GUIDE D'UTILISATION SIMPLIFIÉ

INSTALLER ET UTILISER WATCHGUARD AUTHPOINT SUR VOTRE SMARTPHONE

Guide étape par étape

Installez l'application **WatchGuard AuthPoint MFA** et bénéficiez d'une couche de sécurité supplémentaire grâce à la double authentification.

SOMMAIRE

COMPRENDRE WATCHGUARD AUTHPOINT

L'application **WatchGuard AuthPoint** (MFA) est une solution d'authentification multifactorielle (MFA) qui permet de renforcer la sécurité des connexions aux systèmes et aux applications.
L'application est conçue pour s'assurer que seuls les **utilisateurs autorisés** peuvent accéder à des ressources critiques, en ajoutant une couche supplémentaire de protection par-dessus les mots de passe, qui, seuls, peuvent être vulnérables aux attaques.

À quoi sert WatchGuard AuthPoint ?

- **Sécuriser l'accès aux applications et systèmes** : AuthPoint garantit que même si un mot de passe est compromis, un attaquant ne peut pas accéder à vos systèmes sans une deuxième forme d'authentification.
- **Prévenir les attaques de type phishing et vol d'identifiants** : En utilisant plusieurs méthodes d'authentification (comme une notification push ou un token), il devient beaucoup plus difficile pour un attaquant d'exploiter des informations de connexion volées.
- **Conformité aux normes de sécurité** : De nombreuses réglementations exigent désormais une authentification multifactorielle pour protéger les données sensibles. AuthPoint aide les entreprises à se conformer à ces règles.

Comment utiliser WatchGuard AuthPoint ?

1. Téléchargement et installation,
2. Enregistrement de votre compte (activation de votre jeton),
3. Authentification à deux facteurs :
    a. Saisir vos identifiants habituels (nom d'utilisateur et mot de passe)
    b. Valider la connexion avec AuthPoint (notification push, QR Code, One-Time Password)

Dans quels cas utiliser WatchGuard AuthPoint ?

- Accéder à un **VPN**
- Accéder au **réseau interne** de votre entreprise (facultatif)
- Accéder à des **applications cloud** (facultatif)

Chaque fois que vous vous connectez à une ressource protégée par **AuthPoint**, vous recevrez une notification sur votre téléphone. Vous devrez alors **approuver cette demande** pour accéder à votre compte. Ainsi vous pourrez entre autre l'utilisez pour :

L'application est disponible sur **App Store** et **Google Play,** la mise en place de votre protection nécessite quelques étapes que vous allons expliquer pas à pas dans cette fiche.

INSTALLATION DE L'APPLICATION

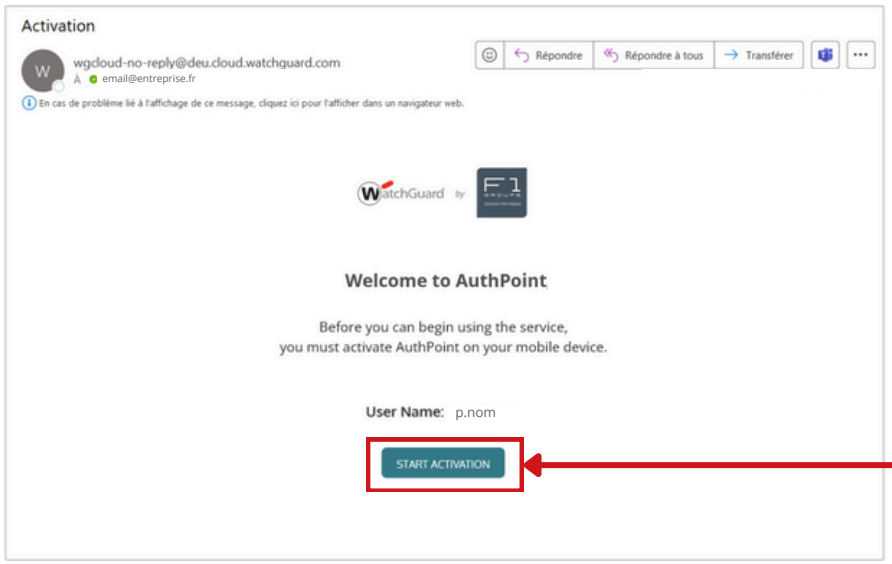
Votre service F1 GROUPE a validé le service WatchGuard MFA, vous devez ainsi avoir reçu un email dans votre messagerie, celui-ci va vous permettre de mettre en place l'application **WatchGuard AuthPoint**.

