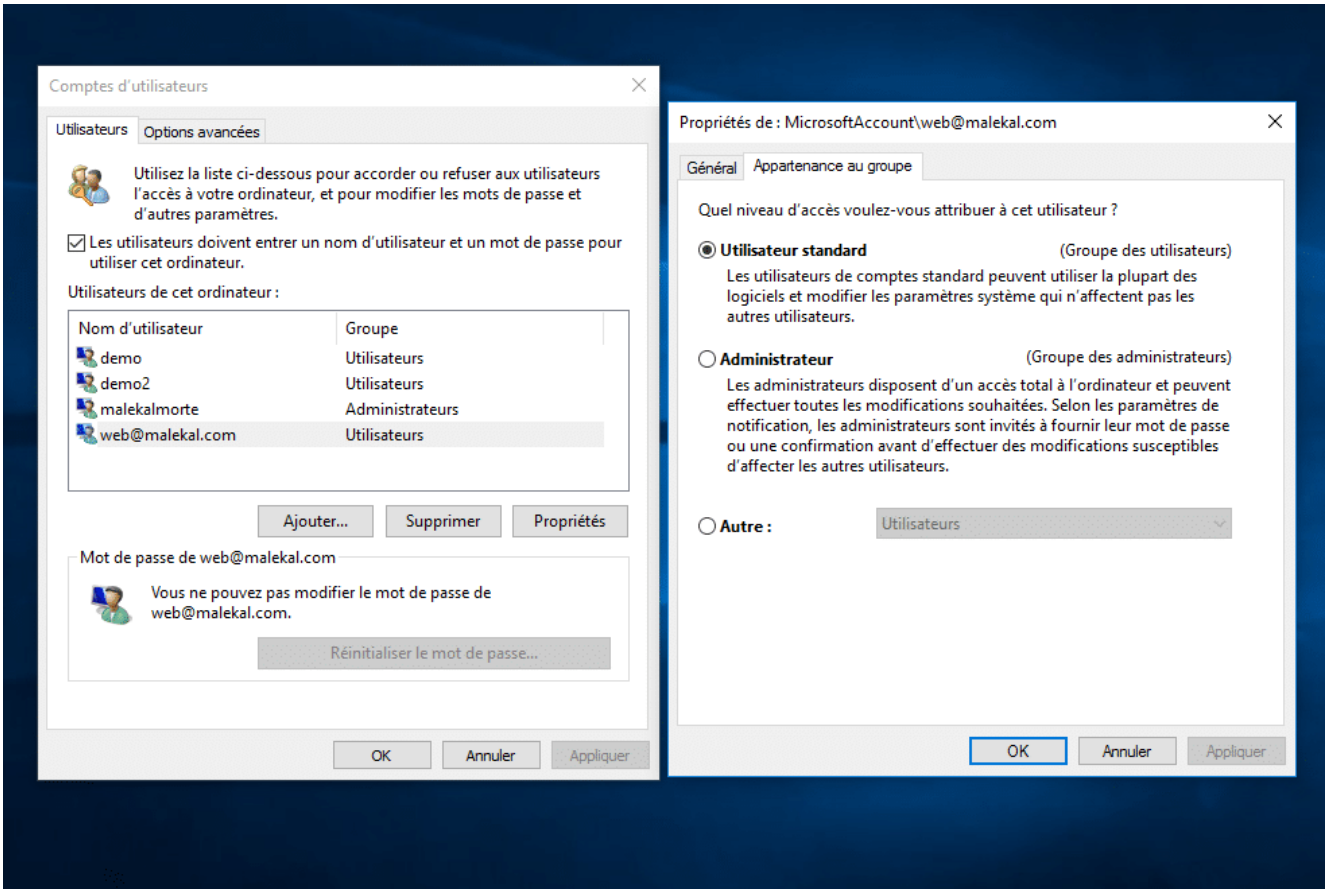
Les droits administrateurs permettent, de faire après peu tout sur Windows. Par exemple :

- Vous pouvez écrire dans tous les dossiers et notamment le dossier Program Files et Windows
- Vous pouvez tuer tous les processus sauf les services Windows
- Créer de nouveaux ou supprimer des services Windows.

Cela peut poser des problèmes de sécurité puisque sur Windows, par défaut le compte créé à l'installation est administrateur.
Par exemple, cela posait des problèmes avec les attaques Drive By download puisque le navigateur tournait en administrateur.
Lors du surf, un WEB Exploit lance un virus qui aura alors accès administrateur.

Microsoft a introduit le contrôle des comptes utilisateurs dites UAC afin de palier à cela.

