

# Mobile Device Management

L'infrastructure téléphonique mobile de l'administration centrale du ministère de la Culture est composée : (de deux infra MDM MobileIron (Prod/Pré-prod) avec des serveurs Core/Sentry).

Core-1	Administration	azenor	VM (Culture)	Prod
Sentry-1 Tunnel-OBM	Messagerie OBM /VPN applicatif /Navigation sécurisée.	budic	VM (Culture)	
Sentry-2 Tunnel-OBM			VM (Culture)	
Sentry-3 Exchange	Messagerie Exchange	erispoe	VM (Culture)	
Sentry-4 Exchange			VM (Culture)	
Core-3	Administration	nominoe	VM (Culture)	Pré-prod
Sentry-5 Tunnel-OBM	Messagerie OBM /VPN applicatif /Navigation sécurisée.	hoel	VM (Culture)	
Sentry-6 Exchange	Messagerie Exchange	eudon	VM (Culture)	

## Gestion des appareils mobiles (MDM, Mobile Device Management) :

MobileIron offre des fonctionnalités de gestion sécurisée des appareils appartenant aux utilisateurs et à l'entreprise, quel que soit leur système d'exploitation. La solution automatise la configuration des appareils et s'intègre directement aux services d'annuaire pour l'authentification et la gestion