Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels
UNIVERSITAT POLITÈCNICA DE CATALUNYA

MASTER THESIS

TITLE: Study, analysis and implementation of an Enterprise Mobility Management System

MASTER DEGREE: Master in Science in Telecommunication Engineering & Management

AUTHOR: David Arance García

DIRECTOR: Roc Meseguer Pallares

SUPERVISOR: Jordi Casanovas Adell

DATE: 26 November 2013

Títol: Study, analysis and implementation of an Enterprise Mobility Management System

Autor: David Arance García

Director: Roc Meseguer Pallares

Data: 26 November 2013

Resum

La gestió de la mobilitat empresarial (EMM), s'ha esdevingut darrerament un tema de molta importància per a les organitzacions empresarials. Aquestes han vist com la incorporació de tablets i smartphones als llocs de treball corporatius, per una part ha suposat un valor diferencial a la forma de fer alguns negocis, mentre que per una altra banda també ha posat al descobert greus carències per a la seva securització i control d'accés.

Aquest document neix com a resposta a la necessitat imperativa de gestionar i controlar de forma remota els dispositius, les aplicacions i els continguts als que tenen accés. Els objectius plantejats inicialment han estat:

Estudiar les principals necessitats i desafiaments que representa la mobilitat empresarial, així com avaluar per què es necessita la seva gestió.

Analitzar les necessitats de mobilitat de negoci en un entorn real i definir una estratègia de gestió de la mobilitat empresarial (EMM) que permeti aprofitar les avantatges sense patir els inconvenients.

Comparar, seleccionar i implementar un sistema de gestió de la mobilitat empresarial (EMMS) i avaluar si compleix les necessitats requerides.

Per a la seva elaboració, s'ha utilitzat una metodologia basada en fases. Primerament, s'ha elaborat un intens treball de camp per analitzar els requeriments de mobilitat en un cas real. A continuació, s'ha dissenyat una solució, basada en un sistema de gestió de la mobilitat empresarial, que satisfés totes les necessitats detectades prèviament. Finalment, a partir dels estudis previs, s'ha elaborat un laboratori on s'han posat en practica totes les tècniques de gestió i control estudiades.

Una vegada finalitzat el projecte, s'ha arribat a les següents conclusions:

Les empreses tenen molt a guanyar si aprenen com desenvolupar les seves activitats en un ecosistema de mobilitat correctament gestionat. En lloc de manifestar una actitud de resistència o prohibició a la mobilitat, és millor adoptar un pensament constructiu i de col·laboració.

Abans de prendre cap mesura cal analitzar l'empresa i els seu negoci, com els usuaris consumeixen i creen continguts, com col·laboren i es comunicar-se per tal de respondre a les seves necessitats de mobilitat.

Gestionar una plataforma de dispositius heterogenis és un gran desafiament gestió, manteniment i suport. Per tant, és essencial identificar el sistema de

gestió de la mobilitat empresarial (EMMS) que millor s'adapti a les necessitats requerides.

La solució final ha de poder mantenir sota control el dispositiu i el seu contingut durant tot el cicle de vida, des del lliurament fins a la retirada. Les capacitats que ha d'incloure son l'administració de dispositius mòbils, la gestió d'aplicacions i la gestió del contingut.

Aquests sistemes per si mateixos suposen millores en la gestió i la seguretat, però no són rellevants a nivell de productivitat i eficiència fins a la seva integració amb els serveis corporatius. Aquest és sens dubte el "leitmotiv" d'aquest tipus de solucions. Però aquesta part també és la més complicada, perquè quan es van incorpora molts dels sistemes actualment presents a les empreses, no es va tenir en compte el seu ús en condicions diferents a les del PC tradicional.

Title: Study, analysis and implementation of an Enterprise Mobility Management System

Author: David Arance García

Director: Roc Meseguer Pallares

Date: 26 November 2013

Overview

The enterprise mobility management (EMM) has recently become a hot topic for business organizations. Enterprises have seen how the introduction of tablets and smartphones to corporate jobs, has supposed in one hand to some a revolution to the way some business are done, while on the other hand has also uncovered serious deficiencies for securing and access control.

This document was created as a response to the imperative need to manage and remotely control devices, applications and content its have access. The initial objectives have been:

Study the main characteristics about enterprise mobility and why is needed to manage it.

Analyse business mobility requirements and define an Enterprise Mobility Management strategy.

Compare, select and implement an Enterprise Mobility Management System and evaluate if it satisfies the needs proposed previously.

For its elaboration, has been used a methodology based on phases. First, has developed an intense fieldwork to analyse the requirements of mobility in a real case study. Next, have designed a solution based on an Enterprise Mobility Management System (EMMS) that fulfil all the needs identified previously. Finally, based on previous studies, has been developed a laboratory where put in practice all the management and control techniques studied.

At the project ends, the following conclusions have been reached:

Companies have much benefits to gain from learn how to develop their activities in a mobility ecosystem. Instead of manifesting an attitude of resistance to this phenomenon, it is better to adopt a constructive and collaborative thinking.

Therefore to define the EMM program, it is necessary to analyse the company and its business, having business units forwarding to IT how they consume, create, collaborate and communicate with their activities in order to respond to their mobility needs.

Manage a heterogeneous device platform is a big management, maintenance and support challenge. It is therefore essential to identify that Enterprise Mobility Management System which best adapt to the needs required, if necessary making a deep comparison between the different options on the

market.

EMM solutions must be able to keep under control the device and its contents during the whole life cycle, from delivery to withdrawal. To do EMMS capabilities must include Mobile Device Management, Mobile Application Management and Mobile Content Management.

These systems by themselves suppose improvements to the management and security, but are not relevant at the level of productivity and efficiency until its integration with corporate services. This is definitely the “leitmotiv” of this type of solutions. But this part also is the most difficult because when many systems currently on the companies was implanted, not taken into account its use in other conditions different from the traditional PC.

SUMMARY

FIGURES INDEX

TABLES INDEX

CHAPTER 1. INTRODUCTION

Smartphones and tablets have become working devices and require a new approach. We are in the "post-PC era" and unlike the "age-PC" is boosted by the users and employees, and affects most companies.

The companies have no control of corporate data that "circulate" in the devices, or services to which they have access. The key is then to have the strategy to the proper management of this issue. According to this situation, this Master Thesis is intended to:

- Study the main characteristics about enterprise mobility and why is needed to manage it.
- Analyse business mobility requirements and define an Enterprise Mobility Management strategy.
- Compare, select and implement an Enterprise Mobility Management System and evaluate if it satisfies the needs proposed previously.

An Enterprise Mobility Management program is composed by phases, so this division is reflected also in the document structure.

CHAPTER 2 contains an overview about the enterprise mobility wave, the trends that have caused its incredible rise, as well as the needs and challenges which it represents for the companies. Also Enterprise Mobility Management System fundamentals are represented at this chapter.

CHAPTER 3 provides a high-level mobility strategy definition to use when implementing an Enterprise Mobility Management program. It is divided in two parts: Phase I, Discovery and Planning, where goals and stakeholders will be identified; and Phase II, Design, where architecture, infrastructure and processes and will be defined. It is important to highlight that this chapter not only explains theoretically the how to's, furthermore each step has been put in practice in a real case study.

CHAPTER 4 puts previous chapters in practice in a laboratory environment. It is divided in two parts: Phase III, Deployment, where all the installations and configurations are done; and Phase IV, Rollout, where some rollout and support guidelines are explained.

CHAPTER 5 presents the main conclusions established during the Master Thesis elaboration and assesses the achievement of the initial objectives.

Finally, CHAPTER 6 exposes references and other bibliography, and CHAPTER 7 contains a glossary for a better reader's understanding.

CHAPTER 2. STATE OF THE ART

This starting chapter takes an overview about the enterprise mobility wave, the trends that have caused its incredible rise during last years, as well as the needs and challenges which it represents for the companies. Not only theoretical concepts are studied, other important points like the market behaviour and new enterprise mobility stakeholders will be covered.

Also in the following sections, will be defined the Enterprise Mobility Management (EMM) concept and the different areas which it covers (Device, applications and content). Moreover, we will establish the maturity level of these solutions, taking into account their short-term evolution.

In order to identify the major device manufacturers, the mobile operative system distribution and the "leaders" in EMM solutions, the reports of global IT analysts will be consulted. Once selected the bests rated in each case, in next chapters a deeper feature comparison between them should be done.

2.1. Enterprise mobility

It is a fact that in recent years technological advances have revolutionized and transformed our homes. Large PC stations and screens, noisy modems and heavy notebooks have been substituted by a new generation of devices more powerful, manageable, fast and light.

The companies haven't been excluded of this trend. Enterprise mobility is a reality that is transforming the way business is done. The workforce knows the possibilities offered by technology and demand new ways to do its work wherever they are (Sales Force, Building Inspection, Field Technician, etc.). Mobility provides relevant information to point of activity/decision at the right time, increasing productivity, efficiency and business competitiveness. [1]

Figure 2.1. Old work model vs. New work model [2]

- High number of very mobile contract employees
- Need access to only a few applications to work
- Business benefits such as scale, agility, cost and customer service may outweigh other risks

These Trends are here to stay, and the best way to don't fail is to manage them.

2.2. Trends: Consumerization, Bring Your Own Device and Corporate Owned Personally Enabled

The Consumerization borns from a younger workforce generation who has grew up with new technologies, like mobile, internet and so on, which doesn't think about the concept of division between personal or corporate technology.

This trend is moved to the company due to this employees expect to be able use its own good technology at work too. The household penetration of tablets is up 17% year over year and for smartphones is a 12%. [3]

The direct consequence has been a change in the way technology enters the marketplace. Instead of new technology flowing down from business to the consumer, as it did with the desktop computer, the flow has reversed and the consumer market often gets new technology before it enters the enterprise. [4]

This mix of personal and business technology is having a significant impact on IT departments, which traditionally issue and control the technology that employees use. Also is important to remark, that this isn't a single peak in time. If we see the data exposed in [Table 2.1], we can observe that the trend is the number of smartphones and tablets grow more than 70% in the next four years.

Table 2.1. Smart Connected Device Market by Product Category, Unit Shipments and Market Share, 2013 and 2017 (shipments in millions) [5]

Product Category	2013 Unit Shipments	2013 Market Share	2017 Unit Shipments	2017 Market Share	2013-2017 Growth
Desktop PC	134.4	8.6%	123.11	5%	-8.4%
Portable PC	180.9	11.6%	196.6	8%	8.7%
Tablet	227.3	14.6%	406.8	16.5%	78.9%
Smartphone	1,013.2	65.1%	1,733.9	70.5%	71.1%
Total	1,556	100%	2,460.5	100%	58.1%

Understand this is critical for get an idea about the importance of try to manage this technology wave which is arriving every day more to the enterprises. Now IT departments should be focused in how to protect corporate content and networks and how to manage technology that they don't provision.

2.2.1. Bring Your Own Device (BYOD)

The term Bring Your Own Device (BYOD) has two meanings.

- In general, it refers to the trend of employees using their personal smartphones and tablets for work tasks. This trend is happening everywhere, with or without IT approval.
- But BYOD can also refer to a business model that allows IT to manage, secure and enable productivity on personally owned devices. [6]

2.2.2. Corporate Owned Personally Enabled (COPE)

COPE (corporate-owned personally-enabled) is a business model in which an organization provides its employees with mobile computing devices and allows the employees to use them as if they were personally-owned notebook computers, tablets or smartphones. [7]

2.2.3. BYOD vs. COPE

The following [Table 2.2] shows a comparison between a BYOD and COPE businesses model from the company's perspective.

Table 2.2. BYOD vs. COPE

	BYOD	COPE
Device Ownership	User	Enterprise
Hardware Cost	Rests with the user	Bulk buying
Data Plan Cost	Agreed with users	Established by Corp
Devices Landscape	Very heterogeneous	Homogeneous
Productivity & Integration with Company Services	Not ensured	Ensured
Helpdesk Support	Difficult, worse	Controlled, Easy
Apps Control	Under user criteria	Under Corp policies
Usability/User Experience	Good	Limited
Device/Content management	Limited to user rights	Space Fully Managed
Remediation Actions	Not all permitted (wipe)	All permitted

In the end, it comes down to the same old battle: management and security concerns versus flexibility and productivity.

2.3. IT role and new stakeholders

The organization of many companies consists in functional silos (HR, legal, business units or IT department) to improve operational efficiency. This structure makes difficult to solve mobility problems because these solutions span many operational domains.

Define a mobility strategy not only implies IT decisions (like information security), also require input from all the teams (HR, legal, business units, sales, etc.) which can be affected by mobility concerns. This will help to consider all issues and dependencies and also make easy the resolution of trade-offs in conflict.

The process of creating mobile solutions often requires that enterprises make decisions between various conflicting tradeoffs ([Figure 2.23]). The effect of "sliding" the user experience tab from "worse" to "better," can move the security risk tab from "less" to "more" and the network tab from "more" to "less". [8]

Figure 2.2. Mobile Architecture

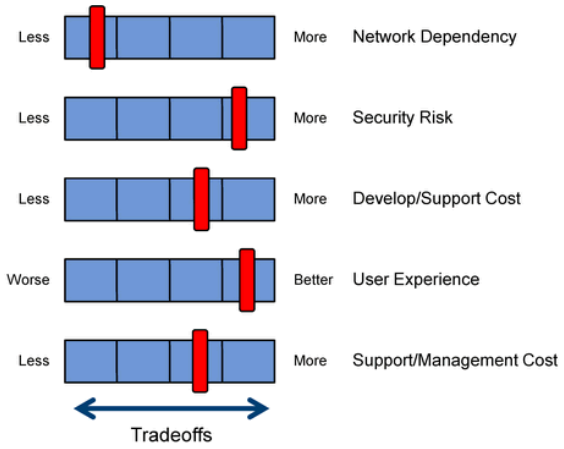


Figure 2.3. Mobility trade-offs

The mobile team should consider the needs of all stakeholders by aligning business, user and IT perspectives. In particular:

- Set mobile requirements such as data mobility, application architecture, identity and security, wireless communication, management and governance.
- Facilitates decision making through a process of methodically making trade-offs among conflicting requirements.
- Adapts to changing requirements by continuous experimentation and learning. [1]

2.4. Challenges and needs

Mobile innovations have carried by themselves a large number of innovations that includes mobile applications, social media, cloud computing, interconnected machines, mobile collaboration and wireless technologies. Technology is accelerating faster than the enterprise adaptation rate. IT organizations that fail to adapt to this new reality will lose effectiveness in front of their competitors.

In contrast with the past, where IT had the tools, time and charter to establish the necessary management and monitoring infrastructure to support those technologies, now IT is burdened by an overwhelming array of regulatory, compliance, security, privacy, expense, organizational and legacy technology constraints that dramatically shapes IT's response to these changes. [8]

The following sections examine mobility challenges from several perspectives: Infrastructure, Users, applications and data, Security and Professional effectiveness.

2.4.1. Infrastructure

The infrastructure provides the foundation upon which enterprises build their mobile solutions. It includes from WLAN technology and mobile cellular network

provider to Virtual Private Networks (VPN), corporate directory services and virtualization technology. Moreover, mobile infrastructure also includes the Enterprise Mobility Management tools which should be added in order to enable support for mobile devices, enforce compliance and mitigate problems efficiently.

- Users want a service that fulfils their everyday work needs, with high performance and seamless mobility.
- Satisfying this expectation is difficult for IT because the number of mobile devices, and mobile communications traffic, is growing exponentially.
- In addition, most of the actual infrastructure systems were not designed for this type of performance. They weren't design for a mobility scenario.
- If a BYOD program is roll out, the enterprise may not own the endpoint, but should ensure the compatibility of it with corporate systems.

When problems arise, IT will have to ensure end-to-end service. So, enterprises need a mobile-ready infrastructure, and for this it's a must invest time and money in order to improve the capacity, reliability and manageability of the actual infrastructure.

2.4.2. Users, Applications and Data

The mobility workforce is driving enterprises to build mobile applications that enable users to access relevant data at anytime, anywhere and on any device.

Also mobile data requirements are emerging as a key factor in the design of mobile applications and user experience. Enterprises must consider requirements such as data input/output, accuracy, synchronization, mobile device storage, back-end storage, processing complexity, risk sensitivity and privacy. These decisions can affect user experience, mobile application design, security, and privacy. [8]

The main challenges in order to make a successful mobile application and data management are:

- Preserve company's sensible data loss, defining products and services which are feasible to use, regardless of security concerns.
- Provide mechanisms for employees and customers to easily access and read documents on varying screen sizes.
- Regulate the of use social media to share, communicate and collaborate.
- Deal with short device life cycles, lack of mobile-friendly legacy applications, privacy concerns, security risks, development costs, application architectures and inadequate mobile application development expertise.

The combination of these complicating factors, coupled with increasingly demanding user requirements, increases the complexity of mobile application environment.

2.4.3. Security and identity

With the raise of enterprise mobility, security risks have no change: Malicious applications, device theft/lost and sensitive data loss, etc. But mobility adds new challenges related with security and user identity:

- Lack Management unsafe devices owned by employees.
- Very heterogeneous operative system environment, there is no industry standard for mobile devices.
- Capabilities security controls such as encryption and application controls vary from device to device.
- Very short device life cycle.
- Traditional endpoint management and security tools don't support mobile devices.
- No control of corporate data that "circulate" in Devices. Although sensitive data requires protection, the data must be available to authorized users.
- How users provide sufficient credentials to satisfy requirements for access to resources when operating smartphones and tablets. Hence, entity at the other end of the transaction has to ensure that is a legitimate user.

Without first assuring all the previous points about the device and the legitimate user, the enterprise cannot take comfort in its other logical access controls to business systems. [8]

2.5. Enterprise Mobility Management (EMM)

Enterprise mobility management (EMM) is the set of people, processes and technology focused on managing the increasing array of mobile devices and related services to enable the use of mobile computing in a business context. EMM helps mobile end users work more productively by providing them new tools to do their jobs on smartphones and tablets. [9] [10]

As a response to the needs and challenge studied in section [2.4], have been developed sophisticated systems designed to reduce the IT labor needed to support broad mobile device use in the enterprise. These systems are generally referred to as Enterprise Mobility Management Systems (EMMS).

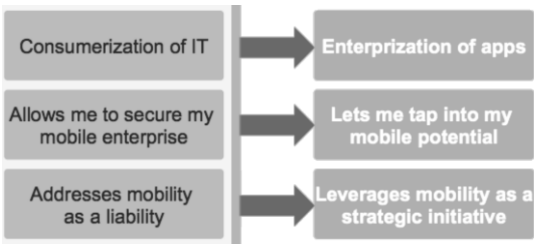


Figure 2.4. From mobility needs to "Mobile First" [11]

Figure 2.5. Mobile Endpoint Uncertainty

Due to the social nature and constant technological evolution of consumerization movement, EMMS are endpoint-independent mobile solutions. Mobile endpoint independence will enable enterprises to support and manage application service levels, regardless of which devices their users want to leverage. [8]

EMMS have to provide an entire lifecycle management, from the provision and initial configuration of the device to the withdrawal; ensuring the policy compliance, and providing relevant information for helpdesk team when the problems arise.

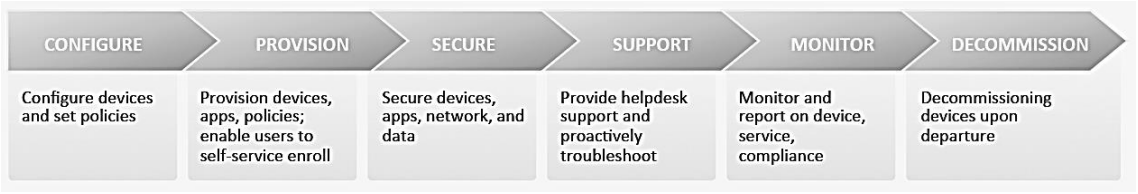


Figure 2.6. Lifecycle management [11]

In order to reach these full management requirements, EMMS are represented by advanced mobile device management (MDM) tools and services with some combination of mobile application management (MAM) and mobile content management (MCM). [12]

2.5.1. Mobile Device Management (MDM)

Mobile device management (MDM) is the administrative area dealing with enrolling, deploying, securing, monitoring, integrating and managing mobile devices, such as smartphones and tablets in the workplace. The intent of MDM is to optimize the functionality and security of mobile devices within the enterprise, while simultaneously protecting the corporate network. MDM tools should include support for either a corporate-owned or personally owned device. [13]

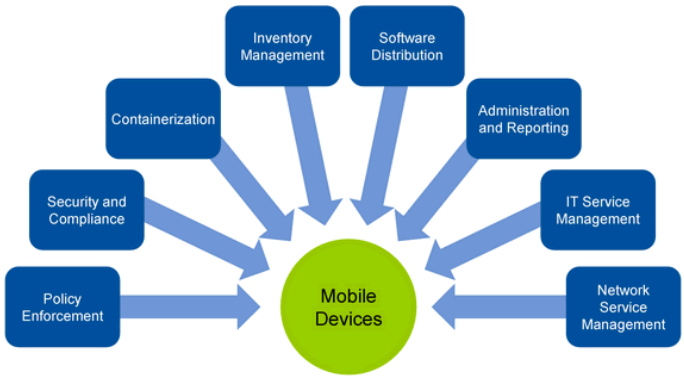


Figure 2.7. MDM capabilities [14]

Although the product capabilities of MDM may differ according to the vendor and OS (Deeper analysis will be done in section [3.2]), each product should have the following main critical components [14]:

- Software management: Distribute, manage and support mobile applications, data and multiple OSs.
- Configuration management: Configure, distribute, and manage Device policies (local settings, email, lock time, Bluetooth, backup, certificates, etc.)
- Network service management: Information of the device, location, usage, cellular and wireless LAN (WLAN) network information, GPS technology.
- Hardware management: Asset management, this includes device provisioning and support.
- Security management: Enforcement and support of device and data security, authentication, and encryption. Application containerization, VPN and encryption software are also part of this capability.

2.5.2. Mobile Application Management (MAM)

Mobile Application Management (MAM) is the delivery and administration of enterprise software to end users' corporate and personal mobile devices. [15] Mobile application managers focus on software delivery, licensing, configuration, maintenance, usage tracking and policy enforcement. The main capabilities of MAM are:

- Compare mobile device type, ownership, user and group to IT defined application policies
- Determining which mobile applications should be provisioned when a new device is activated according OS and model.
- Wiping corporate mobile apps and data from an end user's device and prevent future access.
- Provide an Enterprise Application Storefront for user self-service.
- Enable a secure tunnel to the corporate infrastructure on demand automatically.
- Manage which applications can open company sensible data.
- Manage Volume Purchase Program (VPP) licenses.

2.5.3. Mobile Content Management (MCM)

Mobile Content management (MCM) is a device-agnostic security strategy that involves keeping sensitive data in an isolated container, encrypted and allowing only authenticated users to access or transmit it. [16]

The MDM centrally manages the container so that configurations can be set by the enterprise. Information in managed container can be removed without

affecting other information or applications on the mobile endpoint device. There are three main areas of functionality:

- Securely mobilize files: Can be accessed on the devices and securely stored for offline use.
- Secure email attachments: Are encrypted and can only be viewed with the secure viewer.
- Secure browser: allows access to HTML content and applications that sits behind the firewall, without requiring a VPN client.

2.6. Market Analysis

The objective of this section is to summarize the main conclusions of Enterprise Mobility market study [ANNEX 1.].

2.6.1. Maturity level and expectations about EMMS

In order to evaluate the maturity level and market expectations around EMMS, Gartner Hype Cycle [25] and Market Clock [26] for mobility will be consulted. According to data exposed in [Annex 1.1], we can conclude:

- Tablets: Is a Transformational technology. Enhance customer interactions and workforce productivity through media tablets and apps. Requires support for consumer and personal media tablets.
- Secure corporate email: Is a requirement. Needs products or services that allow you to protect corporate email on personal devices.
- Enterprise Application Store: Is a requirement in a MDM/EMM vendor selections and investments. Enhance user experience and productivity.
- Mobile Containers: Is a requirement in a MDM/EMM vendor selections and investments. Secure and control corporate data and apps.
- Enterprise Mobility Management: Is a point of innovation that starts to create some expectations. During next year EMM requirements should be considered in MDM offerings.
- Mobile Device Management: “If you don’t have it, you’re late”. Replacement in 2-5 years by EMM solutions.

As a conclusion, we can say that according market expectations the Enterprise Mobility Management Systems can fulfil an important missing role during the next 2-5 years. We can assume that EMMS will be perceived as:

- An innovation point which substitute actual MDM-only solutions.
- A mobile-business enabler tool which provides support for transformational elements like tablets.
- A solution for secure corporate information access, like email, and prevent data loss.

2.6.2. About Operating Systems and Manufacturers

Google's Android operating system is dominating mobile operating systems shipments according to both Gartner and IDC and will continue to lead the market through 2017 above iOS and a growing Windows Phone. [17] [18]

The main issue of Android is the fragmentation of operative system versions and feature differences depending on vendor choice. Only a 46,8% of total Android devices runs Jelly bean. More worrying is the fact that almost 30% of devices run a 2-3 years old versions. [19] These data can't be comparable with iOS versions distribution, with a 65~75% of the devices at 7.x versions (2 months), and only ~6% under 6.x version. [20]

In case of top manufacturers, Samsung leads the smartphone market with the 30,4% of total devices, while Apple's tablets has the 29,6% of its market. [21]

In the enterprise, tablets are being widely adopted on a scale that is having a deep impact on conventional PC sales. Additionally, the strength of Apple's iOS platform is also bolstering tablets, While Android it has not been able to stoke strong sales of tablets. That's particularly evident in the enterprise. [22]

2.6.3. About Enterprise Mobility Management Systems

In order to identify the market leaders, we should to consult global IT analyst opinions about MDM vendors. [23] [24] The most valuable vendors for 2013 are Airwatch, Citrix and MobileIron. [14]

Table 2.3. Gartner: MDM software Strengths and Cautions [14]

Vendor	Strengths	Cautions
Airwatch	▪ Supports containerization of corporate resources. ▪ Supports multiple users per device. ▪ Secure file sync and sharing, and application access ▪ Aggressive pricing	▪ Negative feedback experiences regarding implementation and postsales technical support. ▪ Containerization is not equally supported across OS. ▪ Limited executive team. ▪ Low Market visibility.
Citrix	▪ Executive leadership team. ▪ Deep understanding of remote access and mobility needs. ▪ Integrated product solution.with secure containers for smartphones, ▪ tablets, Macs and PCs.	▪ Cloud-first product. ▪ Purchased in two forms:MDM only or all EMM Suite. ▪ Not have a strong consumerization play and nor have small or midsize business (SMB) offering.
MobileIron	▪ Strong vision of EMM, and has executed well in terms of product development, launches and support. ▪ Simple policy management ▪ Usually first to market with an integrated solution. ▪ Proved management, scaling and financial viability	▪ On-premise appliance strength, need strongest cloud version. ▪ Complains with level 1 support made for partners (not mobileiron). But has taken back Level 1 support and has seen increased customer satisfaction.

CHAPTER 3. DEFINING AN ENTERPRISE MOBILITY MANAGEMENT STRATEGY

As discussed in sections [2.1] and [2.2], enterprise is in transition to a new environment where mobility influence becomes higher and challenges arise [2.4]. The IT objective is to lead this transition to mobility without exposing enterprise data security, and without disturb the innovation way.

Chapter 3 provides a high-level mobility strategy definition to use when implementing an Enterprise Mobility Management program. In order to simplify project's kick-off, this initial stage will be divided in two steps:

- Discovery and Planning phase, where goals and stakeholders will be identified.
- Design Phase, where architecture, infrastructure and processes and will be define.

Pay Attention! These bullets highlight key tasks and decisions in a real case!

- *Note: Some data exposed or referenced in this chapter is collected from a real customer. In order to preserve his privacy, proper nouns of people, departments and/or applications will be substituted by generic ones.*

3.1. Phase I: Discovery and planning

The aim of this phase is to discuss about benefits and drawbacks of mobility, meet business and technical requirements, define an interdepartmental EMM team and establish goals, objectives and program milestones.

Case Study 1: The company and its business

In our real case, the company where an EMM program wants to be released is a utilities management company. It has about 6800 employees in Barcelona municipality. The employees are organized in two ways (The hierarchy is shown in [Figure 3.1]):

- Distributed in 10 areas according the territory where public services are managed.
- Distributed in several branch offices.

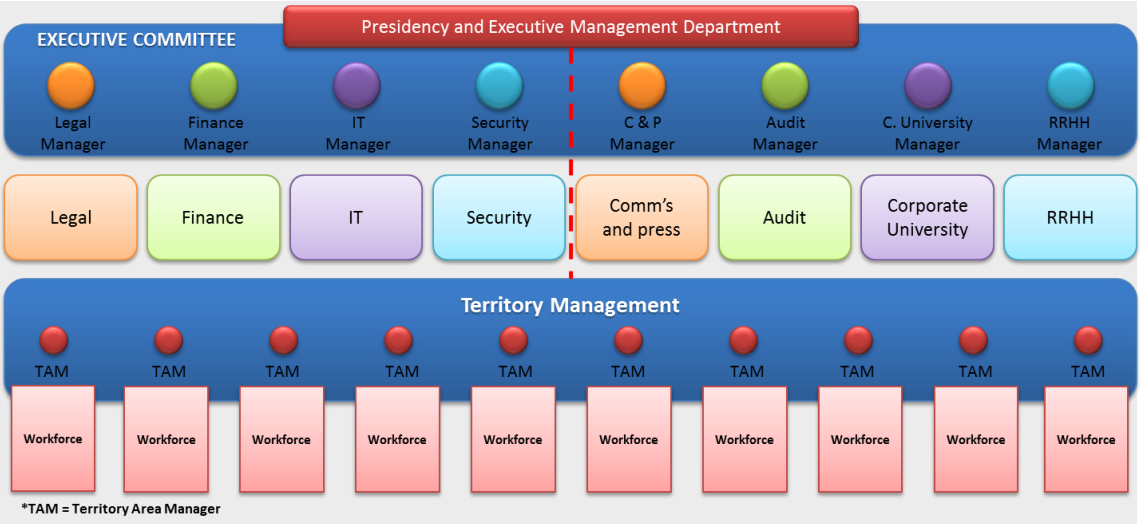


Figure 3.1. Company's organization chart

3.1.1. First Mobility approach

The first step is to define the mobility approach adopted in an EMM strategy. This could range from access prohibition of any mobile device to enterprise resources, to the promotion of mobility as a business enabler mechanism.