Pour vérifier quel utilisateur sont administrateur, le place simple est d'utiliser la commande netplwiz.
Celle-ci donne la liste des utilisateurs et la colonne groupe indique si on est administrateur ou utilisateur

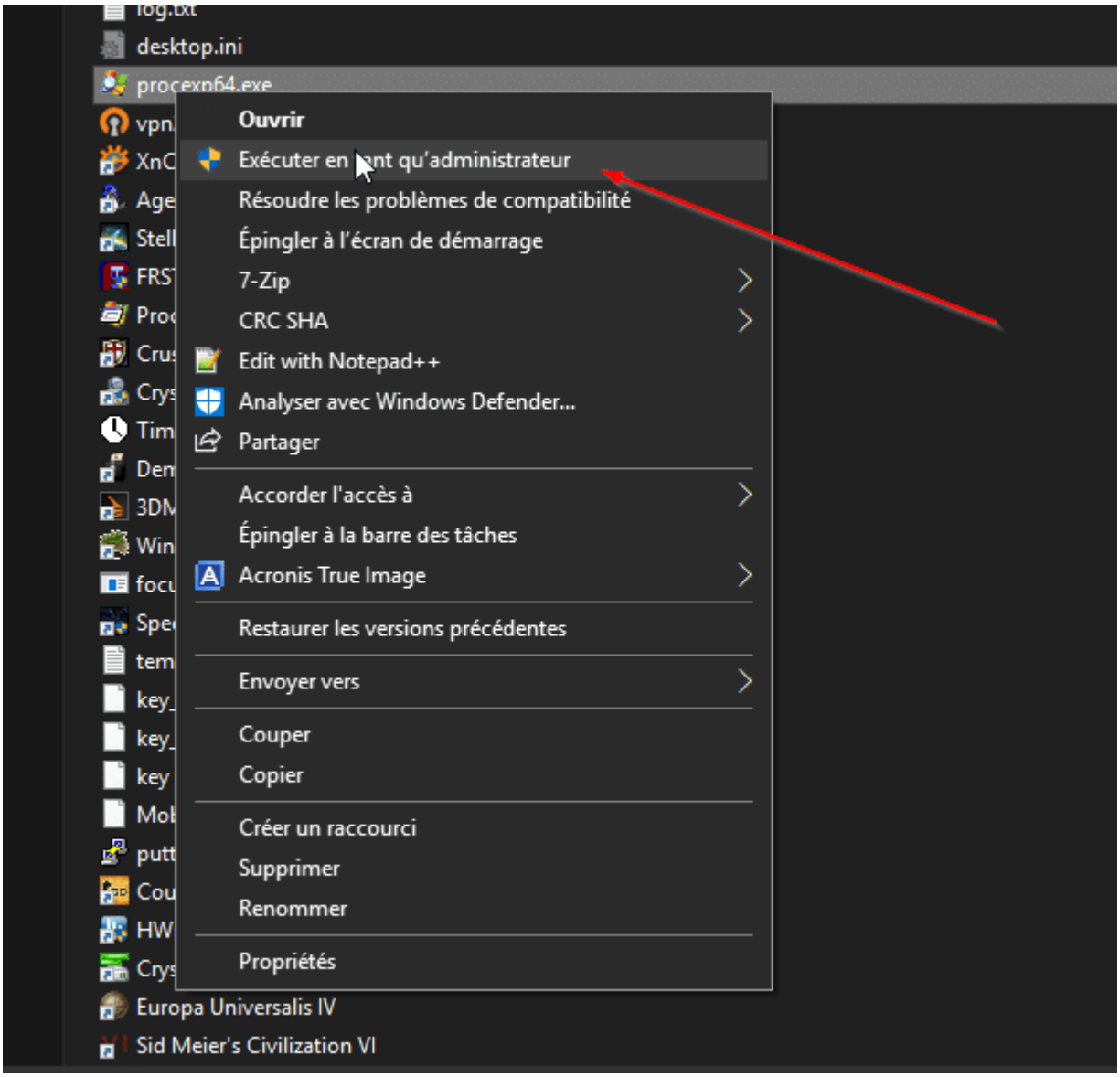


Comprendre le contrôle de comptes utilisateur (UAC)

