

2023-  
2024

BTS SIO1

---

# TP-SYNTHÈSE

Informer les utilisateurs

---

Nicolas Debut

# Mission cybercafé

Un outil compatible avec le problème du client serait WebTitan Cloud.

Quel bénéfice le client pourrait en tirer?

Il s'agit d'une solution cloud donc il n'y a pas besoin de matériel ce qui est un avantage majeur, pas besoin de payer du matériel ni un entretien de matériel pour le client.

Les paramètres de filtrage Internet peuvent être appliqués rapidement.

Une interface intuitive et facile d'utilisation ne nécessitant aucune compétence spécifique.

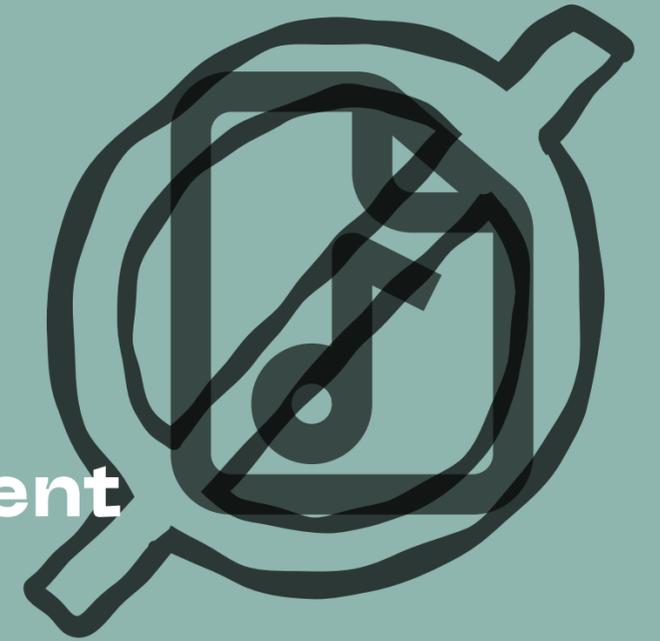
L'outil est adapté pour une utilisation sur des adresses IP statiques et dynamiques. Il intègre également une suite complète de rapports préconfigurés et personnalisable ce qui permet un suivi précis pour le client.

# Comment pourrez vous bloquer les sites dangereux ou inappropriés

Cet outil permet de bloquer des catégories de sites web via votre interface.

Le fournisseur se charge ensuite d'interdire l'accès à ces sites pour votre DNS.

Ainsi lorsque vos clients essaieront de se connecter à un site non-autorisés ils seront rediriger vers une page leur indiquant l'indisponibilité du site.