Case Study 2: In our case, during a mobility program Kick-off meeting [Annex 2.1], customer has expressed that a managed approach should be considered. The key ideas about this strategy was:

- Segment employees in categories (Desktop and Mobile).
- Offer enterprise-purchased mobile devices to those categories where mobility could be a competitive advantage.
- Consider the viability of use of personal devices for enterprise business.
- Provide support in an appropriate way for each group.

Although mobility decisions will imply agreements between technical and business units, as exposed at section [2.3], is required to appoint who will drive the EMM program: Business or IT. Usually IT leads the program, because is who promotes the mobility program start and better knows the technical possibilities. In other cases, when is a specific business process which wants to be mobilized, can be Business who leads the program.

Case Study 3: IT, as mobility sponsor inside the customer, will establish and review planning and also will check the achievement of milestones agreed by EMM team.

3.1.2. Mobility meetings and requirements analysis

Mobility meetings are intended to meet the company and its business deeper as well as to establish the real needs of mobility. The goals of them are:

- Define the key business processes and applications susceptible to be mobilized.
- Identify the target audience within the scope of mobility strategy. In broad terms try to establish the volumes of users and devices.
- Identify the non-technical stakeholders for the EMM Team.
- Create some expectations. Attempt to find a "sponsor" at executive level.
- Find out the existence (or not) of unmanaged devices inside the enterprise.
- Inquire about mobile devices perception and how everyone thinks that mobility can helps to their everyday work.

Case Study 4: In practice, this step has taken about one month because has been necessary to schedule the meetings with the attendant of each company area. All meeting minutes can be consulted at [0].

With the aim to prepare meetings and collect important mobility data, a very detailed Mobility Quiz template was created [Annex 3.1]. In this template, all mobility topics suggested at the starting of this point was asked.

Before meetings, the quiz has been sent to business partners of different departments in order to be completed. Unfortunately, in the great part of cases, the customer has not complied with this previous task, so a simpler template has been used [Annex 3.2].

Once all the meetings have concluded, is time to analyses and present the data collected.

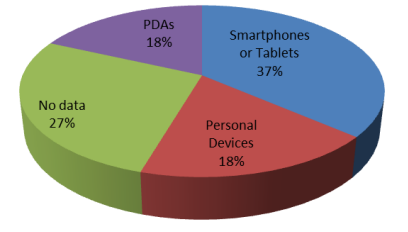


Figure 3.2. Presence of Mobile Devices in departments by type of device

As we can see in [Figure 3.2], at least in 37% of departments have been introduced smartphones and tablets, which are unmanaged. Moreover, in 18% are personal devices that access to corporate email. All these devices imply security risks and data leak point.

On the other hand, exist an 18% of departments where obsolete PDAs are intended to recollect data. There is no synchronization with PCs for do reports, so these tasks are done in a very inefficient way. Substitute them is a must.

According business units [Figure 3.3], at least a 26% of user roles identified can be fully adapted to a mobile work form, improving the efficiency of their tasks. Moreover, has been considered that other 42% of roles can take advantage of mobilize some of their processes.

The departments which take more benefits about mobility are Finance, legal, HHRR and IT, where inspectors, auditors, field technicians and executive units, are only few examples of mobile workers.

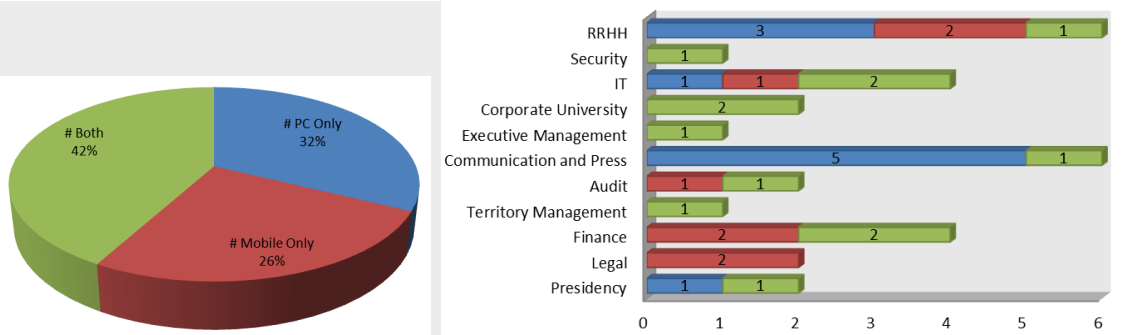


Figure 3.3. Users Distribution by mobility role needs and department.

Finally, will be presented a summary of common user requirements detected:

- Access to corporate email.
- Internet connectivity (Wi-Fi/3G) to find information, update data, access to social networks (Dept. of communication), to publications, etc.
- Availability of basic applications. Office and other applications that allow device from to be productive (Compression, PDF readers, etc.).
- Access to business applications. Either through the web browser and connecting to the corporate network (VPN), through virtualization clients, or through custom developments for mobile devices

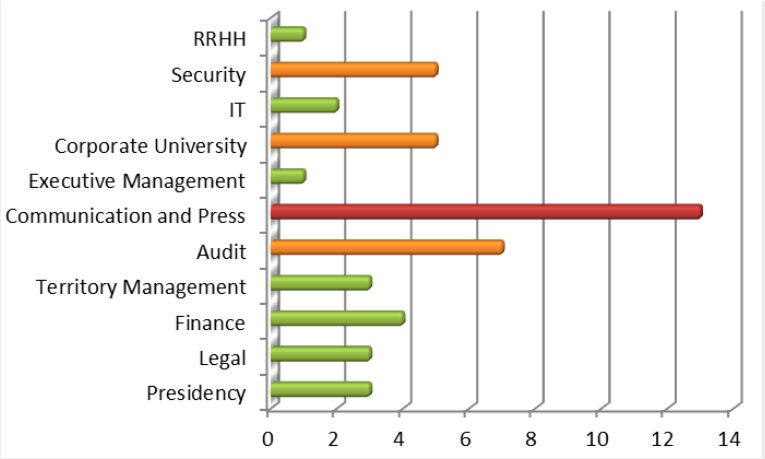


Figure 3.4. Business Apps sensible to mobilize by dept.

- Connectivity to Corporate Network (VPN) that allows remote access to both resources and services, such as infrastructure servers.
- Access to remote folders, which allow access to corporate and personal documents from any location (SharePoint Sites / Notes Project "Corporate Dropbox ", etc.).

3.1.3. EMM board definition

The EMM board is a group formed by employees from different company's departments, technical and non-technical, and the responsible of establish the guidelines of mobility program. The main functions of EMM team are:

- Promote the program internally and provide expert support in mobility area.
- Act as interlocutor between the different departments and agree tradeoffs in cases of conflicting requirements between them.
- Define and review policies that will govern the corporate mobility strategy: use, security, applications, etc. according mobility requirements detected.
- To design support processes to reduce the number of incidents and resolve requests in the shortest time.
- Collaborate in the definition of Standards in order to create a common model for the development of business applications.
- Lead the homologation of corporate and personal devices according to the needs and requirements established.
- Lead the approval of applications, commercial and in-house, to ensure compliance with the requirements and functionalities required.
- Evaluate different EMM solutions, and identify the one that best fits the needs detected.
- Deal with suppliers, manufacturers and other third-party providers, as well as monitor and review Service Level Agreements (SLA).

Case Study 5: At this point, all stakeholders have been identified. Next, it is a must to define the components of an EMM board which leads the program. The idea is to build a permanent group of persons with response capacity and business knowledge to attend mobility needs detected at mobility meetings stage.

Although EMM team is fundamental during design, implementation and mobility program roll-out, also will be very important once the platform be stabilized. From this time, EMM board will be responsible of a continuous evaluation process, where mobility innovations and new business requirements should be attended and, if they add business value, joined to the mobility solution.

The roles defined in our case for the EMM board are shown in [Figure 3.5]:

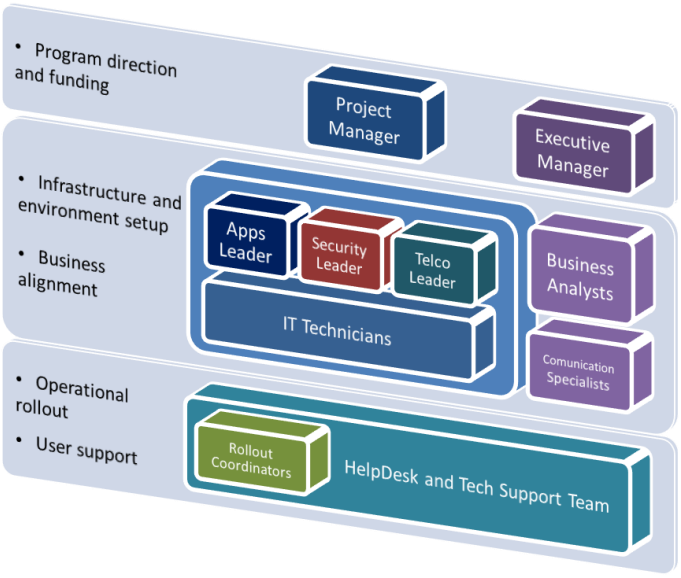


Figure 3.5. EMM board components

As can be seen, in the EMM board are involved from executive level to IT technicians. Each one of them, are intended to perform its own mobility tasks. In [Table 3.1] are explained the main functions of every role inside the team.

Table 3.1. EMM board component descriptions.

Rol	Description
Executive Manager	▪ Involved in evaluation and purchase approval ▪ Align overall program goals and objectives; communicate project to company
Project Manager	▪ Drive project plan and milestones; achieve product roll-out goals and objectives ▪ Coordinate resources, maintain priorities, and drive project tasks and activities
IT Team	▪ Cross-functional technical team comprised of application architectute, network admin, mobility, IT security, infrastructure, server management, and messaging resources ▪ Responsible for up-front architecture design, product deployment and long-term system management and operational support of infrastructure
Business Units	▪ Business analyst and communication specialists to define and deliver program details to end-user community
Operational Rollout and Support	▪ Coordinators for everyday rollout task control ▪ Help-desk team to support end user escalations and cases

Not all roles within the board, especially at executive level, are dedicated exclusively to this project. Mobility program moves forward every day, headed by Project Manager and driven by its permanent mobility team formed by technicians and operational rollout units. Those decisions that require major consensus will be addressed in EMM board meetings, scheduled one or twice a week.

3.1.4. "Under the Hood"

This section is dedicated to provide an overall explanation about how Enterprise Mobility Management System works. Also the different infrastructure elements will be covered. It is true that not all EMMS have exactly the same design and capabilities, but the main entities and its behaviour is almost the same.

3.1.4.1. Infrastructure components

As is shown in [Figure 3.6], the topology of an EMMS has four main entities: EMM core server, App gateway, Email gateway and Device Agent. All three infrastructure items are placed between enterprise resources and end user devices in the Demilitarized Zone (DMZ) while Agent is installed on the device. This allows IT to define and enforce policies around Apps, documents and Devices and manage the access to corporate services.

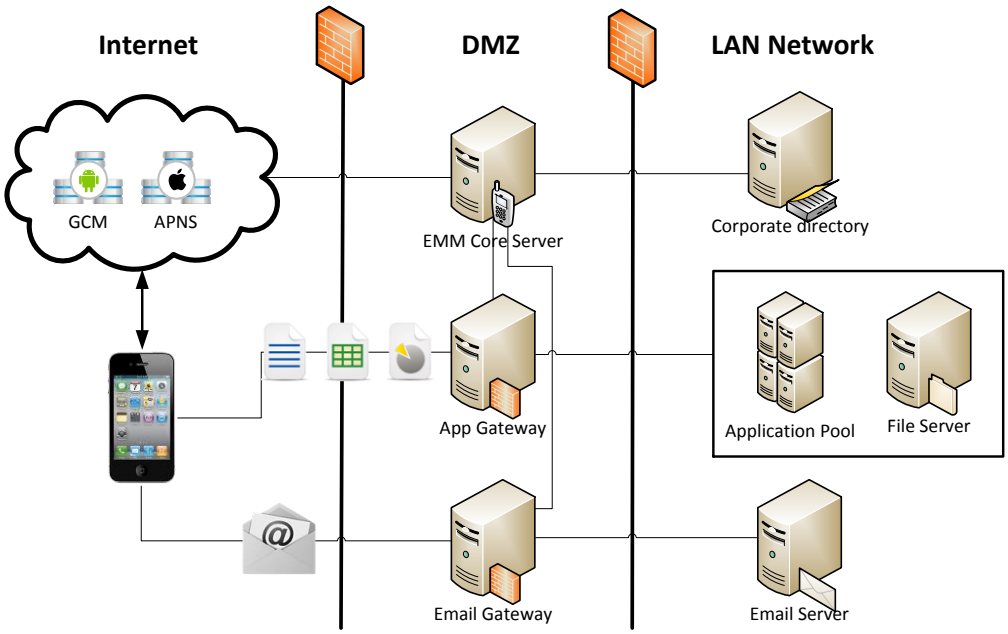


Figure 3.6. Enterprise Mobility Management System topology

- EEM Core Server: It is the core of the platform, the operation brain, where IT defines the management policies for apps (MAM), documents (MCM) and devices (MDM). It determines which users get what, when, with what level of security across multiple mobile operative systems. Also is the responsible of collecting data about device and its policy fulfilment.

  EMM Core Server is who communicates with the directory for setup new users and check corporate identities. When a identity certificate should be issued, it also acts as a proxy for make the request in the name of the device.

- App and Email gateways: Both are almost the same, a secure proxy that sits between enterprise system and the devices and enforces the policy defined in the EMM Core server.

  However each one has different purposes. In one hand, Email gateway is placed in between email flow and is responsible of encrypts both the

email and the attachments. On the other hand, App Gateway is responsible of creates tunnels so that mobile applications can access enterprise data securely.

- Device Agent: It is a piece of software that enforces policies on the device for applications and data at rest.

Other important elements in EMMS working are push services; each operative system has its own. The main objective of it is to inform the device that should connect with the EMMS in order to execute some instructions. Also are useful for notify the device with push messages.

3.1.4.2. Enabling Mobile Device Management

Here is explained the core process of configuration and security management of a new mobile device.

- User downloads and installs Device Agent. Then, he logs into Device Agent app with his corporate credentials. Then, 2 cases are possible:
- EMM Core validates that the user is authorized and device in compliance or the device is provisioned with policies determined by IT.
- These configuration settings are then stored in the EMM Core as well as on the device itself.
- The End User will now have secure access to Email, corporate Wifi, VPN, etc. Now IT will be able to manage the device and set policy directly on that device.

3.1.4.3. Enabling Mobile Application Management

Here are explained how this architecture supports the main App management use cases.

- Once the app is available, the user would access the Enterprise Storefront and download and install the app.
- As the app is managed, IT can enforce policies defined with the EMM Core, on the mobile device
- At runtime the application can talk to the backend using app tunnels through App gateway and with other managed apps, without interacting with user personal apps or data.
- EMM Core can enable dynamically the update of App policies and access or even remove the application from the device.

3.1.4.4. Enabling Mobile Content Management

Here are explained how this architecture supports secure corporate content access.

- App gateway enables secure access to corporate document repositories via the Device Agent Container on the mobile device

- The user profile and permissions are transferred from EMM Core to the device and access is granted to content.
- IT has the ability to selectively remove access to any document secured within Device Agent Container.

3.1.5. Phase I conclusions

All the previous steps of Phase I have to be consolidated in detailed conclusions where all the actions addressed during the program are defined. Also are focused the goals to achieve once the EMM solution has been installed.

3.1.5.1. Characteristics analysis and actions accorded

Case Study 6: First conclusions: characteristics observed and actions accorded

Bellow, the main characteristics about platform status as well as the actions accorded to do by EMM board are exposed:

- High heterogeneity of functions and roles.

It is necessary to define a common hierarchy to establish user profiles with usage guidelines different devices (eg, VIPs, managers, teachers, inspectors, field technicians, security team, etc.).

- Existence of obsolete PDAs.

These devices are used by inspectors, auditors and field technicians to prepare reports or open incidents tickets. They are not suited to the needs of users and in many cases create double work.

It is necessary, the total inventory of existing PDAs, type of use and ownership in order to define a strategy for replacing with new generation devices that allow make these tasks "in situ".

- Presence of unmanaged smartphones and tablets.

These devices, corporate or users owned, have access to email and store corporate information (eg, meeting minutes). They are currently not under any management, so the loss or theft can lead to leakage of sensitive data. It is necessary to define a policy based security, as well as guidelines for the use (or not) of employee-owned devices (BYOD).

- Large volume of business applications.

In later stages, after the program rollout, will require a deeper analysis of existing business applications: type applications, architecture, and its use to assess what should be optimized to be accessible from mobile devices.

For this stage is inside program scope to define which public store apps can be installed, allow access to HTTP-based backend applications through VPN and also establish the processes for in-house apps distribution.

- High demand of remote desktop access.

It is necessary to analyse the real needs. In many cases, the access to corporate documents and some specific services are enough. A model based on mobility management instead of a remote desktop are preferred.

- Integration with basic corporate services (Mail, VPN, printing, etc.).

It is necessary the analysis of the existing infrastructure, to determine the best strategy for integration with the EMM solution.

- Demand of avoid user/password authentication methods.

It is necessary to evaluate the authentication with user certificates via smartphones and tablets and the integration of PKI infrastructure with mobile devices management system.

- Existence of isolated mobility initiatives in different departments.

Detected isolated on-going projects related to mobility solutions (eg, "corporate Dropbox", analysis of desktop applications for tablets, user profiles, etc.).

It is necessary add these initiatives to the program, join synergies and establish a common mobility strategy.

3.1.5.2. EMM Solution Goals

Case Study 7: Enterprise Mobility Management solution goals

In [Table 3.2] are detailed the goals that implanted Enterprise Mobility Management system should fill, according Phase I conclusions and EMM board strategy:

Table 3.2. EMM System goals

	Main Goals
Devices	▪ Support corporate-defined operating systems and device models ▪ Extend security policies to mobile deployments ▪ Enable access to enterprise services and resources ▪ Configure device settings and policies through profiles
Applications	▪ Manage public and purchased apps ▪ Create a custom Enterprise AppStore ▪ Allow distribution and manage of “in-house” apps
Content	▪ Manage access and share corporate documents via secure container ▪ Manage email attachment access ▪ Integrate with file servers, as SharePoint
Security	▪ Enforce restrictions on devices features, apps & web browsing ▪ Support internal PKI and 3rd-party certificates ▪ Establish and enforce compliance rules and actions
Employee-owned devices	▪ Configure policies and settings based on device ownership ▪ Isolate and protect both corporate and personal information

3.2. Phase II: Design

The aim of this phase is to put in practice all the decisions of Phase I.

3.2.1. Definition of mobility profiles

The first step in design phase is to group employees according mobility needs detected and select the technology requirements for each.

Case Study 8: In our case, the users have been grouped into three different profiles regarding the mobility needs and the criticality of the information managed:

Figure 3.7. Mobility profiles

- Basic mobility profile: Users that require work with office applications or administrative management applications. They work in the office but also have a certain level of mobility. (e.g., salesman, communication & press units, secretaries, HHRR technicians, etc.).

The device provided to this type of users will be a tablet.

- Specific mobility functions profile: Users that require specific tools to work with software or hardware, and who usually work out of the office and have a high level of mobility for territory (e.g., field technicians, auditors, security units, etc.).

The device provided to these users will be a tablet or a “phablet” device (tablet-smartphone hybrid).

- Managers and VIPs profile: Users who exercise control or responsibility roles and have mobility needs to exercise its functions (e.g., managers, executive direction, presidency, etc.).

This type of users will be provided of both, tablet and smartphone.

3.2.1.1. Business Model

In chapter [2.2], has been explained the implications of consumerization for the enterprises, and how BYOD and COPE business models works. At this point also is important decide the ownership of the device and if employee owed devices will be permitted.

Case Study 9: The business model adopted for the EMM strategy will be a COPE program. The main reasons to adopt it has been:

- Ensure productivity providing to the user the right tool to do his work.

- Ensure access to the enterprise services due to device is approved.
- Reduce user support cost because are only few device models.
- Full control over the information handled by employee
- Full control of device and full remediation options without worrying about user privacy concerns.

Although a COPE model will be used, BYOD users will be also allowed. These users who want connect its own devices to corporate resources or services (e.g., email), will be considered during policies definition in order to establish a use policy and prevent security concerns.

3.2.1.2. User ID

Another concept to define is de Digital Identity of the user when have a corporate device. Normally each operative system manufacturer (Android, iOS, Windows) has its own ID in order to:

- Maintain settings across different devices.
- Buy apps and access to manufacturer's services which requires authentication.
- Register the product and be assisted by official support.

It has been decided if the ID will be user-created or corporate-owned, and in this last case, how will be the ID's format.

Case Study 10: The ID provided with the mobile device will be user-owned, but with some particularities:

- The ID can have a corporate format or not, but IT should have inventoried.
- The recovery mail should be a corporate one until the employee leaves the enterprise.
- The ID can be employed for any purpose that the user wants (personal or not).

3.2.2. Device selection for COPE program

The next step is to define which specific device models will be provided for each user profile. To facilitate the choice of devices, a comparative study of the main options on the market should be done. Basically, there are 2 variables to analyze: Device hardware capabilities and Operating system management options.

Case Study 11: Hardware comparison

Considering the user profiles defined at [3.2.1], the types of terminal to be rated are smartphones, tablets and phablets. The selected devices have been:

- Smartphones: Apple iPhone 5, Samsung Galaxy S IV, Nokia Lumia 920, BlackBerry Z10 and HTC One.
- Tablets: Apple iPad 4, Samsung Galaxy Note 10.1, Microsoft Surface, Google Nexus 10 and ASUS Pad infinity TF700.
- Phablets: Only Samsung Galaxy Note II has been considered.

A complete comparison between devices can be consulted in [Annex 7.1. Mobile devices comparison chart]. Once analysed the results for each device type, we can conclude:

- There is a wide range of smartphones with hardware specifications very similar between them. However, the most highly rated device at hardware side has been the Samsung Galaxy S IV.
- In tablet market, despite the emergence of different Android models with enterprise functionalities and with technical good enough, the device who stills leads is Apple iPad.
- The new category called "Phablet" consists in a hybrid device in between a smartphone and a tablet. Although, the variety of these devices is increasing a lot, is clearly led by the Samsung Note II device.

Case Study 12: OS management comparison

The EMM capabilities of each operating system maybe are the most important thing to take care in order to select one mobile device for enterprise environment. The considered ones will be the following: Android, Blackberry OS, iOS, Windows Phone.

A complete comparison between devices can be consulted in [Annex 7.1]. Once analysed the results for each operative system, we can conclude:

- The broader features found in iOS thanks to its standardization level software.
- In Android, its management capabilities depend on the API of the device manufacturer. The only which fulfil the requirements is Samsung who has more developed its EMM functionalities.
- The BlackBerry 10 devices management depend on the integration of the EMM tool with Blackberry Enterprise Server. As installation of any third party tool isn't desired, these devices are discarded.
- Finally, although Windows Phone is in a growth phase, It does not have the same capabilities and functions of competitors.

3.2.2.1. Final decision

Before take any decision, all the studies and analyses have to be considered. The device selection establishes, in some way, the strategy about mobility program. The main goal is to provide devices which guarantees productivity, good user experience and complete device management for IT.

Case Study 13: Once studied previous comparisons ([Annex 7.1] and [Annex 7.2]) and the market status reflected at [Annex 1.2], the approved devices have been the following:

- For basic users: Apple iPad (3G and above).
- For specific functions users: Samsung Galaxy Note II (not previous).
- For VIP users: Apple iPhone (4S and above), Samsung Galaxy (S3 and above) and Apple iPad (3G and above).

The reasons behind these decisions have been the following:

- Blackberry devices have been discarded due to company status and low level of device management.
- Although Windows Phone devices don't fulfils management requirements, they should be studied again in 12 months because have great potential in enterprise market.
- The Android market fragmentation has caused that the only manufacturer that satisfies enterprise management needs is Samsung. But not all Samsung devices, only those with latest version of Samsung Approved For Enterprise (S.A.F.E) API fulfils the requirements. Also Samsung provides a Dual-Persona technology (Samsung KNOX), which allows divide personal and corporate data through a secure container for enterprise data. According this situation, the only devices approved are Samsung devices with last OS version (4.2 or above). (SAFE and KNOX technologies are explained in Annex 8.2).
- The high level of homogeneity and the great board of management functions make Apple devices, the best ones for EMM. Also has been considered the existence of this type of devices distributed in some departments. Then a continuity strategy has been selected.
- Even so, the cost of Apple devices is too high, so other possibilities should be analysed in order to find a good alternative at mid-term. So, every iOS device, from iPhone 4 and iPad 2, are approved for enterprise use. (Apple MDM protocol is explained in Annex 8.1).

3.2.3. Defining mobile devices policies

Case Study 14: At Phase 1 closure meeting [Annex 2.13] was defined de interlocutors for policies creation:

- Use Policies: RRHH, Project Manager, Security Leader, and Communication & Press.
- Security Policies: Project Manager, Security Leader.
- App Policies: App Leader, Telco Leader, Project Manager.
- BYOD Policies: Project Leader, RRHH, Security Leader, Legal, Telco Leader.

3.2.3.1. Use Policy for COPE devices

Use policy should define the guidelines to ensure the correct use of corporate mobile devices, data plan options and reimbursements conditions. Also a contract signature requirement can be established at this point.

Case Study 15: Use policy outlines the general use guidelines and data plan for Corporate Mobile Devices. The full document can be consulted at [Annex 6.1. Use Policy], but main guidelines are exposed below:

- Employees whose positions require a mobile device will be provided and covered under a company-sponsored plan billed.
- Protect corporate data on mobile device is a user duty.
- Right device use according province and state laws is a user duty.
- EMM client should always be installed.
- Device must be encrypted and protected with a code.
- After do not connect to EMMS in 7 days, access to corporate resources will be blocked.
- In case of loss/theft all device data will be deleted.
- Upgrade of device OS should be done in a 30-day period after its release. In other case, access to corporate content will be blocked.
- Roaming will be allowed with previous authorization.
- Tethering is not allowed in roaming conditions.
- Not allowed Jailbreak or Rooted devices.
- Company has the right, at any time and without notice, to suspend or deny access to corporate resources.

3.2.3.2. Security Policy for COPE devices

Secure policy should define all the requirements and corporate measures to guarantee security and integrity of corporate data and technology infrastructure. Also at this point, user duties and remediation task can be reflected.

Case Study 16: Security policy outlines the general security and control measures for Corporate Mobile Devices. The full document can be consulted at [Annex 6.1.], but main guidelines are exposed below:

- The user must to protect corporate data.
- In case of loss/theft all device data will be deleted.
- The EMMS client should always be installed.
- Must be corporate antivirus installed.
- The device must be encrypted and protected with a code all the time.
- The Company will never be responsible of any misuse of the device.

- Is not allowed use the SIM in another device.
- All device data is the property of the company.
- It is prohibited any type of corporate data leaks.
- Corporate data must be in secure container or in managed apps.
- Cloud backups are prohibited. Desktop Backups are allowed but must be encrypted.

3.2.3.3. App Policy for both COPE and BYOD devices

The primary value propositions for mobile devices are mobile applications. Mobile Applications Stores provide access to a huge range of applications which enhance the end user experience and increase productivity.

Even though, usage of some applications can represent a security risk for the enterprise. App policy establishes the guidelines of behavior while installing additional mobile applications not installed by default by IT Administrators on Corporate Mobile Devices.

Case Study 17: This policy outlines the applications usage rules for Corporate Mobile Devices. The full document can be consulted at [Annex 6.1.], but main guidelines are exposed below:

- Always use legitimate, official app stores: iOS AppStore (for Apple devices) and Google Play (for Android Devices).
- Be aware of apps that require excessive permissions.
- Do not open any kind of content or install apps from unknown or unauthorized sources via email, web or physical media.
- In corporate owned devices, P2P applications or those with cost for the company are prohibited without previous permission.
- Cloud-based applications are forbidden for company business data.

3.2.3.4. Bring Your Own Device policy

Many companies grants the privilege to its employees to access determined corporate resources from their personal smartphone or tablet. BYOD policy is intended to protect the security and integrity of company data and technology infrastructure. Although, limited exceptions to the policy may occur due to variations in devices and platforms.

Usually, the company reserves the right to revoke this privilege if users do not abide by the policies and procedures defined. For that reason, before employees are able to connect their devices to the company network, they must agree the terms and conditions set.

Case Study 18: This policy outlines the general security control measures and requirements for employee-owned mobile devices accessing corporate

resources. The full document can be consulted at [Annex 6.3. Bring Your Own Device Policy], but main guidelines are exposed below:

Regarding BYOD use policy:

- Approved models will be specified in a public list.
- For executives, managers and sales employees, the Company will reimburse 80% of total data and Voice plan.
- For other user categories with mobility needs the Company will reimburse a flat €15 per month.
- For other users without mobility needs, there are no reimbursements of voice or data charges.
- The EMMS client should always be installed.
- If necessary, there must be an antivirus installed.
- The device should be encrypted and protected with a code.
- After do not connect to EMMS in 7 days, access to corporate resources will be blocked.
- Provide and maintain the mobile device, data plan or any necessary accessories is a user duty.
- Data and corporate information can only be used in corporate email app.
- The upgrade of device OS should be done in a 30-day period after its release. In other case, access to corporate content will be blocked
- If is a corporate SIM, roaming is allowed with previous permission
- If is a corporate SIM, tethering is not allowed in roaming conditions.
- Not allowed Jailbreak or Rooted devices.
- Company do not collect location nor any kind of personal data of employee owned devices
- Company has the right, at any time and without notice, to suspend or deny access to corporate resources.
- Support Team must be notified when a device no longer have to use corporate resources.