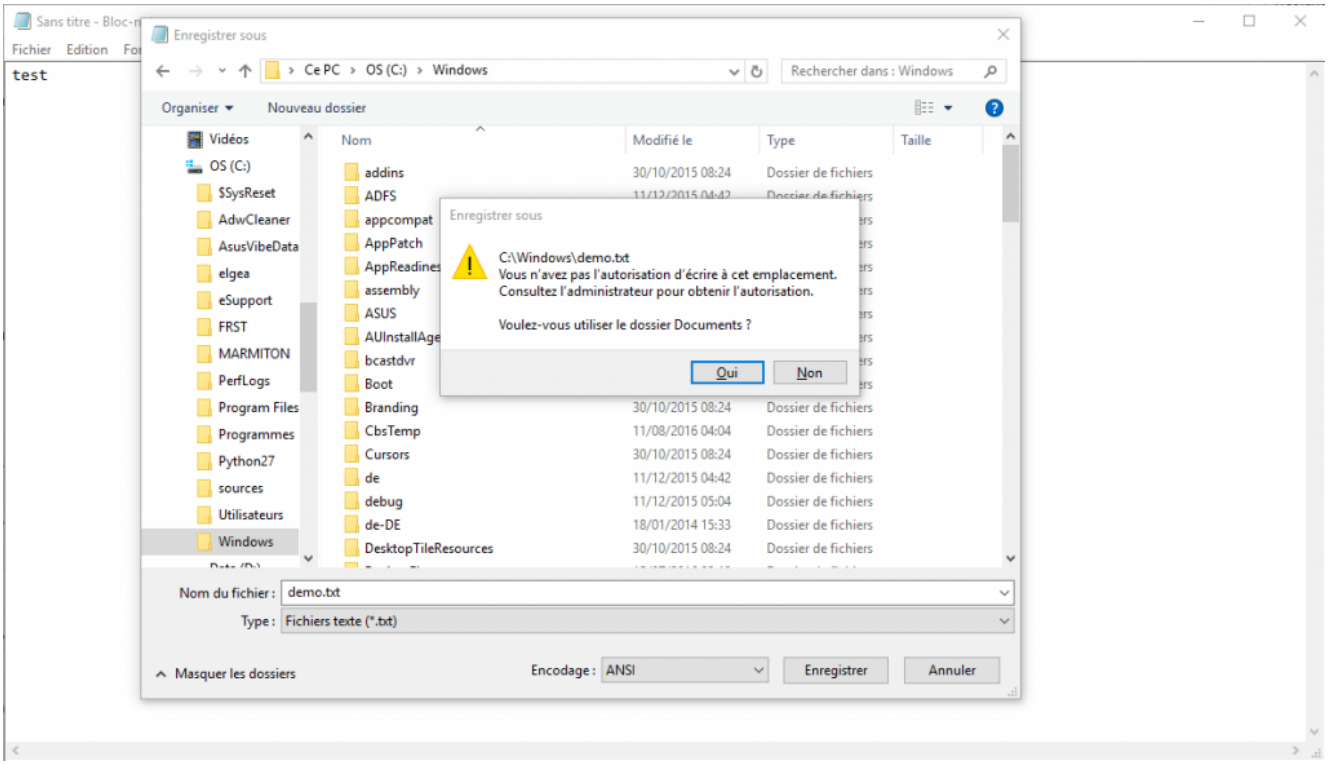
Le contrôle des comptes est un système de virtualisation des droits administrateurs.
Si vous lancez un programme depuis un compte administrateur, l'application ne possède en fait, pas les droits administrateurs.
Une application peut demander à obtenir ces droits.
Cela à travers une popup du Contrôle des comptes utilisateurs où l'utilisateur doit accepter ou non de les donner.
Si c'est le cas, l'application est alors lancée avec un jeton administrateur.

Enfin un utilisateur peut lancer une application en

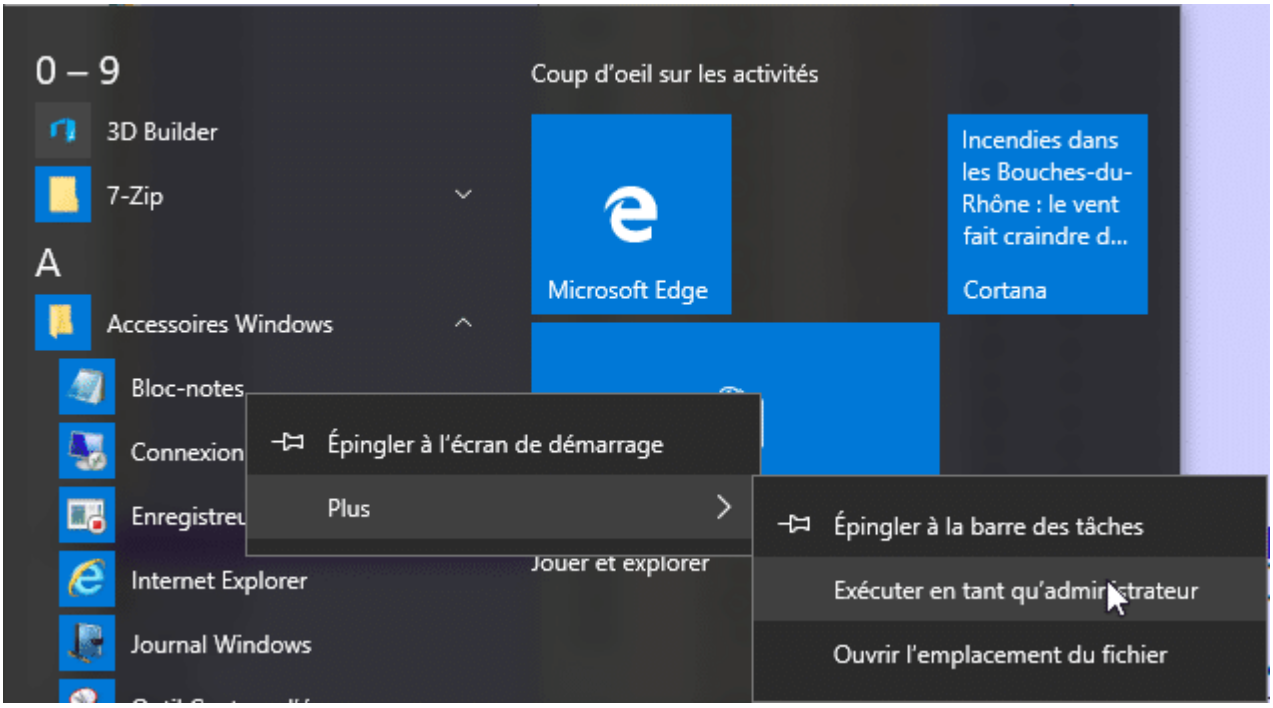
administrateur par **un clic droit puis exécuter en tant qu'administrateur**.
Là aussi la popup de confirmation du contrôle des comptes va s'ouvrir.



