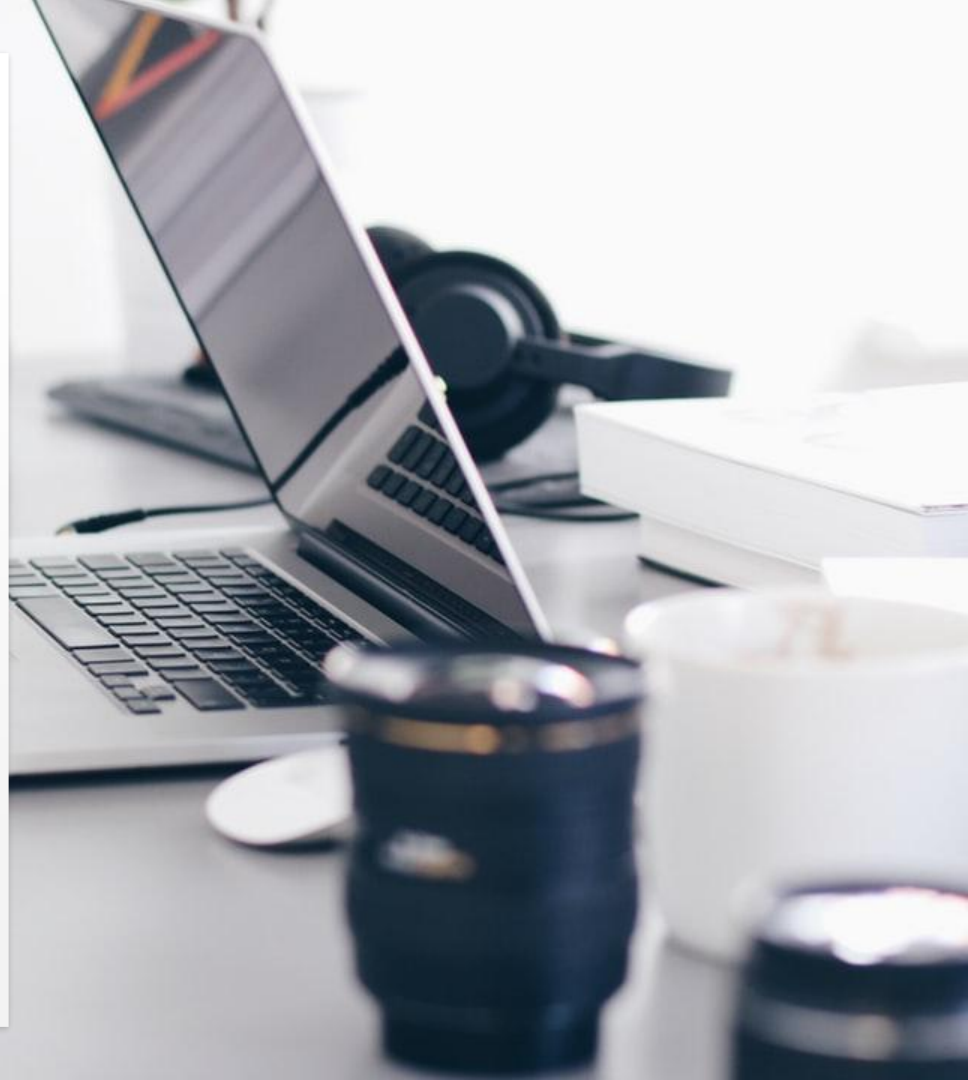


# Estudio de plataformas MDM en arquitecturas distribuidas

**Judit Antoranz García** – 1425210 –  
[judit.antoranz@e-campus.uab.cat](mailto:judit.antoranz@e-campus.uab.cat)  
**Grado en Ingeniería Informática** –  
*Mención en Ingeniería de Computadores*