Regarding BYOD security policy:

- The user must to protect corporate data.
- In case of loss/theft all corporate data will be deleted.
- The EMMS client should always be installed.
- The device must be protected with a code all the time.
- All corporate data is the property of the company.
- It is prohibited any type of corporate data leaks.
- Corporate data must be only in corporate email app.

3.2.4. "Choose your weapon"

The selection of EMMS must be the core of a mobility model. It should consider future trends and can be able to adapt it easily. In this sense, it is needed to make a comparison of different EMM solutions (Enterprise Mobility Management). The purpose of this comparison is to determine which of the tools currently available meet the following requirements:

- Ability to adapt to business needs.
- Meet the functional and technical requirements proposed.
- Streamline implementation costs, maintenance and operation.
- Take advantage of synergies with existing solutions and infrastructure.

These objectives have no value if does not take into account certain criteria and conditions of fundamental importance:

- Implement a solution with a validity of in the long term, on which to build future benefits and services.
- Detect technologies that together with the solution implemented add value.
- Establish a technological solution as open as possible, ensuring the coexistence of different platforms and providing a controlled transition.

Case Study 19: Once analysed market references for three EMM Gartner Leaders and after make a full functionalities comparison the selected EMM solution [Annex 7.3. EMM systems comparison chart], the selected vendor has been MobileIron. The reasons behind these decisions have been the following:

- Has been depicted as a "Gartner Leader" since 2011.
- Has strong vision of EMM, and has executed well in terms of product development, launches and support.
- Usually is the first to market new functionalities or EMM capabilites.
- Provides more required functionalities for MDM, MAM and MCM than the rest of vendors.
- It is the only vendor which has a native user experience for email control and attachment encryption from default email app.
- Virtual environments are out of the project's scope, so management capabilities for desktop or apps virtualization are not significant.
- The quality-cost relation of the solution is acceptable.

3.2.5. EMMS infrastructure design

At this stage, almost the guidelines about mobility approach and main selections have been done. Next, more technical topics, like architecture model, the number of servers and firewall rules should be prepared for the implementation phase.

3.2.5.1. Architecture model

The architecture model can be two: Cloud-based model and on-premise model.

- Cloud-based architecture is a SaaS model where EMM Core appliance is allocated in an external datacentre. Then, its computational cost and firewalling issues are responsible of vendor. This service model is a pay per use one.

  On the other hand, App and email gateways are in DMZ of corporate network in order to provide app tunnelling and email control services. Moreover, an additional element named "enterprise connector" should be installed in order to integrate the solution with company's LDAP or Public Key Infrastructure.

- On-Premise model is a traditional approach where all EMM servers are installed on corporate datacentre. In this case, the cost related to professional services, hardware and firewalling should be covered by the company.

Case Study 20: In our case, the cloud model is not an option due to company's philosophy is to have all data at its own datacentre. So, an on-premise deployment is a must.

As it is desired to take advantage of all EMM capabilities, will be necessary install, at least, the EMM core server and the Email and App gateway.

3.2.5.2. Capacity plan

The capacity plan is basically referred to definition the number of servers which should be installed for guarantee the correct solution performance. Also all the components and requirements for each server (storage, memory, processors, network interfaces, etc.) are specified here.

Case Study 21: The EMM solution wants to be deployed on a virtual infrastructure. According vendor's documentation, for a 6800 employees management the number of servers and its characteristics should be as follows:

Table 3.3. Capacity plan for EMM solution

Component	# Devices supported	Virtual CPUs	Processor architecture	Memory	Storage	# Network interfaces
EMM Core	< 20000	4x2.13 GHz	64-bit	16 Gb	250 Gb	> 2
App gateway	< 8000	2x2-4 GHz	64-bit	6 Gb	30 Gb	> 2
Email gateway*	< 20000	4x2-4 GHz	64-bit	8 Gb	40 Gb	> 2
***Minimum configuration for attachment encryption support**						

3.2.5.3. Firewall requirements

In order to ensure the communication in between solution elements and with mobile devices is usual that some firewall need to be opened.

Case Study 22: According vendor reference, ports that should be opened can be consulted in [Annex 5.1].

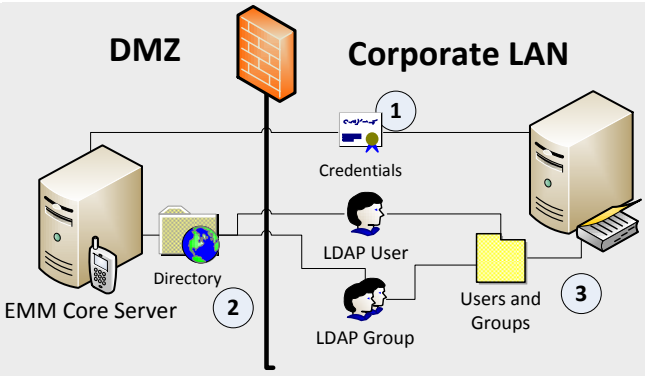
3.2.6. EMM System Integration with corporate infrastructure

Inside design phase is needed to make an approach about infrastructure needs which allows that mobile devices can access to corporate services (Wi-Fi, VPN, email, repositories, etc.). Final full design is shown in [Annex 5.2].

3.2.6.1. Corporate Directory

The LDAP integration is a core feature used by the great majority of companies. The purposes for LDAP integration via EMMS are for authentication of users, access to user attributes and access to group memberships.

Case Study 23: EMM core will be linked with corporate directory as follows:



- EMM Core Try to access to Corporate Directory with user credentials.
- If the credentials are OK, EMM Core can access to Directory Users and Groups folder.
- EMM Core and Corporate Directory are Linked and Synchronized.

Figure 3.8. LDAP Integration

3.2.6.2. Public Key Infrastructure (PKI)

The Public Key Infrastructure provides digital certificates that can identify an individual or an organization and also provides directory services that can store and revoke the certificates if was necessary. The corporate PKI can be linked to EMM Core to issue Certificates for user authentication in corporate services email, Wi-Fi, VPN, etc. There are three secure methods of certificate distribution that EMMS supports.

- Use an on-board EMMS certificate authority, to issue certificates.
- Use EMM Core as SCEP proxy to securely enroll devices into a Microsoft PKI environment without exposing a CA directly to the Internet.
- Use EMM Core as a SCEP proxy to securely enroll devices to a third-party PKI infrastructure, for example, Verisign's Managed PKI platform.

More information about PKI, its benefits and the SCEP use in Mobile devices can be found at [Annex 8.3. PKI, certificates and SCEP]

Case Study 24: In our case EMM core will be used as a proxy for SCEP requests to a Microsoft PKI without compromise CA.

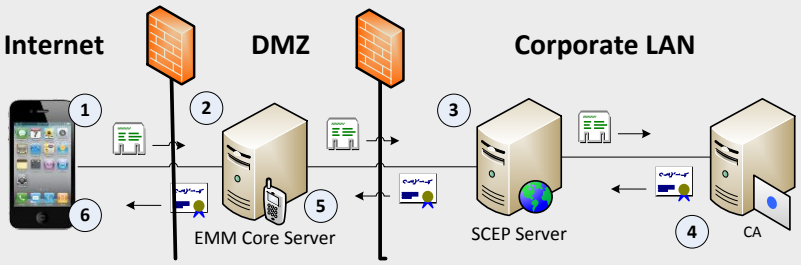


Figure 3.9. PKI Integration

- Device sends a CSR
- EMM Core forwards the CSR to SCEP server according defined template and credentials
- SCEP server forwards CSR to CA
- CA issues the certificate
- EMM Core forwards Certificate to device
- Device installs certificate

3.2.6.3. Email service

One of the most key integration points for EMMS is with an Email Server. Since email is the primary use case for most mobile users, configuring and securing it is a high priority when deploying an EMM solution. The integration point to email servers is through the email gateway.

Case Study 25: A certificate-based authentication is required. Once the device has the certificate, according the method of previous section, email access works as follows.

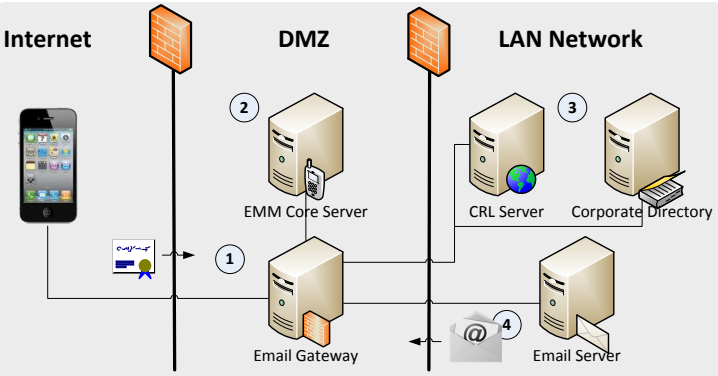


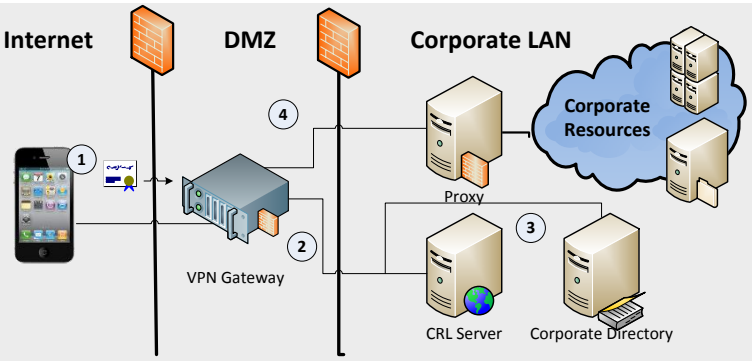
Figure 3.10. Email Integration

- Device shows certificate to Email Gateway
- Email Gateway asks to EMM Core if this devica can access to email
- Email Gateway consult if the certificate validity against CRL and Corporate Directory
- If previous checks are OK, the user can access to email service.

3.2.6.4. Virtual Private Network (VPN)

VPN infrastructure is intended to access corporate backend. Consulting the Intranet or document folders are usually the main goals.

Case Study 26: A certificate-based authentication is required also for VPN service. Once the device has the certificate, according the method explained in previous section, VPN access works as follows.



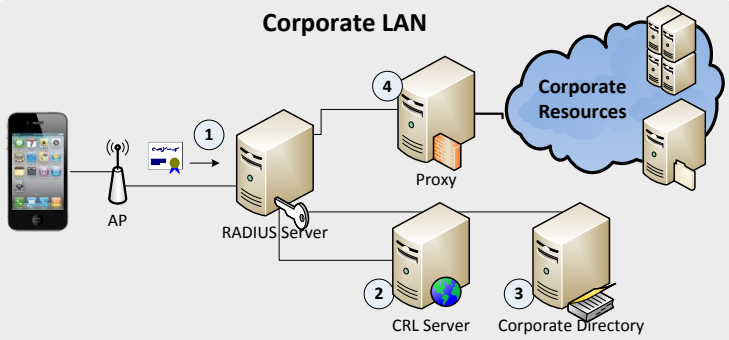
- Device shows certificate to VPN Gateway
- VPN Gateway consult if the certificate validity against CRL and Corporate Directory
- If previous checks are OK, the user can access to enterprise backend.

Figure 3.11. VPN Integration

3.2.6.5. Corporate Wi-Fi

When the users are in company offices, the use of corporate Wi-Fi is a must. Usually it is used to access both internet and corporate resources.

Case Study 27: A certificate-based authentication is required also for Wi-Fi service. Once the device has the certificate, according the method explained in previous section, Wi-Fi access works as follows.



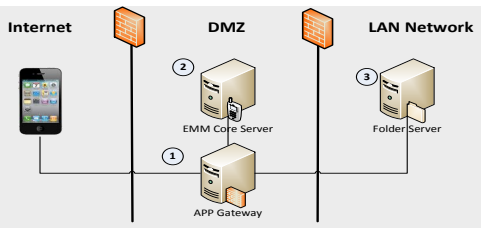
- Device shows certificate to RADIUS server
- RADIUS Server consult if the certificate validity against CRL and Corporate Directory
- If previous checks are OK, the user can access to enterprise backend.

Figure 3.12. Corporate Wi-Fi Integration

3.2.6.6. Corporate corporate repositories

Although with VPN or from corporate Wifi LAN resources will be accessible, App gateway also provides a secure tunnelled connection.

Case Study 28: App gateway tunnelling works as follows.



- Device try to access to corporate resources.
- APP Gateway consult if is an authorized user.
- If a previous check is OK, the user can access to corporate folders.

Figure 3.13. Corporate Folders Access

CHAPTER 4. ENTERPRISE MOBILITY MANAGEMENT SYSTEM DEPLOYMENT

This chapter is intended to in practice the Enterprise Mobility Management System according the decisions made in previous chapters. Unfortunately, the next two phases have not been possible to do in a real business study, so only a laboratory environment has been used to implement the EMMS.

It has been divided in two parts: Phase III, Deployment, where laboratory setup and the EMMS installations and configurations are done; and Phase IV, Rollout program, where rollout and support processes are explained.

Pay Attention! These bullets highlight key tasks in Lab environment!

4.1. Phase III: Deployment

This Phase is intended to develop all implementation and testing tasks: network and server's readiness, Installation and Configuration of EMM Core and Gateways, corporate services integration, system testing, pilot-device enrolment and check full deployment readiness.

4.1.1. Lab environment setup

The setup of a Lab environment is usual before a real production deploy, especially in those cases where corporate infrastructure is complex. The lab allows to test if the install process and configurations will work fine in the production infrastructure.

Lab Case 1: This initial step that usually is made in pre-production conditions will be implemented, in our particular case, as if it was a production deployment. Moreover, it will be installed in a different infrastructure within the means available. A Logical infrastructure diagram is shown below:

As can be seen in [Figure 4.1], hybrid architecture has been used: in one hand EMMS and corporate email are SaaS, because the hardware requirements for an on-premise deployment can't be fulfilled; in other hand, a virtualization hypervisor over a PC has been used in order to create a on-premise lab environment with a LDAP server, a web server and a PKI. This environment will allow implement great part of proposed solution in previous chapters. A very detailed step-by-step laboratory setup process can be consulted at detail of laboratory setup can be consulted in [0and ANNEX 10.].

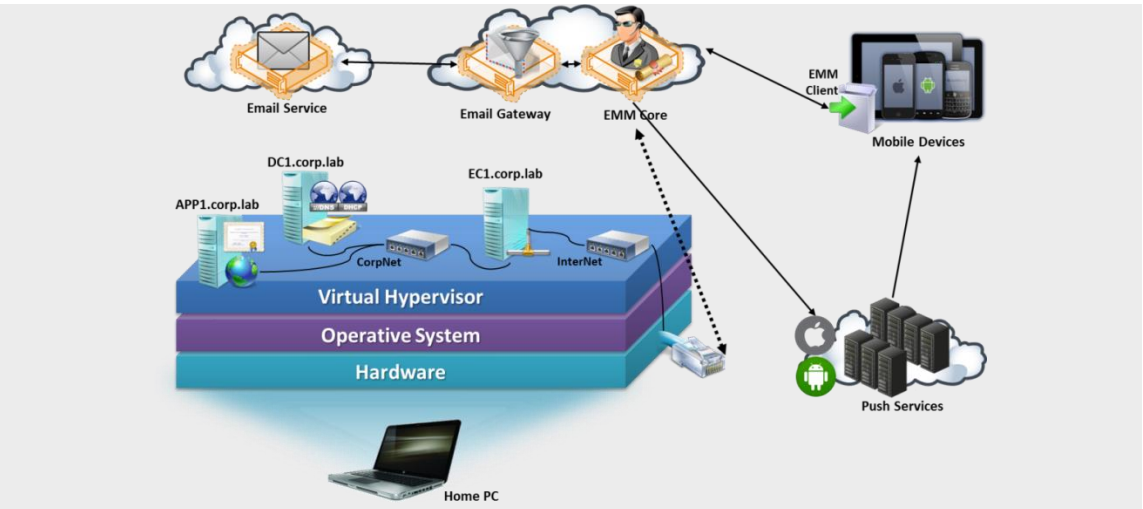


Figure 4.1. Laboratory diagram

4.1.1.1. Infrastructure overview

The detail of servers, operative systems and other tools used in Laboratory setup should be documented to be available to consult when production deployment is done.

Lab Case 2: Although a full document with the detail of laboratory setup can be consulted in [ANNEX 9. and ANNEX 10.], the most relevant steps and systems used are listed below.

Table 4.1. On-premise lab components

Hardware	▪ Processor: 8-Core, Intel Core i7 Q720 @ 1.60 GHz ▪ RAM: 6 GB ▪ Storage: 500 GB ▪ Network card: Gigabit Ethernet Qualcomm Atheros AR8131 PCI-E		
OS	Microsoft Windows 8 Professional		
Hypervisor	Microsoft Hyper-V Client for Windows 8		
Virtual Machines	▪ 2-Virtual Core ▪ 2 Gb RAM ▪ WinServer '12 ▪ AD Domain Services ▪ AD DNS ▪ AD DHCP ▪ Corpnet network (10.0.0.1\24)	▪ 2-Virtual Core ▪ 2 Gb RAM ▪ WinServer '12 ▪ AD Certificate Services ▪ Internet Information Server ▪ Corpnet network (10.0.0.3\24)	▪ 2-Virtual Core ▪ 2 Gb RAM ▪ MobileIron Enterprise Connector ▪ Corpnet and Internet networks (10.0.0.5\24 & 192.168.0.150)

Lab setup steps:

- Enable virtualization hypervisor client at Operative System.
- Create virtual network switches at hypervisor (x2).
- Provision of virtual machines at hypervisor (x3).
- Install operative systems in each server and upgrade it.

- Configure networking of each server.
- Install server roles according each lab component function.

Table 4.2. Cloud lab components

Cloud Provider	Microsoft	MobileIron	
Services	▪ Email and repository service ▪ Other services	▪ EMM Core	▪ App Gateway ▪ Email Gateway

4.1.2. Previous requirements

Once all the hardware details have been satisfied, other requirements should be done before installation start. The main requirements are related with server availability, firewalling and connectivity with Devices manufacturer Push services and between components, and other data required during installation process.

Lab Case 3: In our Connected Cloud solution, according vendor recommendations, the following requirements has been satisfied:

- Corporate Apple ID: A valid corporate Apple ID is required to obtain an iOS MDM certificate: mdm.ios.corp.lab@gmail.com.
- Connectivity requirements for corporate Wi-Fi: Firewall rules from corporate Wi-Fi to vendors' datacentre and to Push Services connectivity. In our case, as corporate Wi-Fi configuration is out of laboratory scope, this is not very important.

Table 4.3. Firewall requirements

IP range	▪ Allow connections of mobile devices to MobileIron's Connected Cloud 37.0.112.0/24
HTTPS 443 and HTTP 8080	▪ Open HTTPS port 443 (and HTTP 8080) from the corporate wifi network to MobileIron VSP instance (for client provisioning traffic)
TCP 9997	▪ Open TCP port 9997 from the corporate Wi-Fi network to MobileIron VSP instance (for TLS secured client sync traffic)
HTTPS 443	▪ Open port 443 (HTTPS) for iOS device access to the MobileIron VSP to support MDM.
TCP 5223	▪ Open port 5223 (TCP) to 17.0.0.0/8 to allow iOS devices using corporate WiFi to access Apple's APNs service.
TCP 5228 and TCP 443	▪ Open ports 5228 (TCP) and 443 (HTTPS) to android.apis.google.com to allow Android devices to access Google's C2DM service

- Connected-Cloud service data

EMM Core; URL: https://de.mobileiron.net/teveris CC Client Port:50171

Email Gateway; URL: sentry-2022.mobileiron.com

4.1.3. EMMS installation and configuration

Once the readiness of all systems has been checked, it is time to install EMMS components (EMM core and gateways) and configure it. A detailed version of all the steps below can be foud at [Annex 10.2].

Lab Case 4: As our EMM core and Sentry are installed on vendors' datacenter, only to configure them for the proper performance is required.

4.1.3.1. Configuring Connector in EMM core:

There are some tasks that need to be completed on the EMM core prior to Connector installation.

- Assign the Connector role to a new service user
- Add Enterprise Connector entry on the EMM core.

4.1.3.2. Provisioning Virtual Machine and installing connector

The requirements for the installation are 2 Gb of RAM memory, 2 Virtual CPUs, 20 Gb of disk and 2 network adapters.

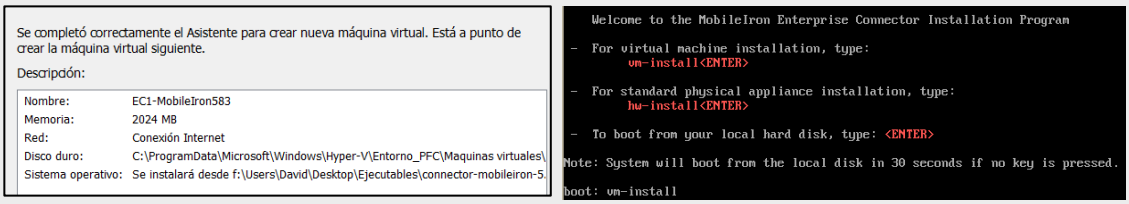


Figure 4.2. Installing Enterprise Connector

4.1.3.3. Configuring connectivity and communication EMM -Connector:

In order to reach the cloud EMM Core instance is necessary to configure some routes in web-based Connector management console.

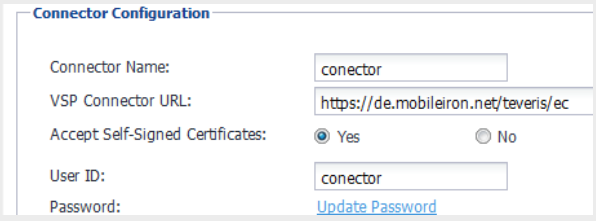


Figure 4.3. Connexion settings

Once EMM Core is reachable, it is needed to specify the *Connector Name* (must match what was configured on the Cloud EMM Core), enter the *EMM Core Connector URL and ID data.*

4.1.4. Enabling iOS MDM support

In order to use Apple's MDM protocol capabilities, it is needed to issue a MDM certificate from Push Certificate Portal which will be uploaded to EMM Core. More information can be consulted at [Annex 8.1. iOS MDM protocol].

Lab Case 5: There are different ways to enable MDM profile use and install certificate, but in our case it will be done by Admin Portal of EMM Core. Firsts, it is required enable MDM profile at EMM core preferences.

Next, it is needed to generate a Certificate Signing Request (CSR), access to the Apple Push Certificates Portal to request the certificate and finally upload it to EMM Core.

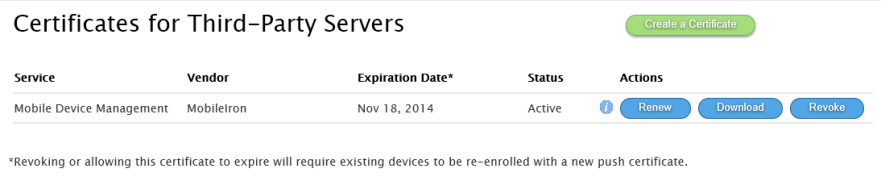


Figure 4.4. Apple MDM certificate

4.1.5. Managing users

After installation is complete, one of the first steps is to add users to the system before enroll devices. Any vendor has its own mechanisms, but more or less all of them allow that users can be added individually or be created through a Bulk Registration in a CSV file. Usually for testing, some local users are added.

Lab Case 6: In our case, there are two user databases:

- System Manager and CLI DB, where users must be added manually.
- Smartphones Manager DB, where users may be added locally or through adding an LDAP to the system.

4.1.5.1. User Roles

User roles are intended to divide administrative functions and user capabilities.

Lab Case 7: It has three types of Roles: SuperUser, which has access to everything; End user, with possibly permissions to self-wipe, lock, locate, and register devices; and HelpDesk user, with a combination of permissions.

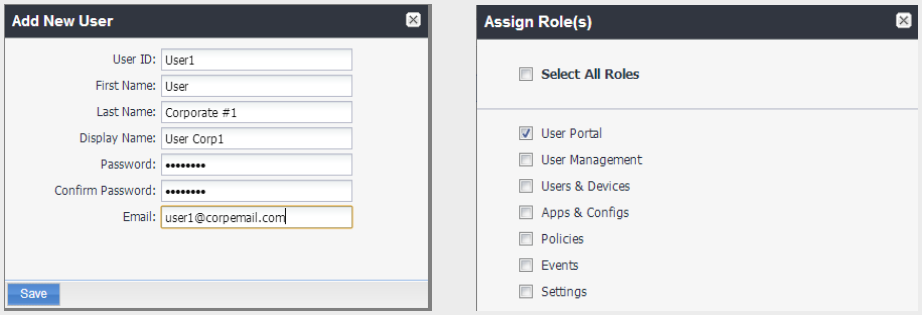


Figure 4.5. Assigning user role

4.1.6. Enrolment of lab devices

The next step is device registering to the users added previously, although the ways to add new devices can be various:

- Admin led single device registration or bulk registration.
- End user self-service portal registration or in-app registration.

During registration and provisioning, EMMS Client is used to pull down an MDM Profile. This profile is then responsible for management of the device. The EMMS client is important for additional features such as inventory, location services, App Storefront but most importantly providing a transport mechanism to get profiles installed.

If the client is removed, the device is still managed but the goodness it offers is gone. If the MDM Profile is removed, all sub-profiles go with it, leaving the device un-managed.

4.1.6.1. Registration process

- Activate the user and associate him to an added device.
- Notifying the user pending registration and provide instructions to download and install the client.
- Completing an initial scan of the Smartphone and synchronizing this information to the EMM Core.

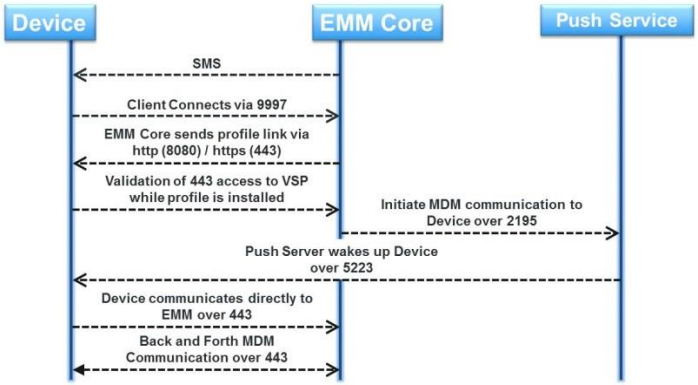
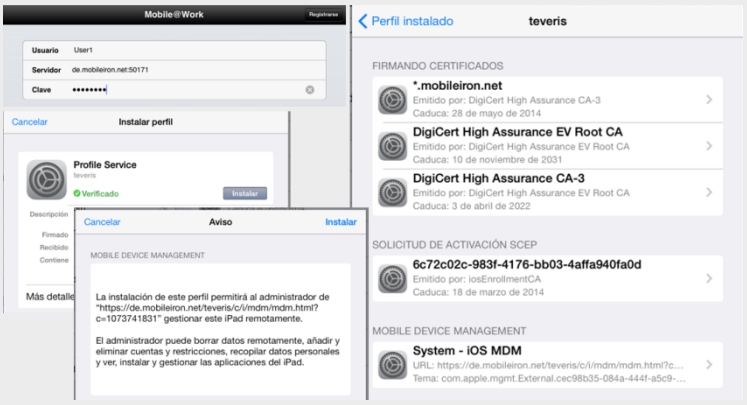


Figure 4.6. Enrolment process

Lab Case 8: In this case, user self-enrollment process will be used, through EMM client which can be downloaded from official app store.

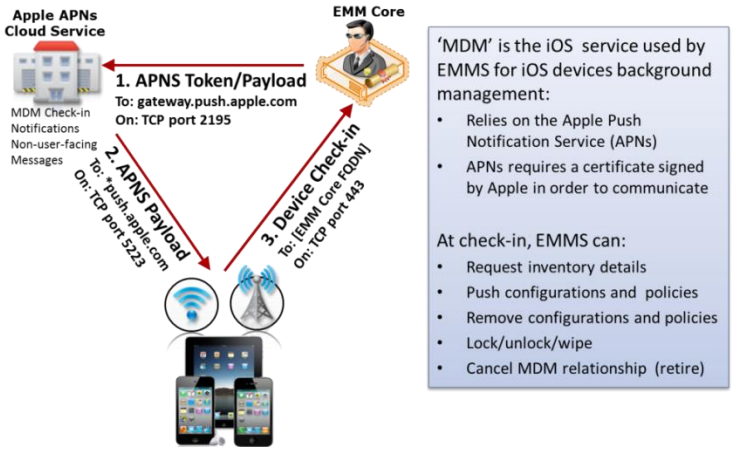


User	Number	Phone	OS	Country	Status	Registered on Date	Last Check-In
User Corp1	PDA	iPad 2	iOS 7.0	Spain	Active	2013-11-18	28 m 19 s

Figure 4.7. EMM enrolment steps and User at EMM console

4.1.6.2. Managing devices

To manage iOS devices using APNs, EMMS triggers a connection over TCP port 2195 to the APNs when choosing a management action on a device such as a Lock or a Wipe. The APNs pings the iOS device over TCP port 5223, signalling the device to check-in with the EMM Core. The device then checks-in to the EMM Core over TCP port 443, where the action is triggered.



The regular syncing takes place on an interval set in the sync policy and requests inventory details, pushes or remove configurations and policies, locks/unlocks/ wipes, and retire a device from MDM management. Forcing a Device Check-in action overrides the normal sync interval and brings the device current immediately.

Figure 4.8. Device Management triangle

4.1.7. Grouping users, devices and policies

Everything that EMMS manages on devices is managed through groups. You can use groups for devices, apps, policies, and events. Hence, it is possible to locate devices quickly in a search, or apply policies based on a device belonging to this group.

It is important to understand that policies are not directly applied to devices. Instead, policies are applied to groups and only devices inside this group receive the policies. Groups usually can either be based on a corporate directory or be manually assigned.