Pour tester, lancez simplement, le bloc-note de Windows et tentez d'enregistrer votre document dans un dossier système.
Par exemple Program Files ou le dossier Windows.
Vous aurez un message qui vous indique que vous n'avez pas les autorisations.



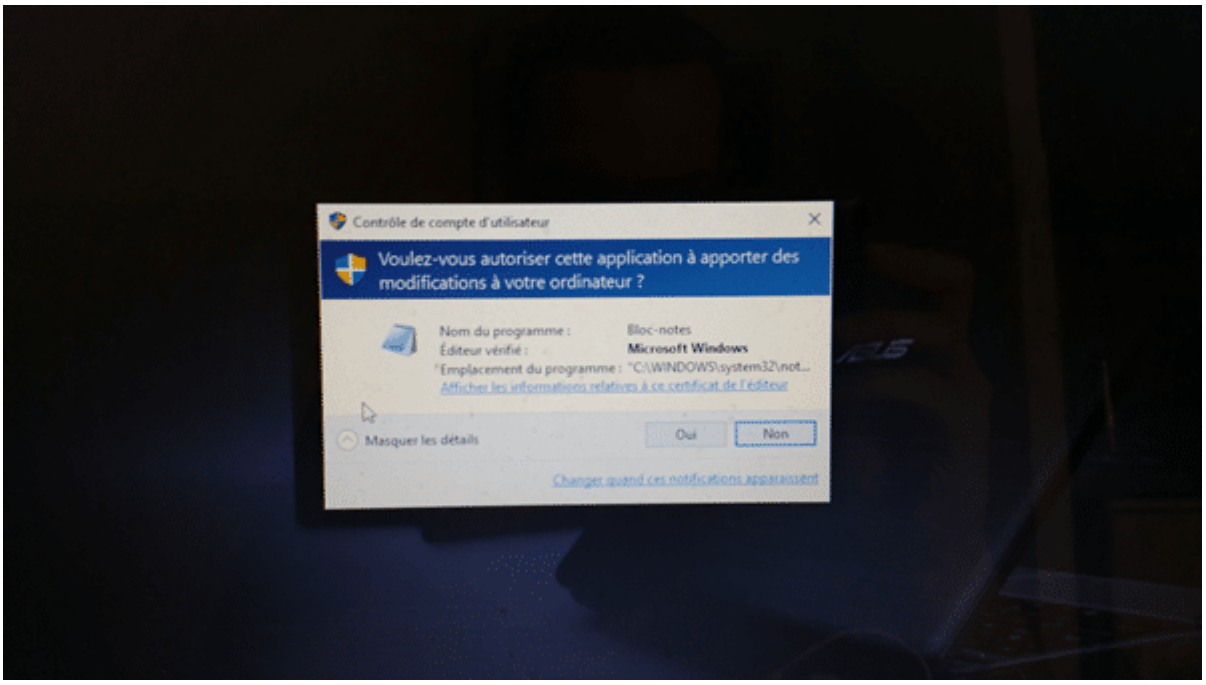
Maintenant, lancez le Bloc-note par un clic droit puis *Exécuter en tant qu'administrateur*.



Puis la fameuse popup du contrôle des comptes utilisateur

s’ouvre.
Vous devez cliquer sur Oui pour confirmer la montée en droit de l’application.

Si vous tentez à nouveau d’enregistrer votre fichier texte dans un dossier système, cela sera possible.
C’est pour cela que si vous désirez éditer le fichier HOSTS de Windows, vous devez lancer l’éditeur de texte en admin.
Sinon vous aurez un message d’erreur « accès refusé » à l’enregistrement.
De même pour passer des commandes admin dans l’invite de commandes de Windows.



