CollègeAhuntsic

Microsoft Authenticator : ce que vous devez savoir

Dans le cadre du renforcement de la sécurité de ses systèmes informatiques, le Collège Ahuntsic utilise l'authentification multifacteur (MFA) pour protéger l'accès aux comptes et aux ressources informatiques.

Microsoft Authenticator est une application qui permet de confirmer votre identité lors d'une connexion à votre compte du Collège.

Nous comprenons que l'installation d'une application professionnelle sur un téléphone personnel puisse soulever des questions concernant la confidentialité et la protection des renseignements personnels.

Cette FAQ vise à répondre à vos préoccupations.

Généralités

1. Qu'est-ce que Microsoft Authenticator?
Microsoft Authenticator est une application gratuite développée par Microsoft. Elle permet de confirmer votre identité lors d'une connexion à votre compte professionnel.

Elle ajoute une deuxième étape de vérification en complément de votre mot de passe afin de réduire les risques d'accès non autorisé à votre compte.

2. Pourquoi le Collège demande-t-il d'utiliser Microsoft Authenticator?
L'authentification multifacteur constitue une mesure de sécurité permettant de mieux protéger les renseignements personnels, les systèmes informatiques et les ressources numériques du Collège.

Même si votre mot de passe est compromis, une personne malveillante ne pourra normalement pas accéder à votre compte sans réussir la deuxième étape de vérification.

3. L'application est-elle gratuite?
Oui. Microsoft Authenticator est offerte gratuitement dans l'App Store d'Apple et le Google Play Store.

Aucun abonnement ou achat n'est nécessaire pour utiliser ses fonctionnalités d'authentification.

4. Est-ce que l'utilisation de cette application est obligatoire?
L'utilisation d'un téléphone personnel n'est pas la seule possibilité.

La configuration d'un facteur d'authentification conforme au niveau d'exigence fixé par le Collège est obligatoire. Quoique la clé d'accès de Microsoft Authenticator reste la méthode qui combine au mieux

facilité d'utilisation et niveau de sécurité optimal, d'autres options peuvent être disponibles, notamment un jeton matériel.

Pour faire une telle demande, veuillez ouvrir un billet Octopus auprès de la DTI.

Protection de la vie privée

5. Est-ce que le Collège peut accéder aux photos et aux vidéos de mon téléphone?
Non. Microsoft Authenticator ne donne pas au Collège accès à vos photos, vidéos ou albums personnels.

6. Est-ce que le Collège peut lire mes messages textes ou mes courriels personnels?
Non. Microsoft Authenticator ne permet pas au Collège de consulter vos messages textes, vos conversations ou vos courriels personnels.

7. Est-ce que le Collège peut consulter mes applications personnelles?
Non. Microsoft Authenticator ne donne pas au Collège un accès général aux applications installées sur votre téléphone.

8. Est-ce que le Collège peut consulter mes contacts ou mon répertoire téléphonique?
Non. Microsoft Authenticator ne permet pas au Collège de consulter vos contacts ou votre repertoire téléphonique.

9. Est-ce que le Collège peut surveiller mon téléphone ou suivre mon utilisation personnelle?
Non. Microsoft Authenticator, ne permet pas au Collège de surveiller votre utilisation personnelle du téléphone, de consulter votre historique de navigation ou de suivre les applications que vous utilisez.

10. Est-ce que le Collège peut effacer le contenu de mon téléphone à distance?
Non. La simple installation de Microsoft Authenticator ne donnent pas au Collège le pouvoir d'effacer le contenu de votre téléphone.

11. Est-ce que Microsoft recueille des renseignements lorsque j'utilise l'application?
Oui. Comme toute application, Microsoft Authenticator recueille certaines informations nécessaires à son fonctionnement et à sa sécurité.

Selon la documentation de Microsoft, cela comprend notamment :

- Les informations du compte ajouté à l'application.
- Des données techniques relatives à l'application comme :
    - Le type d'opération effectuée dans l'application (ajout d'un compte, demande d'authentification, approbation ou refus).
    - Le résultat des opérations (réussite ou échec).

- Les erreurs rencontrées et les informations nécessaires à leur diagnostic.
- La version de l'application et du système d'exploitation.
- Certains identifiants techniques permettant d'assurer le fonctionnement et la sécurité de l'application.

Des journaux de diagnostic peuvent également être transmis à Microsoft lorsque vous choisissez d'envoyer des commentaires ou de signaler un problème. Ces journaux peuvent contenir certaines informations personnelles ou techniques nécessaires au diagnostic.

Microsoft permet également de désactiver le partage facultatif de données d'utilisation supplémentaires dans les paramètres de l'application.

Autorisations demandées par l'application

12. Pourquoi l'application demande-t-elle l'accès à la caméra?
La caméra peut être utilisée pour scanner le code QR nécessaire à l'inscription de votre compte professionnel ou encore lors de l'utilisation de la méthode d'authentification utilisant la clé d'accès.