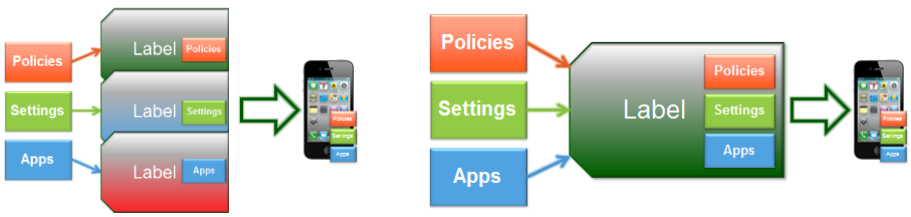


Figure 4.9. Multi-label vs. Single-label

Lab Case 9: As a baseline, three user groups will be defined: Basic Mobility users, specific mobility functions users and Executive users [3.2.1.].

Name	Type	Description
CorpLab Specific Mobility	Filter	Users with specific mobility functions
CorpLab Basic Mobility	Filter	Users with basic mobility requirements
CorpLab VIP Mobility	Filter	Users of executive layer

Name	Type	Description
CorpLab Auditors Only	Filter	Contains only auditor users
CorpLab Managers Only	Filter	Contains only manager users
CorpLab Closed Store	Filter	Contains only users without App Stores

Figure 4.10. Employee groups defined

After this initial configuration, it may has differences between employees inside the same group and require others groups according specific apps, device configurations or policies. In our case, also some departmental-specific configurations have been required (e.g. Managers, Executives and VIPs differences in password expiration).

4.1.8. Device Settings setup

Manage device settings across different smartphones manufacturers and operative systems can mean a high time-investment for IT. One of the most valuable benefits of EMMS is to automate this process by specifying the different types of app settings. The most common are: Exchange, other email, WiFi, VPN, Certificates, SCEP requests, document repositories and others which depends of OS or device model. Note that not all settings are designed to work with all types of smartphones.

Lab Case 10: As a first approach, Wi-Fi, VPN, Exchange and document repository device settings will be configured. Also other settings like iOS restrictions will be contemplate. The detail of settings can be found at [Annex 11.2. Settings details].

CorpLab iOS Control	RESTRICTION		Corporate restrictions for iOS devices
CorpLab Wifi	WIFI		Corporate Wifi
CorpLab VPN	VPN		Corporate VPN connection
CorpLab Repo	DOCS@WORK		Corporate Sharepoint repository
CorpLab Email	EXCHANGE		Exchange account for corporate email

Figure 4.11. Device Settings policies

After these policies are applied to a group, they are installed on the specified devices without user interaction:

Figure 4.12. Repository access and settings profiles in device

4.1.9. Device Policies setup

EMM Core uses policies to control the behaviour of mobile devices, and each policy consists of a set of rules. Multiple policies can be created for a policy type, but only one of each can be applied to a specific device. The main areas for types of policies are:

- Security policies which specify how manage several areas of mobile security.
- Privacy policies specify which files to synchronize, activity or content synchronized for each type of data and information included in log.

- Lockdown policies specify which features should be disabled and when access must be restricted.
- Sync policies specify how EMM Client behaves on the device and interacts with the EMM Core (sync of profiles, configurations, and app inventory).
- Container policies control settings for that feature, specifically whether to enable the 'Open In' capability.

Lab Case 11: According the policies established at [3.2.3.], one device policy of each type will be implemented. The detail of everyone can be found at [Annex 10.3]

Policy Name	Priority	Status	Description	Type	Last Modified
CorpLab Lockdown Policy	LOCKDOWN - 1	Active	Lockdown corporate guideli...	LOCKDOWN	2013-11-19 02:01:56
CorpLab Privacy Policy	PRIVACY - 1	Active	Privacy corporate guideliness	PRIVACY	2013-11-19 01:54:47
CorpLab Security Policy	SECURITY - 1	Active	Corporate security guideliness	SECURITY	2013-11-19 01:47:43
CorpLab Sync Policy	SYNC - 1	Active	Sync corporate guideliness	SYNC	2013-11-19 02:04:10

Figure 4.13. Policies defined at EMM Core

4.1.10. Apps Management

EMMS provides tools for distributing and managing mobile Apps, and companies usually follow a similar process in their management:

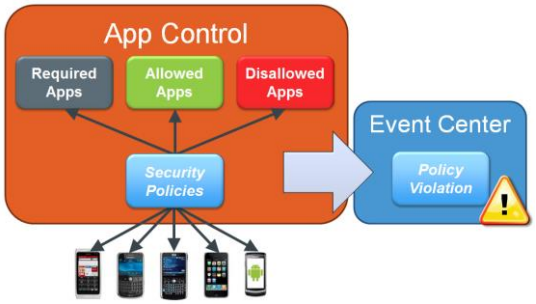


Figure 4.14. App Control diagram

- Configure a security policy defining which Apps should be forbidden, allowed, or required on devices.
- Track all new Apps showing up on devices and evaluating them for inclusion or exclusion.
- Define acceptable and featured Apps by adding Apps to a distribution library and having them appear as choices at enterprise storefront.

4.1.10.1. Controlling Apps

App control enhances visibility into the Apps being installed on managed devices and helps enforce corporate policy. Setting up App control involves the following tasks: configure alerts for a violation, define control rules and assign control rules and remediation tasks in the security policies assigned to devices.

Lab Case 12: According the App corporate policy established at [3.2.3.], an App control policy will be implemented. The detail of this policy can be found at [Annex 11.3].

- Configure Alerts (not only for apps!)
- Define Rules for App compliance

- Activate Rules at security policy and go to devices dashboard

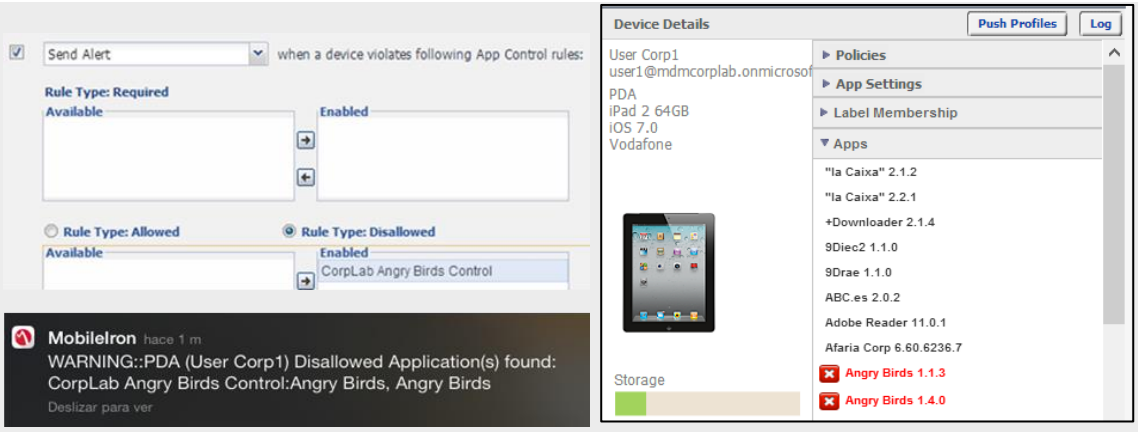


Figure 4.15. Warning rule and dashboards

4.1.10.2. Enterprise App Storefront

Enterprise App Storefront provides a centralized location for corporate Apps. In-house Apps are mobile Apps developed and distributed internally, while Recommended Apps are Apps that can be linked to download from the official stores.

Lab Case 13: In order to use App Storefront, first of all is needed to distribute the Web Clip intended to act as a gateway. Policy details can be consulted at [Annex 11.3].

In our laboratory App Storefront, some applications have been defined as recommended, and one app as featured, and no exists any in-house app.

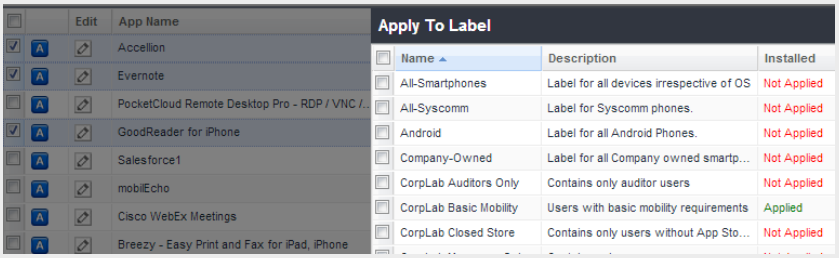


Figure 4.16. Adding Apps in App Storefront

In the device, when the Enterprise Appstore is consulted, these Apps are shown to download.

4.1.11. Corporate services integration

The real benefits of an EMMS are achieved when the solution is integrated with corporate services. In fact, EMMS should be used as a technical solution to provide corporate services that makes users more productive. So in this sense, this section specifies how to add corporate services to the EMM platform.

4.1.11.1. LDAP integration

LDAP integration will provide synchronization of Corporate Directory users and groups with EMMS. This makes ease the administration tasks of company users in the EMM tool.

Lab Case 14: Before integrate the LDAP server, has been needed to install and configure it. The main steps have been (full installation at [Annex 9.2]:

- Install the server and configure it as a Domain Controller.
- Install DNS and DHCP roles for corporate networking.
- Define a new DHCP Scope.
- Edit DNS preferences for Enterprise connector FQDN

Once Enterprise connector is installed, it acts as a gateway to secure the connection between cloud environment and on-premise infrastructure. Then, it is only needed to provide LDAP server connection data in EMM core admin portal.

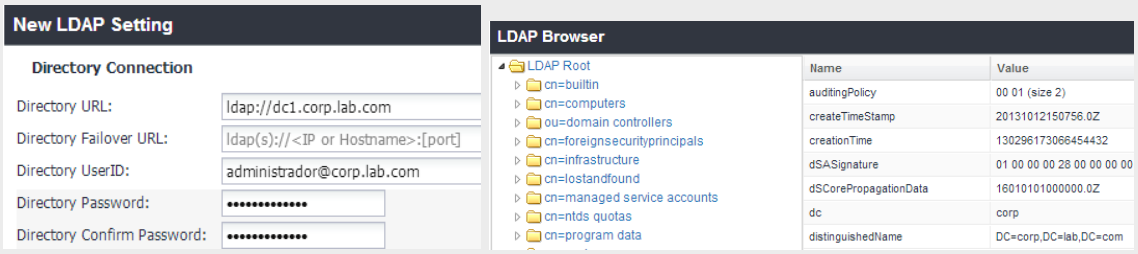


Figure 4.17. LDAP integration settings

Once the data has been provided and you can reach LDAP tree from EMM core admin portal, in order to test connectivity some LDAP users can be added and, if all works fine, the settings can be saved.

Finally, LDAP server data and sync state can be seen from admin portal.

URL	Identity	Domain	State
ldap://dc1.corp.lab.com	administrador@corp.lab.com	corp.lab.com	Enabled

Figure 4.18. LDAP server in EMM core

4.1.11.2. Email integration

Lab Case 15: In our case, an exchange online email service has been used so, first of all an account setup has been needed [Annex 10.4].

Once the email service is running, to provide an email control policy, Email gateway should be added to the EMM Core before.

In EMM admin portal, the main information that should be provided during configuration is: Email gateway IP and port, type of gateway, authentication details and attachment control parameters. For Exchange email service, the server is a generic one “m.outlook.com”.

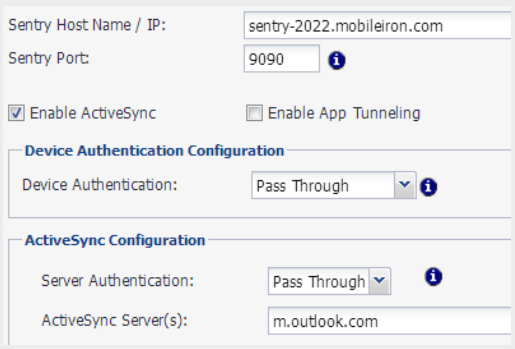
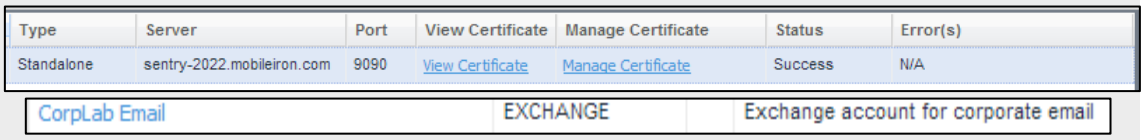


Figure 4.19. Email Gateway configuration details

Once the Email Gateway has been added correctly, EMM Core will show gateway data and connection status. After Email gateway is operative, the email policy configured at [4.1.8] can be used to control email.



Type	Server	Port	View Certificate	Manage Certificate	Status	Error(s)
Standalone	sentry-2022.mobileiron.com	9090	View Certificate	Manage Certificate	Success	N/A

CorpLab Email	EXCHANGE	Exchange account for corporate email

Figure 4.20. Configured email gateway

4.1.11.3. PKI and certificates integration

There are three main uses for certificates in a EMMS:

- Establish secure communications,
- Encrypt payloads
- Authenticate users.

[Figure 4.21] shows where each of the certificates exists in the EMMS architecture.

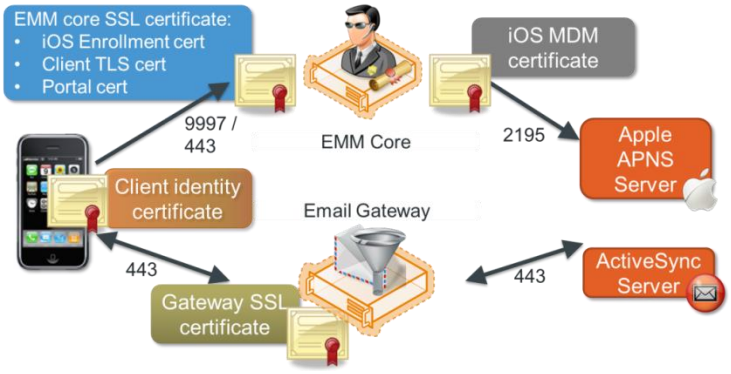


Figure 4.21. Certificates use in EMMS

- The EMM Core SSL certificate is used for many functions: securing communications between devices and the EMM Core (Client TLS and admin portal) and singing iOS payload.
- The iOS MDM certificate secures the communications between the EMM Core and the APNS Server, and between the APNS with the devices.
- The Email Gateway SSL certificate is used to secure the mail delivery.
- The Client identity certificate is used to authenticate the user for services such as email, VPN or Wi-Fi.

When using client identity certificates they are deployed using SCEP configurations. For SCEP the EMM platform supports an on-board CA with a self-signed certificate, intermediate subordinate CA certificate, Microsoft NDES as well as third party hosted PKI systems.

Lab Case 16: The following certificates are present in our Lab environment:

- Cloud infrastructure (EMM Core and Email gateway) SSL certificates.

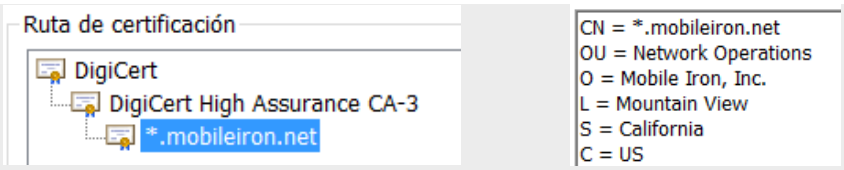


Figure 4.22. EMM Core and Gateway certificate

- iOS MDM certificate, which has been issued and uploaded in [4.1.4].
- User identity certificates are also used, but deserve an especial mention.

For user certificates issue, it has been necessary to build a basic Public Key Infrastructure in on-premise laboratory which acts as a corporate PKI would do. Moreover, in order to automate certificates issue for mobile devices, SCEP service has been setup. As SCEP service is designed for computer certificates request, other custom modifications have been required before it works. The main steps have been (full installation and configuration steps in [Annex 9.3.4 and Annex 9.3.5]):

- Install a web server and configure a basic PKI role (CA).
- Create users for SCEP service and configure the role.
- Modify web server max request length in order that mobile devices can make requests.
- Create a custom certificate for mobile devices and publish it to CA.
- Change SCEP default template to be compliance with mobile devices requirements.

4.1.11.4. Verifying all services work well

With the aim of check that all the services are running in the correct way, a verify process from admin portal can be done.

Service	Date	Status	Message
LDAP	2013-11-22 21:46:16	Success	LDAP server ldap://dc1.corp.lab.com is reachable. --Reachable via connector conector.
SENTRY	2013-11-22 21:46:18	Success	No Integrated Sentry server(s) configured. Standalone Sentry sentry-2022.mobileiron.com is reachable. + ActiveSync server: m.outlook.com:443 is reachable
CONNECTOR	2013-11-22 21:46:18	Success	Connector conector is reachable. --Status: Connector is Connected - it is healthy and is ready to receive work orders

Figure 4.23. Corporate services status dashboard

If LDAP, Email gateway and Connector are running the results will show a “Success” status.

4.2. Phase IV: Rollout

This section is intended to provide the main guidelines that any rollout should follow. A successful EMM program is rolled out in phases to manage and adjust the original deployment processes and documents to real conditions.

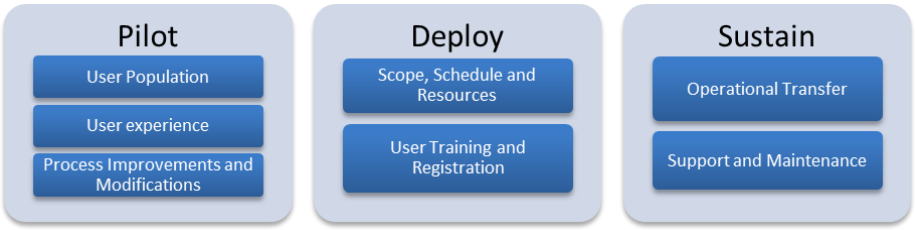


Figure 4.24. Rollout Phases

The production deployment begins after the technical infrastructure has been built, tested and approved. Rolling out to live users allows IT to validate assumptions, streamline processes, improve documentation and identify gaps in the deployment planning. The following phases describe a typical rollout of an EMM program.

4.2.1. Pilot

The pilot is a production test to verify that the infrastructure, documentation, registration and support processes are valid and functional before deployment to the general user population. It is an opportunity to collect user feedback to identify what is working fine and what requires modifications.

4.2.1.1. User Population

The pilot population should be a reflection of the overall user base. In fact, would be better that it will contain most business users to get an understanding of a normal user experience. Also a small number of operations staff should also be included to identify issues that may be overlooked by the general population and to provide a technical point of view.

4.2.1.2. User Experience

In order to know users feedback, surveys are an effective tool. They are used to capture metrics, determine business value, identify costs and discover devices. There are three basic surveys:

- Pre-deployment survey: Baseline for user metrics before registration and used to demonstrate business value and improvements as the rollout progresses.
- Registration Survey: Identify breakdowns in workflows and those steps in the documentation that are unclear or incorrect.
- Closing Survey: Collect information about user experience ratings, whether expectations were met and what improvements are needed.

4.2.1.1. Process Improvements and Modifications

Once surveys are analysed, the feedback during the pilot should be translated in adjustments and improvements to the production system before the general deployment phase. Troubleshooting and escalation procedures often need several iterations of improvements before offer a consistent level of service.

4.2.2. Deploy

Once the pilot has been completed and user registration and support processes have been updated and tested, the production rollout phase can begin. The Deploy is the ultimate production step, where all the goodness or badness of previous work will be reflected

4.2.2.1. Scope, Schedule and Resources

Usually deployment is setup in phases, whether by geography, business unit or job function. In this sense, the resources available for each phase should be matched with the number of users being deployed. Another advantage of the phased approach is to identify any impacts on performance and availability of the mobile infrastructure as well as connected downstream and interrelated services.

4.2.2.2. User Training and Registration

One of the most important pre-requisites for user deployments is effective user training before registration into the program. It saves time, aggravation, cost, help desk incidents and phone calls. Training can be done in person, online, via computer-based courses or with written documentation. It must address user's questions and concerns, and provide resources and guides for resolving problems when they occur.

4.2.3. Sustain

After the deployment, It is needed to ensure the correct behaviour in daily work.

4.2.3.1. Operational Transfer

This step normally involves a transfer of ownership of the service from IT to support team. Activities required include: knowledge transfer, documentation reviews, help desk procedures development, support and escalation process design, and a knowledgebase creation. This process can be quite rigorous and labour intensive, especially when transitioning to outsourced or third party support centres.

4.2.3.2. Support and Maintenance

Most questions and help desk incidents center on a set of issues that account for the majority of user requests and problems. Answers and resources should be available to quickly solve repetitive problems, such as email or password problems. Many incidents can be resolved with minimal effort on the part of the user without help desk involvement.

Although an initial support requirements have been captured during the pilot, the production help desk statistics will provide real time data on where users are having the most problems. This information should be used as feedback for the user training programs, which must be kept updated with most prevalent issues and questions in order to anticipate support incidents.

CHAPTER 5. CONCLUSIONS

Once at the end of this thesis, and after reflecting on the different premises initially proposed and those that have been presented during the performance of the project, it is time to highlight those aspects, ideas and answers assimilated.

5.1. About the study of enterprise mobility and why is needed to manage it

From the study of enterprise mobility, it has been found that the growing popularity of consumer computing, or consumerization of technology, represents an inflection point for the way business is done.

This fact for IT has resulted in legions of employees going armed with all kinds of devices, ready to storm the stronghold that once had been a completely controlled environment.

Few years ago, corporate environments were clearly ahead of personal environments, but this phenomenon has been completely reversed. Every day more people for who use corporate devices for work instead personal ones supposed to evoke the past or an inefficient duplication abound.

Obviously, this fact brings with it a whole set of problems (Bring Your Own Disaster). Manage a heterogeneous group of devices means leave to use shared management policies, increase support and maintenance needs, add an unknown number of security vulnerabilities, etc. Therefore it is an imperative need to manage these new devices from an Enterprise Mobility Management solution.

Companies have much benefits to gain from learn how to develop their activities in a mobility ecosystem, where diversity is increasing because each employee will use the device which make him more productive.

5.2. About the business mobility analysis and the definition of an EMM strategy

This situation can be approached as a terrible problem that needs “discipline” or as an opportunity to enhance the functions that each mobility role develops.

During the execution of this project has reached the conclusion that instead of manifesting an attitude of resistance to this phenomenon, it is better to adopt a constructive and collaborative thinking, of serving an employee whose needs

and habits are constantly evolving. It is the first step towards the definition of an Enterprise Mobility Management strategy.

Starting from this premise, the following steps go through guide mobility towards productivity and improving the user experience, without losing sight of aspects such as cost control, security and IT systems governance. This balance is no different than others subject to IT for years. The difference between now and then lies in most learned and motivated employees, and simpler products.

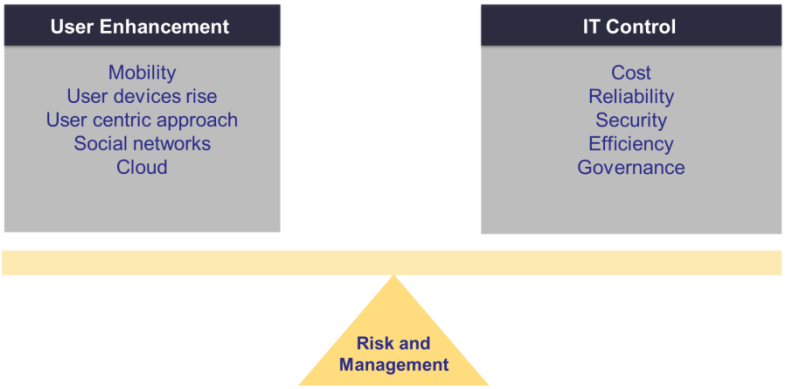


Figure 5.1. Balance between user experience and IT control

Therefore to define the EMM program, it is necessary to analyze the company and its business, having business units forwarding to IT how they consume, create, collaborate and communicate with their activities in order to respond to their mobility needs. To do this a whole series of meetings, questionnaires and analysis to define mobility requirements and focus the target audience is essential.

Also this results in the definition of an EMM board that drives the program and which is formed by a set of employee who know both IT and business systems.

Some Issues that are essential for the design of the EMM solution are: Define mobility roles according employee functions, provide the appropriate device type to the task performed, define corporate policies to enforce, select an EMMS which satisfies real needs and allow obtain a ROI in short to medium term and define the requirements for integrate the solution with corporate services, enhancing users to be completely productive in mobility conditions.

The final goal should be to evolve to a work platform where systems are provisioned and managed dynamically, and where the agility setting up services allow to anticipate business needs. This will require an efficient, dynamic and highly managed EMM platform that allows access to applications and services at any time, from anywhere and from any mobile device.

5.3. About the Enterprise Mobility Management System and its performance

As discussed, manage a heterogeneous device platform is a big management, maintenance and support challenge. It is therefore essential to identify that Enterprise Mobility Management System which best adapt to the needs

required, if necessary making a deep comparison between the different options on the market.

EMM solutions must be able to keep under control the device and its contents during the whole life cycle, from delivery to withdrawal. To do EMMS capabilities must include Mobile Device Management, Mobile Application Management and Mobile Content Management. But in particular, those characteristics that define the top EMMS are: multi-OS management of mobile devices, advanced security features, access control to corporate email, data leak prevention, safe navigation, simple and centralized management, user self-provision of applications and access control to corporate repositories.

These systems by themselves suppose incremental improvements to the management and security, but are not relevant at the level of productivity and efficiency until its integration with corporate services. This is definitely the “leitmotiv” of this type of solutions. But this part also is the most difficult because when many systems currently on the companies was implanted, not taken into account its use in other conditions different from the traditional PC.

Technically, not only issues related to the installation and configuration of EMMS has been addressed, also has been necessary to create a lab environment with corporate services in order to implement the proposed solution. A virtualization hypervisor over a PC has been used. Over it have been installed a corporate directory, a web server and a Public Key Infrastructure with SCEP service. This also entails the creation of virtual machines, install operating systems and roles as well as server, network and firewall configurations to ensure the appropriate behavior with mobile devices.

Finally, once the system is operational and tested, it was considered essential to define delivery procedures of devices and support processes for most common tasks. To have these processes defined will be very important during the first months of program deployment.

5.4. Last comments

Personally, the achievement of this project has been a great challenge, because not only was part of my academic path towards obtaining the Master, it also has been the top step to acquire a job. Despite this, it has been highly gratifying to see how during the project making, many of the skills acquired in the last two years have been very helpful in face the challenges that arose.

The thesis not only contains the theoretical exposition of ideas, trends and protocols studied. It also contains an important load of practical fieldwork, where many of the courses taken during the Master are reflected in some way.

To conclude, I hope that this work has satisfied the expectations created before reading and has contribute, in some way, to increase the knowledge on enterprise mobility management of the reader.

David Arance García
November 2013

CHAPTER 6. REFERENCES AND BIBLIOGRAPHY

[1] D. J. Sharony, «Enterprise Mobility: Empowering the Mobile Workforce,» January 2012. [En línea]. Available: http://www.mobiusconsulting.com/papers/EnterpriseMobility-MobiusConsulting-9-23-09.pdf. [Último acceso: May 2013].

[2] Gartner, «Bring your Own Device (BYOD): Mobility Trends and Securing the Transition,» 15 January 2013. [En línea]. Available: http://www.gartner.com/it/content/2272200/2272223/january_15_bring_your_own_decive_lpingree.pdf?userId=57601660. [Último acceso: May 2013].

[3] Consumer Electronics Association (CEA), «Mobile Devices Lead Electronics Purchases, Finds CEA's Annual Ownership Study,» CEA, 22 April 2013. [En línea]. Available: http://www.ce.org/News/News-Releases/Press-Releases/2013-Press-Releases/Mobile-Devices-Lead-Electronics-Purchases,-Finds-C.aspx. [Último acceso: June 2013].

[4] «What is IT consumerization (information technology consumerization),» TechTarget, 7 November 2011. [En línea]. Available: http://searchconsumerization.techtarget.com/definition/IT-consumerization-information-technology-consumerization. [Último acceso: May 2013].

[5] IDC, «Tablet Shipments Forecast to Top Total PC Shipments in the Fourth Quarter of 2013 and Annually by 2015, According to IDC,» IDC, 11 September 2013. [En línea]. Available: http://www.idc.com/getdoc.jsp?containerId=prUS24314413. [Último acceso: October 2013].

[6] I. Wigmore, «What is Bring Your Own Device (BYOD),» TechTarget, October 2012. [En línea]. Available: http://whatis.techtarget.com/definition/BYOD-bring-your-own-device. [Último acceso: May 2013].

[7] C. Steele, «What is COPE (corporate-owned, personally-enabled),» TechTarget, June 2013. [En línea]. Available: http://searchconsumerization.techtarget.com/definition/COPE-corporate-owned-personally-enabled. [Último acceso: Agust 2013].

[8] G. C. M. D. M. D. K. K. E. M. J. S. E. S. C. W. Paul DeBeasi, «Enterprise Mobility and Its Impact on IT. Gartner, ID Number: G00233483,» 16th April 2012. [En línea]. Available: http://www.gartner.com/resources/233400/233483/enterprise_mobility_and_its__233483.pdf. [Último acceso: marzo 2013].

[9] M. Rouse, «What is Enterprise mobile management,» TechTarget, 4 April 2013. [En línea]. Available: http://searchconsumerization.techtarget.com/definition/enterprise-mobility-management-EMM. [Último acceso: May 2013].

[10] Wikipedia, «Enterprise mobility management,» 17 September 2013. [En línea]. Available: http://en.wikipedia.org/wiki/Enterprise_mobility_management. [Último acceso: 6th October 2013].

[11] I. Citrix Systens, «Citrix Knowledge Center: Mobility Solutions,» December 2012. [En línea]. Available: http://support.citrix.com/proddocs/topic/cloudgateway/xmob-landing-con.html. [Último acceso: may 2013].

