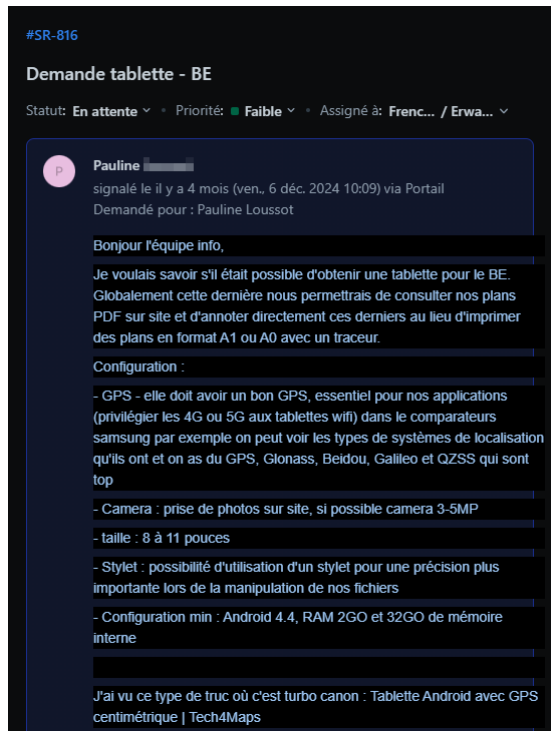


Configuration d'un profil professionnel sur Android dans Intune

Je dois préparer une tablette conforme à la demande de Pauline. Elle souhaite principalement consulter des fichiers PDF sur chantier et annoter des plans de grande taille avec une application comme AutoCAD.



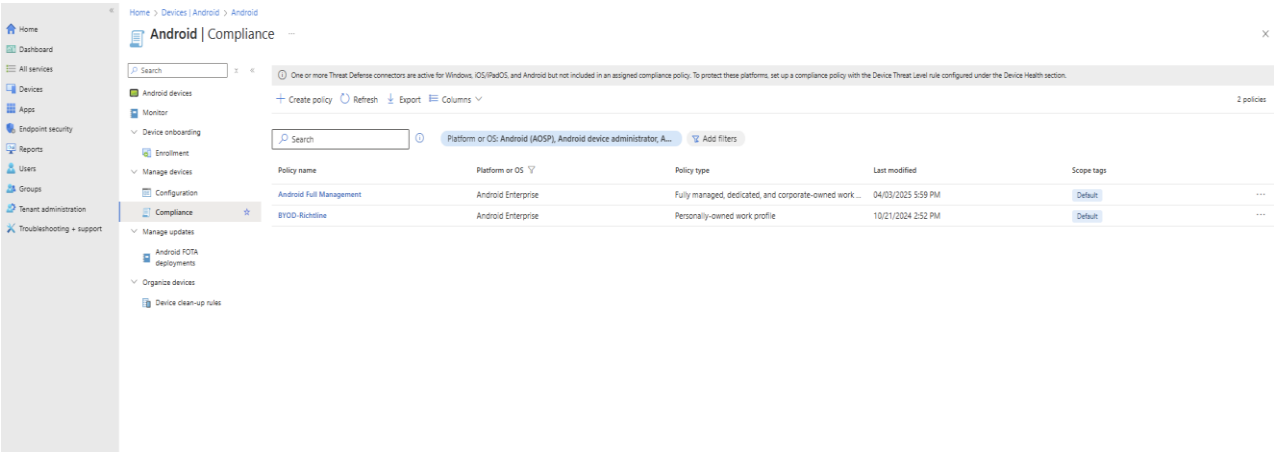
J'ai configuré la tablette en y installant uniquement un profil professionnel. Ce choix permet de séparer clairement l'usage personnel et professionnel, garantissant ainsi une meilleure sécurité des données sensibles liées à ses applications métiers et aux plans annotés sur chantier. Ce profil limite également les risques liés aux téléchargements non autorisés ou à l'installation d'applications non professionnelles. De plus, cette configuration facilite l'administration et la gestion à distance, ainsi que l'application uniforme des politiques de sécurité définies par notre entreprise Volkswind et AXPO. Cela permet enfin à Pauline de disposer d'un environnement de travail optimisé, stable et dédié exclusivement à ses activités professionnelles sur le terrain.

J'ai créé une politique « Android Full Management » sous Intune pour gérer pleinement la tablette de manière professionnelle. Cette politique permet d'appliquer automatiquement des paramètres précis comme la sécurité, les restrictions d'installation d'applications, ainsi que la configuration de fonctionnalités spécifiques nécessaires à l'utilisation professionnelle exclusive.