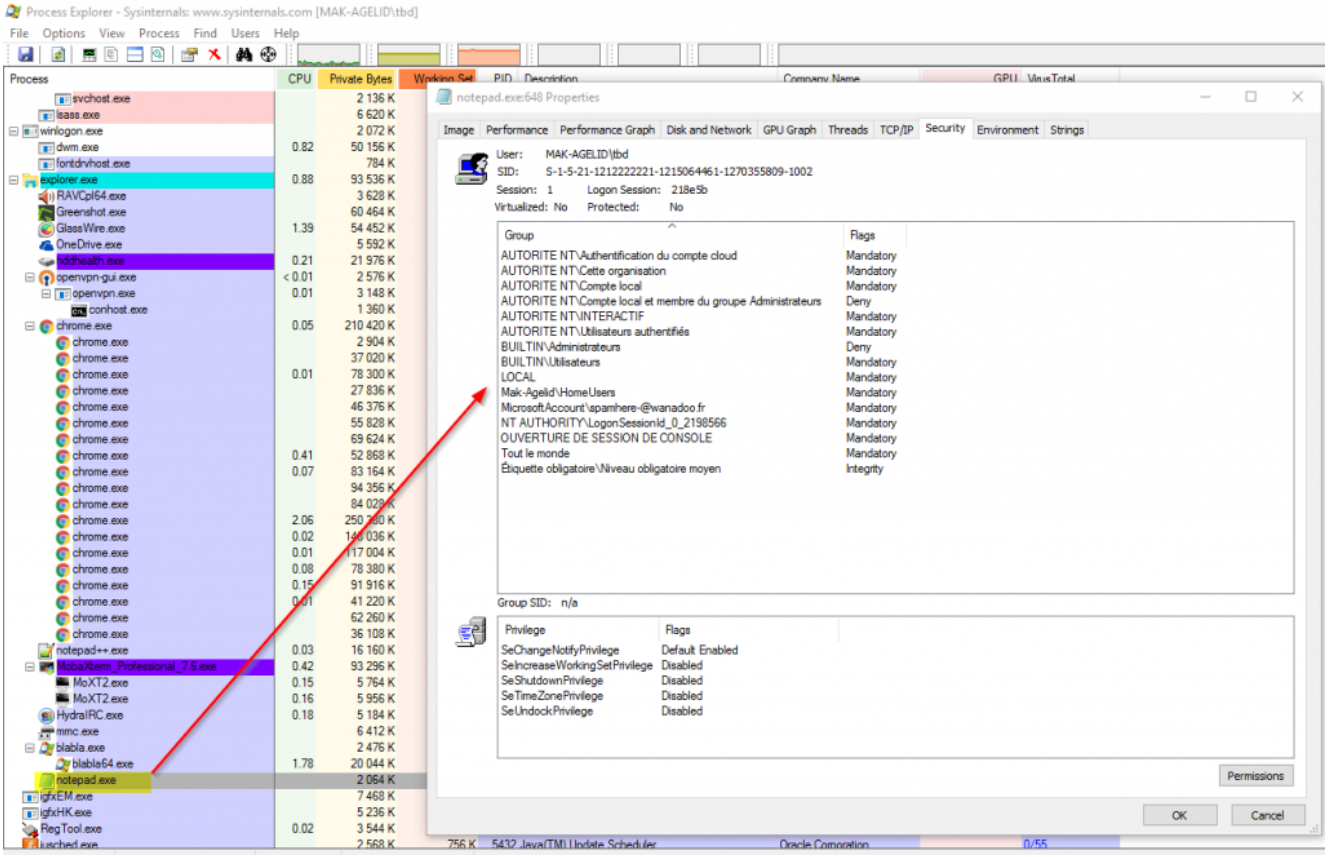
Pour écrire dans les dossiers systèmes de la partition C de Windows, même chose, vous devez donc lancer un jeton administrateur.
Sinon vous obtiendrez un message « accès refusé » lors de l’écriture.

Enfin seul le compte administrateur intégré n’est pas soumis à l’UAC.

Le jeton administrateur

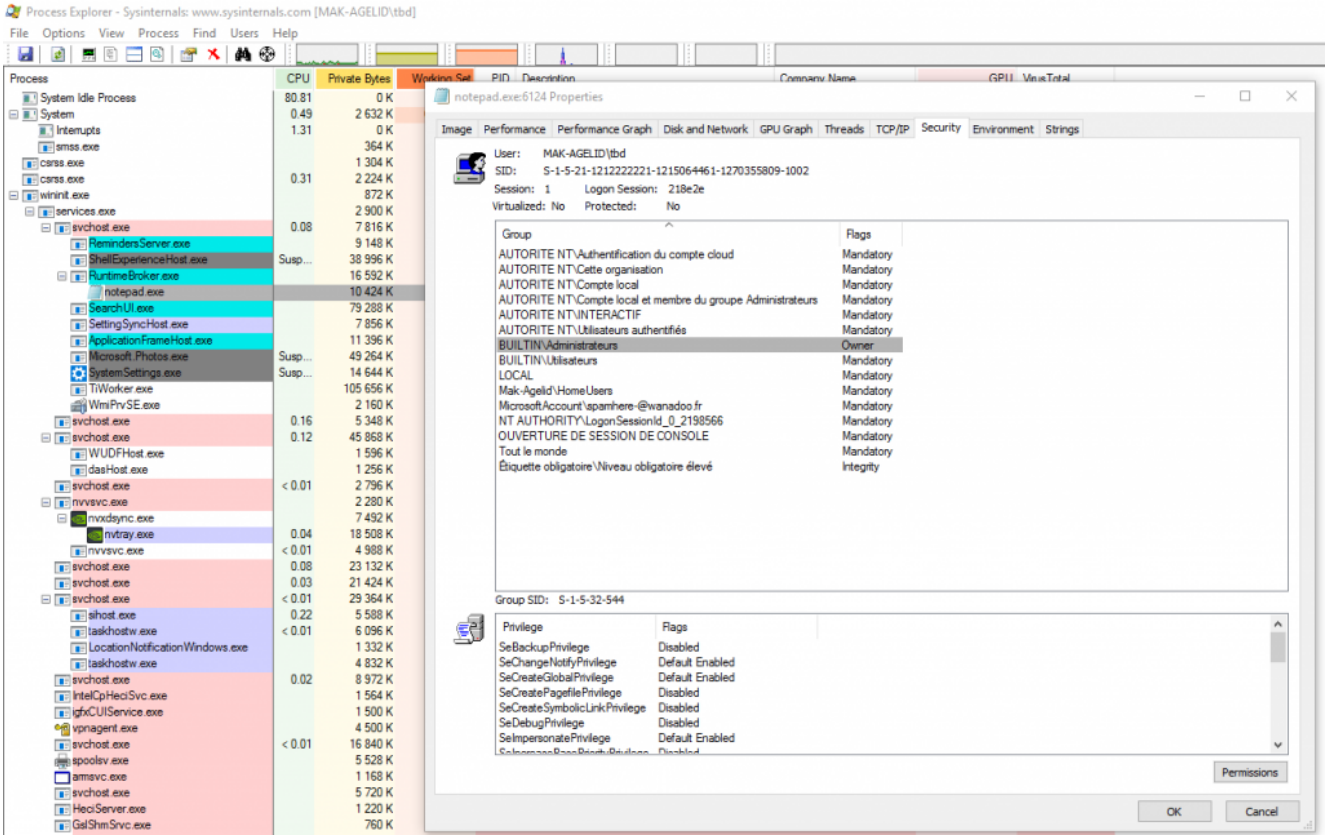
Les différences sont visibles facilement sur Process Explorer, depuis l’onglet Security où les privilèges s’affichent.

