Mode sécurisé

Il est important de comprendre la différence entre le mode normal et le mode sécurisé, car chacun offre un niveau d'isolation différent et n'autorise pas les mêmes interactions avec la machine hôte.

5TQ 6TQ

Le mode sécurisé (ProtectedClient)

```
<ProtectedClient>Enable</ProtectedClient>
```

Le paramètre `<ProtectedClient>` permet de démarrer Windows Sandbox dans un **mode de sécurité renforcé**.

Ce mode est conçu pour **réduire la surface d'attaque** et **empêcher les interactions involontaires** entre l'hôte et la sandbox.

🎯 Objectif

Limiter au strict minimum les canaux de communication entre la sandbox et la machine hôte afin d'empêcher :

- la fuite de données,
- la manipulation de ressources sensibles,
- la propagation d'un contenu malveillant depuis la sandbox.

🛡️ Ce que le mode sécurisé désactive automatiquement

Lorsque le mode sécurisé est activé, Windows Sandbox coupe plusieurs fonctionnalités :

Fonctionnalité	Effet en mode sécurisé
Presse-papier	Copier-coller complètement désactivé
Dossiers mappés	Interdits, même si définis dans le `.wsb`
Redirection imprimante	Désactivée
Micro et webcam	Désactivés
Partages implicites	Désactivés
Intégration hôte ↔ sandbox	Réduite au minimum
Accès GPU	Peut être bloqué selon configuration
Interop COM / OLE	Réduites ou bloquées

En résumé : **le mode sécurisé isole davantage la sandbox et coupe tout ce qui pourrait servir de pont d'attaque entre la sandbox et l'hôte.**

✔️ Quand l'utiliser ?

Il est recommandé lorsque :

- tu analyses un logiciel non fiable ou suspect ;
- tu ouvres un fichier qui pourrait contenir du code malveillant ;
- tu veux réduire au maximum les risques d'exfiltration de données vers l'hôte ;
- tu fais des tests "boîte noire" qui ne nécessitent aucun échange entre la sandbox et ta machine réelle.

❌ Quand éviter de l'utiliser ?

Évite-le si tu as besoin de :

- copier/coller du texte ou du code ;
- exécuter automatiquement un script via un dossier partagé ;
- transférer des fichiers entre l'hôte et la sandbox ;
- utiliser le GPU (par exemple tester une application graphique) ;
- imprimer ou capturer du son/vidéo.

🔍 Exemple de fichier `.wsb` avec mode sécurisé activé

```
<Configuration>
  <ProtectedClient>Enable</ProtectedClient>
  <Networking>Default</Networking>
  <VGpu>Disable</VGpu>
</Configuration>
```

📝 Note : même avec `<ProtectedClient>Enable</ProtectedClient>`, la sandbox **garde un accès réseau**, sauf si tu spécifies :

```
<Networking>Disable</Networking>
```

Comparaison : mode normal vs mode sécurisé

Fonctionnalité	Mode normal	Mode sécurisé
Presse-papier	✔ Activé (copier/coller possible)	❌ Désactivé
Dossiers mappés	✔ Autorisés	❌ Bloqués même s'ils sont définis
Imprimantes	✔ Redirection active	❌ Désactivée
Micro / Webcam	✔ Disponibles si activés	❌ Désactivés
Accès GPU (vGPU)	✔ Actif par défaut	⚠️ Peut être restreint ou désactivé
Interop hôte ↔ sandbox	✔ Étendue (partages, redirections)	❌ Réduite au strict minimum
Accès réseau	✔ Activé par défaut	✔ Activé (sauf si `<Networking>Disable</Networking>`)
Commandes de démarrage	✔ Autorisées	✔ Autorisées
Utilisation prévue	Tests courants, développement, isolation légère	Analyse de fichiers suspects, tests logiciels dangereux, isolement maxima
Surface d'attaque	Plus large	🔒 Significativement réduite

Résumé simple

- **Mode normal** : pratique, flexible, idéal pour tester un logiciel ou faire du dev → mais les échanges hôte ↔ sandbox sont ouverts.
- **Mode sécurisé** : isolement renforcé, aucune redirection, aucun pont non essentiel → recommandé pour analyser des fichiers douteux ou réduire les risques.

> Le mode sécurisé fermet tous les accès sauf le réseau.