# Propuesta de proyecto



Transports  
Metropolitans  
de Barcelona



Workspace ONE™

3144  
dispositivos  
actuales



8021  
dispositivos  
futuros



# Objetivos

- ❑ **O.G.1.**Búsqueda de distintas plataformas MDM.
- ❑ **O.G.2.**Analizar el parque móvil de TMB.
- ❑ **O.G.3.**Crear usuarios y agruparlos en una OG o Smart Group
  - **O.E.1.**Creación de usuarios.
  - **O.E.2.**Agrupación de usuarios.
- ❑ **O.G.4.**Dar de alta dispositivos y vincularlos a un usuario.
  - **O.E.3.** Dar de alta un dispositivo.
  - **O.E.4.**Vincular un dispositivo a un usuario.
- ❑ **O.G.5.**Análisis de las políticas de seguridad.
  - **O.E.5.**Análisis de las políticas de seguridad.
  - **O.E.6.**Analizar para qué se utiliza una política u otra.
- ❑ **O.G.6.**Análisis de los modos de gestión.
  - **O.E.7.**Análisis del modo Legacy.
  - **O.E.8.**Análisis del modo Enterprise.

# Objetivos

- ❑ **O.G.7.**Definición de un perfil y políticas de seguridad.
  - **O.E.7.**Restricciones para la definición de un perfil.
  - **O.E.8.**Definición de una política de seguridad.
- ❑ **O.G.8.**Definición de un plan de migración.
  - **O.E.7.**Definición de un plan de migración.
  - **O.E.8.**Realización de la migración.



# Metodología - KANBAN

- ☐ Gestión de trabajo mediante tareas.
- ☐ Identificación de recursos necesarios para el desarrollo.
- ☐ Fechas de inicio y finalización de las tareas.
- ☐ Maximización de la visualización del trabajo pendiente.
- ☐ Gestión del flujo de trabajo.

# Plataformas MDM - ¿Por qué surgen?

Debido al aumento del uso de dispositivos móviles como herramienta de trabajo, que favorece la flexibilidad, movilidad y eficiencia de los trabajadores.

Esto causa un aumento de la necesidad de soporte, administración y seguridad en el dispositivo sin perjudicar su uso.

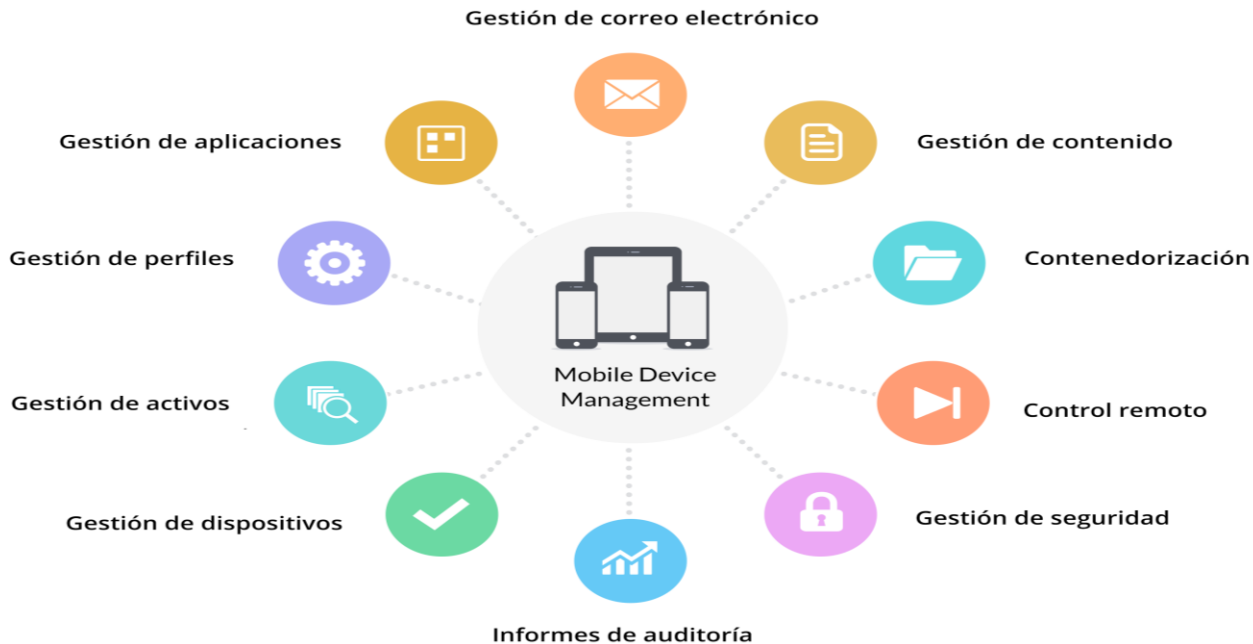
# Plataformas MDM - ¿Qué son?