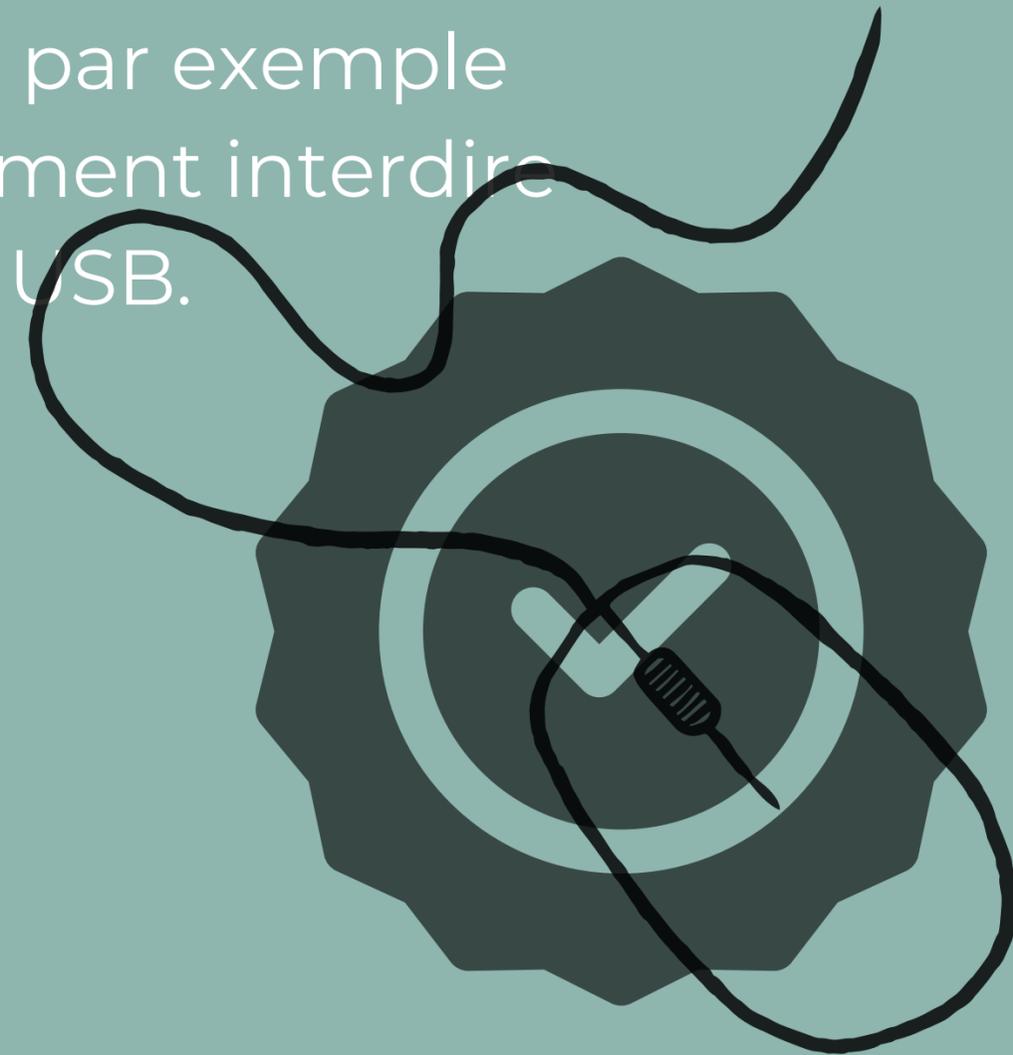


**Ce blocage concerne également les différents fichiers, vous pourrez ainsi bloquer le téléchargement de fichiers du type MP3...**

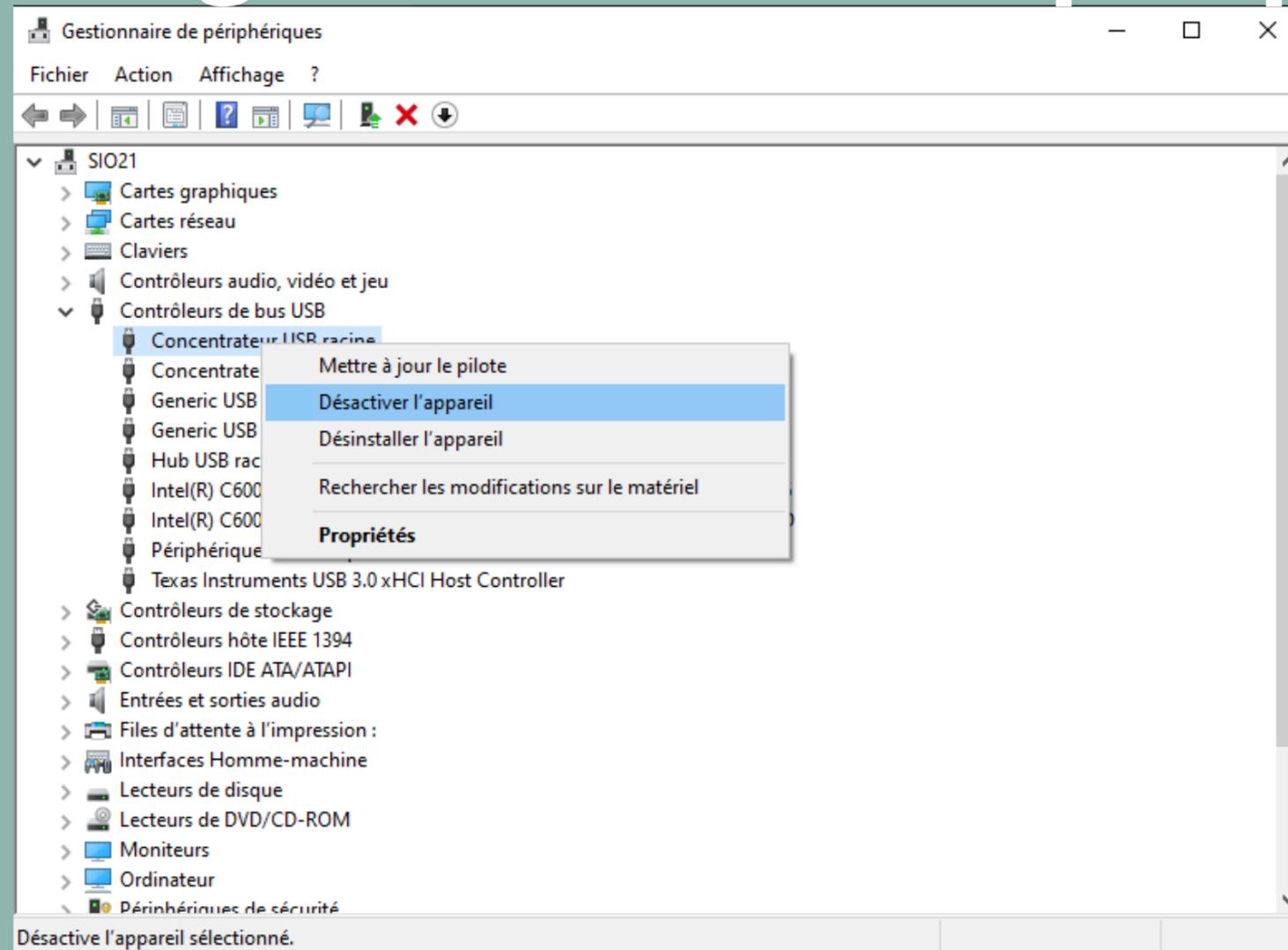
**Ce filtrage permet également de se protéger contre les malwares, le phishing et d'autres menaces en ligne.**



