


## User Account Control (UAC) - Benutzerkontensteuerung

Mitglieder der Gruppe **Administratoren** erhalten ein Split-Token.

	Standard Token	elevated Token
Mitgliedschaft in der Gruppe Administratoren	„nur zum Ablehnen“	normal
Integritätslevel	Medium	High
Anzahl der Privilegien (Berechtigungen)	5	23

Die meisten Elemente des Access-Tokens werden mit dem Befehl `whoami /all` angezeigt.  
Die Berechtigungen können mit Gruppenrichtlinien eingestellt werden:

*Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Lokale Richtlinien -> Zuweisen von Benutzerrechten*

Nach der Anmeldung hat der Benutzer das Standard-Token.  
Versucht er eine Aktion auszuführen, die Administratorrechte erfordert (gekennzeichnet durch das Symbol ) , erscheint ein Dialog in einer der vier Farben:

- blau (Windows-Programm)
- silber (zertifiziertes Programm)
- gelb (unzertifiziertes Programm)
- rot (böses Programm)

Beim Klicken auf „Ja“ erhält der Benutzer das „elevated“ Token  
und der entsprechende Prozess wird mit Administratorrechten und hohem Integritätslevel ausgeführt.