Sans le jeton administrateur, on constate que le Bloc-note (notepad.exe) a pour parent explorer.exe et un Deny sur le groupe administrateurs.
La liste des privilèges en bas est sur Disable.



Au contraire avec le jeton administrateur, ce n’est pas la même chose, notepad.exe est lancé par svchost.exe

Le groupe administrateurs est le propriétaire.
Enfin on constate aussi dans que la liste des privilèges est plus longue et certains sont activés (Enable).



Ainsi donc, le navigateur WEB n’est pas lancé avec les droits administrateurs.
Dans le cas où Mozilla Firefox lance une popup du contrôle des comptes utilisateurs, il peut s’agir d’une mise à jour du navigateur.

Contournement UAC par les malwares

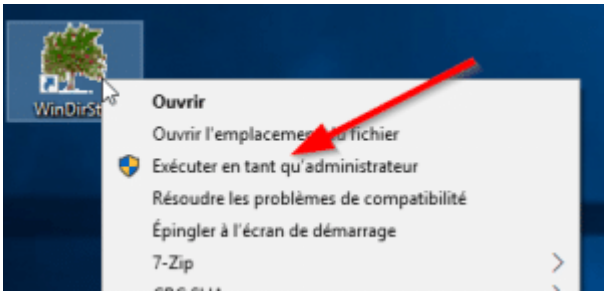
Les logiciels malveillant tente de contourner la restriction UAC.
Le but est de pouvoir lancer le malware en administrateur afin

d’avoir plus de pouvoir dans le système d’exploitation.
Pour se faire, par exemple, on boucle sur la demande, l’utilisateur n’a aucun choix que de répondre Oui.
Soit avec des mécanismes plus ancien, par exemple avec Sirefef, il y a quelques années : [ZeroAccess social engeenering contre l’UAC via Adobe Flash]

Présentation de l’UAC en vidéo :

Exécuter une application en administrateur

Pour lancer une application en administrateur, vous pouvez faire un clic droit puis exécuter en tant qu’administrateur.
Mais d’autres méthodes existent, reportez-vous sur la page : [Comment exécuter une application en administrateur sur Windows 7, 8.1 ou 10]