13. Pourquoi l'application demande-t-elle l'autorisation d'envoyer des notifications?
Les notifications permettent de recevoir les demandes d'approbation lorsqu'une connexion à votre compte nécessite une vérification.

14. Pourquoi l'application pourrait-elle demander l'accès à ma localisation GPS?
Dans certaines configurations de sécurité avancées, Microsoft peut exiger une vérification de la localisation GPS afin de confirmer que l'utilisateur se trouve dans un pays autorisé à accéder à certaines ressources.

Cette fonctionnalité **n'est pas activée** par le Collège.

Si cette fonctionnalité est activée, Microsoft Authenticator peut transmettre les coordonnées GPS afin de déterminer le pays où se trouve l'appareil. Le nom du pays est conservé et peut être communiqué au système de gestion de la sécurité informatique du Collège. Selon la documentation de Microsoft, les coordonnées GPS réelles ne sont pas conservées sur ses serveurs.

15. Est-ce que je dois activer Face ID ou la reconnaissance des empreintes digitales?
Non. L'utilisation de la biométrie n'est pas requise pour utiliser Microsoft Authenticator.

Selon la configuration de votre appareil et les fonctionnalités activées, vous pourriez utiliser le code de déverrouillage de votre téléphone plutôt que la biométrie.

Les données biométriques utilisées pour déverrouiller votre téléphone sont gérées par les mécanismes de sécurité de votre appareil. Elles ne sont pas transmises au Collège par le simple fait d'utiliser Microsoft Authenticator.

16. Est-ce que je dois donner mon numéro de téléphone personnel au Collège?
L'utilisation de Microsoft Authenticator ne nécessite pas de fournir un numéro de téléphone personnel.

L'inscription du compte s'effectue principalement à l'aide de votre adresse courriel professionnelle et du processus de configuration fourni par Microsoft.

Utilisation au quotidien

17. Est-ce que je recevrai des notifications chaque fois que j'utilise mon téléphone?
Non. Les notifications sont associées aux demandes d'authentification de votre compte professionnel.

Elles ne sont pas liées à votre utilisation générale du téléphone.

18. Est-ce que je dois avoir accès à Internet pour utiliser l'application?
Cela dépend de la méthode utilisée.

- Les approbations par notification nécessitent une connexion Internet, par Wi-Fi ou par réseau cellulaire.

- Les codes de vérification générés directement dans l'application ou l'utilisation d'une clé d'accès peuvent fonctionner sans connexion Internet.

19. Est-ce que l'application utilise mes données cellulaires?
Les notifications d'authentification peuvent utiliser une connexion Internet, soit par Wi-Fi, soit par réseau cellulaire.

L'utilisation des données dépend de votre connexion et de votre utilisation de l'application. L'application ne nécessite pas un forfait de données particulier.

20. Est-ce que je peux désinstaller l'application lorsque je ne suis pas au travail?
L'application doit demeurer disponible pour permettre les authentifications exigées lors de vos connexions aux ressources du Collège.

Sa désinstallation pourrait vous empêcher de vous authentifier et d'accéder à certains services.

21. Que se passe-t-il si je change de téléphone?

Vous devrez configurer Microsoft Authenticator sur votre nouvel appareil avant de vous départir de votre ancien et faire mettre à jour les méthodes d'authentification associées à votre compte.

Il est important de retirer l'ancien appareil de votre compte lors que le transfert est fait afin que les demandes d'authentification ne continuent pas à lui être envoyées.

22. Que se passe-t-il si je perds mon téléphone?
Vous devez communiquer rapidement avec la DTI afin de faire retirer l'appareil perdu de vos méthodes d'authentification.

La DTI pourra vous accompagner pour rétablir l'accès à votre compte et configurer une nouvelle méthode d'authentification.

Solutions de remplacement et assistance

23. Que faire si je ne possède pas de téléphone intelligent?
Veuillez ouvrir un billet Octopus auprès de la DTI afin que nous puissions évaluer votre situation et vous proposer une solution.

24. Que faire si je ne souhaite pas installer une application professionnelle sur mon téléphone personnel?
Nous comprenons cette préoccupation. Le Collège prévoit des solutions de remplacement pour les personnes qui ne souhaitent pas utiliser leur téléphone personnel pour l'authentification multifacteur.

Veuillez ouvrir un billet Octopus auprès de la DTI afin que nous puissions évaluer votre situation et vous proposer une solution.

25. À qui dois-je m'adresser si j'ai des questions ou si j'éprouve des difficultés?
La DTI est disponible pour vous accompagner dans la configuration de Microsoft Authenticator et répondre à vos questions.

Pour obtenir de l'aide, veuillez ouvrir un billet dans Octopus.
Portail de soutien : https://collegeahuntsic.octopus-itsm.com/Web/CreateRequest.aspx

- Service informatique (DTI)\Accès\Demande de jeton