Conforman un tipo de software que se dedica a:

- ☐ Gestión y administración de dispositivos móviles.
- ☐ Implementado, mayormente, con productos de terceros.
- ☐ Securización de datos empresariales.

Normalmente están implementados en empresas con un parque móvil de gran tamaño.

# Plataformas MDM - Características





# Estructura del proyecto

## 1ª parte - Analítica:

- Análisis de la arquitectura.
- Análisis de la estructura organizativa del parque móvil.
- Análisis de los modos Legacy y Enterprise.

## 2ª parte - Implementación:

- Creación de usuarios.
- Creación de Smart Groups.
- Device Enrollment.
- Creación de perfiles de seguridad.
- Creación de un plan de migración.

# ¿Qué es VMWare Workspace ONE?

- ☐ Plataforma MDM.
- ☐ Distribuye y gestiona dispositivos móviles.
- ☐ Gestión del control de acceso.
- ☐ Control de aplicaciones instaladas.
- ☐ Segregación y seguridad en los datos empresariales.
- ☐ Generación de perfiles de seguridad.
- ☐ Modos de gestión Android y Legacy.

# Modo de gestión Legacy

Modo de gestión para dispositivos que usan SO Android 5.0 o inferior.

Permite:

- Establecer políticas de seguridad.
- Integrar aplicaciones empresariales.
- Usuario final realiza tareas por si solo.
- Limitación de acceso a usuarios autorizados.
- Restricción de acceso a aplicaciones concretas.

# Modo de gestión Enterprise

Modo de gestión para dispositivos que usan SO Android 5.0 o superior. Permite lo mismo que el modo Legacy y además contiene dos modos de gestión propios.

Modo Work Profile:

- Apto para dispositivos BYOD.
- Crea dos espacios de datos (personal y trabajo).
- Workspace sólo gestiona el espacio de trabajo.

Modo Work Managed Device:

- Totalmente gestionado por Workspace ONE.
- Se necesita autorización para instalación de aplicaciones.

# Desarrollo y resultados



# Entorno de pruebas

Organization Group	Active Devices	Inactive Devices
▼ ZZZ-TFG-Antoranz	0	4
ZZZ-TFG-Antoranz-AE	0	4
ZZZ-TFG-Antoranz-Legacy	0	0

# Creación de usuarios

## Add/Edit User

General Advanced

Security Type \*

BASIC

DIRECTORY

Username \*

ZZZ-TFG-Antoranz-User1

Password \*

.....

shc

Confirm Password \*

.....

shc

Full Name \*

Antoranz-User1

Middle Name

Antora

Display Name

## List View

Filters

1

X

ADD

V

Security Type

>

General Info

Enrollment Organization Group

ZZZ-TFG-Antoranz

V

Enrollment Status

>

User Group

>

User Role

>

Status

>

ZZZ-TFG-Antoranz-User1

Antoranz-User1 Antoranz-User1

ZZZ-TFG-Antoranz-User2

Antoranz-User2 Antoranz-User2

ZZZ-TFG-Antoranz-User3

Antoranz-User3 Antoranz-User3

ZZZ-TFG-Antoranz-User4

Antoranz-User4 Antoranz-User4

# Creación de Smart Groups

## Create New Smart Group

Name

ZZZ-TFG-Antoranz-Smart Group 1

Managed By ZZZ-TFG-Antoraz

Choose Type

CRITERIA

DEVICES OR USERS

▼ Devices ⓘ

Enter device friendly name.