Appliquer cette politique est essentiel car cela centralise et automatise la gestion des appareils mobiles, garantissant ainsi la conformité aux normes de sécurité de l'entreprise et simplifiant considérablement l'administration. De plus, cela permet une gestion à distance efficace, essentielle pour maintenir la tablette à jour et sécurisée sur le terrain.

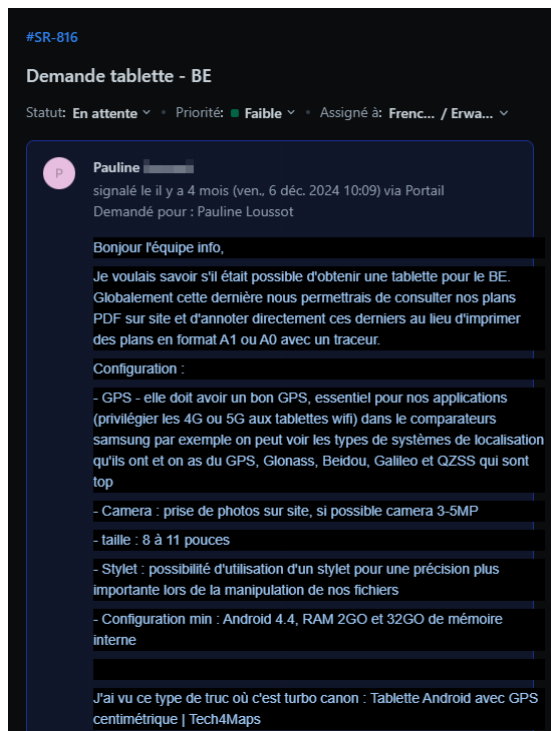
La politique de sécurité vérifie en premier lieu l'intégrité de l'appareil à travers le verdict "Play Integrity" afin de détecter d'éventuelles modifications non autorisées. Elle exige une version minimale d'Android (11.0) pour garantir un niveau de sécurité à jour. De plus, elle impose obligatoirement le chiffrement des données stockées localement et vérifie l'intégrité des applications exécutées via Intune. Concernant la sécurité du dispositif, un mot de passe numérique d'au moins 4 caractères est requis avec une rotation obligatoire après cinq changements. Enfin, la règle verrouille automatiquement l'appareil après 5 minutes d'inactivité pour limiter les risques en cas de perte ou de vol.

Nous exigeons que tous les appareils mobiles soient conformes (« compliant ») aux politiques de sécurité définies dans Intune, conformément aux standards établis par notre entreprise. Cette exigence est indispensable pour garantir la sécurité des données professionnelles, prévenir toute fuite ou accès non autorisé, et protéger l'intégrité des systèmes d'information. En imposant cette conformité, nous assurons également que chaque appareil dispose des mises à jour et paramètres nécessaires pour se défendre efficacement contre les cybermenaces.



Configuration d'un profil professionnel sur Android dans Intune

Je dois préparer une tablette conforme à la demande de Pauline. Elle souhaite principalement consulter des fichiers PDF sur chantier et annoter des plans de grande taille avec une application comme AutoCAD.



J'ai configuré la tablette en y installant uniquement un profil professionnel. Ce choix permet de séparer clairement l'usage personnel et professionnel, garantissant ainsi une meilleure sécurité des données sensibles liées à ses applications métiers et aux plans annotés sur chantier. Ce profil limite également les risques liés aux téléchargements non autorisés ou à l'installation d'applications non professionnelles. De plus, cette configuration facilite l'administration et la gestion à distance, ainsi que l'application uniforme des politiques de sécurité définies par notre entreprise Volkswind et AXPO. Cela permet enfin à Pauline de disposer d'un environnement de travail optimisé, stable et dédié exclusivement à ses activités professionnelles sur le terrain.