[12] M. Basso, «Gartner. Hype Cycle for Wireless Devices, Software and Services, 2013,» 31 July 2013. [En línea]. [Último acceso: Agost 2013].

[13] M. Rouse, «What is Mobile Device Management,» TechTarget, June 2013. [En línea]. Available: http://searchmobilecomputing.techtarget.com/definition/mobile-device-management. [Último acceso: Agost 2013].

[14] J. G. T. C. M. B. Phillip Redman, «Gartner. Magic Quadrant for Mobile Device Management software 2013,» 23 May 2013. [En línea]. [Último acceso: May 2013].

[15] M. Rouse, «What is Mobile Application Management (MAM),» TechTarget, 15 June 2012. [En línea]. Available: http://searchconsumerization.techtarget.com/definition/mobile-application-management. [Último acceso: June 2013].

[16] M. Rouse, «What is Mobile Information Management (MIM),» TechTarget, 7 May 2013. [En línea]. Available: http://searchconsumerization.techtarget.com/definition/mobile-information-management-MIM. [Último acceso: June 2013].

[17] IDC, «Worldwide Mobile Phone Market Forecast to Grow 7.3% in 2013 Driven by 1 Billion Smartphone Shipments, According to IDC,» IDC, 4 September 2013. [En línea]. Available: http://www.idc.com/getdoc.jsp?containerId=prUS24302813. [Último acceso: October 2013].

[18] IDC, «IDC Worldwide Quarterly Tablet Tracker,» March 2013. [En línea]. Available: http://www.idc.com/getdoc.jsp?containerId=prUS24002213. [Último acceso: October 2013].

[19] IDC, «IDC. Worldwide Mobile Phone Tracker,» 25 July 2013. [En línea]. Available: http://www.idc.com/getdoc.jsp?containerId=prUS24239313. [Último acceso: October 2013].

[20] Android, «Android Developers. Platform version dashboard,» Android, 2 October 2013. [En línea]. Available: http://developer.android.com/about/dashboards/index.html. [Último acceso: October 2013].

[21] Mixpanel, «Mixpanel trends. iOS7 Adoption.,» October 2013. [En línea]. Available: https://mixpanel.com/trends/#report/ios_7. [Último acceso: October 2013].

[22] Good Technology, «Good Technology Mobility Index Report Q2 and Q3 2013,» October 2013. [En línea]. Available: http://media.www1.good.com/documents/Good-Q2-Q3-2013-Device-Activations.pdf. [Último acceso: October 2013].

[23] J. G. L.-O. W. Phillip Redman, «Gartner. Magic Quadrant for Mobile Device Management software 2011,» 13 April 2011. [En línea]. [Último acceso: May 2013].

[24] J. G. M. B. Phillip Redman, «Gartner. Magic Quadrant for Mobile Device Management software 2012,» 17 May 2012. [En línea]. [Último acceso: May 2013].

[25] M. Basso, «Gartner. Hype Cycle for Wireless Devices, Software and Services, 2013,» 31 July 2013. [En línea]. Available: http://www.gartner.com. [Último acceso: August 2013].

[26] B. T. Monica Basso, «Gartner. IT Market Clock for Enterprise Mobility, 2013,» 6 September 2013. [En línea]. Available: http://www.gartner.com. [Último acceso: October 2013].

[27] IDC, «IDC. Worldwide Tablet Tracker,» 30 October 2013. [En línea]. Available: http://www.idc.com/getdoc.jsp?containerId=prUS24420613. [Último acceso: November 2013].

[28] Intrepidus Group, Inc., «The iOS MDM Protocol,» 3 August 2011. [En línea]. Available: http://media.blackhat.com/bh-us-11/Schuetz/BH_US_11_Schuetz_InsideAppleMDM_WP.pdf. [Último acceso: May 2013].

[29] Apple Inc., «Configuration Profile Reference,» 22 October 2013. [En línea]. Available: https://developer.apple.com/. [Último acceso: October 2013].

[30] Apple Inc., «Over-the-Air Profile Delivery and Configuration,» August 2010. [En línea]. Available: https://developer.apple.com/. [Último acceso: May 2013].

[31] MobileIron Corp., «Choosing Which Android Devices to Support,» 21 May 2013. [En línea]. Available: https://mobileiron-support.force.com. [Último acceso: September 2013].

[32] Samsung Electronics Co., «Samsung For Enterprise,» January 2013. [En línea]. Available: http://www.samsung.com/us/business/samsung-for-enterprise. [Último acceso: July 2013].

[33] Samsung Corp., «White Paper : An Overview of Samsung KNOX™,» June 2013. [En línea]. Available: http://www.samsung.com/global/business/business-images/resource/white-paper/2013/06/Samsung_KNOX_whitepaper_June-0.pdf. [Último acceso: September 2013].

[34] Microsoft Corp., «Microsoft SCEP implementation whitepaper,» Agust 2009. [En línea]. Available: http://www.microsoft.com/en-us/download/details.aspx?id=1607. [Último acceso: May 2013].

[35] MobileIron, «Connected Cloud Admin Guide,» November 2013. [En línea]. Available: http://support.mobileiron.com. [Último acceso: November 2013].

[36] Gartner, «Forecast: Mobile Devices by open operating system, worldwide, 2009-2016,» July 2012. [En línea]. Available: http://www.gartner.com/it/content/2272200/2272223/january_15_bring_your_own_decive_lpingree.pdf?userId=57601660. [Último acceso: July 2013].

[37] OpenSignal, «Android Fragmentation Visualized,» August 2012. [En línea]. Available: http://opensignal.com/reports/fragmentation.php. [Último acceso: May 2013].

Other Bibliography

- Gartner. Checklist for Determining Enterprise Readiness to Support Employee-Owned Devices, Published: 18 June 2012, Analyst(s): Andy Rowsell-Jones, Nick Jones
- Airwatch inc., AirWatch Samsung Platform Guide, 2013.
- US Government. Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs, August 23, 2012.
- Apple Inc. iOS Security, May 2012.
- Australian Government, DoD. iOS 5 Hardening Guide, March 2012.
- NIST. Guidelines for managing and securing mobile devices in enterprises (Draft), July 2012.
- Apple Inc. Local and Push Notification Programming Guide, 2011.
- Samsung electronics Co. Samsung For Enterprise, SAFE. 2013.
- Samsung electronics Co. Samsung KNOX whitepaper, June 2013.
- General Dynamics C4 Systems. Assertion Framework for BYOD.
- Gartner. Seven Steps to Planning and Developing a Superior Mobile Device Policy, ID:225405, 2012.
- Gartner. iPad and Beyond - The Media Tablet in Business ID:211735
- Gartner. iPad and Beyond - Top 10 Business Applications for Tablets
- Gartner. iPads and Beyond - What the Future of Computing Holds
- Gartner. iPhone and iPad Security Assessment ID: 233334
- Gartner. Support Apple and BYOD With Application Design and Delivery Practices That Isolate the IT Infrastructure ID: 238821
- Gartner. The Impact of App Stores on Your Application Strategy ID: 213351

CHAPTER 7. GLOSSARY

BYOD
- Bring your own device (BYOD) is an alternative strategy allowing employees, business partners and other users to utilize a personally selected and purchased client device to execute enterprise applications and access data.

COPE
- Corporate-Owned Personally-Enabled, is a business model in which an organization provides its employees with mobile computing devices and allows the employees to use them as if they were personally-owned notebook computers, tablets or smartphones

EMM
- Enterprise Mobility Management, is the set of people, processes and technology focused on managing the increasing array of mobile devices and related services to enable the use of mobile computing in a business context

EMMS
- Enterprise Mobility Management System, systems designed to reduce the IT labor needed to support broad mobile device use in the enterprise

PKI
- Public-key infrastructure (PKI) was developed mainly to support secure information exchanges over unsecure networks. It has been used to ensure that the person identified as sending a transaction is the originator, that the person receiving the transaction is the intended recipient and that the transaction data has not been compromised.

SCEP
- Simple Certificate Enrollment Protocol, used to handling certificates for large-scale implementation

NDES
- Microsoft SCEP protocol

PC
- Personal computer, PCs are are what most of us use on a daily basis for work or personal use. A typical PC includes a system unit, monitor, keyboard, and mouse.

MDM
- Mobile device management (MDM) includes software that provides the following functions: software distribution, policy management, inventory management, security management and service management for smartphones and media tablets.

MAM
- Mobile Application Management, is the delivery and administration of enterprise software to end users' corporate and personal mobile devices.

MCM
- Mobile Content management, is a device-agnostic security strategy that involves keeping sensitive data in an isolated container, encrypted and allowing only authenticated users to access or transmit it.

PDA
- Personal Digital Assistant, Data-centric handheld computer weighing less than 1 pound that is designed primarily for use with both hands.

VPN
- A virtual private network (VPN) is a system that delivers enterprise-focused communication services on a shared public network infrastructure and provides customized operating characteristics uniformly and universally across an enterprise.

LAN
- Local-Area Network, a geographically limited communication network that connects users within a defined area.

WLAN
- Wireless Local-Area Network (WLAN) is a LAN communication technology in which radio, microwave or infrared links take the place of physical cables.

GPS	▪ Global Positioning System, is a global positioning technology that was introduced in the U.S. in 1996, and was originally developed for military purposes.
VPP	▪ Volume Purchase Program, is a enterprise tool for buy large number of applications and manage them.
OS	▪ Operative System
HTML	▪ Hypertext Markup Language, A document-formatting language derived from the Standard Generalized Markup Language (SGML), predominately used to create Web pages.
IT	▪ Information Technology department
DMZ	▪ Demilitarized Zone is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet
SIM	▪ Subscriber Identity Module Card, Programmable smart card in a mobile device that gives access to a network.
LDAP	▪ Lightweight Directory Access Protocol, A server-to-server interface for directory information exchange among directories, devised as a low-cost, simpler implementation of the X.500 Directory Access Protocol.
CSR	▪ Certificate Signing Request is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate.
CSV	▪ Comma Separated Values, Contains data sets separated by commas, where each new line represents a new row; values can be organized into cells by a spreadsheet program or inserted into a database
TCP	▪ TCP/IP (Transmission Control Protocol/Internet Protocol), A set of protocols covering (approximately) the network and transport layers of the seven-layer Open Systems Interconnection (OSI) network model.
DHCP	▪ Dynamic Host Configuration Protocol." A network server uses this protocol to dynamically assign IP addresses to networked computers.
DNS	▪ Domain Name System, used to translate formal nouns of resources to Ips
CA	▪ certification authority (CA) is an internal or third-party entity that creates, signs and revokes digital certificates that bind public keys to user identities.
IP Address	▪ is a code made up of numbers separated by three dots that identifies a particular computer on the Internet.

Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels

UNIVERSITAT POLITÈCNICA DE CATALUNYA

ANNEXOS

TITLE: Study, analysis and implementation of an Enterprise Mobility Management system

MASTER DEGREE: Master in Science in Telecommunication Engineering & Management

AUTHOR: David Arance García

DIRECTOR: Roc Meseguer Pallares

SUPERVISOR:

DATE: November 8th 2013

ANNEXES SUMMARY

Figures Index

Tables Index

ANNEX 1. MARKET STUDY

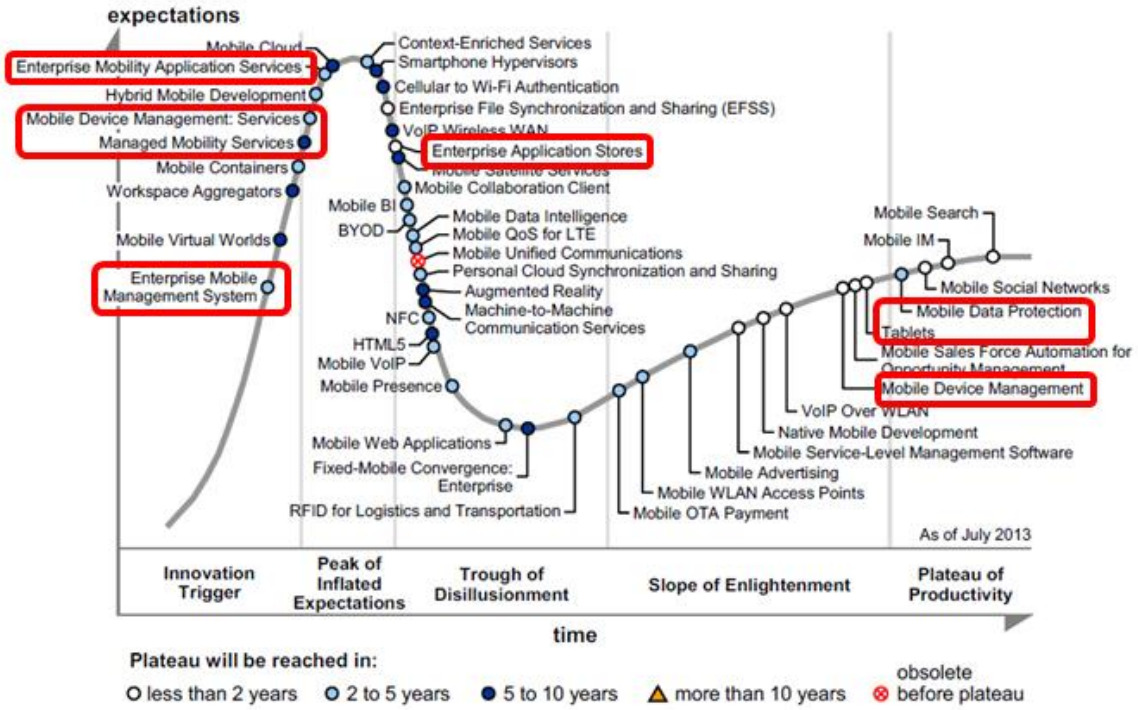
Annex 1.1. Maturity level and expectations about EMMS

In order to evaluate the maturity level and market expectations around EMMS, Gartner Hype Cycle and Market Clock for mobility will be consulted. This analysis helps us to ensure a short-term return of investment (ROI) by:

- If now is the opportune moment for make an inversion in one of these tools according to market standardization, number of suppliers, expertise of skills.
- If EMMS reports us a real competitive advantage or in contrast, will be a cost hole where we spent time and money without benefits.

To understand the performance of these two graphics, some indications are explained below:

- In Hype cycle, there are 3 variables: X-axis express evolution in time, since innovation to plateau of productivity (standardization). Y-axis expresses the level of expectation that this technology arouses. The bullet colours express the speed which this technology takes from its actual position to the plateau productivity.
- In Market Clock, there are 3 variables: Clock position expresses the useful market life (Adventatge, cost, choice, retirement). Clock radial distance expresses the level of commoditization (Standarization, number of suppliers, expertise.). The bullet colours express the time which this technology takes from its actual position to the next stage.



Annex Fig. 1 HypeCycle for Wireless Devices, Software & Services 2013 [25]

Annex Fig. 2. Market Clock for Wireless Devices, Software Services 2013 [26]

According to Previous diagrams, we can assume:

- Tablets: Is a Transformational technology. Enhance customer interactions and workforce productivity through media tablets and apps. Requires support for consumer and personal media tablets.
- Secure corporate email: Is a requirement. Needs products or services that allow you to protect corporate email on personal devices.
- Enterprise Application Store: Is a requirement in a MDM/EMM vendor selections and investments. Enhance user experience and productivity.
- Mobile Containers: Is a requirement in a MDM/EMM vendor selections and investments. Secure and control corporate data and apps.
- Enterprise Mobility Management: Is a point of innovation that starts to create some expectations. During next year EMM requirements should be considered in MDM offerings.
- Mobile Device Management: "If you don't have it, you're late". Replacement in 2-5 years by EMM solutions.

As a conclusion, we can say that according market expectations the Enterprise Mobility Management Systems can fulfil an important missing role during the next 2-5 years. We can assume that EMMS will be perceived as:

- An innovation point which substitute actual MDM-only solutions.
- A mobile-business enabler tool which provides support for transformational elements like tablets.

A solution for secure corporate information access, like email, and prevent data loss.

Annex 1.2. About Device manufacturers and Operative Systems

Google's Android operating system is dominating mobile operating systems shipments according to both Gartner and IDC and will continue to lead the market through 2017. The Tab1 shows a IDC's analysis where 75,3% of all smartphones and 48.8% of all tablets runs the Android operating system in 2013.

Looking to 2017, the trend in smartphone market is that Windows Phone grows up to 6% at expenses of Android devices. On the other hand, in tablet market Windows Phone devices also increase 5%, but now in detriment of two major players equally.

Annex Tab. 1 Top Smartphone and Tablets Operating Systems, Forecast Market Share and CAGR, 2013–2017 [17] [18]

OS	2013 Smartphone Market Share	2017 Smartphone Market Share	2013 Tablet Market Share	2017 Tablet Market Share
Android	75.3%	68.3%	48.8%	46.0%
iOS	16.9%	17.9%	46.0%	43.5%
Windows Phone	3.9%	10.2%	2.8%	7.4%
BlackBerry OS	2.7%	1.7%	1.9%	2.7%
Others	1.2%	1.9%	0.6%	0.4%
Totals	100.0%	100.0%	100.0%	100.0%

In case of top manufacturers, as shows Tab 1, Samsung leads the smartphone market with the 30,4% of total devices, while Apple's tablets has the 29,6% of this market.

Also is important to remark that the trend is that other minor players like Lenovo, Huawei and Acer grows in both market shares.

Annex Tab. 2Top Five Smartphone and Tablet Vendors, Shipments, and Market Share, 2013 Q2 (Units in Millions) [19] [27]

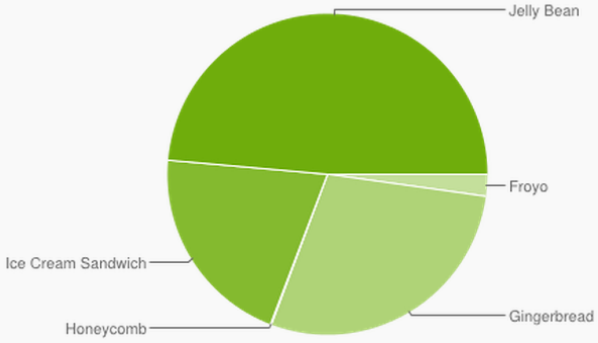
Vendor	2Q13 Unit Shipments	2Q13 Market Share	Vendor	3Q13 Unit Shipments	3Q13 Market Share
Samsung	72.4	30.4%	**Apple**	14.1	29.6%
Apple	31.2	13.1%	**Samsung**	9.7	20.4%
LG	12.1	5.1%	**Asus**	3.5	7.4%
Lenovo	11.3	4.7%	**Lenovo**	2.3	4.8%
ZTE	10.1	4.2%	**Acer**	1.2	2.5%
Others	100.8	42.4%	**Others**	16.8	35.3%
Total	237.9	100.0%	**Total**	47.6	100.0%

Annex 1.2.1. The Android market fragmentation

The main issue of Android is the fragmentation of operative system versions and feature differences depending on vendor choice.

In the case of operative system, only a 46,8% of total Android devices runs Jelly bean. Take into account that the first release was released at July 2012, we can say that the adoption rate is too slow. More worrying is the fact that almost 30% of devices run a 2-3 years old versions.

Version	Codename	API	Distribution
2.2	Froyo	8	2.2%
2.3.3 - 2.3.7	Gingerbread	10	28.5%
3.2	Honeycomb	13	0.1%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	20.6%
4.1.x	Jelly Bean	16	36.5%
4.2.x		17	10.6%
4.3		18	1.5%



Data collected during a 7-day period ending on October 2, 2013.

Annex Fig. 3 Android versions distribution. [20]

This issue also applies to screen resolution and pixel density, making that apps behaviour and user experience change from device to device.

These data can't be comparable with iOS versions distribution, with a 65~75% of the devices at 7.x versions in 2 months, and only a ~6% under 6.x version.

For the screen resolution and pixel density in iOS environment only are 2 types, Retina display (~77%) and non-retina display (~23). [21]

Annex Tab. 3. Top Android Smartphone Vendors, Shipments, and Market Share, Q2 2013 (Units in Millions)

Vendor	2Q13 Unit Shipments	2Q13 Market Share	2Q12 Unit Shipments	2Q12 Market Share	Year-over-Year Change
Samsung	73.3	39.1%	48	44.4%	52.7%
LG	12.1	6.5%	5.8	5.4%	108.6%
Lenovo	11.4	6.1%	4.9	4.5%	132.7%
Huawei	10.2	5.4%	6.5	6.0%	56.9%
ZTE	10.2	5.4%	6.4	5.9%	59.4%
Others	70.2	37.5%	36.4	33.7%	92.9%
Total	187.4	100.0%	108.0	100.0%	73.5%

According [**¡Error! No se encuentra el origen de la referencia.**] Samsung represents the ~42% of the total android market. Its phones represented 59% of the phones in our overall sample of Android phones, and its tablets represented 42% of the tablets.

Annex 1.2.2. The business market

In the enterprise, tablets are being widely adopted on a scale that is having a deep impact on conventional PC sales. Additionally, the strength of Apple's iOS platform is also bolstering tablets, which are used primarily to run apps, as opposed to phones, which can be functionally used just for making phone calls and checking messages. [22]

Annex Tab. 4 Total device activations in enterprise Q2 & Q3 [22]

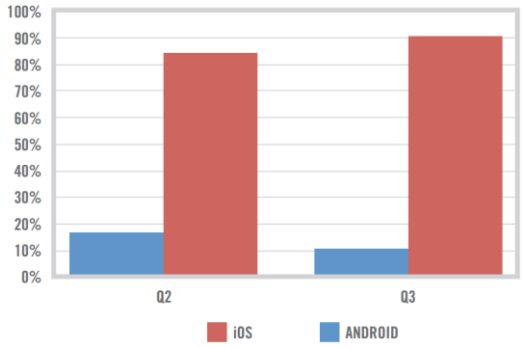
OS	3Q13			2Q13		
	Smartphone	Tablet	Total	Smartphone	Tablet	Total
iOS	51%	21%	72%	48%	21%	69%
Android	25%	2%	27%	27%	3%	30%
Windows Phone	-	-	~1%	-	-	~1%

Another differentiating factor of Apple's success among enterprise users relates to hardware. While Android has been very successful in powering smartphones, it has not been able to stoke strong sales of tablets. That's particularly evident in the enterpris

In Q3, 90% of total tablet activations were iOS. While Android dipped back from 16% to 10% percent.

One explanation for why Apple leads among business users' devices involves custom application development.

While Android is gaining enterprise market share (21% to 27%) on the device side, iOS dominates as platform of choice for enterprise app deployment, with more than 95% of total app activations.



Annex Fig. 4 Total tablet activations rate in Enterprise in 3Q2013. [22]

Annex 1.3. About Enterprise Mobility Management Systems

As has been explained in previous sections, the EMMS are MDM solutions with advanced features. So, in order to identify the market leaders, we should to consult global IT analyst opinions about MDM vendors.

Annex Fig. 5 Magic Quadrant for MDM Software 2011-2013. [23] [24] [14]

To understand the performance of this graphic, some indications are explained below:

- X-axis represents the vendors' "completeness of vision". This means the technological purpose to short and long term.
- Y-axis represents de vendors' ability to execute its purpose. How well it works.

According to previous figures, since 2011 the number of vendors and its distribution has changed a lot; however, the major players are almost the same. This implies that the strategy of these vendors follows the real market needs and also a major expertise than the rest.

The most valuable vendors for 2013 are Airwatch, Citrix and MobileIron. The following table shows a summary of main strengths and cautions about EMM leaders. [14]

Annex Tab. 5 Gartner: MDM software Strengths and Cautions [14]

Vendor	Strengths	Cautions
Airwatch	▪ Supports containerization of corporate email, browsing, content and applications. ▪ Supports multiple users per device. ▪ Secure file sync and sharing, and application access ▪ Aggressive pricing	▪ Negative feedback experiences regarding implementation and postsales technical support. ▪ Containerization is not equally supported across OS. ▪ Limited executive team. ▪ Low Market visibility (no community).
Citrix	▪ Executive leadership team. ▪ Deep understanding of remote access and mobility needs. ▪ Integrated product solution.with secure containers for smartphones, ▪ tablets, Macs and PCs.	▪ Cloud-first product. ▪ Purchased in two forms:MDM only or all EMM Suite. ▪ Not have a strong consumerization play and nor have small or midsize business (SMB) offering.
MobileIron	▪ Strong vision of EMM, and has executed well in terms of product development, launches and support. ▪ Beyond simple policy management ▪ Usually first to market with an integrated solution focused on EMM. ▪ Proved management, scaling and financial viability	▪ On-premise appliance strength, need strongest cloud version. ▪ Complains with level 1 support made for partners (not mobileiron). But has taken back Level 1 support and has seen increased customer satisfaction.

ANNEX 2. PHASE 1 MEETING MINUTES

Annex 2.1. Kick-off meeting

<table>
<tr><td colspan="4">Enterprise Mobility Management Program</td></tr>
<tr><td>Convocats</td><td>▪ Executive Manager [EM]
▪ Project manager [PM]
▪ App leader [AL]
▪ Telecomunications leader [TL]
▪ Security leader [SL]
▪ everis</td><td>Assistents</td><td>▪ Executive Manager [EM]
▪ Project manager [PM]
▪ App leader [AL]
▪ Telecomunications leader [TL]
▪ Security leader [SL]
▪ everis</td></tr>
<tr><td>Data:</td><td colspan="3">4 de març de 2013</td></tr>
<tr><td colspan="4">EMM program – Meeting minutes Kick-Off</td></tr>
<tr><td colspan="4">▪ TL pregunta sobre l’abast de la definició de l’arquitectura que es durà a terme durant el projecte d’estratègia i definició de l’oficina de mobilitat del lloc de treball (MMS). Everis comenta que l’abast d’aquest projecte és el de detallar els requeriments d’infraestructura necessaris per a poder dur, en un futur, una implantació d’una eina EMM, així com per donar suport als 8ssume8o de negoci a mobilitzar.
▪ AL pregunta sobre la definició d’aplicacions que es realitzarà. Everis explica que el que es farà per la part d’aplicacions és, segons les requeriments de negoci, definir les línies base que es necessitaran per mobilitzar cadascun dels 8ssume8o i estudiar la viabilitat d’ús d’una 8ssume8one comercial, existent als Markets corresponents o bé l’ús d’una 8ssume8one desenvolupada a mida. Queda fora de l’abast, la presa de requeriments concreta pel desenvolupament funcional de les aplicacions o per la reenginyeria d’aplicacions ja existents. En cada cas, caldrà concretar projectes específics per 8ssume8o aquesta/es tasques.
▪ SL comenta que en seguretat 8ssum a punt d’entrar nous dispositius i que en la mesura del 8ssume8 seria convenient fer entrar aquests nous dispositius. PL comenta que el servei no està encara definit i que entrarà en el 8ssume8 que ho estigui, i que per tant, no és viable i que haurà de continuar com s’ha fet fins el 8ssume8.
▪ AL comenta la possibilitat de contemplar els ordinadors portàtils com a mobilitat. PL i everis comenten, que la plataforma de desktop tradicional, ja sigui com a estació de treball fixe o 8ssume8o, està fora del programa de mobilitat. Actualment els entorns de 8ssume8one sor8a, i els entorns de smartphones i tablets es gestionen encara mitjançant eines no consolidades.
▪ EM indica que aquesta separació pot no ser entesa per part dels Responsables de negoci quan es faci la presa de requeriments durant la primera fase. Indirectament, el que es transmet cap a l’equip de IT és que arrencar la fase 1 contemplant només els entorns en mobilitat pot representar problema de 8ssume8one s i comprensió.
▪ EM actua en representació de la seva 8ssume8on i assignarà el perfil corresponent un cop identificades les necessitats.

