# L'UAC de Windows Vista

**Date de dernière mise à jour : 23/07/2007 à 19:17**



L'UAC (**User Account Control**) est une nouveauté de Windows Vista. Sous Windows XP, lorsqu'un utilisateur était créé et ajouté dans le groupe des administrateurs, il disposait des pleins pouvoirs. L'utilisateur créé à l'installation de Windows était également placé en compte administrateur par défaut sans même que l'utilisateur s'en aperçoive étant donné qu'il ne recevait jamais de messages de mise en garde quant à l'utilisation d'un tel niveau de privilèges. L'UAC vise à augmenter le niveau de sécurité du système en ne donnant uniquement aux utilisateurs que des privilèges limités, et ce même si ils sont administrateurs.

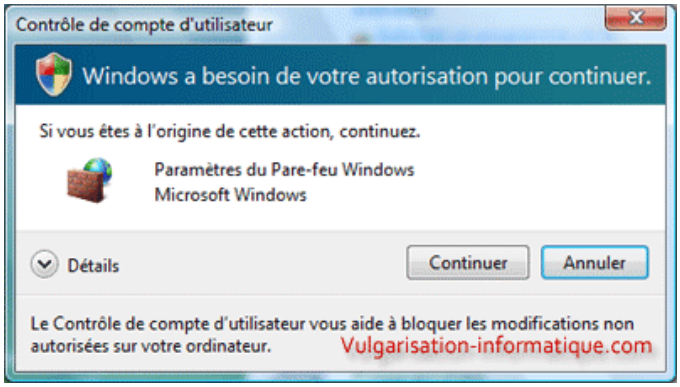
Les administrateurs auront la possibilité de faire tout ce que bon leur semble comme avant, mais en confirmant leur action via une boîte de dialogue (désactivable). Avec Windows Vista, les utilisateurs standards (ayant des comptes limités) pourront effectuer certaines actions normalement ouvertes uniquement aux administrateurs si ils en possèdent le mot de passe, ce qui était impossible ou très difficile avec Windows XP (vous disposiez parfois pour lancer vos programmes de l'option **Exécuter en tant que**, et encore ...). Ces nouvelles autorisations sont les suivantes :

-Affichage de l'horloge et du calendrier systèmes et paramétrage du fuseau horaire.
-Installation du protocole de sécurisation de données WEP (Wired Equivalent Privacy).
-Modification des paramètres d'affichage ou de gestion de l'alimentation.
-Installation de polices.
-Ajout de périphériques ayant leurs pilotes déjà installés sur l'ordinateur ou fournis par un administrateur.
-Création et configuration d'une connexion VPN (**Virtual Private Network**- ou réseau privé virtuel).
-Téléchargement et installation de mises à jour à l'aide de Windows Update.

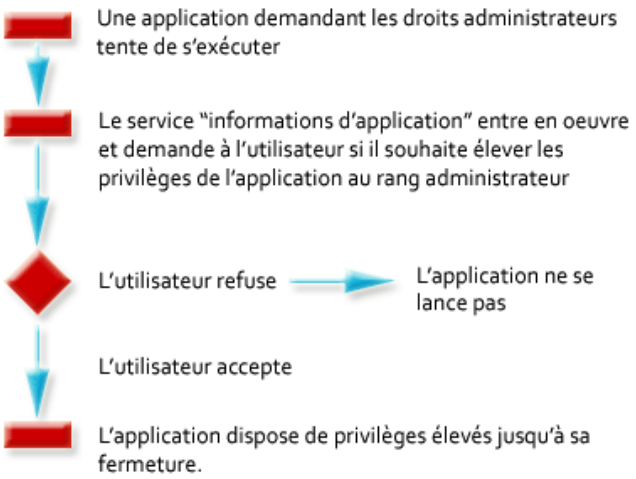
Avec l'UAC, il est désormais possible de savoir si oui ou non vous avez le droit d'effectuer telle ou telle action. Cela est rendu possible par l'ajout d'une icône symbolisant un bouclier lorsque les droits d'administrateur sont requis :

Fonctionnement de l'UAC :