Comment retrouver l'email reçu ?

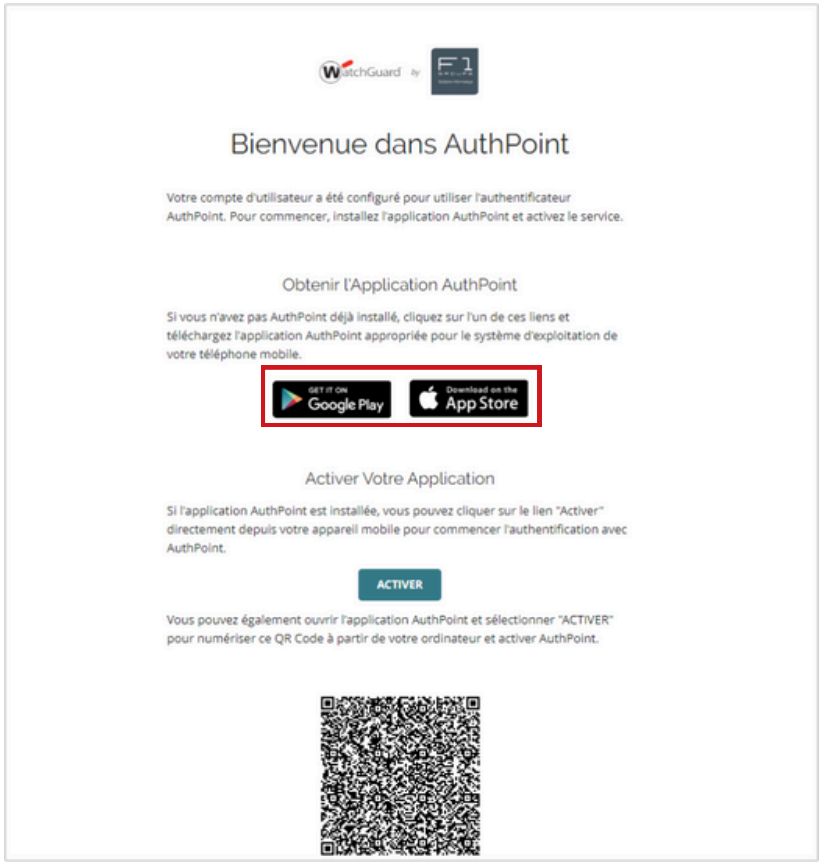
Depuis votre messagerie, vous pouvez rechercher l'email avec ces informations :.

- Objet de l'email : **Activation**
- Adresse de l'expéditeur : **wgcloud-no-reply@deu.cloud.watchguard.com**

Si vous ne le trouvez pas, pensez à regarder vos courriers indésirables.



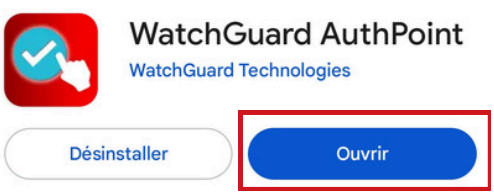
Cliquez sur le bouton d'activation.



La fenêtre suivante s'ouvre.

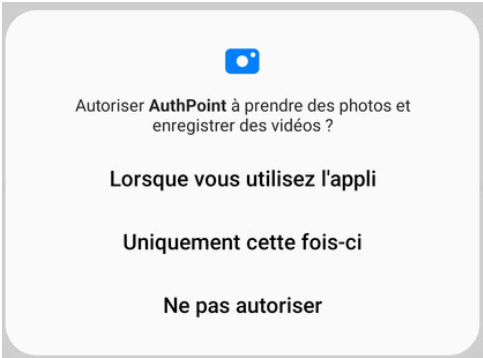
Prenez à présent votre smartphone, rendez-vous dans "**Google Play**" ou "**App Store**" selon votre téléphone, afin de télécharcher l'application "**WatchGuard AuthPoint**"

Une fois le téléchargement terminé, ouvrez l'application



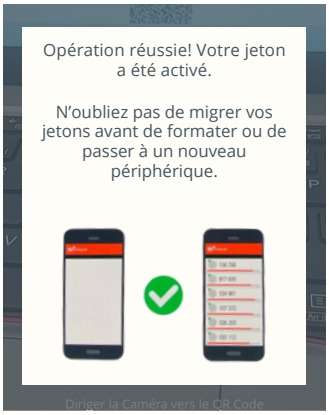
Appuyez sur le bouton "**Activer**"

Vous devez autoriser l'accès à la caméra de votre téléphone pour permettre de scanner le QR Code qui contient toutes les informations nécessaires pour lier votre compte à l'application.