Vous pourrez pour sécuriser encore plus vos pc modifier l'action qu'à chaque périphériques USB. Vous pourrez par exemple interdire l'utilisation de certains port ou directement interdire certains périphériques comme les clé USB.



# Vous pouvez désactiver vos ports USB depuis le gestionnaire de périphériques

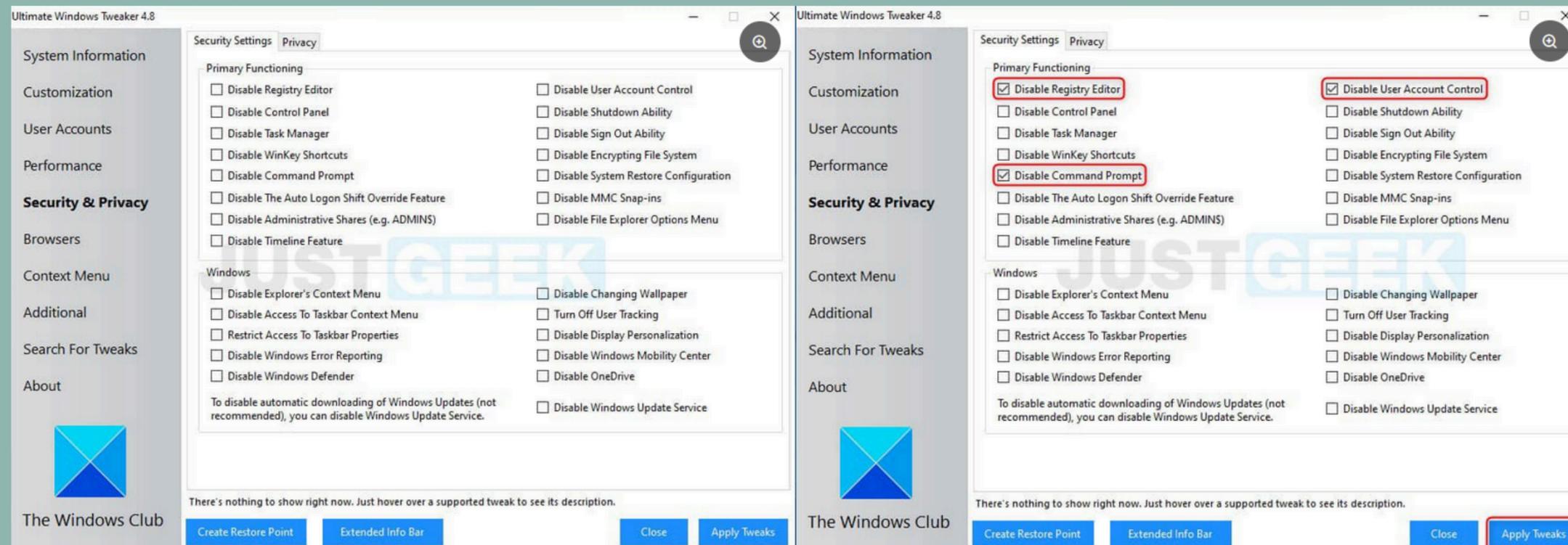


# Pour désactiver la lecture de disque amovible directement

The screenshot shows the Windows Settings application with the 'Exécution automatique' (Automatic execution) page selected in the left sidebar. The main content area is titled 'Exécution automatique' and contains the following elements:

