GUIDE UTILISATEUR

# Gestion des Profils et Politiques de sécurité

Console MSP Neoditel

DOCUMENT DE RÉFÉRENCE

## Objectif du cours

Ce cours présente la gestion des profils et des politiques de sécurité dans Samsung Knox Manage. À l'issue de cette formation, vous serez capable de créer, configurer et appliquer des profils de sécurité adaptés aux différents usages métiers, et de gérer les politiques associées pour garantir la conformité et la protection des terminaux supervisés.

## Prérequis

Avant de suivre ce cours, il est recommandé de maîtriser les fondamentaux de Samsung Knox Manage (interface, navigation, gestion des terminaux). Une connaissance des concepts MDM (Mobile Device Management) et des bonnes pratiques de sécurité mobile est un plus.

## 1. Concepts clés : profils et politiques de sécurité

Dans Knox Manage, un profil de sécurité définit un ensemble de règles (mot de passe, chiffrement, restrictions applicatives, etc.) qui peuvent être appliquées à un ou plusieurs terminaux. Une politique (policy) regroupe ces règles et permet leur déploiement ciblé via les groupes d'organisations ou d'appareils.

### a) Différence entre profil et politique

Le profil est le contenant technique (paramètres et valeurs), tandis que la politique est l'objet déployable qui peut être associée à des terminaux. Une politique peut faire référence à plusieurs profils (configuration, restriction, application).

### b) Stratégies de sécurité recommandées

- Verrouillage écran avec code à 6 chiffres minimum.
- Chiffrement du stockage activé.
- Restriction de l'installation d'applications hors store.
- Désactivation des fonctions (USB debugging, factory reset, etc.).

### c) Héritage et conflits de profils

En cas de profils multiples sur un même terminal, Knox Manage applique la règle la plus restrictive par défaut. L'ordre d'évaluation suit la hiérarchie des organisations : groupe parent > groupe enfant > appareil.

## 2. Créer et configurer un profil de sécurité

La création d'un profil passe par le menu Profils > Ajouter un profil. Vous définissez ensuite le type (Android, iOS, Windows), les paramètres de mot de passe, de chiffrement, les restrictions fonctionnelles, et les applications autorisées ou interdites.

### a) Paramètres de mot de passe et verrouillage

Définissez la longueur minimale du code, le délai d'expiration, le nombre de tentatives avant verrouillage, et l'obligation de caractères complexes (chiffres, lettres, symboles).

> **Point de vigilance**
>
> Définissez une longueur minimale de 6 chiffres pour les codes PIN et activez le verrouillage automatique après 5 minutes d'inactivité.

### b) Restrictions fonctionnelles et applicatives

- Bloquer la réinitialisation d'usine (factory reset).
- Désactiver le débogage USB et les options développeur.
- Restreindre l'installation d'applications hors Play Store.
- Forcer l'utilisation du navigateur d'entreprise.

## 3. Appliquer une politique à un groupe d'appareils

Une politique est appliquée à un groupe d'appareils via l'onglet Appareils. Sélectionnez les terminaux cibles, cliquez sur Politique > Appliquer, et choisissez la politique à déployer. La propagation prend quelques minutes.

### a) Sélection des appareils cibles

Utilisez les filtres de l'onglet Appareils pour cibler par plateforme, modèle, version OS, ou statut (en ligne, hors ligne). Vous pouvez sélectionner jusqu'à 1000 appareils simultanément.

### b) Suivi du déploiement

Une fois la politique appliquée, surveillez le statut depuis l'onglet Tâches. Les états possibles sont : En attente, Réussi, Échec. En cas d'échec, consultez les logs pour identifier la cause (terminal hors ligne, profil incompatible, etc.).

**À retenir**

• Un profil contient les paramètres de sécurité, une politique les déploie.

• En cas de conflit, Knox Manage applique la règle la plus restrictive.

• Toute modification de politique majeure doit être testée sur un groupe pilote avant déploiement global.

## 4. Bonnes pratiques et maintenance

### a) Audit régulier des profils

Planifiez un audit trimestriel des profils et politiques pour vérifier leur pertinence. Supprimez les profils obsolètes et harmonisez les règles au sein de l'organisation.

### b) Gestion des exceptions

Pour les terminaux nécessitant une configuration spécifique (direction, terrain), créez des politiques dédiées plutôt que d'assouplir la politique globale.

**Point de vigilance**

Ne désactivez jamais le chiffrement du stockage ou la politique de mot de passe pour résoudre un incident utilisateur : créez plutôt une politique d'exception ciblée.