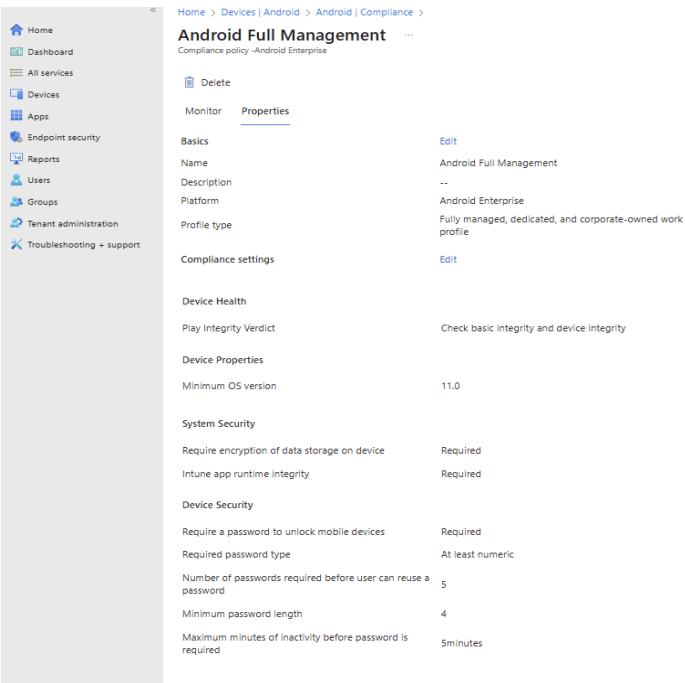
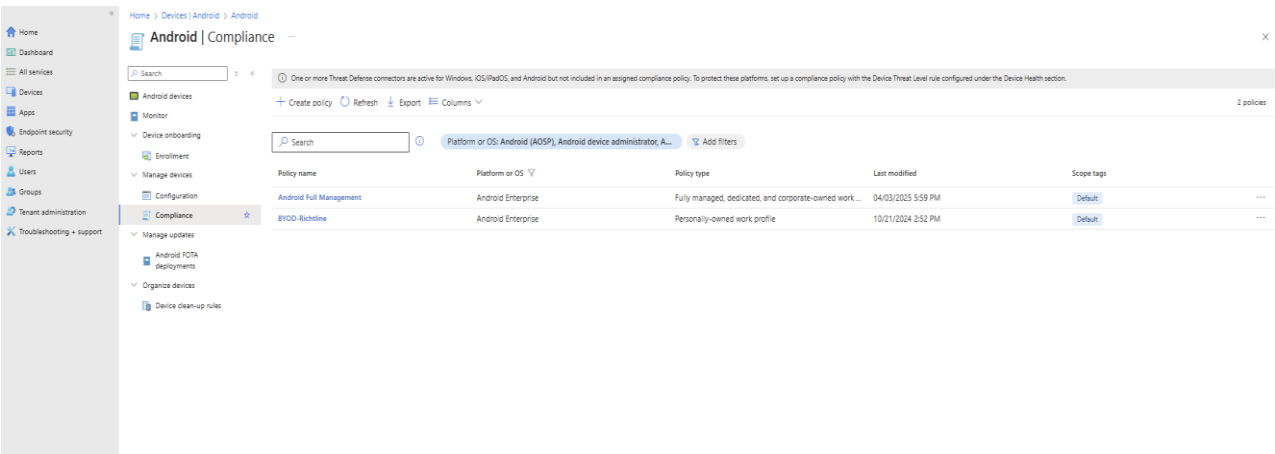
J'ai créé une politique « Android Full Management » sous Intune pour gérer pleinement la tablette de manière professionnelle. Cette politique permet d'appliquer automatiquement des paramètres précis comme la sécurité, les restrictions d'installation d'applications, ainsi que la configuration de fonctionnalités spécifiques nécessaires à l'utilisation professionnelle exclusive.

Appliquer cette politique est essentiel car cela centralise et automatise la gestion des appareils mobiles, garantissant ainsi la conformité aux normes de sécurité de l'entreprise et simplifiant considérablement l'administration. De plus, cela permet une gestion à distance efficace, essentielle pour maintenir la tablette à jour et sécurisée sur le terrain.

La politique de sécurité vérifie en premier lieu l'intégrité de l'appareil à travers le verdict "Play Integrity" afin de détecter d'éventuelles modifications non autorisées. Elle exige une version minimale d'Android (11.0) pour garantir un niveau de sécurité à jour. De plus, elle impose obligatoirement le chiffrement des données stockées localement et vérifie l'intégrité des applications exécutées via Intune. Concernant la sécurité du dispositif, un

mot de passe numérique d'au moins 4 caractères est requis avec une rotation obligatoire après cinq changements. Enfin, la règle verrouille automatiquement l'appareil après 5 minutes d'inactivité pour limiter les risques en cas de perte ou de vol.

