# Mercredi 25 septembre 2024

Hier nous avons trouvé une information cruciale : les fichiers de plus de 3Mo ne sont pas pris en compte par le copilote si l’option d’IA générative est activée.   
Or, nous avons vu que l’option d’IAG était utile pour le bon fonctionnement d’un copilote, elle fonctionne comme un agent pour le choix de rubrique, permet une meilleure expérience d’utilisation pour l’utilisateur. Néanmoins, si cette option empêche l’utilisation de fichiers de plus de 3Mo, cela peut poser un problème étant donné que la quantité de fichiers de plus de 3Mo n’est pas déterminée mais pourrait être importante, et nous ne pouvons pas nous permettre des creux.

Pour palier à ce problème, j’avais initialement pensé à créer une boucle qui permettrait de désactiver l’option d’AIG quand le fichier requis pour répondre à la demande utilisateur fait plus de 3Mo. Je m’apprêtais à créer un flux power automate que j’aurais incorporé dans le copilote mais il semblerait qu’il existe déjà des solutions, notamment l’index sémantique pour Copilot.

Avant de me lancer dans les procédures pour mettre en place un index sémantique, j’ai voulu essayer d’utiliser le copilot pour lui poser une question sur un fichier (< 3Mo) du sharepoint (Knowledge source) simplement et aucuns résultats n’est sorti.

Ce n’est qu’après avoir regardé plusieurs vidéos que je me suis rendu compte qu’il fallait gérer l’authentification manuellement via Azure Active Directory afin de pouvoir alimenter le copilote avec la source de knowledge (SharePoint)

Après avoir effectuer plus de recherches dans la documentation, voici ce que j’ai trouvé :

1. **Personnalisation avec Microsoft Copilot Studio et Authentifications**
   1. **Personnalisation** : MCS permet de créer des copilotes personnalisables, avec des expériences conversationnelles uniques grâce à des fonctions telles que l’intégration d’IA générative, l’orchestration des actions, les connecteurs Power Automate, etc…
   2. **Authentification automatique**: utilisée (notamment via Teams), elle fait perdre la capacité de configuration des aspects plus complexe, comme l’accès aux connecteurs premium ou la génération de secrets pour sécuriser les accès. L’authentification automatique est utile pour des scénarios plus simples où ces personnalisations ne sont pas nécessaires, mais elle limite l’exploitation complète des fonctionnalités avancées de Copilot Studio.
   3. **Authentification manuelle** : via Azure, cela vous donne un contrôle plus poussé sur l’accès aux données, notamment l’accès aux connecteurs premium, essentiels pour des intégrations plus sophistiquées avec des services comme SharePoint et pour des scénarios nécessitant une sécurité et une gestion des accès plus pointue.
2. **Le Copilote Teams comme boîte Noire** 
   1. Lorsqu’un copilote est utilisé uniquement via teams avec l’authentification automatique, il peut paraître comme une boîte noire dans le sens où vous n’avez pas de visibilité et un contrôle complet sur ses comportements internes. En effet, l’authentification automatique et l’utilisation via Teams limitent les options de personnalisation, et il est difficile d’ajuster les paramètres au niveau de la sécurité, des accès et de l’intégration avec d’autres système.
   2. **Contrôle limité**: On ne peut pas exploiter certaines fonctionnalités avancées de gestion d’identités et des accès qui sont disponibles via l’authentification manuelle, rendant potentiellement le copilote moins adaptable à des besoins spécifiques, surtout en entreprise où la gestion fine des accès et des permissions est souvent critique.
3. **Manuel vs Automatique : Quel Choix pour Bénéficier des Avantages ?**
   1. **Scénarios Simples : Authentification Automatique** : Si votre utilisation se limite à des réponses simples ou à une assistance dans des tâches routinières sans besoins complexes d'intégration ou de sécurité, l'authentification automatique avec Teams pourrait suffire.
   2. **Scénarios Complexes : Authentification Manuelle** : Pour tirer pleinement parti des capacités de **Microsoft Copilot Studio**, telles que l'intégration avancée avec Power Automate, l’utilisation des connecteurs premium, et la possibilité de créer des actions génératives ou des expériences conversationnelles enrichies, l'authentification manuelle est recommandée. Elle permet d’avoir un contrôle complet sur les flux de données et les accès sécurisés à SharePoint et d’autres services essentiels​.

J’ai par la suite effectué une liste concrète des différences notables entre un copilote à authentification automatique et un copilote à authentification manuelle que voici :

**1. Contrôle des accès et sécurité**

* **Authentification automatique (Teams)** :
  + Basé sur les **permissions Microsoft 365** existantes (Teams, SharePoint).
  + Pas de personnalisation des accès au-delà des droits standards.
* **Authentification manuelle** :
  + **Personnalisation des accès** via Azure Active Directory (Azure AD).
  + Possibilité de configurer des **politiques d’accès spécifiques** et des mécanismes de sécurité avancés (ex : secrets d'API).

**2. Fonctionnalités et personnalisation**

* **Authentification automatique (Teams)** :
  + Fonctionnalités **limitées** (réponses conversationnelles, automatisation simple).
  + Pas d'accès aux **connecteurs premium** ni de possibilité d'orchestration avancée.
* **Authentification manuelle** :
  + Accès aux **connecteurs premium** et **personnalisés**.
  + **Intégration multi-canal** (web, mobile, plateformes tierces).
  + Orchestration des actions, génération de réponses par l'IA, exécution de **flux complexes** via Power Automate.

**3. Scénarios d'utilisation**

* **Authentification automatique (Teams)** :
  + Idéal pour des **scénarios internes simples** (FAQ, tâches de support).
  + Utilisation limitée à **Teams**.
* **Authentification manuelle** :
  + Convient aux **scénarios complexes** nécessitant des intégrations avec des systèmes externes (CRM, ERP).
  + Déploiement possible sur **plusieurs canaux** (web, apps).

**4. Maintenance et gestion**

* **Authentification automatique (Teams)** :
  + **Simplicité de gestion**, héritage des permissions existantes.
  + Moins flexible si les besoins évoluent (difficulté à ajouter des fonctionnalités avancées).
* **Authentification manuelle** :
  + **Configuration initiale plus complexe** (via Azure AD), mais flexibilité totale sur la gestion des accès et des fonctionnalités.
  + Permet une adaptation continue aux besoins de l’entreprise.

**5. Exemples concrets**

* **Authentification automatique (Teams)** :
  + Requêtes simples, comme "Accès à un fichier SharePoint" avec respect des permissions standards.
* **Authentification manuelle** :
  + Requêtes et **actions complexes** : envoi de notifications, mise à jour de fichiers SharePoint, déclenchement de processus métier.

Quelles sont nos marges de manœuvre

Comment améliorer les performances du copilote ?