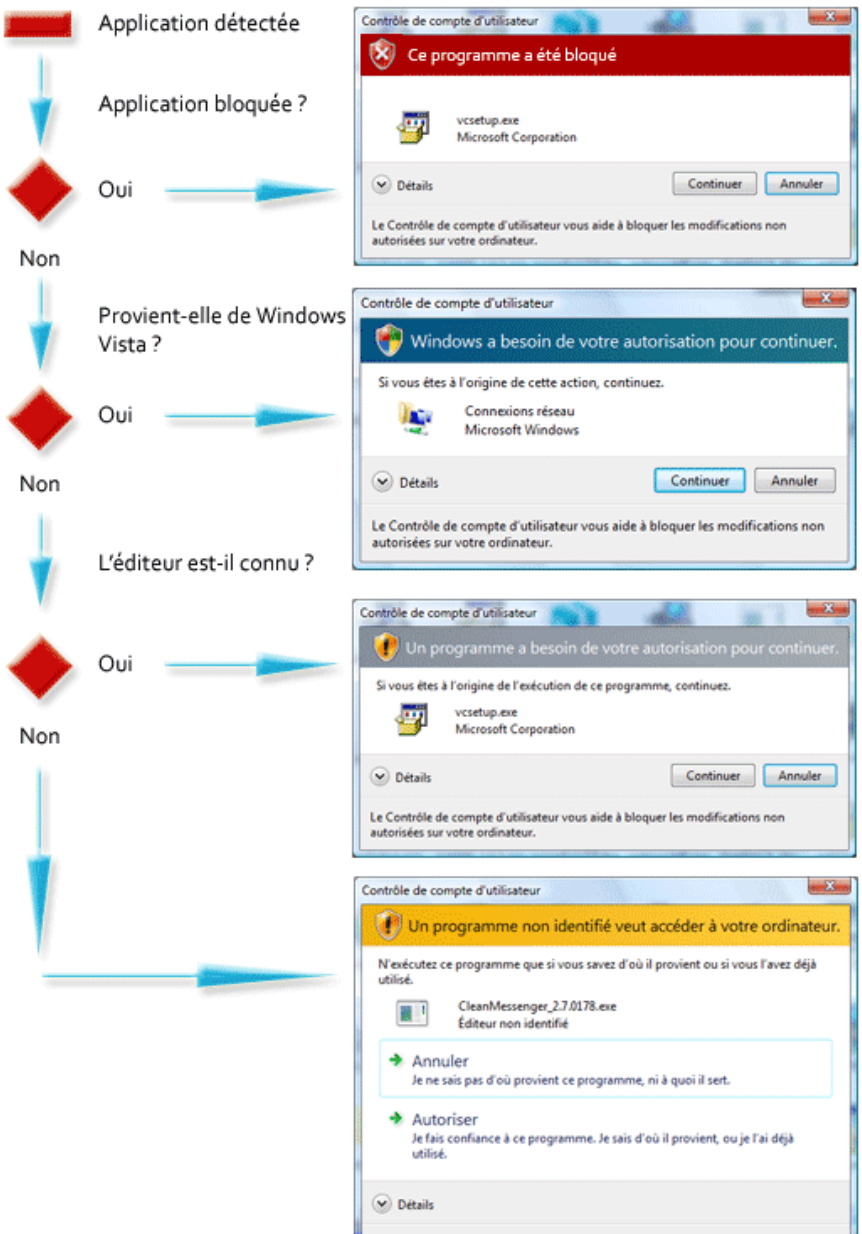
L'UAC oeuvre dès l'ouverture de session. Si celle-ci n'a en apparence pas changé par rapport à Windows XP, en réalité elle a subi de profondes modifications. Quand un administrateur ouvre une session, il reçoit désormais deux jetons d'accès : l'un de niveau standard (comme les autres utilisateurs) qui va permettre de lancer le processus principal (**Explorer.exe**) ainsi que toutes les autres applications. Là où la différence intervient avec les autres utilisateurs possédant un compte standard est que l'administrateur dispose d'un second jeton lui octroyant des droits plus élevés. Si l'utilisateur a besoin de ces droits plus élevés (ou une application), l'UAC élève momentanément ses privilèges. Cela se produit généralement de cette façon (ici une tentative de modification des paramètres du pare-feu Windows) :



Lorsqu'une application a besoin de droits plus élevés que ceux dont elle dispose, le service**Informations d'application** entre en oeuvre et élève les privilèges pour l'application concernée uniquement. Si ce service est arrêté, les applications nécessitant une élévation de privilèges ne pourront plus fonctionner correctement.




Pour savoir si l'application a besoin de droits plus élevés pour fonctionner, Windows Vista utilise différents procédés, le plus courant étant l'analyse heuristique destinée à savoir de quel type d'application il s'agit (installeur, etc.). En fonction de la signature numérique et du type de programme, l'UAC va afficher un message présenté différemment.



En plus de tout ça, pour les applications incompatibles avec l'UAC, Microsoft a codé une sorte de base de registres virtuelle : lorsqu'une application récupère les droits administrateurs sans être compatible avec l'UAC et tente d'écrire des valeurs dans le registre, l'UAC intercepte la commande et la redirige dans la clé **HKEY_CLASSES_ROOT/VirtualStore**.