- A search bar at the top left of the settings page with the placeholder text 'Rechercher un paramètre'.
- A sidebar on the left with the following categories: Accueil, Périphériques, Bluetooth et autres appareils, Imprimantes et scanners, Souris, Saisie, Stylet et Windows Ink, Exécution automatique (highlighted), and USB.
- The main content area is titled 'Exécution automatique' and includes the text: 'Utiliser l'exécution automatique pour tous les médias et tous les périphériques'. Below this is a toggle switch labeled 'Activé' which is currently turned on.
- A section titled 'Choisir les paramètres par défaut de l'exécution automatique' contains three dropdown menus:
  - 'Lecteur amovible' with the option 'Ne rien faire' selected.
  - 'Carte mémoire' with the option 'Choisir une application par défaut' selected.
  - 'Apple iPhone' with the option 'Choisir une application par défaut' selected.
- At the bottom right, there are links for 'Paramètres associés', 'Paramètres d'application par défaut', 'Obtenir de l'aide', and 'Donner des commentaires'.

# Pour être certain que ces paramètres restent ainsi le clients pourra installer un outils nommé Ultimate Windows Tweaker pour désactiver l'accès aux paramètres...





**Lorsqu'un utilisateur souhaitera accéder aux paramètres ceci s'affichera.**

## **Des mises a jour récurrentes nécessaires**

- Pour être sûr de garder une bonne sécurité sur le système des mise à jours régulières sont nécessaires pour ce faire Windows Update est un outil indispensable pour effectuer ces actions.
- Il est possible de faire ces mise à jours à la main mais cela relèvera d'un travail très fastidieux.

## **Option alternative:**

**Il est également possible d'effectuer les mise à jours via un Windows serveur à l'aide de l'outil wsus update cela permettra de lancer la mise à jours une seule fois pour qu'elle se déploie sur tout les ordinateurs liés au serveur cela sera utile surtout pour un parc plus important.**

**Il est indispensable de mettre à jour son système régulièrement car c'est via ces mise à jours que certaines failles vont être résolues**

# Des outils supplémentaires pour sécuriser l'utilisation des ordinateurs.

## Un anti-virus

Il offre la possibilité de détecter les menaces, d'analyser votre système et de supprimer tous les logiciels malveillants trouvés sur votre ordinateur. Notre conseil est de toujours avoir un antivirus à jour et garanti pour offrir une meilleure sécurité.

## Un pare-feu

Un pare feu à comme fonction essentielle de bloquer les connexions qui peuvent représenter un problème pour votre système. Vous pouvez le configurer comme vous le souhaitez, en autorisant ou non certains programmes à utiliser le réseau.



## Mission lycée

Mise en place d'une  
charte informatique.

Il devra figurer plusieurs choses sur cette charte.

Tout d'abord concernant les mots de passe:

L'utilisation d'un mot de passe devra être unique il ne faut pas qu'il y ai le même mot de passe pour deux usages différents.

Il est important que le mot de passe respecte un minimum de complexité comme l'utilisation de 12 caractères minimum avec un chiffre, une majuscule, une minuscule et un caractère spécial.

Le dit mot de passe ne doit pas être en lien avec la personne par exemple le prénom de son animal de compagnie ne peut pas faire l'objet d'un mot de passe.

Un mot de passe ne doit pas rester statique et doit être changer régulièrement afin de garder un accès plus sûr.

Si possible un bannissement automatique d'un utilisateur suspect doit être mis en place, ce bannissement prenant effet après plusieurs tentatives de connexion infructueuses

Une sensibilisation sur la sécurité des mots de passes doit être mise en place afin que les étudiants comprennent la nécessité de sécuriser leurs mots de passes(tout les ans pour les premières années)

De préférence il faudrait privilégier une phrase de passe pour que ça soit plus simple pour les étudiants de le retenir et cela reste tout aussi complexe.

# Recommandation pour ces deux années

Pour ces deux années il vous est recommandé de suivre les directives de l'ANSSI  
c'est à dire:

Veillez à ce que vos mots de passes respectent bien les critères de sécurité.  
Changez vos mots de passe régulièrement (tous les trois à six mois environs).  
Si cela est possible pour votre établissement il faudrait qu'une sensibilisation soit  
réalisée pendant les deux années de BTS.

N'utilisez pas un mot de passe ayant un lien direct avec vous comme le prénom  
d'un proche ou d'un animal de compagnie.