des utilisateurs. Les administrateurs peuvent mettre des appareils en quarantaine et/ou en supprimer de façon sélective les données d'entreprise. Les utilisateurs ont accès à leur messagerie professionnelle depuis leurs terminaux.

## Gestion des applications mobiles (MAM, Mobile Application Management) :

MobileIron contribue à la gestion du cycle de vie des applications en mettant un catalogue d'applications publiques et d'entreprise à la disposition des utilisateurs. Le service sécurise les applications d'entreprise sur les terminaux des utilisateurs et les sépare des applications personnelles.

## Gestion du contenu mobile (MCM, Mobile Content Management) :

MobileIron intègre une application grâce à laquelle les utilisateurs ont la possibilité de stocker le contenu d'entreprise en toute sécurité sur leurs terminaux mobiles. Les administrateurs peuvent appliquer des règles relatives à l'authentification, au partage de fichiers et autres restrictions, par exemples des fonctions de copier/coller.

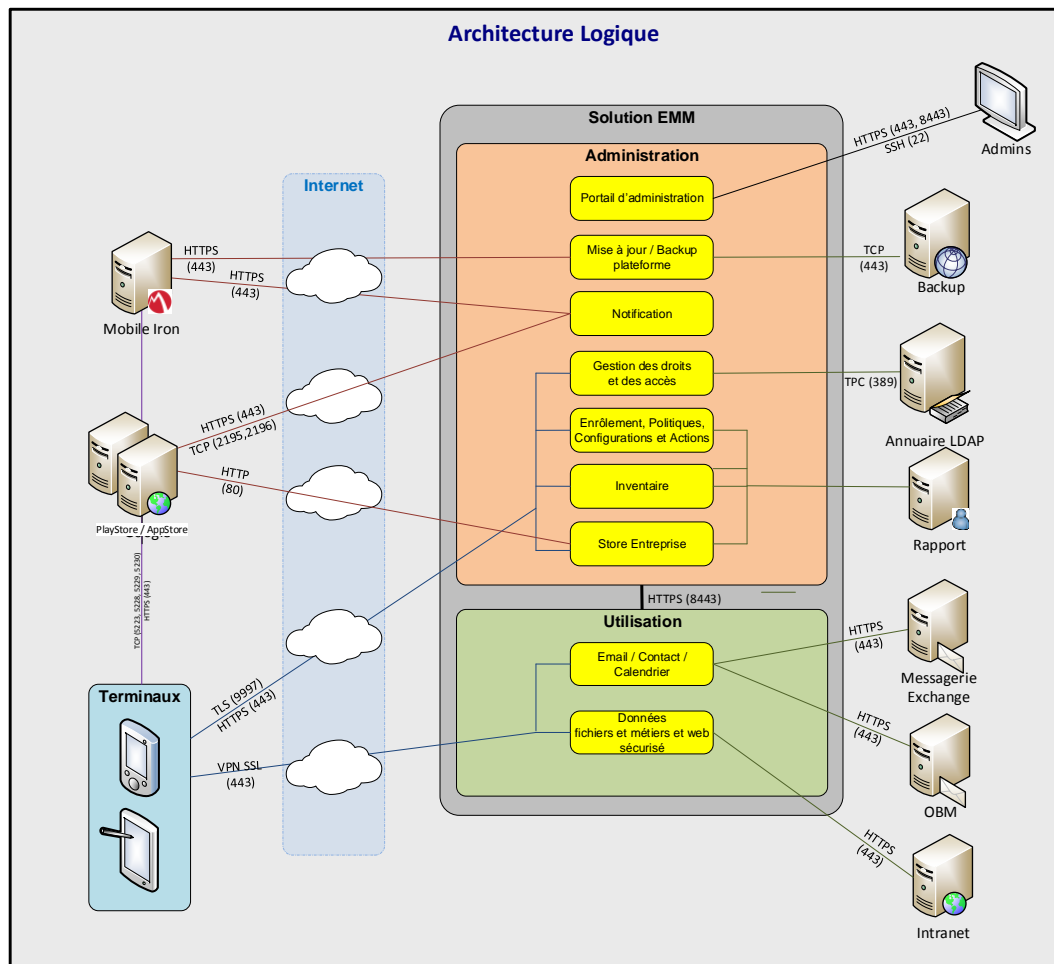
## Core :