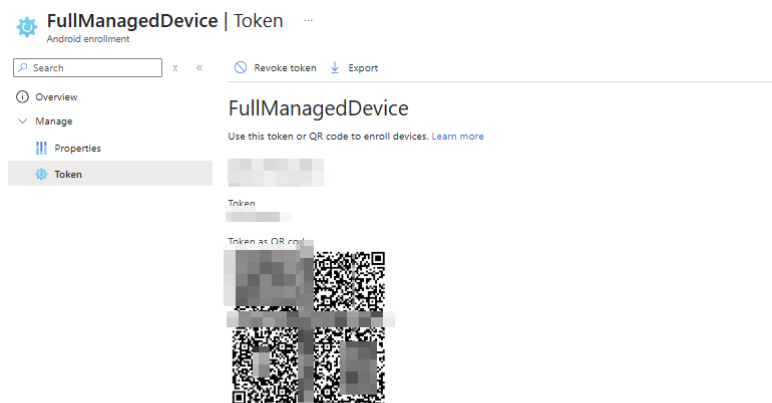
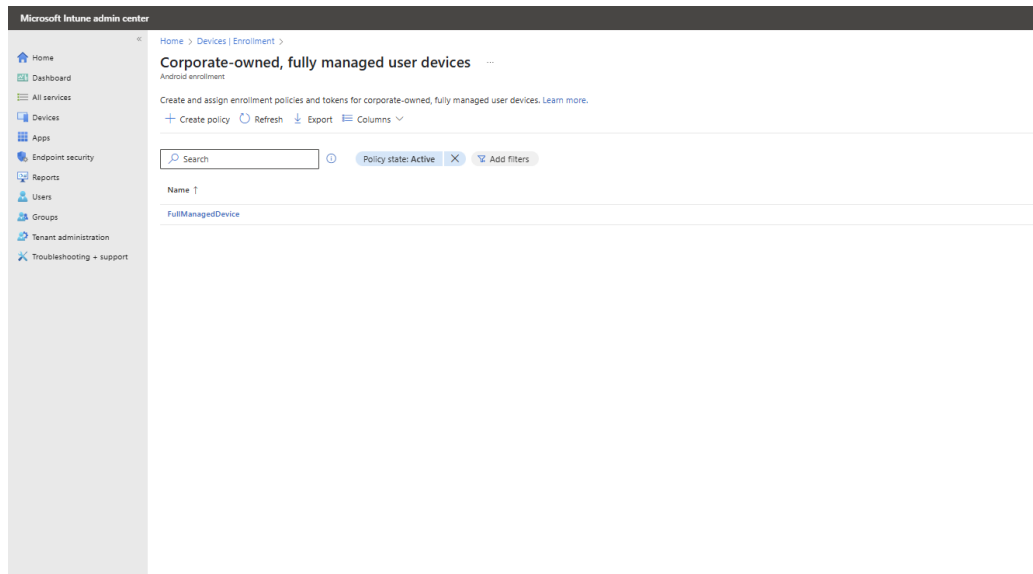
Nous exigeons que tous les appareils mobiles soient conformes (« compliant ») aux politiques de sécurité définies dans Intune, conformément aux standards établis par notre entreprise. Cette exigence est indispensable pour garantir la sécurité des données professionnelles, prévenir toute fuite ou accès non autorisé, et protéger l'intégrité des systèmes d'information. En imposant cette conformité, nous assurons également que chaque appareil dispose des mises à jour et paramètres nécessaires pour se défendre efficacement contre les cybermenaces.



J’ai créé une politique active nommée « FullManagedDevice » configurée dans Microsoft Intune pour les appareils Android entièrement gérés par l'entreprise (« corporate-owned, fully managed »). La mise en place de cette politique est nécessaire pour préparer et automatiser l’enrôlement d'un appareil Android en mode entièrement géré dès sa première activation à l’aide du Token qui va servir d'identifiant sécurisé reliant

automatiquement l'appareil à l'environnement Intune de l'entreprise lors du premier démarrage. Ainsi, il garantit que seuls les appareils autorisés puissent accéder au profil d'entreprise et appliquer automatiquement les paramètres de gestion et de sécurité définis préalablement.

Il y a aussi un QR code généré afin de le scanner lors de l'installation de la tablette qui téléchargera automatiquement les configurations prédéfinies, notamment les paramètres de sécurité et les restrictions requises par notre entreprise.



Ensuite pour inscrire l'appareil Android, nous devons réinitialiser la tablette aux paramètres d'usines.

Lors du démarrage de la tablette à l'écran « Bienvenue », il faut cliquer 6 fois sur l'écran pour lancer l'inscription Assistant Android Enterprise. Ensuite l'assistant nous demandera de renseigner la token ou le QR code généré précédemment. L'appareil installera systématiquement l'application Portail Entreprise et appliquera toutes les politiques d'entreprise avec seulement un espace professionnel.