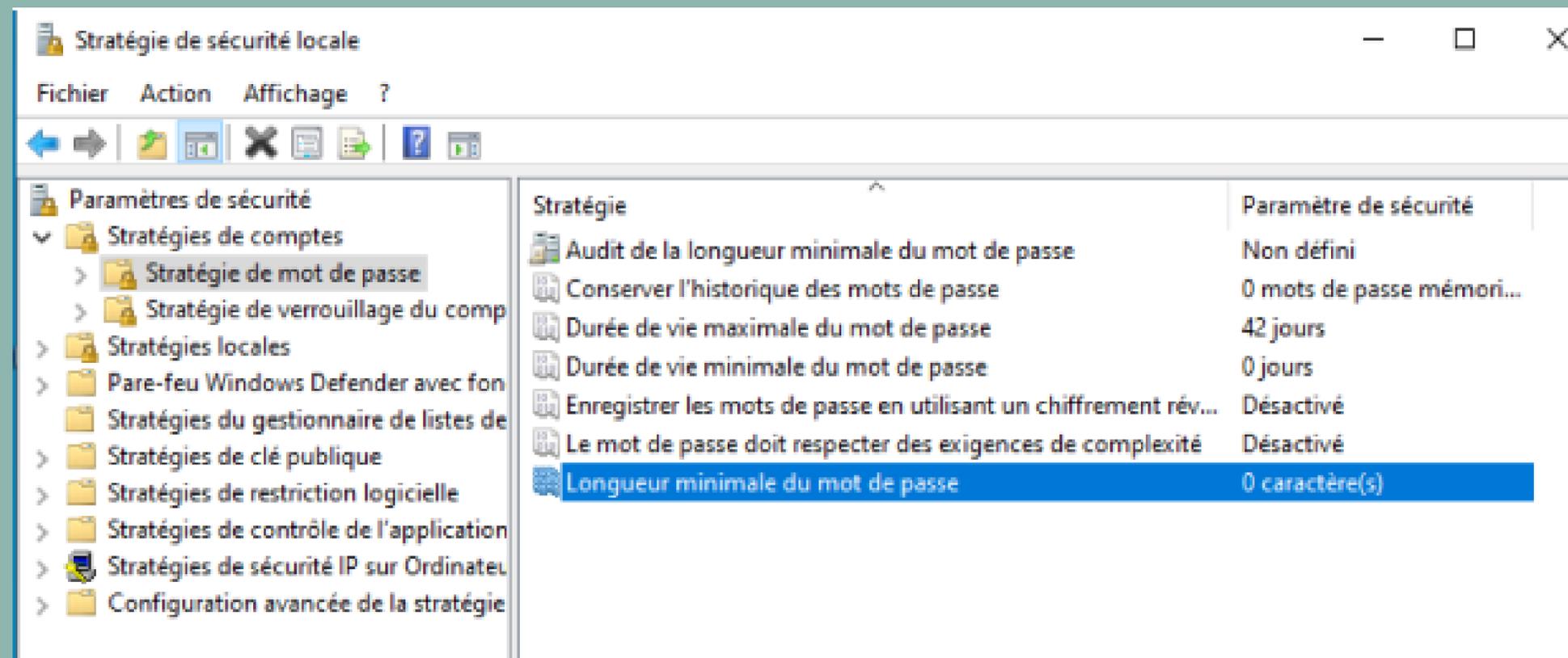
L'utilisation d'une passphrase peut être une solution pour ce faire deux méthodes s'offrent à vous:

Composition aléatoire de mots	Sélection de mots significatifs
<p>Cette méthode consiste à choisir un ensemble de mots au hasard pour former la passphrase. Ces mots peuvent être sélectionnés à partir d'une liste prédéfinie ou générés de manière aléatoire. L'idée est de choisir des mots qui n'ont pas de lien logique entre eux, ce qui rend la passphrase plus robuste contre les attaques par dictionnaire.</p>	<p>Dans cette approche, les utilisateurs choisissent des mots qui ont un sens pour eux mais qui peuvent sembler aléatoires pour d'autres. Cela peut inclure des combinaisons de mots, des acronymes, ou des mots liés à des expériences personnelles.</p>



Voici l'interface d'un Windows Server; comme vous pouvez le voir plusieurs critères de sécurité sont spécifiés.

Ici nous voyons qu'aucun mot de passe ne pourra être enregistré sur le serveur, les mots de passes sont à changer entre 0 et 42 jours et il n'y a pas d'exigence de complexité de mot de passe ainsi que de longueur minimale de mot de passe.



## L'outils proposer par vos professeurs propose de nombreux avantages et inconvénients tels que:

Avantages	Inconvénients
Gratuit et open source	Interface utilisateur peut sembler datée
Stockage sécurisé des mots de passe	Nécessite une gestion manuelle des bases de données
Portabilité sur plusieurs plateformes	Pas de stockage cloud intégré Besoin d'une clé USB pour transporter les données
Forte sécurité avec cryptage fort	Peut nécessiter des mises à jour manuelles