*Le Core est un composant clé de la plateforme MobileIron. Intégré aux systèmes informatiques back-end de l'entreprise, Le Core permet aux administrateurs de définir des règles de gestion et de sécurité pour les applications, les contenus et les terminaux mobiles, quel que soit le système d'exploitation. Outre la délégation de l'administration, le Core propose d'autres fonctions disponibles sous la forme d'API compatibles avec les produits de partenaires Technology Alliance, notamment dans les domaines de la sécurité, de la gestion des risques et de la réputation des applications, de l'identité et de l'authentification, du contrôle d'accès, de la veille et de l'analyse réseau.*

## Sentry :

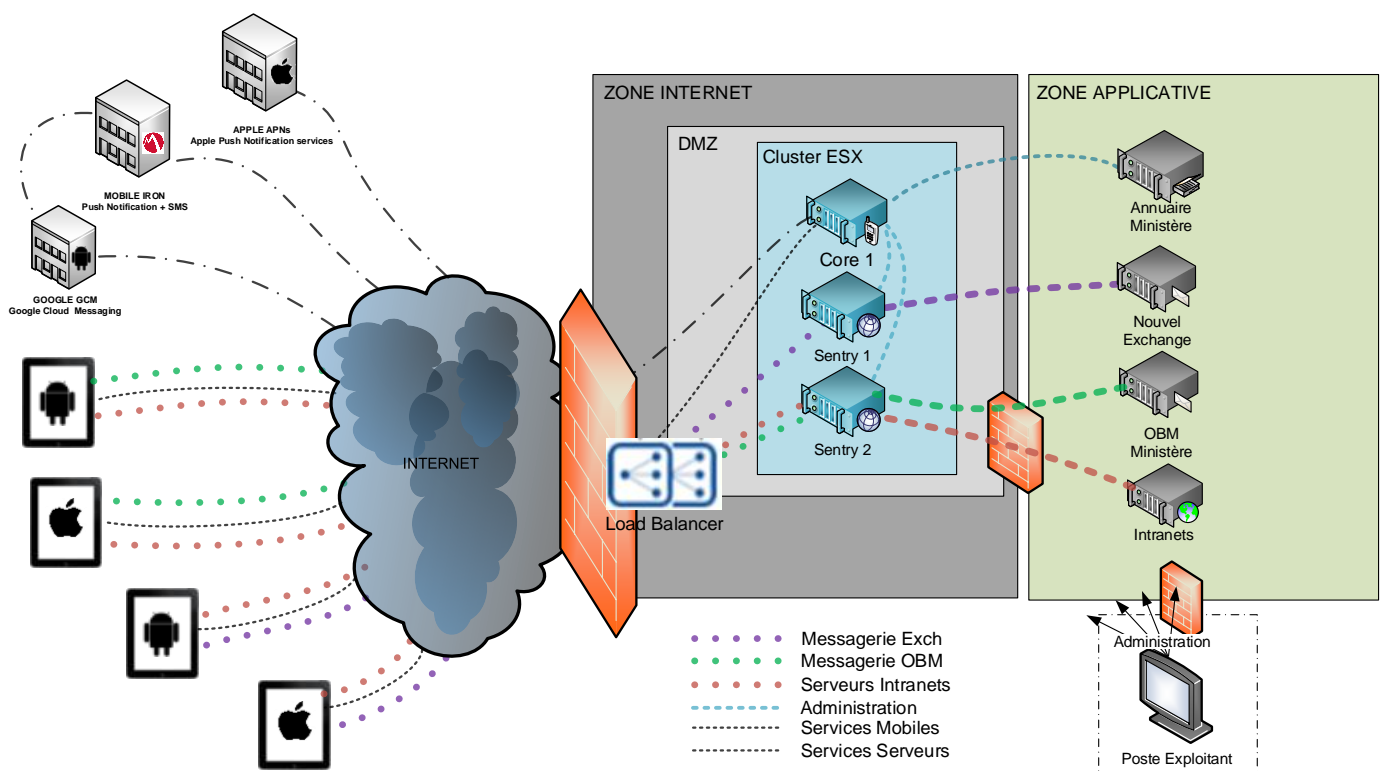
*La Sentry est un autre composant clé de la plateforme MobileIron. Cette passerelle intégrée gère, chiffre et sécurise le trafic entre les terminaux mobiles et les systèmes back-end de l'entreprise. L'entreprise bénéficie ainsi de trois avantages fondamentaux : la sécurité, l'évolutivité et une expérience utilisateur optimale.*