ADD

▼ Users ⓘ

2 Selected

☒ Antoranz-User1 Antoranz-User1 (ZZZ-TFG-Antoranz-User1)  
jantoranz@tmb.cat

☒ Antoranz-User2 Antoranz-User2 (ZZZ-TFG-Antoranz-User2)  
jantoranz@tmb.cat

Enter username, first name or last name.

ADD

## Assignment Groups

Filters

»

+ ADD SMART GROUP



Groups

Managed By



ZZZ-TFG-Antoranz-Smart Group 1

ZZZ-TFG-Antoraz



ZZZ-TFG-Antoranz-Smart Group 2

ZZZ-TFG-Antoraz



ZZZ-TFG-Antoranz-Smart Group 3

ZZZ-TFG-Antoraz



ZZZ-TFG-Antoraz (ZZZ-TFG-Antoraz)

ZZZ-TFG-Antoraz

- ❑ Creación de Smart Groups mediante “Devices or Users” o “Criteria”.



# Device Enrollment

## Add Device

User

Search Text

ZZZ-TFG-Antoranz-User1

SEARCH

Security Type \*

Basic



Username \*

ZZZ-TFG-Antoranz-User1

Password \*

.....

CHANGE

First Name \*

Antoranz-User1

Middle Name

Expected Friendly Name

ZZZ-TFG-Antoranz-User1's Device



Organization Group \*

ZZZ-TFG-Antoraz



Ownership

Corporate - Dedicated



Platform \*

Android



Show advanced device  
information options



Model

Android



OS

Android 9.0.0



UDID

Serial Number

R58K517GW5W

IMEI

354070099223252

- ❑ Device Enrollment en dos fases, una en la plataforma y otra en el dispositivo.

# Device Enrollment

Benvolgut/da Antoranz-User1,

El seu dispositiu mòbil ha estat aprovat per a l'accés corporatiu mòbil. Al següent [enllaç](#) trobarà totes les dades necessàries per a la inscripció.

Si us plau, no introduïu cap informació personal ni corporativa fins que l'aplicatiu AirWatchMDM Agent estigui instal·lat al teu dispositiu, el trobaràs representat amb una icona com la de l'imatge a continuació:



**Descarregueu l'aplicació només des de l'app store oficial del seu dispositiu, fent recerca de Airwatch MDM Agent:**

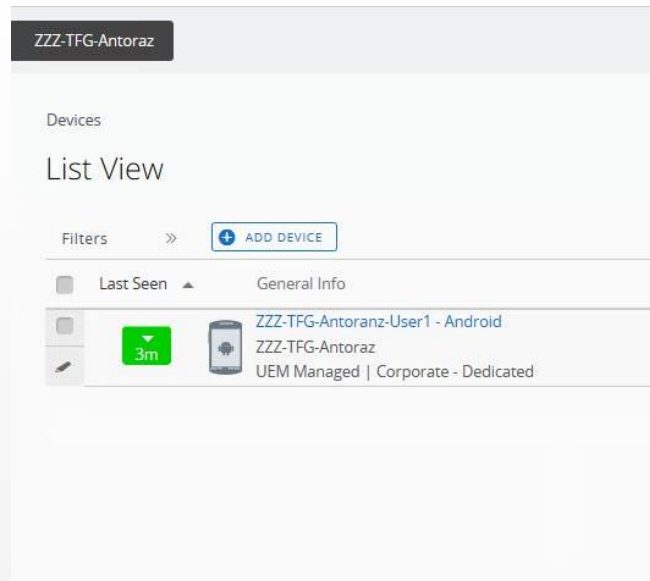
- [iTunes](#)
- [Play Store](#)