Compromisos:

▪ En relació al punt aixecat per EM, everis assumeix el compromís d’inventariar també les peticions de mobilitat sobre equips de 8ssume8one sor8a de Desktop clàssica. D’aquesta manera s’elimina la fragmentació cap als diversos clients. Everis agruparà les peticions rebudes durant la primera fase i les traslladarà per a el seu estudi i eventual incorporació en el seu treball.</td></tr>
</table>

Annex 2.2. Audit Meeting

<table>
<tr><th colspan="4">Enterprise Mobility Management Program</th></tr>
<tr><td>Convocats</td><td>▪ Audit Department partner
▪ Project Manager
▪ IT Team partner
▪ everis</td><td>Assistents</td><td>▪ Audit Department partner
▪ Project Manager
▪ IT Team partner
▪ everis</td></tr>
<tr><td>Data:</td><td colspan="3">14 de març de 2013</td></tr>
<tr><td colspan="4">EMM program – Meeting minutes Audit</td></tr>
<tr><td colspan="4">▪ Inspeccions: llicències i inspecció: coordinen necessitats d’inspecció. Van amb una PDA obsoleta a fer les inspeccions i sincronitzen via USB. S’està plantejant l’evolució de l’aplicació que utilitzen a HTML5.
▪ Actualment hi ha 150 PDAs.
▪ Les inspeccions són per Zona de territori o departament, tot i que hi ha inspeccions genèriques i el sistema no està preparat per això.
▪ El model de llicenciament està canviant, segons les noves normatives, amb l’objectiu de fer-lo més senzill i àgil, això canviarà el perfilat de l’usuari augmentant el públic objectiu.
▪ Medi ambient: Motoristes pel carrer que quan detecten alguna incidència, com per exemple, sacs de runa (tenen una plataforma de planificació de rutes) fan fotos i un informe. El dia següent tornen a visitar per veure si hi ha el mateix sac i torna a fer una foto i un informe per iniciar un procés sancionador
▪ Inventari espai públic: Realitzen tasques sobre l’arbrat urbà (1 cop l’any) revisió de cadascun dels arbres de la ciutat (uns 150.000 i pot durar entre 4 a 6 mesos)
▪ Catàleg del patrimoni arquitectònic: mobilitzar l’inventari per poder-ho fer in-situ
▪ Espai urbà: neteja, pavimentació; espais verds; fonts;
▪ Enllumenat: llevat de neteja, les inspeccions en aquestes àrees les realitzen junt amb l’inventari, els dispositius són de proveïdors
▪ Neteja: inspeccions de neteja (els terminals PDAs amb els que es realitzen les inspeccions són de l’empresa)
▪ Guals i Obres: en cas que per posar un nou gual o fer una obra s’hagi de retirar un arbre, un inspector va amb una PDA per fer la valoració in-situ de l’impacte i valoració econòmica i ambiental de fer el moviment (aprox. 10 usuaris)
▪ Reports als gerents amb indicadors sobre les actuacions realitzades al 9ssume9on. Accés a aquests reports des d’un dispositiu mòbil.
▪ Totes les accions d’inspecció, són susceptibles de ser mobilitzades en millors condicions de les actuals, amb dispositius mòbils de nova generació, amb una 9ssume9one mobilitzada que compleixi tots els requeriments necessaris i que permeti fer tots els tràmits en mobilitat, estalviant el temps de sincronització amb els equips de Desktop Clàssic.
▪ COPE: estació de treball + tablet (W8?) + telèfon mòbil + telèfon fixe + reunions virtuals + fòrums de coneixement + treball col·laboratiu (Sharepoint) + impressió
▪ BYOD: correu + accés a repositoris de fitxers + impressores + accés segur a aplicacions d’escriptori</td></tr>
</table>

Annex 2.3. Communication and Press Meeting

<table>
<tr><th colspan="4">Enterprise Mobility Management Program</th></tr>
<tr><td>Convocats</td><td>Communication and Press Department partner
Project Manager
IT Team partner
everis</td><td>Assistents</td><td>Communication and Press Department partner
everis</td></tr>
<tr><td>Data:</td><td colspan="3">19 de març de 2013</td></tr>
<tr><td colspan="4">EMM program – Meeting minutes Communication and Press</td></tr>
<tr><td colspan="4">Els diferents Serveis són: telèfon, oficines comunicació (11 oficines), Kioscos i BackOffice
Serveis de Gestió a la Informació: gestionen la informació d’equipaments i actes d’agenda utilitzant un CRM (la creació del qual està en curs).
Departament d’Internet: encarregat de la part funcional de Webs (per sol·licituds internes)
Backoffice: les aplicacions que usen són Plataforma HOST i Middleware de tràmits
Les oficines utilitzen les següents eines:
Repositori de tràmits i requeriments + manteniment de la informació dels tràmits existent al portal de tràmits)
Agenda i equipaments, si es cau, fan servir la versió web
Els requeriments de mobilitat per totes les eines descrites anteriors són de Desktop Clàssic, és a dir, poder accedir remotament (des d’un PC) a les diferents aplicacions
Departament d’Incidències, Reclamacions o sol·licituds:
gestor documental
obrir incidències i reclamacions a la via pública.
accés ofimàtic i a doc corporativa
Serveis Publicitaris: ús d’aplicacions ofimàtiques i photoshop amb necessitat de molt d’espai en disc i intercanvi de documentació (amb tercers externs). Ús d’imatges i vídeo d’alta qualitat
Xarxes socials: són redactors, periodistes, fotògrafs, vídeo.
Accés a contingut (multimèdia) en mobilitat
Coordinació: no apliquen solucions de mobilitat
Requeriments de Lloc de Treball (LldT) i mobilitat:
Direcció Global de Comunicació: els usuaris haurien de disposar d’un dispositiu mòbil (telèfon)
Serveis d’imatge i producció editorial (editorial/impremta): necessitat de mobilitzar (desktop clàssic) per poder-hi accedir de mode remot des de qualsevol ubicació. Aquest col·lectiu té uns requeriments d’ús d’imatges i d’equips de treball pel disseny gràfic i la maquetació (MAC Osx)
L’ús de dispositius, tant mòbils com estacions de treball han d’estar orientades al disseny gràfic i l’edició de contingut multimèdia
Accedir de mode remot a contingut corporatiu: carpetes de xarxa i correu
La direcció hauria de tenir accés a navegació i l’aplicació de planificació i control de campanyes publicitàries
Planificació d’events: no apliquen solucions de mobilitat
Estan treballant en requeriments de mobilitat per cartografia.</td></tr>
</table>

Annex 2.4. Corporate University Meeting

<table>
<tr><th colspan="4">Enterprise Mobility Management Program</th></tr>
<tr><td>Convocats</td><td>▪ Corporate University partner
▪ Project Manager
▪ IT Team partner
▪ everis</td><td>Assistents</td><td>▪ Corporate University partner
▪ everis</td></tr>
<tr><td>Data:</td><td colspan="3">21 de març de 2013</td></tr>
<tr><td colspan="4">EMM program – Meeting minutes Corporate University</td></tr>
<tr><td colspan="4">▪ Perfils del lloc de treball:
▪ 2 perfils (VIP i Tècnics). L’Anna explica que ja s’ha fet el perfilat dels usuaris (també s’ha fet per Educació)
▪ Centres de Investigació:
▪ Aplicació d’inventari, i també per documentar (l’aplicació és de baixa qualitat i la sincronització de dades és complexa). Poden haver-hi zones sense cobertura (magatzems, bodegues, etc.)
▪ Aplicació que té el registre de eines que es deixen o cedeixen. Té el mateix problema que l’anterior aplicació.
▪ Events formatius: control de les persones de l’organització que es mouen per l’event (acreditacions, gestió equip). Té com a objectiu l’acreditació de persones de forma àgil i mòbil.
▪ Valorar la possibilitat de fer streaming dels events
▪ Innovació: Telecomunicacions i Mobilitat. Necessiten d’amples de banda grans per poder fer events (creació d’idees, xarxes social, etc.)
▪ Biblioteques: PCs amb accés a internet, pantalles noticies, quioscos. S’està fent una reorganització.
▪ Hi ha una zona que permet sol·licitar un PC amb connexió a internet (possibilitat de posar tablet que permeti moure’s amb accés als mateixos continguts que amb un PC)
▪ Hi ha un projecte per passar a fibra òptica la connexió a internet.
▪ Centres de Ciències:
▪ Tenen 4 àmbits de treball: difusió, conservació, investigació, administració
▪ Per aquests museus, treballen una sèrie de 11ssume11, en camp obert, que fan recollida d’informació: es valora la possibilitat de dotar-los amb dispositius mòbils amb els que poder capturar la informació (text; fotos; vídeo; so) i que pugui geo-localitzar el lloc de la troballa i enviar la informació en temps real.
▪ Formació
▪ 2 línies de negoci:
▪ 1 aplicació que fa la gestió administrativa dels centres formadors(preinscripció, matriculació, informes assistència, permanències, dietes, malalties, etc.) en internet i extranet gestionat per la direcció. Intentar mobilitzar l’aplicació web per poder usar-la des de dispositius mòbils
▪ Línia d’innovació: oberts 4 fronts, línies de projecte per a que l’alumne sigui partícip de les noves tecnologies. Aquestes 4 línies encara estan en procés de definició.</td></tr>
</table>

Annex 2.5. Executive Direction Meeting

Enterprise Mobility Management Program			
Convocats	▪ Executive Direction partner [EDP] ▪ Project Manager ▪ IT Team partner ▪ everis	Assistents	▪ Executive Direction partner ▪ everis
Data:	27 de març de 2013		
EMM program – Meeting minutes Executive Direction			
▪ [EDP] està ubicat a la seu de Pl. Sant Jaume. ▪ No estan identificades les necessitats de mobilitat. ▪ Executive Direction: les necessitats fonamentals són les de poder accedir a la informació compartida de les carpetes de xarxa des de qualsevol ubicació i dispositiu. ▪ Els VIPs i les seves secretàries disposen d'iPads. Les secretàries prenen notes de les reunions en els dispositius. Es desconeix l'aplicació que utilitzen per aquesta fi. ▪ Un membre utilitza una aplicació en els dispositius (iOS i Android) anomenada **WiFi-Doc** que permet projectar documents en mode col·laboratiu (fins a 4 dispositius) i prendre en control de la presentació segons la necessitat, cada usuari des del seu dispositiu. S'està estudiant l'ús generalitzat d'aquesta aplicació. ▪ Hi ha demanda de poder imprimir a les impressores de la xarxa corporativa directament des dels dispositius iOS. ▪ **COMPROMISOS** ▪ [EDP] parlarà amb el personal de Executive Direction per tal d'identificar altres necessitats, tant de mobilitat com del PC clàssic.			

Annex 2.6. Finance Meeting

Enterprise Mobility Management Program			
Convocats	▪ Finance partner [FP] ▪ Project Manager ▪ IT Team partner ▪ everis	Assistents	▪ Finance partner ▪ everis
Data:	19 de març de 2013		
EMM program – Meeting minutes Finance			
Direcció finances ▪ Directors amb accés des de casa al seu escriptori, a dades i informació ▪ Comptabilitat de costos, processos (proj. En fase embrionària) pensant en accés on-line per part de directius en reunions (tablet) Resta usuaris finances: ▪ Nomes correu per alguns usuaris. No caldria accés des de casa per la mena de tràmits que es realitzen (com a màxim, tenir accés a l'escriptori i informació personal) Promoció econòmica, inversió, nous negocis: Idem que anterior			

- Hi ha un inspector o supervisor que gestiona incidències, reclamacions. Usen portàtils de gama baixa i l'aplicació client que utilitzen no compleix els requeriments necessaris. Tanmateix, la connexió de dades es deficitària
- En [FP] comenta que els Managers haurien de tenir accés a la següent informació i aplicacions:
- accés a informació personal, Correu, Escriptori
- Aplicació gestor de demanda i projectes (web-j2ee)
- Aplicació d'aprovacions financeres
- **BYOD: si, amb política molt clara d'ús i compromís**

Annex 2.7. Human Resources Meeting

Enterprise Mobility Management Program			
Convocats	▪ HHRR partner [HP] ▪ Project Manager ▪ IT Team partner ▪ everis	Assistents	▪ HHRR partner [HP] ▪ Project Manager ▪ IT Team partner ▪ everis
Data:	14 de març de 2013		
EMM program – Meeting minutes HHRR			

- Hi ha hagut peticions d'iPads però no han estat ateses. No hi ha iPads corporatius a Gerència de Recursos (només l'Alcalde i els Gerents Municipals)
- Hi ha un projecte que consisteix en donar als càrrecs un iPad com eina de treball.
- Hi ha en marxa un estudi de les aplicacions utilitzades (desktop) per veure si es poden utilitzar al iPad
- Es té com a objectiu eliminar el paper a les reunions (docs: Ordres del dia; actes; …)
- Requisits de mobilitat:
- Càrrecs alts: tots amb portàtil i iPad
- Serveis Generals: Logística i Manteniment (falicity management), iPad per entrar les ordres de treball
- Interventor: signatura digital mòbil
- Arxiu: no apliquen necessitats de mobilitat
- Inspectors: mobilitzar lloc de treball per apropar-lo al lloc on es realitzen les consultes (desktop clàssic)
- Contractació: no apliquen necessitats de mobilitat
- Administració General: desktop clàssic (accés a recursos en remot)
- Compres: desktop clàssic (accés a recursos en remot)
- Serveis Jurídics (serveis generals): Entorn treball col·laboratiu: Sharepoint
- Subvencions: no apliquen necessitats de mobilitat
- Participació: no apliquen necessitats de mobilitat
- Patrimoni: lligat amb eina de Facility Management
- RRHH: desktop clàssic (accés a recursos en remot)

Annex 2.8. IT Meeting

Enterprise Mobility Management Program			
Convocats	▪ IT Executive Manager [ITEM] ▪ Project Manager ▪ IT Team partner ▪ everis	Assistents	▪ IT Executive Manager ▪ everis
Data:	21 de març de 2013		
EMM program – Meeting minutes IT			
▪ [ITEM] informa, que hi ha noves modalitats d'horari presencial, s'hauran de reflectir.(Lloc de treball amb mobilitat, treball en remot des de domicili...) ▪ Existeixen de 14 Direccions a IT, els requeriments d'algunes, s'especifiquen a continuació: ▪ Gerències: mobilitat amb accés a informació: accés al PC en remot i als repositoris d'arxius ▪ Direcció de Processos: millora dels processos de tramitació: accés al PC en remot i als repositoris d'arxius. Treballen en dependència municipal administrativa (sense requeriments de mobilitat) ▪ Direcció de Projectes: treballen en dependències, treball intern. ▪ Direcció tràmits electrònics : departament tècnic d'Internet. Lloc de treball amb mobilitat esporàdic. Depèn del perfil de la persona, accés al PC en remot i als repositoris d'arxius ▪ Direcció de Administració: contractació administrativa (sense requeriments de mobilitat) ▪ Direcció d'Atenció al Client: accés al PC en remot i als repositoris d'arxius ▪ Direcció Explotació i Sistemes: són tècnics de camp. Actualment els tècnics es desplacen i han de connectar-se a una estació de treball que estigui a la ubicació visitada. ▪ Les aplicacions a tenir en remot pels tècnics: Eines de ticketing ▪ [ITEM] proposa un model híbrid: tablet i smartphone (com el Samsung Galaxy Note) com dispositiu ideal per als tècnics de camp. ▪ Direcció de Desenvolupament de Projectes: no apliquen solucions de mobilitat ▪ Direcció RRHH: no apliquen solucions de mobilitat ▪ Direcció Govern TIC i Seguretat: no apliquen solucions de mobilitat			

Annex 2.9. Legal Meeting

Enterprise Mobility Management Program			
Convocats	▪ Legal Partner [LP] ▪ Project Manager ▪ IT Team partner ▪ everis	Assistents	▪ Legal Partner ▪ everis
Data:	22 de març de 2013		
EMM program – Meeting minutes Legal			
▪ Hi ha inspectors que fan ús de PDAs. Aproximadament 10 inspectors que sincronitzen amb aplicació de desktop ▪ Hi ha part dels informes que no s'introdueixen a l'aplicació i es realitzen a mà i s'envien per			

correu electrònic o s'entreguen en mà sense que siguin introduïts a l'aplicació corresponent.

- Advocats: es mouen entre oficines amb xarxa corporativa. Accés a dades, documents, repositori d'arxius, etc. Seria convenient que poguessin disposar de dispositius mòbils per accedir a aquest contingut en mobilitat i que tinguessin accés remot a les aplicacions de desktop.
- Aplicacions d'ERP (gestió) a mida que no estan a la xarxa corporativa:
- Hi ha una aplicació que està al núvol
- Una altra aplicació està en servidors paral·lels a la xarxa corporativa que no tenen accés extern.
- [LP] destaca que com a Manager, té necessitat de poder teletreball (no MetaFrame) i que li caldria disposar d'una connexió 3G al seu PC portàtil
- BYOD: Si, amb polítiques d'ús definides.

Annex 2.10. Presidency Meeting

Enterprise Mobility Management Program			
Convocats	▪ Presidency Partner ▪ Project Manager ▪ IT Team partner ▪ everis	Assistents	▪ Presidency Partner ▪ everis
Data:	19 de març de 2013		
EMM program – Meeting minutes Presidency			
▪ El perfil dels usuaris és el del back-office de presidència ▪ Per tots els usuaris, caldria poder disposar de la documentació dels arxius de xarxa compartits (Accedir-hi de forma fàcil fora de l'entorn de l'oficina, i amb dispositius diferents al PC –una cosa similar a Dropbox- amb accés de lectura i edició dels documents) ▪ Els usuaris ofimàtics haurien de poder navegar por internet ▪ Aplicacions de Negoci: ▪ Aplicació de registre i seguiment de correspondència que entra a presidència (és una aplicació Client/Servidor) ▪ Aplicació d'Organització dels actes i events de l'alcaldia ▪ Mailing de l'alcaldia basat en Notes. ▪ **iPad per a alts càrrecs** ▪ S'entén mobilitat com tot allò mòbil, és a dir, el lloc de treball tradicional, inclòs el PC domèstic			

Annex 2.11. Security Meeting

Enterprise Mobility Management Program			
Convocats	▪ Security Partner ▪ Project Manager ▪ IT Team partner ▪ everis	Assistents	▪ Security Partner ▪ Project Manager ▪ everis

Data:	19 de març de 2013

EMM program – Meeting minutes Security

- S'han rebut peticions d'smartphones però no s'estan atenent o fomentant.
- Hi ha usuaris amb els seus terminals (telèfon i tablet) amb accés al correu corporatiu.
- PC mòbil entre oficines com un PC corporatiu. Aquests equips ha de poder disposar de les mateixes funcionalitats que en el PC de xarxa
- Aplicació (C/S amb versió web) d'emergències per poder veure les entrades que s'associen a un incident (està en el PC mòbil). També mobilitzat en tablet. S'està fent un pilot.
- Aplicació que garanteix la gestió de RRHH i recursos materials. Es poden assignar tasques a les Unitats Territorials des de l'aplicació.
- BBDD Documental: aplicació Notes que consulta on hi ha totes les ordres i directrius pel funcionament dels serveis
- S'està duent a terme la posada en marxa de l'auto-servei de l'empleat: accés a la intranet municipal des d'internet per executar Aplicacions i la Base de Dades a més de la informació personal de cada usuari (nòmines, etc.) i fer certs tipus de peticions
- Els requeriments de mobilitat, més enllà de la mobilització en tablet són els de desktop clàssic, és a dir, poder accedir a totes les aplicacions de desktop des de qualsevol PC a l'abast dels usuaris així com als repositoris de documentació.

Annex 2.12. Territory Management Meeting

Enterprise Mobility Management Program			
Convocats	▪ Territory Management Partner [TMP] ▪ Project Manager ▪ IT Team partner ▪ everis	Assistents	▪ Territory Management Partner ▪ Project Manager ▪ everis
Data:	22 de març de 2013		

EMM program – Meeting minutes Territory Management

- Com a premissa, es detecta la necessitat de poder realitzar la autenticació amb certificat des d'un dispositiu mòbil (en tots les aplicacions amb 16ssume16one s)

Per àmbits:

- Territory Area Managers: Accés a quadres de comandament i reporting (fins ara s'envien per correu un cop al mes). Caldria poder accedir-hi des de dispositius mòbils si aquests estiguessin disponibles, ja sigui com aplicació de Quadre de Comandament o accedint al repositori d'arxius.

Aplicacions:

- 1 component d'intranet que fa seguiment de temes importants per Executive Management (en J2EE)

Coordinació Territorial:

- inspeccions de districtes
- Direcció serveis al territori:
- Aplicació d'informes utilitzats pels tècnics. Hauria de ser accessible des d'internet. És una aplicació per fer actes de reunions.

BYOD: Si, amb polítiques d'ús definides.

Com a consideracions a tenir en compte, la [TMP] destaca:

- El Servei de VPN és deficitari
- Hi ha tècnics o treballadors en Branch Offices sense accés a la xarxa corporativa.
- S'hauria de disposar d'accés a totes les aplicacions de Desktop i a les carpetes corporatives.

Annex 2.13. Phase 1 Closure Meeting

Enterprise Mobility Management Program			
Convocats	▪ Executive Manager [EM] ▪ Project manager [PM] ▪ App leader [AL] ▪ Telecomunications leader [TL] ▪ Security leader [SL] ▪ everis	Assistents	▪ Executive Manager [EM] ▪ Project manager [PM] ▪ App leader [AL] ▪ Telecomunications leader [TL] ▪ Security leader [SL] ▪ everis
Data:	23 d'Abril de 2013		
EMM program – Meeting minutes Phase 1 Closure			

everis presenta les conclusions obtingudes, pel que fa als requeriments de mobilitat recollits en la Fase 1 del projecte mitjançant les entrevistes realitzades amb els diferents Business Units.

- Les conclusions es divideixen en una sèrie de requeriments comuns, realitzats per la gran majoria Business Units i de requeriments particulars de cadascuna de les àrees o direccions.

Everis explica la 2a fase del projecte i les activitats que es realitzaran. Entre aquestes activitats, es focalitza en la part de polítiques, posant en comú els interlocutors que everis havia identificat a l'inici del projecte i identificant si manca alguna de les direccions entre els interlocutors. Finalment, s'identifica que els interlocutors han de ser:

- Polítiques d'ús – RRHH, Project Manager, Security Leader, Communication & Press i everis.
- Polítiques de seguretat – Project Manager, Security Leader, everis.
- Polítiques d'aplicacions – App Leader, Telco Leader, Project Manager i everis.
- Polítiques BYOD – Project Leader, RRHH, Security Leader, Legal, Telco Leader i everis.

Les properes passes a realitzar seran:

- everis proposarà les dates per fer les següents reunions per acabar de definir les polítiques.
- A finals de la primera quinzena de maig, sempre que s'hagin pogut fer les sessions de definició de les diferents polítiques, es farà una nova reunió per fer un seguiment de l'estat de la segona fase.

ANNEX 3. PHASE 1 MOBILITY QUESTIONARIES

Annex 3.1. Full Quiz Template

Client:	
Empleat:	
Càrrec:	
Departament:	
Responsable:	
Data:	

Percepció de la mobilitat

- Quin es l'objectiu del seu departament?
- Descriviu breument la funció i/o les tasques habituals dintre del vostre departament.
- Quin es el número total d'empleats del seu departament? Quants son dintre de l'abast?

Total: Contemplats:

- Quina es la previsió de creixement del seu departament durant els pròxims 6 mesos?
- Quins rols podeu definir al vostre departament segons les seves funcions?
- Quina es la ubicació habitual del seus treballadors, oficina o fora? Viatgen habitualment?
- Quines aplicacions i/o serveis considereu imprescindibles per a la vostra tasca diària?
- Creu que la tasca que desenvolupa la podria fer únicament amb un dispositiu mòbil i accés als serveis i aplicacions esmenats anteriorment?
- Quins processos de negoci creieu que poden millorar-se amb dispositius mòbils?
- Com definiria cadascun dels rols al seu departament, creador o consumidor de contingut?

A cadascun dels següents blocs, marqui les 2 opcions que consideri més importants:

1. Eficiència operativa i reducció de costos

Reduir temps operatius	
Ràpida resolució d'aprovacions i decisions	
Facilitar la col · 18ssume18one d'activitats laborals	
Augmentar l'eficiència d'actius.	
Reduir els costos d'atenció a client / usuari.	

2. Creixement en productivitat i avantatge competitiu

Obrir nous canals de negoci	
Establir major seguiment dels clients / usuari.	
Millorar satisfacció	
Fomentar la innovació	
Potenciar el coneixement dels empleats	

Demanda

- Al seu departament, actualment disposen de telèfons mòbils tradicionals corporatius? En cas afirmatiu, indiqui el número total y el número dels que es volen substituir per dispositius de nova generació.

Total: A canviar:

- Al seu departament, actualment disposen de smartphones i/o tablets corporatius? En cas afirmatiu, indiqui el número de dispositius dins de l'abast de la solució de mobilitat:

	iOS	Android	BlackBerry	Symbian	Windows P.
Mòbil					
Smartphone					
Tablet					

- Quina es la previsió inicial de desplegament de dispositius mòbils al seu departament?

	iOS	Android	BlackBerry	Windows P.	Altres
Smartphone					
Tablet					

- Els usuaris que no tinguin un dispositiu corporatiu, podran utilitzar el seu personal (BYOD)? A quins serveis i/o aplicacions corporatives podran accedir?
- SI □ ▪ Correu □ ▪ Intranet □ ▪ Repositoris □ ▪ Altres:
- NO □ ▪ VPN □ ▪ Aplicacions □ ▪ A TOT □
- Disposeu actualment d'aplicacions de negoci/corporatives desenvolupades per a dispositius mòbils? En cas afirmatiu, Quines? En cas negatiu, Quines voldríeu tenir a curt termini?
- Quins d'aquests aspectes creu que són més necessaris dins d'una solució de mobilitat?

	Gens	Poc	Molt	Imprescindible
Compra i provisió de nous dispositius				
Gestió de garanties i stock				
Compra d'aplicacions i gestió de compres per volum				
Gestió de targetes telefòniques				
Gestió del dispositiu (config., seguretat, inventari,etc.)				
Desenvolupament d'apps de negoci per a dispositius				
Servei de suport i formació a nous usuaris				
Gestió del desplegament de la solució				
Gestió de la recollida o canvi de dispositius				

- Marqui quines de les següents capacitats d'una solució de mobilitat vol aprofitar:

Gestió d'actius per inventariar estat i característiques del dispositiu, llistat d'aplicacions, etc.	
Gestió de la seguretat per bloquejar, esborrar i/o aplicar polítiques de seguretat en els dispositius o en part del seu contingut.	

Control d'ActiveSync per regular l'accés al correu corporatiu.	
Gestió de dispositius per administrar les configuracions dels dispositius (VPN, WiFi, Bloqueig, Certificats, etc.).	
Gestió d'aplicacions, incloent AppStore empresarial, inventari d'aplicacions, llista negra / llista blanca d'aplicacions, etc.	
Capacitats de "Reporting", estat i seguiment del disposiu, gestió d'alertes, etc.	

Annex 3.2. Reduced Quiz Template used with Answers

Annex 3.2.1. Audit Mobility Quiz

Personal – Organització del departament:

Rols/Càrrecs	Necessitats de Mobilitat	LIdT	Dispositiu Mòbil
Gerent	Informes de les actuacions realitzades al territori.		X
Inspector	Obertura, consulta i seguiment d'informes, incidències, etc.		X

Processos i Tasques – Processos de negoci sensibles de millora amb la incorporació de dispositius mòbils.

- Inspeccions – Canvi dels dispositius PDA per altres de nova generació (Tablet i/o Smartphone) que permetin la generació "in-situ" dels respectius informes, tiquets i/o incidències.
- Seguiment i Reporting – Dashboards i quadres de comandament sobre l'estat de les diferents actuacions.

Dispositius – Existència de dispositius mòbils de nova generació (Smartphones i/o Tablets):

- No. Existència PDAs per als inspectors (~200 dispositius).
  Existència de dispositius de tercers (externs) que es connecten als sistemes i de dispositius que es deixen a tercers (externs).

Aplicacions o Serveis – Existeixen aplicacions de negoci desenvolupades per a dispositius mòbils? En cas afirmatiu, Quines? En cas negatiu, Quines voldríeu tenir a curt termini?

- Existeixen aplicacions per a PDAs dels inspectors:
  - Aplicació inspectors (Possible evolució a HTML5).
  - Sistema de tercers connectat.
  - Aplicació inspector (valoració in-situ de l'acció a realitzar)
  - Aplicació de tercers.

  Aplicacions no presents per a dispositius mòbils:
  Inventari espai públic, espais verds, etc.
  Catàleg patrimoni

Aplicacions o Serveis – Respecte als dispositius no corporatius (BYOD), quins serveis i/o aplicacions corporatives han de ser accessibles?

TOT □		**Repositoris de dades X**		**Intranet** □
CAP □	**A definir** □	**Correu X**	**VPN** □	**Aplicacions X**

Objectius – Eficiència operativa i la reducció de costos

- **Reduir temps operatius** X
- **Ràpida resolució d'aprovacions i decisions**
- **Facilitar la col · 20ssume20one d'activitats**

laborals

- **Augmentar l'eficiència d'actius.** X
- **Reduir els costos d'atenció a client / usuari.** X

Objectius – Creixement en productivitat i avantatge competitiu

- **Obrir nous canals de negoci/treball** X
- **Establir major seguiment dels clients / usuari.** X
- **Millorar satisfacció**
- **Fomentar la innovació**
- **Potenciar el coneixement dels empleats**

Observacions – Pròxims passos per definir una estratègia de mobilitat:

- Inventariar el total de dispositius PDA existents, el tipus d'ús i la propietat.
- Definir les necessitats concretes de cadascuna de les inspeccions per tal d'establir el millor dispositiu per fer-les (substitució PDAs).
- Estudiar cadascuna de les aplicacions que actualment s'estan utilitzant a través de PDAs i planificar els canvis necessaris per a la transició cap a Smartphones i Tablets.
- Valorar els sistemes de tercers que actualment es connecten i/o s'utilitzen a les inspeccions.
- Definir les necessitats de reporting cap als Directors/Gerents.

Annex 3.2.2. Communication and Press Mobility Quiz

Personal – Organització del departament:

Rols/Càrrecs	Necessitats de Mobilitat	LldT	Dispositiu Mòbil
Direcció Comunicació	PC remot + Smartphone – Ofimàtic + Documentació corporativa	X	X
Dept. Internet	PC remot – Part 21ssume21one Webs	X	
Servei Tlf I Oficines	PC remot – Atenció ciutadana	X	
Dept. Incidències, reclamacions o sol·licituds	PC remot – Atenció incidències	X	
Serveis Publicitaris	PC remot – Edició multimèdia + Xarxes socials + accés a documentació	X	
Servei imatge I producció editorial	PC remot – Disseny 21ssume21 I edició multimèdia	X	
Coordinació	No aplica		
Planificació events	No aplica		

Processos i Tasques – Processos de negoci sensibles de millora amb la incorporació de dispositius mòbils.

- "Millora de les capacitats de seguiment de les activitat.
- Millors capacitats de treball dels tècnics desplaçats.
- Accés a contingut multimèdia corporatiu en mobilitat.
- Accés remot a repositoris de documents.

Dispositius – Existència de dispositius mòbils de nova generació (Smartphones i/o Tablets):

- No o no hi ha dades.

Aplicacions o Serveis – Existeixen aplicacions de negoci desenvolupades per a dispositius mòbils? En cas afirmatiu, Quines? En cas negatiu, Quines voldríeu tenir a curt termini?

Direcció comunicació:

- Planificació I control campanyes publicitàries

Departament Internet:

- Plataforma Host.
- Middleware portal de tràmits.

Servei Telefònic I oficines

- Portal de tràmits.
- Agenda I equipaments (versió WEB SATEC)

Departament d'Incidències

- Gestor Documental
- Incidències
- Accés Frameworks Desenvolupament (Drupal, Wordpress, Vignette).

Serveis Publicitaris:

- Xarxes socials I contingut 22ssume22one

Direcció Estudis I Avaluacions:

- Estadístiques
- Anàlisi Tweets
- Registre enquestes I estudis

Imatge I producció editorial:

- Aplicacions disseny gràfic, maquetació i edició multimèdia.

Aplicacions o Serveis – Respecte als dispositius no corporatius (BYOD), quins serveis i/o aplicacions corporatives han de ser accessibles?