## Schéma d'architecture logique

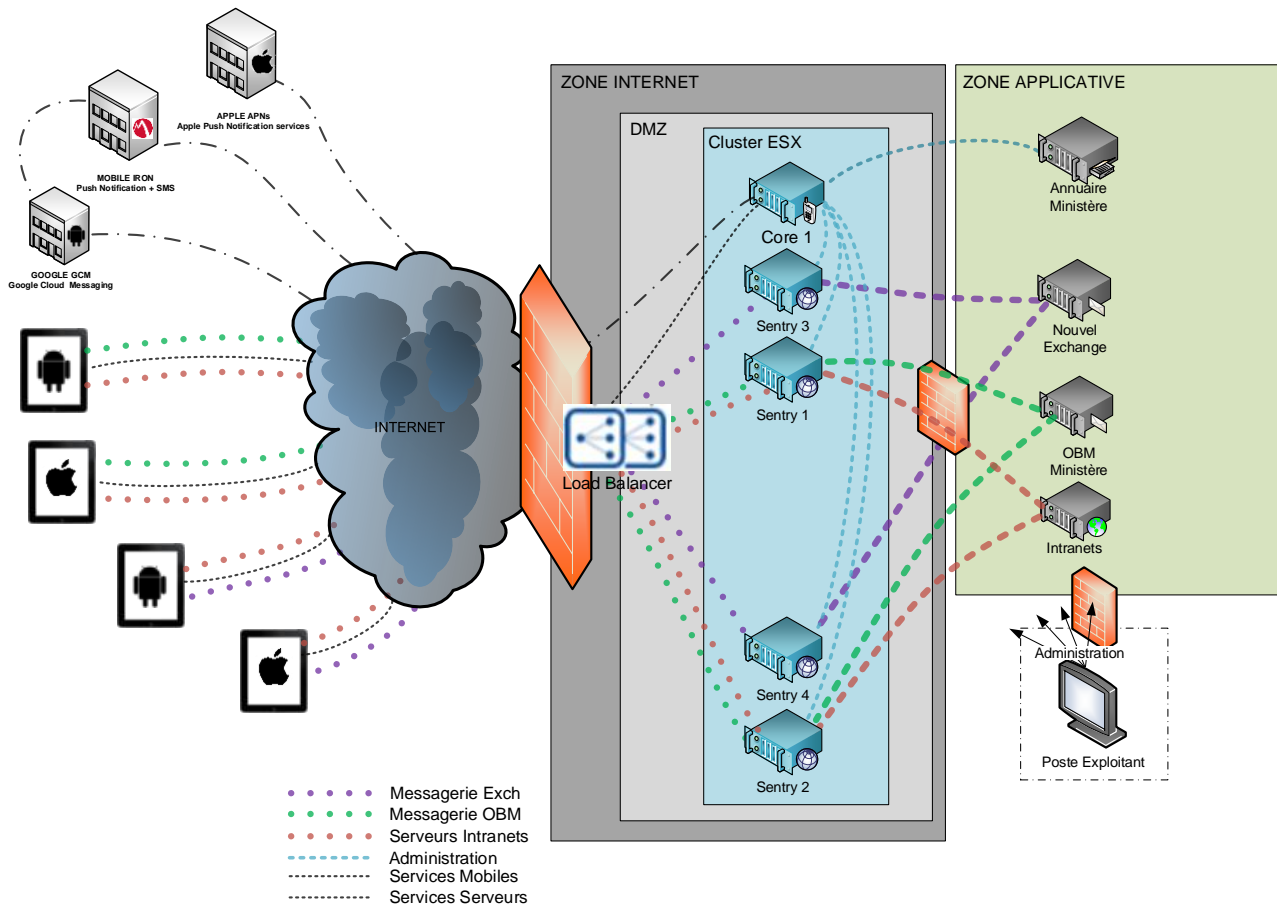


## Schéma d'architecture physique.

Pour l'environnement de Pré-prod :



Pour l'environnement de Production :



La Configuration des (Smartphones/Tablettes) du MDM de la Culture est en Google Entreprise en (COPE/BYOD/COBO), avec l'enrôlement KME de Samsung.

**COPE:** corporate-owned, personally enabled device. (avec des appareils individuels fournis par la société).

Le MC achète le terminal et laisse l'employé l'utiliser comme si c'était le sien sur l'espace Personnel, et maintient un contrôle total sur l'espace Professionnel.

**COBO :** company-issued business only. (avec des appareils professionnels distribués par la société). Le MC maintient un contrôle total sur l'appareil, (dispose uniquement d'un espace Professionnel).

**BYOD:** Bring Your Own Device. (avec des appareils Personnels).

L'employé apporte volontairement au travail son terminal personnel comme outil de travail. Le MC limitera le contrôle sur l'appareil.

**KME (Knox Mobile Enrollment) :** Ajoutez simultanément des milliers d'appareils Samsung à votre flotte mobile. Déployez en masse vos appareils qui seront configurés et enrôlés à votre MDM/EMM (Enterprise Mobility Management) dès qu'ils seront connectés au réseau.

Le mode le plus utiliser est le **COPE**.