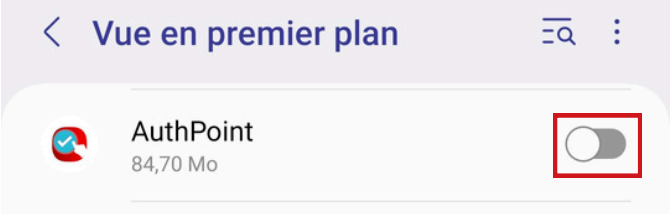


L'application vous propose de scanner un QR Code.
Dirigez votre téléphone sur la fenêtre ouverte depuis l'email reçu pour scannez le QR Code inclus.

Apparaît alors sur l'écran de votre smartphone, la validation d'activation de votre jeton.

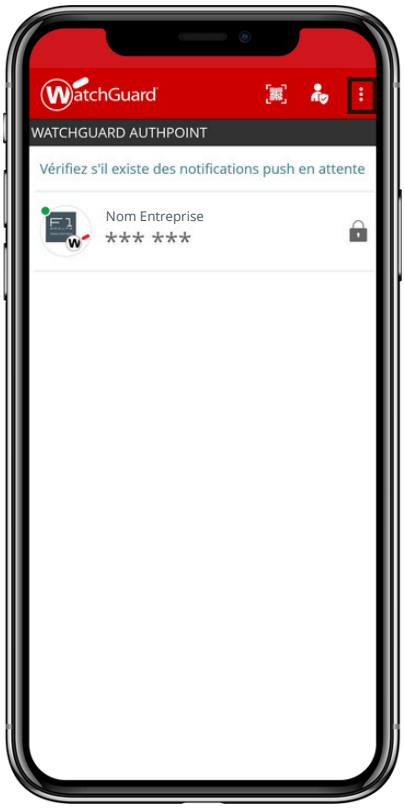


Vous devrez peut-être autoriser l'application à s'exécuter en arrière-plan. Cochez la case correspondante.



CRÉATION DE VOTRE CODE PIN

Afin de finaliser l'installation de votre application, il est essentiel à présent de définir un code PIN unique. Cette étape est d'ailleurs indispensable pour compléter l'activation.



Sur la page d'accueil de l'application, appuyez sur les 3 points en haut à droite de l'écran pour accéder aux paramètres.

Sélectionnez **Sécurité des Jetons**

Dans la page qui s'ouvre, allez dans la partie **GESTION DES PIN**:
Cochez la case afin d'activer la protection avec la création d'un code PIN qui protégera votre ou vos jeton.s

Portez une attention particulière dans le choix de votre code PIN, faites en sorte d'en choisir un que vous êtes certain de vous souvenir.

Une fois votre code PIN créé, l'application vous communique une code PUK que nous vous conseillons de sauvegarder.

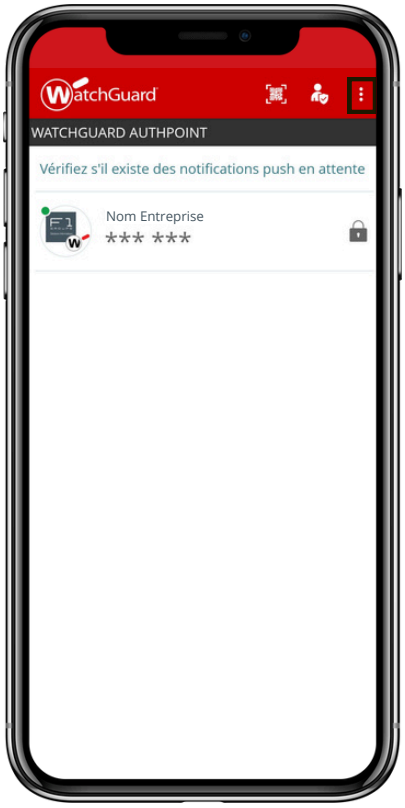
L'application **WatchGuard AuthPoint** est à présent installée, et protégée par votre code PIN et votre jeton est activé. Vous pouvez utiliser l'application dès à présent.

- CETTE ÉTAPE EST FACULTATIVE MAIS FORTEMENT RECOMMANDÉE -

Vous avez la possibilité, si vous le souhaitez de vous authentifier grâce à vos données biométriques uniques (empreinte digitale, reconnaissance faciale).