TOT □		**Repositoris de dades** □	**Intranet** □	
CAP □	**A definir X**	**Correu** □	**VPN** □	**Aplicacions** □

Objectius – Eficiència operativa i la reducció de costos

Reduir temps operatius	X
Ràpida resolució d'aprovacions i decisions	
Facilitar la col · 22ssume22one d'activitats laborals	
Augmentar l'eficiència d'actius.	X
Reduir els costos d'atenció a client / usuari.	X

Objectius – Creixement en productivitat i avantatge competitiu

Obrir nous canals de negoci/treball	
Establir major seguiment dels clients / usuari.	
Millorar satisfacció	X
Fomentar la innovació	X
Potenciar el coneixement dels empleats	X

Observacions – Pròxims passos per definir una estratègia de mobilitat:

- Definir clarament la 23ssume23on de cadascun dels departaments i com s'interrelacionen.
- Definir política d'ús per a usuaris BYOD.
- Anàlisi exhaustiu de les aplicacions de negoci existents: Tipus d'aplicacions, arquitectura, així com el seu ús, per tal de valorar quines haurien d'optimitzar-se per ser 23ssume23one des d'altres tipus de dispositius (no PC).

Annex 3.2.3. Corporate University Mobility Quiz

Personal – Organització del departament:

Rols/Càrrecs	Necessitats de Mobilitat	LIdT	Dispositiu Mòbil
VIP	PC remot + Smartphone/tablet	X	X
Técnic	Tablet		X

Processos i Tasques – Processos de negoci sensibles de millora amb la incorporació de dispositius mòbils.

- Events – Control de les persones de l'organització a l'event. Acreditació de persones Ágil i Móbil.
- Biblioteques – Servei de 23ssume23 de Tablets que permeti la consulta d'informació igual que el PC però amb mobilitat.
- Centres de Ciencies – Millora en la 23ssume23one s d'informació en temps real (Text, fotos, 23ssume, GPS, etc.).

Dispositius – Existència de dispositius mòbils de nova generació (Smartphones i/o Tablets):

- No o no hi han dades.

Aplicacions o Serveis – Existeixen aplicacions de negoci desenvolupades per a dispositius mòbils? En cas afirmatiu, Quines? En cas negatiu, Quines voldríeu tenir a curt termini?

Centres de Investigació:

- Inventari
- Magatzems – Registre peces cedides o deixades.

Centres Formadors:

- Aplicació per a tota la gestió administrativa d'inscripcions.

Aplicacions en projecte o fase d'anàlisi:

- Consorci dels Museus de Ciencies:
- Aplicació per 23ssume23 de camp que faciliti la tasca de recollida d'informació.
- Alumnes particeps de les noves 23ssume23one .

Aplicacions o Serveis – Respecte als dispositius no corporatius (BYOD), quins serveis i/o aplicacions corporatives han de ser accessibles?

TOT □	**Repositoris de dades** □	**Intranet** □		
CAP □	**A definir X**	**Correu** □	**VPN** □	**Aplicacions** □

Objectius – Eficiència operativa i la reducció de costos

- **Reduir temps operatius** X
- **Ràpida resolució d'aprovacions i decisions**
- **Facilitar la col · 23ssume23one d'activitats laborals**

- **Augmentar l'eficiència d'actius.** X
- **Reduir els costos d'atenció a client / usuari.** X

Objectius – Creixement en productivitat i avantatge competitiu

- **Obrir nous canals de negoci/treball** X
- **Establir major seguiment dels clients / usuari.**
- **Millorar satisfacció** X
- **Fomentar la innovació** X
- **Potenciar el coneixement dels empleats** X

Observacions – Pròxims passos per definir una estratègia de mobilitat:

- Analitzar el perfilat dels usuaris que ja s'ha realitzat, per tal de comnençar a definir les diferents polítiques.
- Definir tipus de dispositius de préstec per a biblioteques .
- Definir política d'ús per a usuaris BYOD.
- Estudi per a l'optimització de les aplicacions per a dispositius móbils.

Annex 3.2.4. Executive Direction Mobility Quiz

Personal – Organització del departament:

Rols/Càrrecs	Necessitats de Mobilitat	LIdT	Dispositiu Mòbil
VIPs	Smartphone/Tablet		X

Processos i Tasques – Processos de negoci sensibles de millora amb la incorporació de dispositius mòbils.

- Accés als arxius de la xarxa corporativa desde dispositius móbils.

Dispositius – Existència de dispositius mòbils de nova generació (Smartphones i/o Tablets):

- Els VIPs I les seves secretaries disposen d'iPads.

Aplicacions o Serveis – Existeixen aplicacions de negoci desenvolupades per a dispositius mòbils? En cas afirmatiu, Quines? En cas negatiu, Quines voldríeu tenir a curt termini?

- No identificades (Wifi-Doc,...)

Aplicacions o Serveis – Respecte als dispositius no corporatius (BYOD), quins serveis i/o aplicacions corporatives han de ser accessibles?

TOT □ **Repositoris de dades** □ **Intranet** □

CAP □ **A definir X** **Correu** □ **VPN** □ **Aplicacions** □

Objectius – Eficiència operativa i la reducció de costos

- **Reduir temps operatius** X
- **Ràpida resolució d'aprovacions i decisions**
- **Facilitar la col · 24ssume24one d'activitats laborals** X
- **Augmentar l'eficiència d'actius.**
- **Reduir els costos d'atenció a client / usuari.** X

Objectius – Creixement en productivitat i avantatge competitiu

- **Obrir nous canals de negoci/treball** X
- **Establir major seguiment dels clients / usuari.** X
- **Millorar satisfacció**
- **Fomentar la innovació**

- **Potenciar el coneixement dels empleats** X

Observacions – Pròxims passos per definir una estratègia de mobilitat:

- Estudi per identificar els diferents Rols i les necessitats de mobilitat tant des de dispositius de nova generació com de PC tradicional.
- Definir política per a dispositius no corporatius (BYOD).
- Estudi de les aplicacions de negoci i valorar les adaptacions necessàries per 25ssume25o-les des de dispositius mòbils.
- Estudi del sistema de impresio per tal d'habilitar-ho desde dispositius móbils.

Annex 3.2.5. Finance Mobility Quiz

Personal – Organització del departament:

Rols/Càrrecs	Necessitats de Mobilitat	LIdT	Dispositiu Mòbil
Directors	PC Remot + Tablet	X	X
Inversió	Repositori Dades + Correu		X
Inspector	Obertura, consulta i seguiment d'incidències, reclamacions, etc.		X
Managers	PC Remot + Tablet	X	X

Processos i Tasques – Processos de negoci sensibles de millora amb la incorporació de dispositius mòbils.

- Inspeccions – Canvi dels dispositius per altres de nova generació (Tablet i/o Smartphone) que permetin la generació "in-situ" de reclamacions o incidències.
- Aprovacions, Seguiment i Reporting a Gerència – Dashboards i quadres de comandament sobre l'estat de les diferents actuacions.
- Empleats BYOD – Accés a correu corporatiu i informació personal de forma remota.

Dispositius – Existència de dispositius mòbils de nova generació (Smartphones i/o Tablets):

- No o no hi ha dades

Aplicacions o Serveis – Existeixen aplicacions de negoci desenvolupades per a dispositius mòbils? En cas afirmatiu, Quines? En cas negatiu, Quines voldríeu tenir a curt termini?

- No hi ha aplicacions per a dispositius Mòbils.
- Aplicació d'escriptori per a Inspectors.
- Peticions de servei (Web – J2EE).
- Gestor de demanda i projectes (Web – J2EE).
- Processos d'aprovacions financeres.

Aplicacions o Serveis – Respecte als dispositius no corporatius (BYOD), quins serveis i/o aplicacions corporatives han de ser accessibles?

TOT □	**Repositoris de dades** □		**Intranet** □	
CAP □	**A definir X**	**Correu** □	**VPN** □	**Aplicacions** □

Objectius – Eficiència operativa i la reducció de costos

- **Reduir temps operatius** X
- **Ràpida resolució d'aprovacions i decisions** X
- **Facilitar la col · 25ssume25one d'activitats laborals** X
- **Augmentar l'eficiència d'actius.**

- **Reduir els costos d'atenció a client / usuari.**

Objectius – Creixement en productivitat i avantatge competitiu

- **Obrir nous canals de negoci/treball** X
- **Establir major seguiment dels clients / usuari.**
- **Millorar satisfacció** X
- **Fomentar la innovació**
- **Potenciar el coneixement dels empleats** X

Observacions – Pròxims passos per definir una estratègia de mobilitat:

- Definir més clarament la política d'ús per a usuaris BYOD.
- Definir les necessitats reals d'accés a l'escriptori de forma remota.
- Estudiar les aplicacions de negoci existents així com el seu ús, per tal de valorar la seva idoneïtat per a Smartphones i Tablets.

Annex 3.2.6. HHRR Mobility Quiz

Personal – Organització del departament:

Rols/Càrrecs	Necessitats de Mobilitat	LIdT	Dispositiu Mòbil
Alt Càrrec	Portàtil + Tablet	X	X
Serveis Generals	Tablet per Ordres de treball		X
Interventor	Signatura digital móbil		X
Arxiu	No aplica		
Contractació	No aplica		
Admin. Gral.	Accés a recursos en remot	X	
Compres	Accés a recursos en remot	X	
Serveis Jurídics	Repositori de dades remot (SharePoint)	X	
Subvencions	No aplica		
Participació	No aplica		
Patrimoni	Tablet per Ordres de treball		X
RRHH	Accés a recursos en remot	X	
Secretari	No hi ha dades		
Dir. Adm. Gral.	Tablet		X

Processos i Tasques – Processos de negoci sensibles de millora amb la incorporació de dispositius mòbils.

- Processos 26ssume26on I 26ssume de treball, autoritzacions I aprovacions, realització I seguiment d'inspeccions I consultes.

Dispositius – Existència de dispositius mòbils de nova generació (Smartphones i/o Tablets):

- Peticions no ateses. Projecte iPad per càrrec VIP.

Aplicacions o Serveis – Existeixen aplicacions de negoci desenvolupades per a dispositius mòbils? En cas afirmatiu, Quines? En cas negatiu, Quines voldríeu tenir a curt termini?

- Elaboració de ordres de treball.
- Estudi d'aplicacions en curs.

Aplicacions o Serveis – Respecte als dispositius no corporatius (BYOD), quins serveis i/o aplicacions corporatives han de ser accessibles?

TOT □ **Repositoris de dades** □ **Intranet** □

CAP □ **A definir** □ **Correu X** **VPN** □ **Aplicacions** □

Objectius – Eficiència operativa i la reducció de costos

- **Reduir temps operatius**
- **Ràpida resolució d'aprovacions i decisions** X
- **Facilitar la col · 27ssume27one d'activitats laborals** X
- **Augmentar l'eficiència d'actius.** X
- **Reduir els costos d'atenció a client / usuari.**

Objectius – Creixement en productivitat i avantatge competitiu

- **Obrir nous canals de negoci/treball** X
- **Establir major seguiment dels clients / usuari.**
- **Millorar satisfacció** X
- **Fomentar la innovació** X
- **Potenciar el coneixement dels empleats** X

Observacions – Pròxims passos per definir una estratègia de mobilitat:

- Informació adicional sobre els projectes "Ipad per VIPs" I "Dropbox Corporatiu".
- Conclusions sobre l'estudi de les aplicacions d'escriptori que esta en procés.
- Analitzar la 27ssume27o d'impressió actual i la seva 27ssume27one s per tal de proposar millores.
- En el cas de l'accés a recursos de forma remota desde PC tradicional, definir en detall les necesitats i valorar la millor 27ssume27o.

Annex 3.2.7. IT Mobility Quiz

Personal – Organització del departament:

Rols/Càrrecs	Necessitats de Mobilitat	LIdT	Dispositiu Mòbil
Gerència	PC Remot + repositoris d'arxius	X	X
Dir. Processos	No aplica		
Dir. Projectes	No aplica		
Dir. Tramits electrònics	PC Remot + repositoris d'arxius	X	X
Dir. Atenció al Client	PC Remot + repositoris d'arxius	X	
Dir. Explotació i Sistemes	Smartphone/Tablet (tècnics de camp)		X
Dir. Desenvolupament de projectes	No aplica		
Dir. Govern TIC I Seguretat	No aplica		

Processos i Tasques – Processos de negoci sensibles de millora amb la incorporació de dispositius mòbils.

- Connectivitat a la xarxa 27ssume27one en tot moment.
- Disponibilitat de recursos i serveis remotament.
- Seguiment de les actuacions dels tècnics de camp en temps real.
- Possibilitat de realitzar informes I obrir incidències "in-situ".

Dispositius – Existència de dispositius mòbils de nova generació (Smartphones i/o Tablets):

- No o no hi han dades.

Aplicacions o Serveis – Existeixen aplicacions de negoci desenvolupades per a dispositius mòbils? En cas afirmatiu, Quines? En cas negatiu, Quines voldríeu tenir a curt termini?

- Eines de "Ticketing"

Aplicacions o Serveis – Respecte als dispositius no corporatius (BYOD), quins serveis i/o aplicacions corporatives han de ser accessibles?

TOT □	**Repositoris de dades** □	**Intranet** □		
CAP □	**A definir X**	**Correu** □	**VPN** □	**Aplicacions** □

Objectius – Eficiència operativa i la reducció de costos

- **Reduir temps operatius** X
- **Ràpida resolució d'aprovacions i decisions** X
- **Facilitar la col · 28ssume28one d'activitats laborals**
- **Augmentar l'eficiència d'actius.**
- **Reduir els costos d'atenció a client / usuari.** X

Objectius – Creixement en productivitat i avantatge competitiu

- **Obrir nous canals de negoci/treball** X
- **Establir major seguiment dels clients / usuari.** X
- **Millorar satisfacció**
- **Fomentar la innovació** X
- **Potenciar el coneixement dels empleats** X

Observacions – Pròxims passos per definir una estratègia de mobilitat:

- Analitzar les necessitats de lloc de treball remot, veure la possibilitat de anar cap a un model basat en dispositius mòbils o un model d'escriptori remot (PC).
- Estudiar els treballs dels diferents tècnics de camp per 28ssume28one les necessitats.
- Estudi de les aplicacions de negoci i valorar si son aptes per accedir des de Smartphones i Tablets (si fos necessari).

Annex 3.2.8. Legal Mobility Quiz

Personal – Organització del departament:

Rols/Càrrecs	Necessitats de Mobilitat	LIdT	Dispositiu Mòbil
Inspectors	Smartphone/Tablet: Elaboració informes		X
Advocats	Smartphone/tablet: Consulta repositoris documentals i Apps corporatives		X

Processos i Tasques – Processos de negoci sensibles de millora amb la incorporació de dispositius mòbils.

- Inspectors – Elaboració "in-situ" de informes i valoracions, directament a l'aplicació i amb sincronització amb la plataforma servidora.
- Advocats – Accés a dades, documents i repositoris d'arxius de forma remota.
- Potenciació del teletreball.
- Utilització de les aplicacions corporatives des de dispositius mòbils.

Dispositius – Existència de dispositius mòbils de nova generació (Smartphones i/o Tablets):

- PDAs els inspectors

Aplicacions o Serveis – Existeixen aplicacions de negoci desenvolupades per a dispositius mòbils? En cas afirmatiu, Quines? En cas negatiu, Quines voldríeu tenir a curt termini?

- Aplicació inspectors.

Aplicacions de negoci (ERP):

- Aplicació al núvol.
- Aplicació interna sense accés des de l'exterior.

Aplicacions o Serveis – Respecte als dispositius no corporatius (BYOD), quins serveis i/o aplicacions corporatives han de ser accessibles?

TOT □	**Repositoris de dades** □	**Intranet** □		
CAP □	**A definir X**	**Correu** □	**VPN** □	**Aplicacions** □

Objectius – Eficiència operativa i la reducció de costos

Reduir temps operatius	X
Ràpida resolució d'aprovacions i decisions	
Facilitar la col · 29ssume29one d'activitats laborals	X
Augmentar l'eficiència d'actius.	
Reduir els costos d'atenció a client / usuari.	X

Objectius – Creixement en productivitat i avantatge competitiu

Obrir nous canals de negoci/treball	X
Establir major seguiment dels clients / usuari.	X
Millorar satisfacció	
Fomentar la innovació	
Potenciar el coneixement dels empleats	X

Observacions – Pròxims passos per definir una estratègia de mobilitat:

- Definir política per a dispositius no corporatius (BYOD).
- Estudi de les aplicacions de negoci i valorar les adaptacions necessàries per utilitzar-les des de dispositius mòbils.
- Estudi infraestructura VPN per poder accedir a l'entorn corporatiu.

Annex 3.2.9. Presidency Mobility Quiz

Personal – Organització del departament:

Rols/Càrrecs	Necessitats de Mobilitat	LIdT	Dispositiu Mòbil
VIP	PC Remot + Tablet (iPad)	X	X
Usuari	PC Remot – Usuaris Backoffice (ofimàtic + Internet)	X	

Processos i Tasques – Processos de negoci sensibles de millora amb la incorporació de dispositius mòbils.

- Millora de la disponibilitat de la documentació corporativa entre usuaris, des de fora de l'oficina i amb dispositius diferents al PC.

Dispositius – Existència de dispositius mòbils de nova generació (Smartphones i/o Tablets):

- No o no hi ha dades.

Aplicacions o Serveis – Existeixen aplicacions de negoci desenvolupades per a dispositius mòbils? En cas afirmatiu, Quines? En cas negatiu, Quines voldríeu tenir a curt termini?

- Correspondència Presidency.
- Actes i events Presidency.
- Mailing Presidency (basat en Notes).
- iPad per a Càrrecs VIP.

Aplicacions o Serveis – Respecte als dispositius no corporatius (BYOD), quins serveis i/o aplicacions corporatives han de ser accessibles?				
TOT □	**Repositoris de dades** □	**Intranet** □		
CAP □	**A definir X**	**Correu** □	**VPN** □	**Aplicacions** □

Objectius – Eficiència operativa i la reducció de costos	
Reduir temps operatius	
Ràpida resolució d'aprovacions i decisions	X
Facilitar la col · 30ssume30one d'activitats laborals	X
Augmentar l'eficiència d'actius.	
Reduir els costos d'atenció a client / usuari.	

Objectius – Creixement en productivitat i avantatge competitiu	
Obrir nous canals de negoci/treball	X
Establir major seguiment dels clients / usuari.	
Millorar satisfacció	X
Fomentar la innovació	
Potenciar el coneixement dels empleats	

Observacions – Pròxims passos per definir una estratègia de mobilitat:

- Analitzar els diferents perfils d'usuari per tal d'establir les necessitats d'escriptori.
- Valorar la possibilitat de fer el pas cap a dispositius de nova generació en alts càrrecs.
- Analitzar les aplicacions de negoci i determinar la millor opció de cara a mobilitzar-les.

Annex 3.2.10. Security Mobility Quiz

Personal – Organització del departament:

Rols/Càrrecs	Necessitats de Mobilitat	LIdT	Dispositiu Mòbil
Agent	Tablet – Igual a PC Xarxa.	X	X

Processos i Tasques – Processos de negoci sensibles de millora amb la incorporació de dispositius mòbils.

- Millora en el seguiment d'emergències o incidents.
- Millors capacitats d'elaboració d'informes i reporting a superiors.
- Flexibilitat en el treball col·laboratiu entre unitats.

Dispositius – Existència de dispositius mòbils de nova generació (Smartphones i/o Tablets):

- S'han rebut peticions però no s'estan atenent.
- Hi ha usuaris amb accés al correu corporatiu des del seus terminals (Smartphone i/o Tablet).

Aplicacions o Serveis – Existeixen aplicacions de negoci desenvolupades per a dispositius mòbils? En cas afirmatiu, Quines? En cas negatiu, Quines voldríeu tenir a curt termini?

- Aplicació C/S amb versió Web.
- Gestió RRHH i recursos materials.
- BBDD documental – aplicació Notes amb totes les ordres i directrius.

Aplicacions Mòbils:

- Intranet (en procés) – Auto-servei de l'empleat, accés des de internet a Dades personals i Peticions.

Aplicacions o Serveis – Respecte als dispositius no corporatius (BYOD), quins serveis i/o aplicacions corporatives han de ser accessibles?

TOT □	**Repositoris de dades** □	**Intranet** □		
CAP □	**A definir X**	**Correu** □	**VPN** □	**Aplicacions** □

Objectius – Eficiència operativa i la reducció de costos

- **Reduir temps operatius** X
- **Ràpida resolució d'aprovacions i decisions**
- **Facilitar la col · 31ssume31one d'activitats laborals** X
- **Augmentar l'eficiència d'actius.**
- **Reduir els costos d'atenció a client / usuari.** X

Objectius – Creixement en productivitat i avantatge competitiu

- **Obrir nous canals de negoci/treball** X
- **Establir major seguiment dels clients / usuari.** X
- **Millorar satisfacció**
- **Fomentar la innovació** X
- **Potenciar el coneixement dels empleats**

Observacions – Pròxims passos per definir una estratègia de mobilitat:

- Definir els rols de cadascun dels cossos/departaments per tal de valorar la disposició de nous dispositius i les necessitats d'accés a l'escriptori de forma remota.
- Definir més clarament la política d'ús per a usuaris BYOD que actualment tenen accés al correu corporatiu.
- Estudiar les aplicacions de negoci existents així com el seu ús, per tal de valorar la seva idoneïtat per a Smartphones i Tablets.

Annex 3.2.11. Territory Mobility Quiz

Personal – Organització del departament:

Rols/Càrrecs	Necessitats de Mobilitat	LIdT	Dispositiu Mòbil
Gerència	PC Remot + Dashboards + repositoris d'arxius	X	X

Processos i Tasques – Processos de negoci sensibles de millora amb la incorporació de dispositius mòbils.

- Territory Area Manager & Executive Management – Accés a quadres de comandament en temps real i als repositoris d'arxius.
- Millorar el procés de connexió a la xarxa corporativa a través de VPN.
- Utilització de la signatura electrònica des de dispositius mòbils.

Dispositius – Existència de dispositius mòbils de nova generació (Smartphones i/o Tablets):

- No o no hi ha dades.

Aplicacions o Serveis – Existeixen aplicacions de negoci desenvolupades per a dispositius mòbils? En cas afirmatiu, Quines? En cas negatiu, Quines voldríeu tenir a curt termini?

- Seguiment de temes importants.
- Coordinació Territorial + Guals i Via Pública:

- Inspeccions districtes.

Direcció de serveis al territori:

- Informes i actes de reunions.
- Accés a totes les aplicacions de desktop i a les carpetes corporatives.

Aplicacions o Serveis – Respecte als dispositius no corporatius (BYOD), quins serveis i/o aplicacions corporatives han de ser accessibles?				
TOT □	**Repositoris de dades** □	**Intranet** □		
CAP □	**A definir X**	**Correu** □	**VPN** □	**Aplicacions** □

Objectius – Eficiència operativa i la reducció de costos	
▪ **Reduir temps operatius**	X
▪ **Ràpida resolució d'aprovacions i decisions**	X
▪ **Facilitar la col · 32ssume32one d'activitats laborals**	
▪ **Augmentar l'eficiència d'actius.**	X
▪ **Reduir els costos d'atenció a client / usuari.**	

Objectius – Creixement en productivitat i avantatge competitiu	
▪ **Obrir nous canals de negoci/treball**	X
▪ **Establir major seguiment dels clients / usuari.**	
▪ **Millorar satisfacció**	X
▪ **Fomentar la innovació**	X
▪ **Potenciar el coneixement dels empleats**	

Observacions – Pròxims passos per definir una estratègia de mobilitat:

- Definir política per a dispositius no corporatius (BYOD).
- Estudi de les aplicacions de negoci i valorar si son aptes per accedir des de Smartphones i Tablets.
- Analitzar el sistema de signatura electrònica amb certificat d'usuari des de dispositius mòbils.
- Analitzar la infraestructura VPN present i proposar millores.per a Smartphones i Tablets.

Annex 3.3. Summary of Mobility requirements detected

Annex 3.3.1. Mobility needs by user role

Àrees	Rols/Càrrecs	Necessitats de Mobilitat	PC	Dispositiu Mòbil
Presidency	VIPs	PC Remot + Tablet (carpeta de l'electe)	✓	✓
	Usuari	PC Remot – Usuaris Backoffice (ofimàtic + Internet)	✓	
Legal	Inspectors	Smartphone/Tablet: Elaboració informes		✓
	Advocats	Smartphone/tablet: Consulta repositoris documentals I Apps corporatives		✓
Finance	Directors	PC Remot + Tablet	✓	✓
	Inversió	Repositori Dades + Correu		✓
	Inspector	Obertura, consulta i seguiment d'incidències, reclamacions, etc.		✓
	Manager	PC Remot + Tablet	✓	✓
Territory Management	Cos Gerencial	PC Remot + Dashboards + repositoris d'arxius	✓	✓

Audit	Gerent	Informes de les actuacions realitzades al 33ssume33one.		✓
	Inspector	Obertura, consulta i seguiment d'informes, incidències, etc.		✓
Executive Mgmnt	VIPs	Smartphone/Tablet		✓
Communication and Press	Direcció Comunicació	PC remot + Smartphone – Ofimàtic + Documentació corporativa	✓	✓
	Dept. Internet	PC remot – Part 33ssume33one Webs	✓	
	Servei Tlf i oficines	PC remot – Atenció usuaris	✓	
	Incidències	PC remot – Atenció incidències, reclamacions o sol·licituds	✓	
	Serveis Publicitaris	PC remot – Edició multimèdia + Xarxes socials + accés a documentació	✓	
	Servei imatge I p. editorial	PC remot – Disseny 33ssume33 I edició multimèdia	✓	
Corporate University	VIP	PC remot + Smartphone/tablet	✓	✓
	Técnic	Tablet/portátil	✓	✓
IT	Gerència	PC Remot + repositoris d'arxius	✓	✓
	e-Tràmits	PC Remot + repositoris d'arxius	✓	✓
	At. Al Client	PC Remot + repositoris d'arxius	✓	
	Explotació	Smartphone/Tablet (tècnics de camp)		✓
Security	Agent	Tablet. Igual a PC Xarxa.	✓	✓
RRHH	Alt Càrrec	Portàtil + Tablet	✓	✓
	SSGG	Tablet per Ordres de treball (App SIGEF)		✓
	Interventor	Signatura digital móbil		✓
	Admin. Gral.	Accés a recursos en remot	✓	
	Compres	Accés a recursos en remot	✓	
	RRHH	Accés a recursos en remot	✓	

Annex 3.3.2. Apps and Services sensible to mobilize by company's departments

Àrea	Dispositius mòbils actuals	Requeriments específics de mobilitat (Aplicacions, serveis, accessos, etc.)
Presidency	iPad per a càrrec VIP	▪ Correspondència Presidency ▪ Actes I events Presidency ▪ Mailing Presidency (basat en Notes).
Legal	PDAs (inspectors)	▪ Aplicació inspectors. ▪ Aplicació al núvol. ▪ Aplicació interna sense accés des de l'exterior.
Finance	No o no hi han dades	▪ Aplicació d'escriptori per a Inspectors. ▪ Peticions de servei (Web – J2EE). ▪ Gestor de demanda I projectes (Web – J2EE). ▪ Processos d'aprovacions financeres.
Territory Mgmnt	No o no hi han dades	▪ Gerència ▪ Seguiment de temes importants. ▪ Coordinació Territorial:

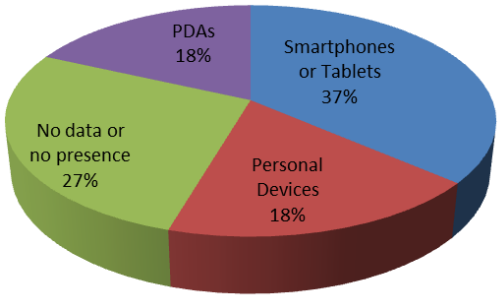
		▪ Inspeccions districtes. ▪ Direcció de serveis al 34ssume34one: ▪ Informes i actes de reunions. ▪ *Sistema de signatura 34ssume34one amb certificat d'usuari des de dispositius mòbils.*
Audit	PDAs (Inspectors ~200) + Dispositius de tercers + Altres dispositius	▪ Aplicacions per a PDAs dels inspectors: ▪ Aplicació inspectors (Possible evolució a HTML5). Usuari intern. ▪ Aplicació inspectors (sacs de runa, contenidors metàlics, enganxines, cartells…) (No 34ssume34one). Usuari extern. ▪ Aplicació corporativa sobre PDA per valoració afectació arbrat via pública (guals, obres…). Usuari intern. ▪ Aplicació corporativa sobre PDA per control de qualitat contractes de serveis. Usuari extern. ▪ Aplicació d'empreses contractistes per servei. Usuari extern. ▪ Aplicacions no presents per a dispositius mòbils: ▪ Control inventari espai públic, espais verds, pavimentació, fonts, enllumenat… ▪ Consulta i actualització catàleg patrimoni ▪ *Els Managers hauríen de disposar de tablets, igual que perfils Gerents I Directors*
		▪ *Solució d'impressió per a dispositius mòbils* ▪ **Direcció comunicació:** ▪ Planificació I control campanyes publicitàries ▪ **Departament Internet:** ▪ Plataforma Host. ▪ Middleware portal de tràmits. ▪ Servei Telefònic I oficines: ▪ Portal de tràmits. ▪ Agenda equipaments ▪ **Departament d'Incidències:** ▪ Gestor Documental ▪ Incidències ▪ Accés Frameworks Desenvolupament (Drupal, Wordpress, Vignette). ▪ **Serveis Publicitaris:** ▪ Xarxes socials I contingut multimèdia ▪ **Direcció Estudis I Avaluacions:** ▪ Estadístiques ▪ Anàlisi Tweets ▪ Registre enquestes I estudis ▪ **Imatge I producció editorial:** ▪ Aplicacions disseny gràfic, maquetació i edició multimèdia.
Executive Mgmnt	VIPs	▪ No hi han dades (WiFI-Doc)