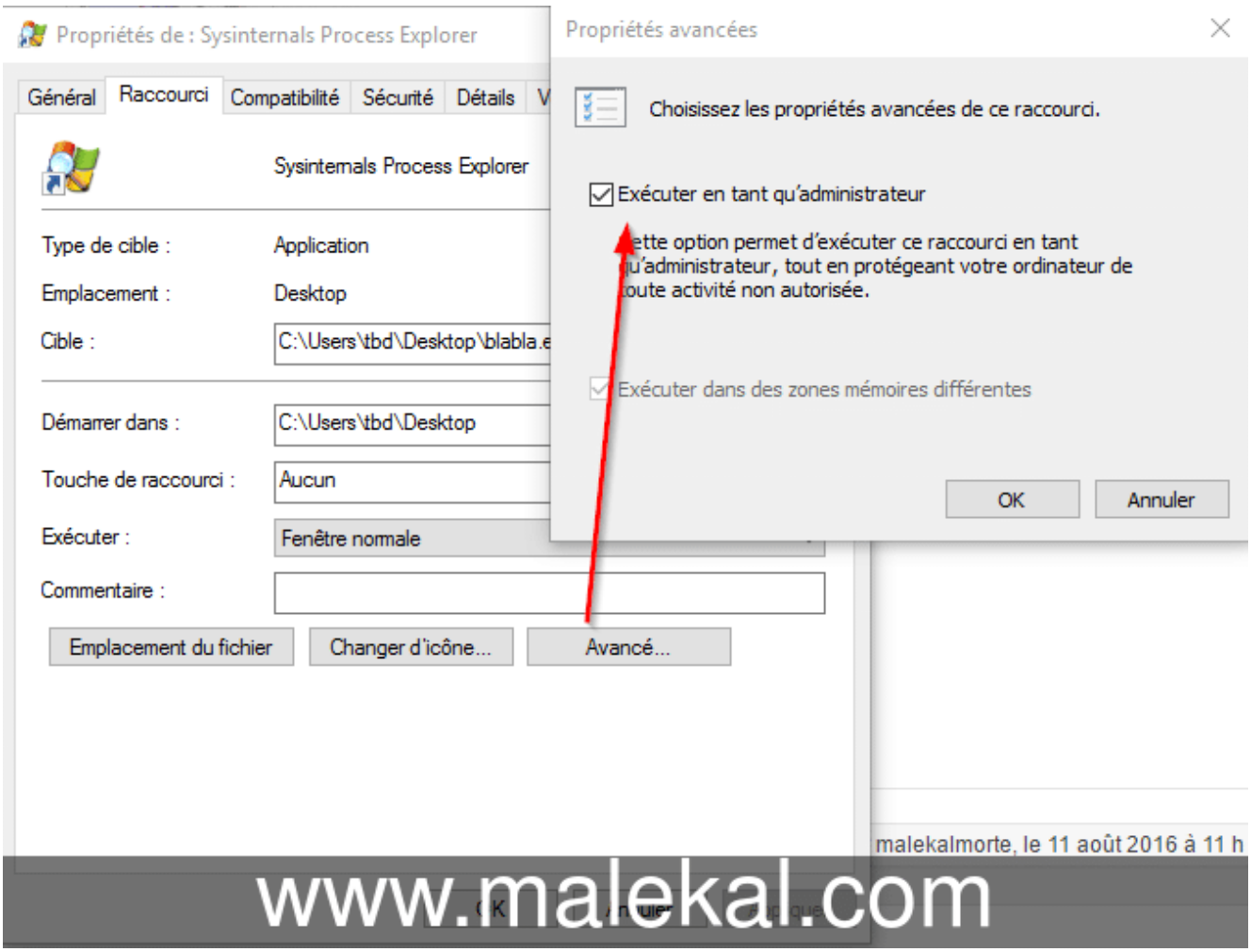
Forcer l’UAC sur une application

Si vous en avez marre d’effectuer un clic droit, il est

possible de forcer le lancement en administrateur.
Pour cela,

- Sur le raccourci de lancement de l'application, faites un clic droit puis Propriétés.
- Ensuite cliquez en bas sur le bouton Avancé.
- Enfin dans la nouvelle fenêtre, cochez l'option : *Exécuter en tant qu'administrateur*

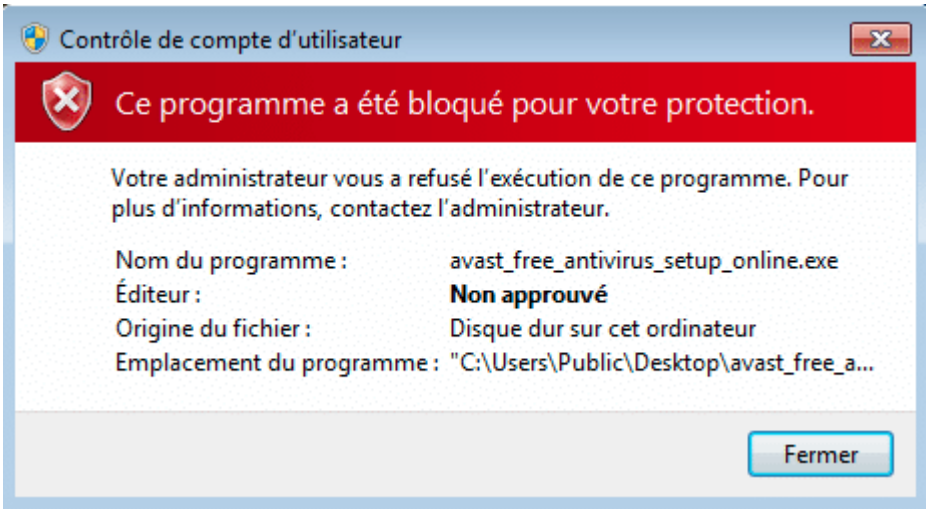
Au lancement de l'application, la popup des contrôles des comptes va alors se lancer systématiquement.



Programme bloqué par le contrôle de compte d'utilisateur

Parfois, il peut arriver que l'UAC bloque l'exécution de programmes, ainsi, vous vous retrouvez avec le message

Protection de l'ordinateur – Ce programme a été bloqué par votre protection.
Votre administrateur vous a refusé l'exécution de ce programme.