L'activation de cette option est une excellente manière de sécuriser vos comptes mais également de simplifier votre expérience utilisateur. Un simple geste suffit pour vous connecter.

À noter cependant, que cela est possible uniquement si votre smartphone est compatible avec la reconnaissance biométrique.



Pour cela depuis la page d'accueil de l'application, appuyez sur les 3 points en haut à droite de l'écran pour accéder aux paramètres.

Sélectionnez **Sécurité des Jetons**

À présent allez dans la partie **PROTECTION BIOMÉTRIQUE** :
Cochez la case afin d'activer la protection via vos données biométriques, ainsi vous n'aurez plus à saisir le code PIN que vous avez créé.

Points à noter :

- Vous pourrez réaliser cette étape uniquement après avoir créé votre code PIN
- L'application utilisera la méthode de déverrouillage configurée sur votre téléphone (empreinte digitale ou reconnaissance faciale)

Chaque fois que vous vous connectez à une ressource protégée par **AuthPoint** (ex : *VPN de votre entreprise, messagerie email, accès à un CRM...*)

Lors de votre connexion, vous entrez les informations suivantes :

- Identifiant utilisateur : Il s'agit généralement de votre adresse email professionnelle ou d'un nom d'utilisateur fourni par votre administrateur système.
- Mot de passe : Votre mot de passe personnel pour accéder au service ou à l'application en question.

Ensuite, une étape supplémentaire d'authentification sera requise, soit par **OTP**, soit par **Push**.

Les deux méthodes d'authentification proposées par AuthPoint :

1. **Authentification par OTP** (One-Time Password)

- Fonctionnement de cette méthode : *un code unique est envoyé sur votre smartphone. Ce code doit être saisi lors de la connexion pour confirmer votre identité.*
- Cas d'utilisation *: méthode particulièrement adaptée dans un environnement hors ligne ou dans une zone sans couverture réseau (pas de Wi-Fi ni données mobiles)*

- **Génération du code OTP :**

Lors d'une connexion, le système demande une authentification supplémentaire.

Ouvrez l'application WatchGuard AuthPoint sur votre smartphone.

Sélectionnez le compte pour lequel vous souhaitez générer un code OTP. Authentifiez-vous.

Un code à usage unique (OTP) de 6 chiffres apparaîtra à l'écran. Ce code est valide pour une durée limitée (généralement 30 secondes).

- **Utilisation du code OTP :**

Lors d'une demande de connexion, après avoir entrez votre identifiant et mot de passe habituel, le système demande une authentification supplémentaire, saisissez alors le code OTP affiché dans l'application AuthPoint.

2. Authentification par Push

- Fonctionnement de cette méthode : *une notification s'affiche directement sur votre smartphone lorsqu'une tentative de connexion est détectée. Il suffit alors de l'approuver ou de la refuser.*
- Cas d'utilisation *: méthode à privilégier, elle est idéale pour un accès fréquent à des systèmes ou applications, elle offre un haut niveau de sécurité en toute simplicité et rapidité.*

- **Réception de la notification Push :**

Lors d'une connexion, une notification Push est envoyée sur votre smartphone via l'application WatchGuard AuthPoint.

- **Validation de la notification Push :**

- Ouvrez la notification Push sur votre smartphone. *

- Vérifiez les détails de la demande de connexion (comme l'heure et l'emplacement).

- Si les informations sont correctes, appuyez sur "Approuver" pour valider la connexion.

- Si les informations ne sont pas correctes ou si vous n'êtes pas à l'origine de la demande, appuyez sur "Refuser".

** Dans le cas où la notification n'apparaît pas sur votre smartphone, ouvrez tout simplement l'application Authpoint.*

Recommandations générales pour l'utilisation de AuthPoint :

- Sécurisez votre smartphone : Activez un code PIN, un verrouillage biométrique ou tout autre moyen pour empêcher l'accès non autorisé.
- Mettez à jour régulièrement l'application : Assurez-vous de toujours utiliser la dernière version d'AuthPoint pour bénéficier des dernières fonctionnalités et correctifs de sécurité.
- Activez les notifications : Vérifiez que les notifications AuthPoint sont bien activées sur votre téléphone pour ne pas manquer une demande PUSH.
- Favorisez l'utilisation des notifications PUSH : idéale pour une connexion rapide et sans effort, tout en garantissant une sécurité optimale