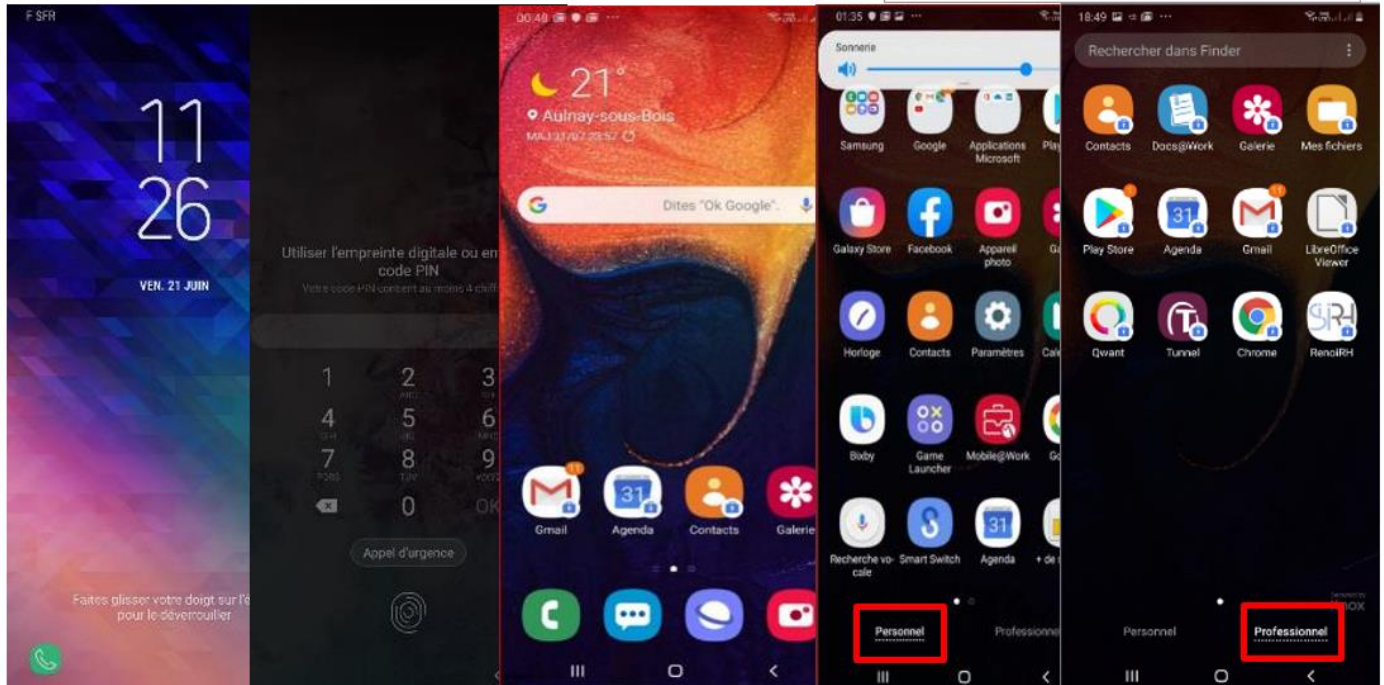
## Prise en main de votre terminal sécurisé

Après avoir allumé votre téléphone, vous devrez entrer votre code de déverrouillage :

Déverrouiller le téléphone chiffré : entrer le code de déverrouillage du téléphone

Glisser de bas en haut pour accéder aux espaces

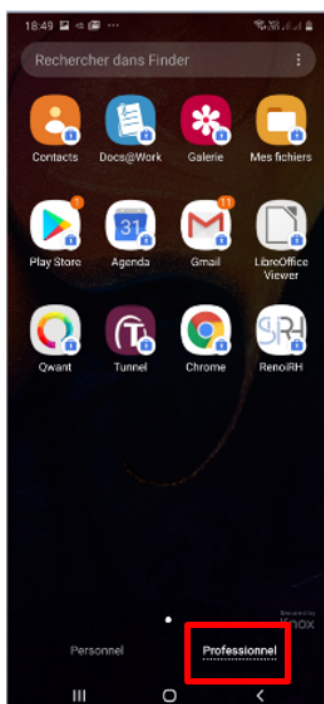
Deux espaces sont à disposition : **Personnel** ou **Professionnel** pour y accéder cliquer sur le nom d'un espace



## Prise en main de votre terminal sécurisé : découverte de l'espace Professionnel

Votre **Profil Professionnel** est réservé aux applications professionnelles du Ministère.

La liste des applications sécurisées installées par défaut côté Profil Professionnel :



-  Client de messagerie professionnelle (Mail Ministère)
-  Agenda professionnel (Agenda Outlook)
-  Contact professionnel (Contact Outlook)
-  Magasin d'applications du Ministère
-  Application pour lire, modifier et créer des documents Microsoft office
-  Application pour lire des documents Libre office
-  Application pour lire des photos reçues par mail
-  Explorateur de fichiers
-  Application pour activer la navigation sécurisée
-  Navigateurs sécurisés (identique au PC)
-  Applications Renoir RH (pas encore en service)

On identifie les applications sécurisées du **Profil Professionnel** par le Cadenas bleu 