Dans ces cas précis, rendez-vous sur la page suivant pour débloquer l'exécution du programme : Programme bloqué par la protection de votre ordinateur : Editeur non approuvé

Désactiver le contrôle de compte d'utilisateur

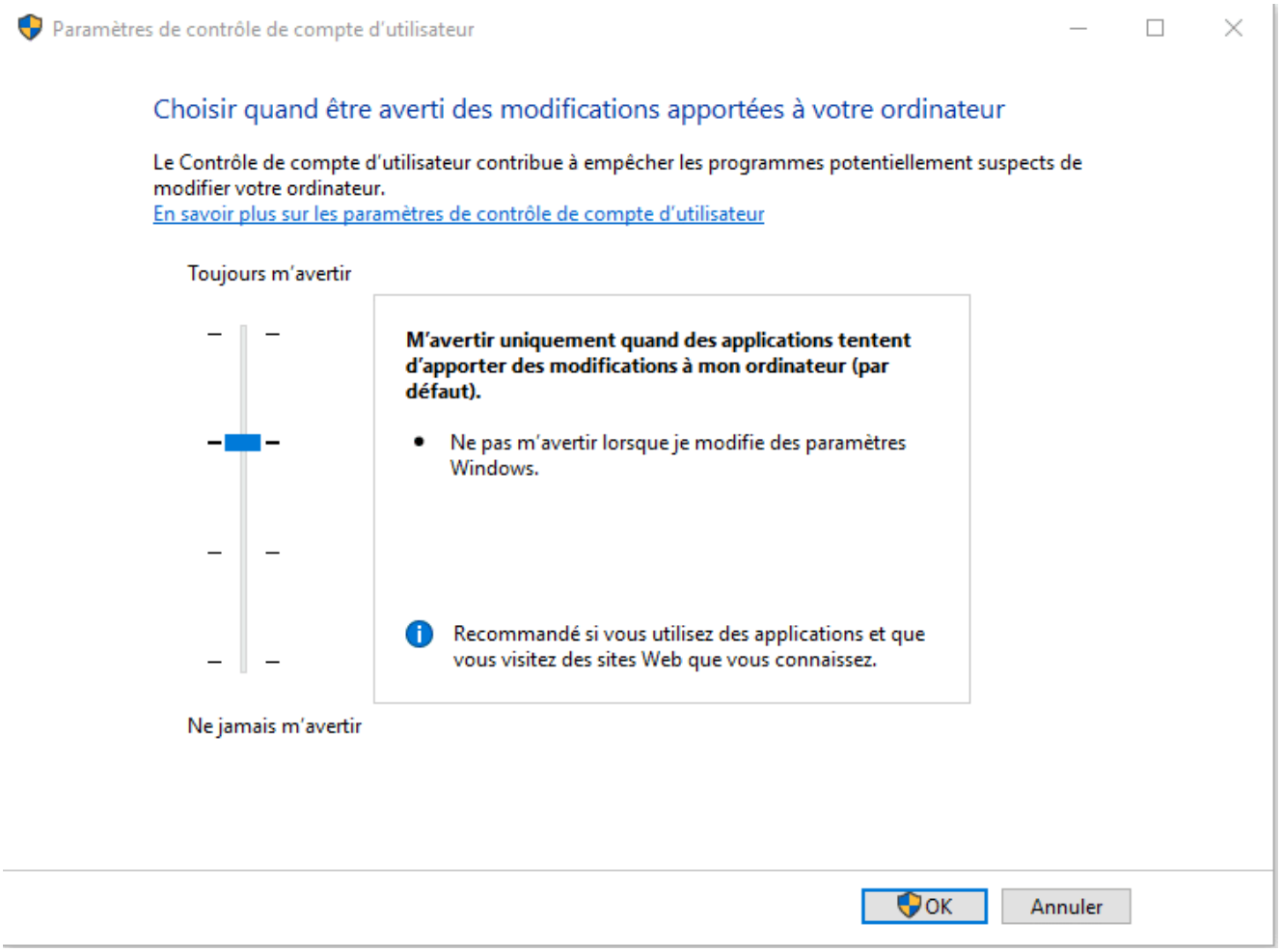
Il est bien sûr possible de désactiver l'UAC, ce qui n'est pas conseillé.
A ce propos, vous pouvez lire : UAC : Pourquoi ne pas le désactiver

Plusieurs méthodes sont données sur la page suivante : Comment désactiver le contrôle des comptes utilisateur (UAC) de Windows

Voici la méthode la plus simple :

- Depuis le Panneau de configuration ouvrez le Comptes d'utilisateurs
- Ensuite cliquez sur le bouton « Modifier les paramètres du contrôle de compte de l'utilisateur »

- Enfin abaissez la jauge au minimum pour désactiver l'UAC.
- Cliquez sur OK puis redémarrez Windows .



Ca y est, le contrôle des comptes est maintenant désactivé.

Liens connexes

Enfin pour terminer quelques liens autour de l'UAC et la sécurité.

- UAC : Pourquoi ne pas le désactiver

Tous les tutoriels liés au compte administrateur et utilisateur de Windows :

- Fonctionnement utilisateurs et sessions Windows.
- Le contrôle des comptes (UAC) : comprendre le contrôle des comptes (UAC)
- Différence entre compte administrateur et utilisateur sur Windows
- mot de passe utilisateur Windows perdu et Windows 10 : mot de passe perdu
- Supprimer la demande de mot de passe au démarrage
- Les utilisateurs AUTORITE NT