Les vostres credencials es troben a continuació:

**Correo electrónico:** jantoranz@tmb.cat  
**Token:** YU9AX8 caduca el 10/04/2021 19:51:00

**\*URL del servidor:** ds556.awmdm.com **YID de grupo:** TMB-TFGSi  
**obligatorio**

També pot escanejar el codi QR per començar l'inscripció:



# Creación de perfiles de seguridad

Find Payload

**General**

Passcode

Restrictions

Wi-Fi

VPN

Email Settings

Exchange ActiveSync

**Application Control**

Bookmarks

Credentials

Workspace ONE Launcher

Global Proxy

Date/Time

Sound

Firewall

Display

Advanced

Custom Settings

## General

Name \* zzz-TFG-Antoranz-Corporative Security-legacy

Version 1

Description

Profile Scope Production

Assignment Type Auto

Allow Removal With Authorization

Password \* \*\*\*\*\*

Managed By ZZZ-TFG-Antoranz

Smart Groups Start typing to add a group

Exclusions NO YES

VIEW DEVICE ASSIGNMENT

Passcode Knox

Chrome Browser Settings

**Restrictions Knox**

Exchange ActiveSync

Public App Auto Update

Credentials

Custom Messages

Application Control

Proxy Settings

System Updates

Wi-Fi

VPN

Permissions

Single App Mode

Date/Time Knox

Workspace ONE Launcher

Firewall Knox

APN Knox

Enterprise Factory Reset Protection

Custom Settings

Name \* zzz-TFG-Antoranz-CN - AE - Corporate Security

Version 1

Description Profile for LLAA devices

OEM Settings ENABLE DISABLE

Select OEM Samsung

Profile Scope Production

Assignment Type Auto

Allow Removal With Authorization

Password \* \*\*\*\*\*

Managed By ZZZ-TFG-Antoranz

Smart Groups Start typing to add a group

Exclusions NO YES


VIEW DEVICE ASSIGNMENT


- ❑ Muchas opciones a considerar en la configuración de los perfiles.

# Creación de un plan de migración

Select Migration Type

Choose the type of legacy Android migration that you would like to create.

  
Work Profile  
Migrate personally owned devices from device administrator to work profile.

  
Work Managed  
Migrate corporate owned devices from device administrator to work managed. Requires Zebra devices running Android 7 and higher.

CANCEL

NEXT

## Summary

A notification will be sent to eligible devices in the selected Smart Groups informing the migration and prompting them to take action to proceed. You can monitor Legacy Android Migration page.

Search

Device Name	Username	Organization Group	Eligibility Status
ZZZ-TFG-Antoranz-User2 - Android	ZZZ-TFG-Antoranz-User2	ZZZ-TFG-Antoranz	Eligible
ZZZ-TFG-Antoranz-User1 - Android	ZZZ-TFG-Antoranz-User1	ZZZ-TFG-Antoranz	Unknown

- ❑ El modo Work Managed sólo está disponible para dispositivos Zebra.

# Conclusiones



- ❑ Gran especificidad en las OG.
- ❑ Perfiles de seguridad específicos para dispositivos o grupos concretos.
- ❑ Migración por Smart Group.



- ❑ Especificidad en los perfiles de seguridad limita su aplicación.
- ❑ Migración a modo Work Managed no disponible para dispositivos que no sean Zebra.

# Estudio de plataformas MDM en arquitecturas distribuidas

**Judit Antoranz García** – 1425210 –  
[judit.antoranz@e-campus.uab.cat](mailto:judit.antoranz@e-campus.uab.cat)  
**Grado en Ingeniería Informática** –  
*Mención en Ingeniería de Computadores*

Muchas  
gracias por su  
atención.

**UAB**  
Universitat Autònoma  
de Barcelona

**UAB**  
**e** escola  
d'enginyeria  
**Informàtica**