Corporate University	Smartphones Tablets	▪ Centres de Investigació: ▪ Inventari Centre ▪ Magatzems – Registre peces I moviments. ▪ Acreditacions ▪ Centres Formadors: ▪ Aplicació per a tota la gestió administrativa d'inscripcions. ▪ Centres de Ciències: ▪ Aplicació per a (tècnics de camp que faciliti la tasca de recollida d'informació. (a proposar)
IT	Dispositius personals amb correu corporatiu	▪ Direcció d'Explotació I Sistemes: ▪ Eines de "Ticketing" ▪ Geréncia TIC: ▪ Requeriments de negoci propi. ▪ Directors I Gerents: e-identitat I e-signatura ▪ Nous Canals: proves de desenvolupament de *.mobi ▪ Explotació I Sistemes: Eines d'atenció a usuaris pels referents in situ (referents i/o tècnics camp)
Security	Dispositius personals amb correu corporatiu	▪ Aplicacions de Negoci: ▪ Aplicació C/S amb versió Web. ▪ Gestió RRHH I recursos materials (GUB I Bombers). ▪ BBDD documental – 35ssume35one Notes amb totes les ordres i directrius. ▪ Aplicacions Mòbils: ▪ Intranet (en procés) – Auto-servei de l'empleat, accés des de internet + Dades personals i Peticions.
RRHH	iPad per a càrrec VIP	▪ Elaboració de ordres de treball. ▪ *Solució d'impressió per a dispositius mòbils*

Annex 3.3.3. Mobility Requirements Analysis

Annex 3.3.3.1. Existence of Mobile Devices by departments

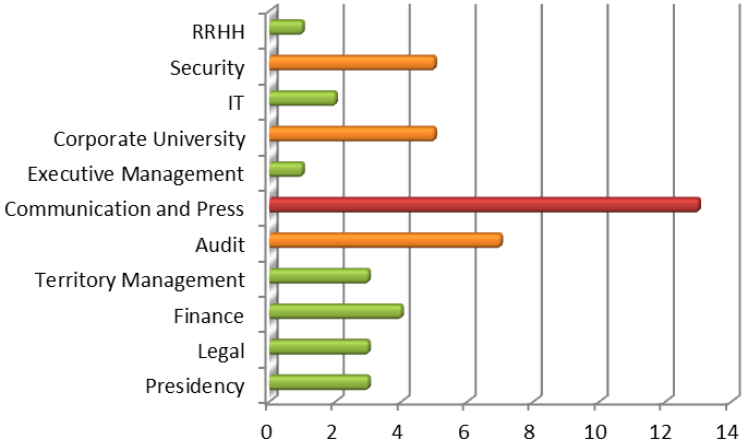
Device Type	# of Departments
Smartphones / Tablets	4
Personal Devices	2
No data or no presence	3
PDAs	2
Total	11



Annex Tab. 6 Mobile devices by departments **Annex Fig. 6 Devices distribution**

Annex 3.3.3.2. Business Apps sensible to mobilize by department

Area	# Apps
Presidency	3
Legal	3
Finance	4
Territory Management	3
Audit	7
Comm's and Press	13
Executive Management	1
Corporate University	5
IT	2
Security	5
RRHH	1

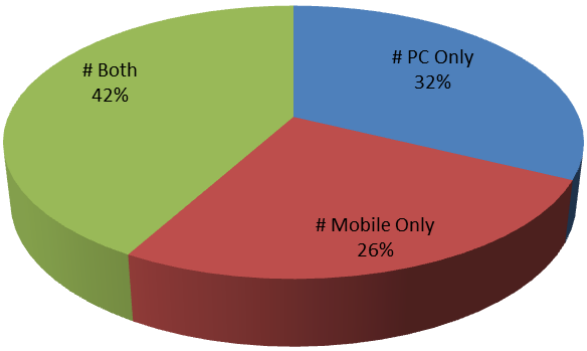


Annex Tab. 7 Apps per department **Annex Fig. 7 Apps per department**

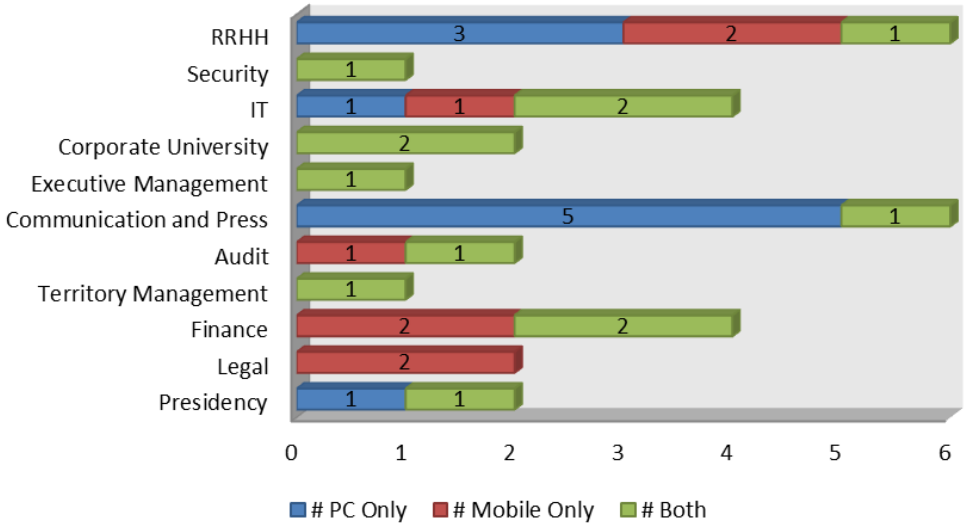
Annex 3.3.3.3. Roles distribution by mobility needs and dept.

Annex Tab. 8 Roles distribution by department

Area	# Roles	# PC Only	# Mobile Only	# Both
Presidency	2	1		1
Legal	2		2	
Finance	4		2	2
Territory Management	1			1
Audit	2		1	1
Communication and Press	6	5		1
Executive Management	1			1
Corporate University	2			2
IT	4	1	1	2
Security	1			1
RRHH	6	3	2	1
Total	**31**	**10**	**8**	**13**



Annex Fig. 8 Mobility needs distribution



Annex Fig. 9 Roles per department and quantity

ANNEX 4. PHASE 1: EMM PROGRAM SCOPE AND PLANING

Annex 4.1. EMM program scope and planning

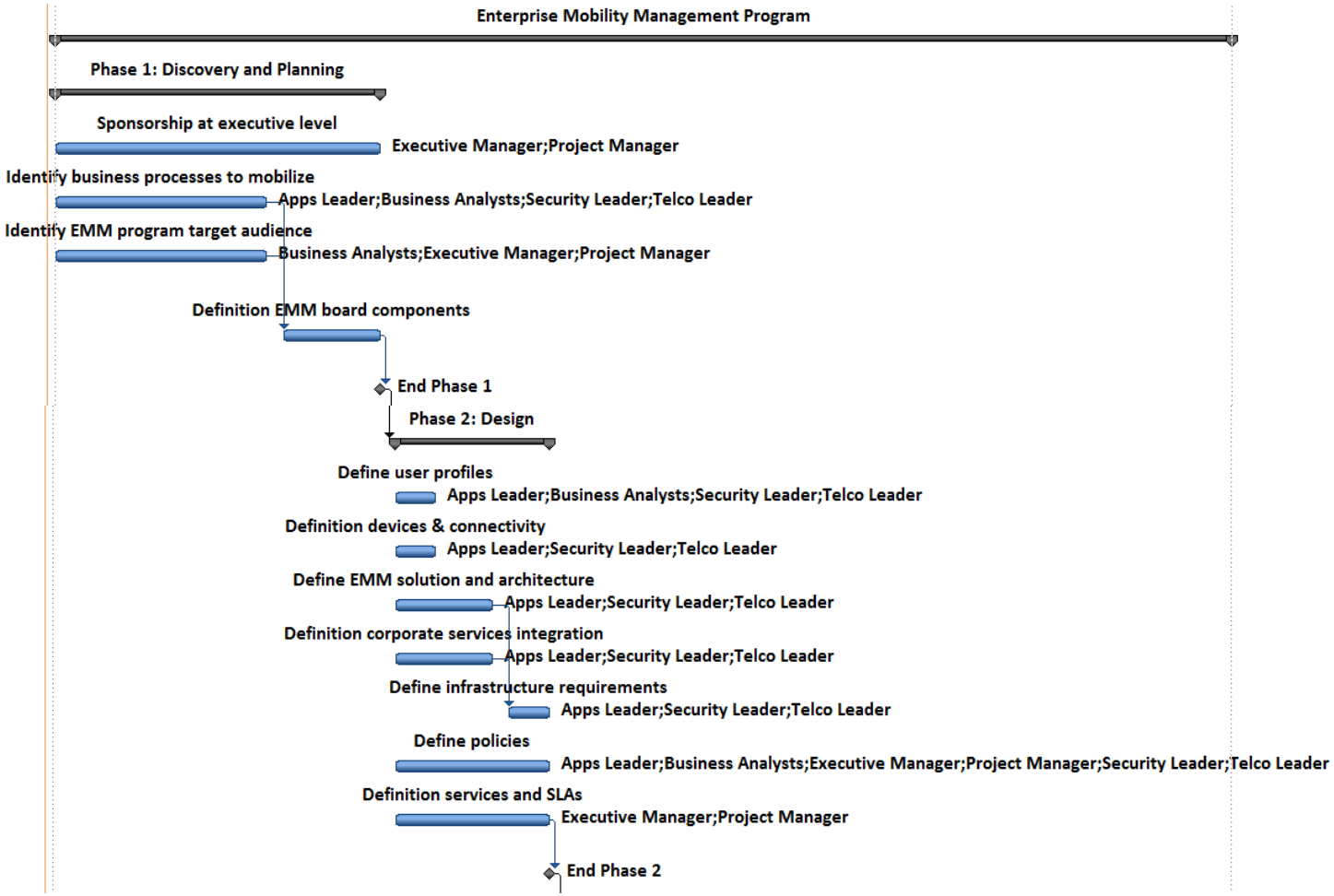
The EMM program scope summarizes the aims, activities and milestones to reach at each phase. Also a detailed Gantt diagram with all tasks, duration and resources used at each one can be consulted at [ANNEX 4.].

Annex Tab. 9 Enterprise Mobility Management program scope

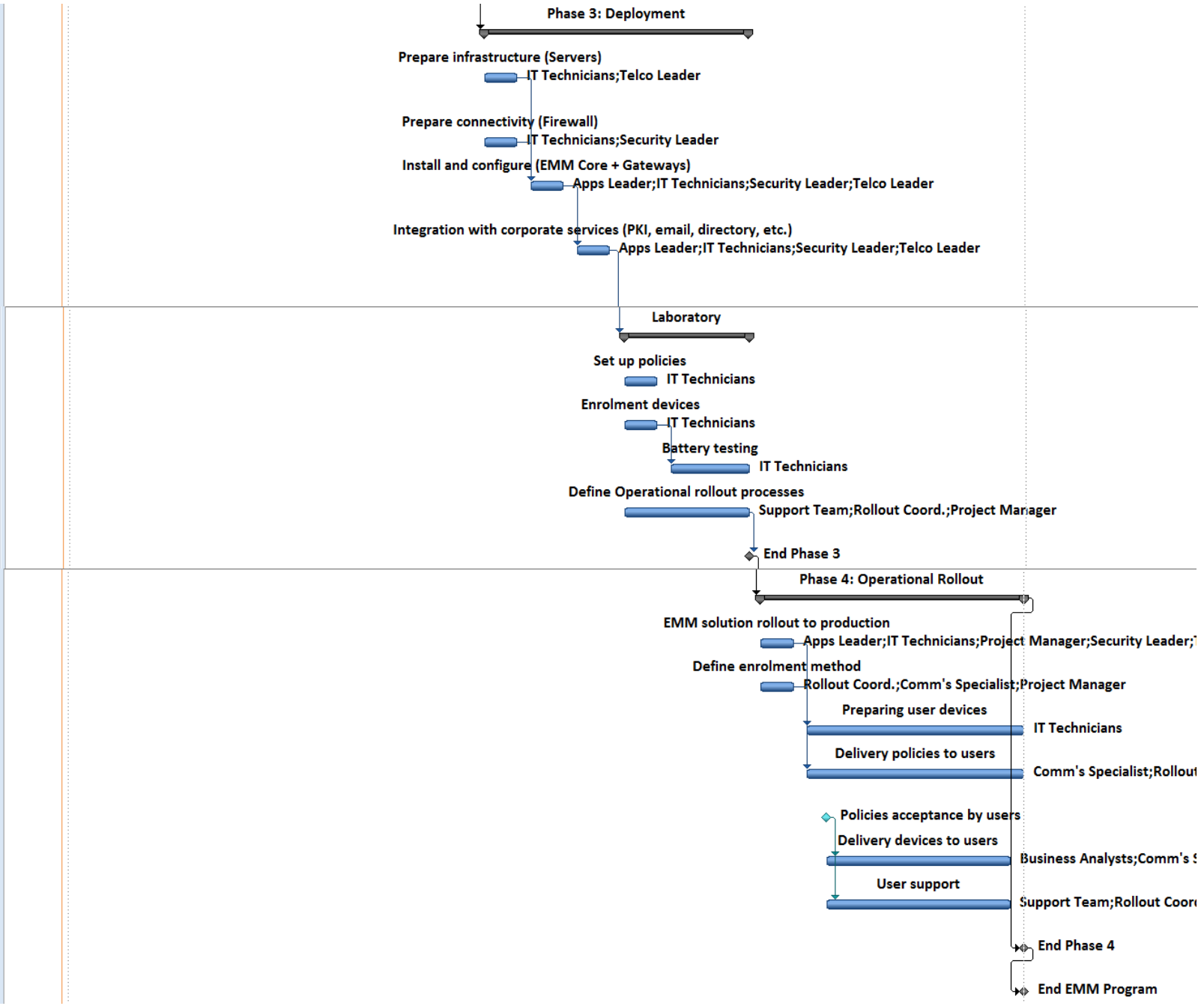
	Key activities	Milestones
Phase 1: Discovery and Planning	▪ Definition EMM board components ▪ Identify business processes to mobilize. ▪ Identify the target audience within the EMM program. ▪ Sponsorship at executive level.	▪ Project Kick-off with technical and project team members ▪ Finalized Business Requirements ▪ Clearly defined goals, scope, resources and time
Phase 2: Design	▪ Define user profiles. ▪ Analysis and definition of devices and connectivity requirements needed. ▪ Define EMM solution and its architecture (Cloud / On-Premise). ▪ Define infrastructure requirements needed to implement the EMM tool. ▪ Definition of integrated corporate services (Wi-Fi, VPN, Email, etc.). ▪ Define policies (use, security, applications, etc.). ▪ Definition of services and Service Levels Agreements (SLA) from suppliers.	▪ Deployment Architecture and Design Diagram ▪ Policies Summary Design Documents ▪ Corporate services Integration Design Approach
Phase 3: Deployment	▪ Preparation of installation infrastructure (Servers). ▪ Preparation of the technical requirements of connection (Firewall). ▪ Installation and configuration of the solution (EMM + Core Gateways). ▪ Integration with corporate services (Wi-Fi, PKI, email, directory, etc.). ▪ Setting up policies and enrolment laboratory devices. ▪ Preparation battery testing and operational rollout processes definition.	▪ Deployment environment readiness confirmed prior to install ▪ Installation and configuration complete ▪ Testing complete ▪ Device enrolment and registration complete for pilot users
Phase 4: Operational rollout	▪ EMM solution rolls out into production environment. ▪ Preparing user devices according defined mobility services. ▪ Define devices EMM system enrolment method (IT or user auto-enrolment). ▪ Delivery policies to users (usage, security and applications). ▪ Managing the delivery of devices to users. ▪ User support during the deployment.	▪ Provision of devices. ▪ Acceptance of policies by users. ▪ IT team Readiness for Technical Support and Escalations ▪ Clearly Defined deployment Processes

Annex 4.1. Extended Gantt diagram of project

Enterprise Mobility Management Program	**105 días**
Phase 1: Discovery and Planning	**30 días**
Sponsorship at executive level	30 días
Identify business processes to mobilize	20 días
Identify EMM program target audience	20 días
Definition EMM board components	10 días
End Phase 1	0 días
Phase 2: Design	**15 días**
Define user profiles	5 días
Definition devices & connectivity	5 días
Define EMM solution and architecture	10 días
Definition corporate services integration	10 días
Define infrastructure requirements	5 días
Define policies	15 días
Definition services and SLAs	15 días
End Phase 2	0 días



Phase 3: Deployment	**30 días**	
Prepare infrastructure (Servers)	5 días	
Prepare connectivity (Firewall)	5 días	
Install and configure (EMM Core + Gateways)	5 días	
Integration with corporate services (PKI, email, directory, etc.)	5 días	
Laboratory	**15 días**	
Set up policies	5 días	
Enrolment devices	5 días	
Battery testing	10 días	
Define Operational rollout processes	15 días	
End Phase 3	0 días	
Phase 4: Operational Rollout	**30 días**	
EMM solution rollout to production	5 días	
Define enrolment method	5 días	
Preparing user devices	25 días	
Delivery policies to users	25 días	
Policies acceptance by users	0 días	
Delivery devices to users	20 días	
User support	20 días	
End Phase 4	0 días	
End EMM Program	0 días	



Annex 4.2. Mobility program tasks by role

Project Manager

- *Sponsorship at executive level*
- *Identify EMM program target audience*
- *Definition EMM board components*
- *Define policies*
- *Definition services and SLAs*
- *Define Operational rollout processes*
- *EMM solution rollout to production*
- *Define enrolment method*

Executive Manager

- *Sponsorship at executive level*
- *Identify EMM program target audience*
- *Definition EMM board components*
- *Define policies*
- *Definition services and SLAs*

Business Analysts

- *Identify business processes to mobilize*
- *Identify EMM program target audience*
- *Define user profiles*
- *Define policies*
- *Delivery devices to users*

Security Leader

- *Identify business processes to mobilize*
- *Define user profiles*
- *Definition devices & connectivity*
- *Define EMM solution and architecture*
- *Definition corporate services integration*
- *Define infrastructure requirements*
- *Define policies*
- *Prepare connectivity (Firewall)*
- *Install and configure (EMM Core + Gateways)*
- *Integration with corporate services (PKI, email, directory, etc.)*
- *EMM solution rollout to production*

Comm's Specialist

- *Define enrolment method*
- *Delivery policies to users*
- *Delivery devices to users*

Rollout Coord.

- *Define Operational rollout processes*
- *Define enrolment method*

Telco Leader

- *Identify business processes to mobilize*
- *Define user profiles*
- *Definition devices & connectivity*
- *Define EMM solution and architecture*
- *Definition corporate services integration*
- *Define infrastructure requirements*
- *Define policies*
- *Prepare infrastructure (Servers)*
- *Install and configure (EMM Core + Gateways)*
- *Integration with corporate services (PKI, email, directory, etc.)*
- *EMM solution rollout to production*

Apps Leader

- *Identify business processes to mobilize*
- *Define user profiles*
- *Definition devices & connectivity*
- *Define EMM solution and architecture*
- *Definition corporate services integration*
- *Define infrastructure requirements*
- *Define policies*
- *Install and configure*
- *Integration with corporate services*
- *EMM solution rollout to production*

IT Technicians

- *Prepare infrastructure (Servers)*
- *Prepare connectivity (Firewall)*
- *Install and configure (EMM Core + Gateways)*
- *Integration with corporate services (PKI, email, LDAP, etc.)*
- *Set up policies*
- *Enrolment devices*
- *Battery testing*
- *EMM solution rollout to production*
  - *Preparing user devices*

ANNEX 5. PHASE 2 TECHNICAL RESOURCES

Annex 5.1. Firewall rules for on-premise deployment

Annex Tab. 10 From DMZ to corporate LAN:

▪ **EMM Core - LDAP / Active Directory**	TCP 636/389
▪ **EMM Core - SMTP Relay for SMS and Email Notifications**	TCP 25
▪ **EMM Core - DNS Lookup**	UDP 53
▪ **EMM Core - NTP Time Synchronization Service**	UDP 123
▪ **EMM Core - Certificate / SCEP Server**	HTTP 443
▪ **App/mail gateway - CIFS-based Content Server**	TCP 445
▪ **App/mail gateway - Certificate / SCEP Server**	HTTP/S 80/443
▪ **App gateway - App Server for AppTunnel**	HTTP/S 80/443
▪ **Mail gateway - Exchange ActiveSync**	HTTP/S 80/443
▪ **App/mail gateway - DNS Lookup**	UDP 53
▪ **App/mail gateway - NTP Time Synchronization Service**	UDP 123
▪ **App/mail gateway - LDAP / Active Directory**	TCP/UDP 389

Annex Tab. 11 From corporate LAN to DMZ:

▪ **Administrator Portal Access and Self-Service Portal - EMM Core**	HTTPS 443
▪ **Administrator Access - EMM Core**	SSH 22
▪ **Admin Portal Access and Self-Service Portal - App/mail gateway**	HTTPS 443
▪ **Gateway Administrator Access - App/mail gateway**	SSH 22

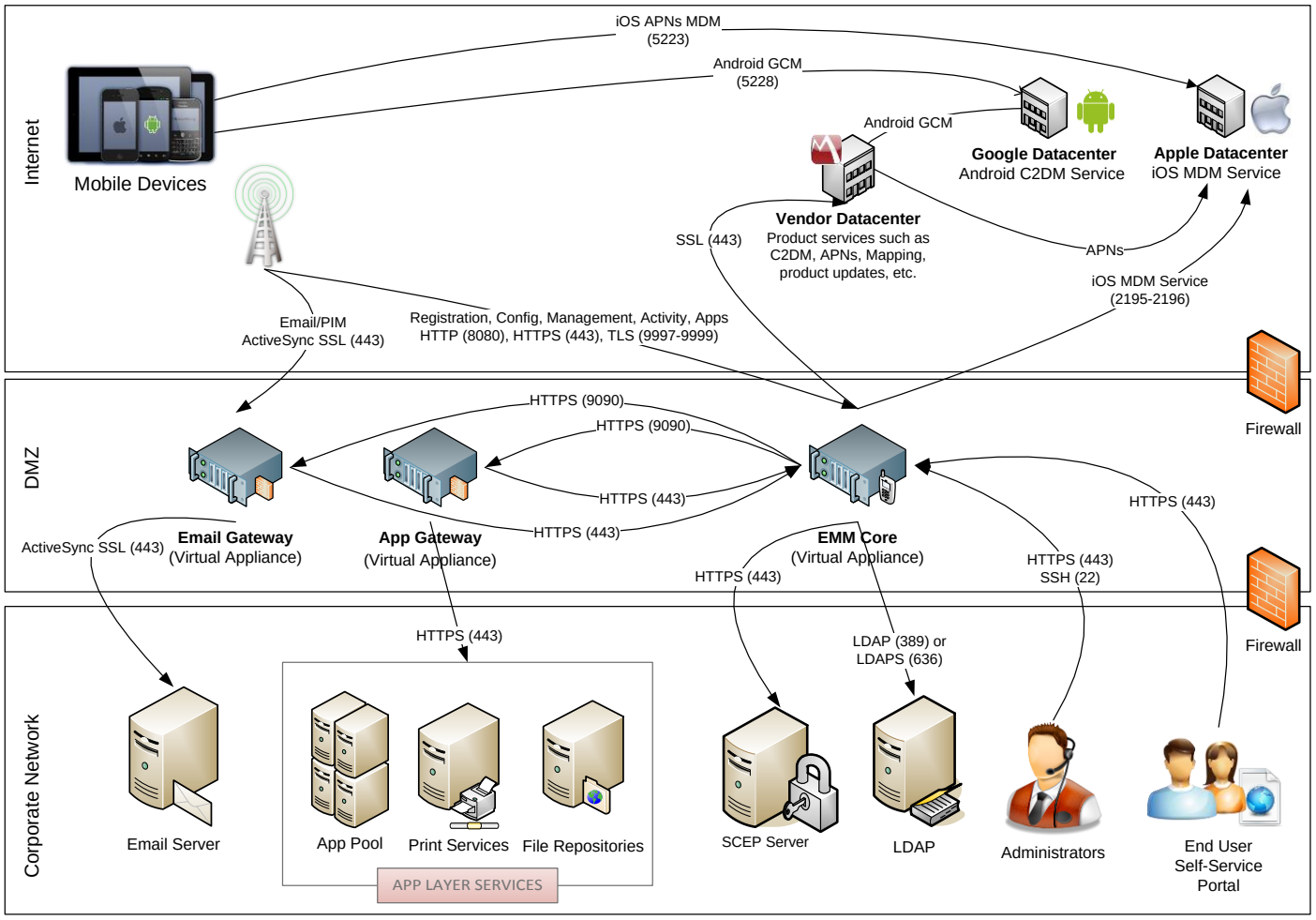
Annex Tab. 12 From Internet to DMZ:

▪ **End user devices - EMM Core**	TCP 9997
▪ **iOS end user devices - EMM Core**	HTTPS 443
▪ **Access Email via Sentry or to Access AppTunnel - App/mail gateway**	HTTP/S 80/443

Annex Tab. 13 From DMZ to Internet:

▪ **EMM Core – Vendor gateway**	HTTPS 443, SSH 22
▪ **EMM Core - Apple APNS and MDM Services**	TCP 2195, 2196
▪ **EMM Core - iTunes, Antivirus, and Maps/Location**	HTTP 80
▪ **App/mail gateway – Vendor Software update**	HTTPS 443, SSH 22

Annex 5.2. Final Infrastructure design



Annex Fig. 10 Full solution Topology diagram

ANNEX 6. PHASE 2 CORPORATE POLICY TEMPLATES

Annex 6.1. Use Policy for COPE devices

Data Plan Policy
▪ All new employees whose positions require them to use a mobile device will be provided equipment that is covered under a Company-sponsored plan billed directly to the Company. However, excessive personal usage or excessive/unnecessary roaming and international charges will be billed to the employee. ▪ No reimbursement, equipment or connectivity will be provided to any employee who does not agree to these policies.
User Agreement
▪ I will be using the mobile device for conducting company business and it is my responsibility, in addition to the efforts of Company, to protect corporate data on my mobile device. ▪ That Company will only reimburse for mobile device usage in accordance with the Company mobile device policy above. ▪ When using the mobile device I shall observe all applicable local and state laws including all such laws restricting the use of mobile devices while driving. ▪ That the EMM agent will be installed on the mobile device to provide security and remote management to protect my business/personal data by erasing contents from the device in the event of a security breach or notification from the end-user that the device has been lost/stolen/misplaced. ▪ Company reserves the right to wipe all data from the mobile device in the event of employee or contractor separation from the company. Where possible, reasonable attempts will be made to preserve personal data on the device. However, if Company deems it necessary, a full device wipe will be issued. ▪ That a password on the mobile device must be maintained at all times. After X failed password attempts to log into the device the device will be automatically wiped. Passwords must be kept private. Do not share passwords with anyone, write them down or use them in public or common areas without adequate precautions. ▪ That Company has the right, at any time and without notice, to suspend or deny access to corporate resources, including email, to mobile devices that fail to meet Company's standards for mobile security and management, including minimum hardware and software versions, password policies, compromised OS, encryption and application restrictions. ▪ I have read and will abide by the Company Mobile Device Policy.

Annex 6.2. Security Policy for COPE devices

Device Security Policy
▪ All Corporate Mobile Devices must be secured and managed by Company. This includes running the Enterprise Mobility Management (EMM) software client to allow security policy configuration and device compliance monitoring and control. The

EMM client uninstallation by end user is forbidden and detectable by the EMM platform. The EMM platform will automatically block corporate access if the EMM client is uninstalled or unconfigured.

- All mobile devices must have an approved AntiVirus security application installed. At the time of this policy, the approved AntiVirus application is avast! Mobile Security. AntiVirus Mobile Security application protects the mobile device against malware and other malicious attacks. The uninstallation of this application by end user is prohibited and detectable by the EMM platform.
- All Mobile devices must be protected with passcode and encrypted to secure corporate data. The specific requirements are specified below.
- All Mobile Devices automatically check in periodically to the EMM platform for surveillance and configuration updates. The EMM platform will automatically. The EMM platform will block corporate email access if a device has not checked in in 7 days until the next check-in.
- The EMM platform can “Wipe” managed mobile devices remotely in case of theft or loss.

Encryption Policy

- All Mobile Devices must be encrypted irrespective of the type of network connection. (Example: 3G, WiFi, etc...)
- Native on-device data at rest encryption may be hardware or software based. Full device encryption and/or application-based encryption are acceptable
- All devices must support certificates for registration, authentication, and data encryption.
- All corporate data must be at rest in managed apps or in secure container.

PIN Lock Policy

- All devices must be locked with a PIN meeting the following requirements:
  - Minimum length of 4 digits
  - Automatically wipe the device after a maximum of 10 failed login attempts
  - Require Mobile Device PIN change every 60 days
- Set inactivity idle time-out to 5 minutes maximum (auto-lock)
- Set grace period to 15 minutes maximum (re-enter PIN)

Reporting

- Users must report lost, stolen, missing or replaced devices to the Service Desk. Notification should be immediate, but no later than 24 hours.

Annex 6.3. Bring Your Own Device Policy

Data Plan Policy

- For executives, managers and sales employees, the Company will reimburse 80% of all approved voice and data plans (the Company assumes that 20% of usage is personal). A copy of the bill must be at your expense report.
- For non-executive, non-managers and non-sales employees whose positions require them to use their personal cell/smartphone for Company business, the

Company will reimburse a flat €15 per month (but not more than the cost of the plan) directly on your paycheck for approved voice and data plans.

- For all other employees, approved personal smartphones can be used to connect to corporate email and resources without any reimbursement of voice or data charges.
- No reimbursement, equipment or connectivity will be provided to any employee who does not agree to these policies.

User Agreement

- I will be using the mobile device for conducting company business and it is my responsibility, in addition to the efforts of Company, to protect corporate data on my mobile device.
- That I am responsible for providing and maintaining my mobile device, cellular service plan for my device, any necessary equipment and accessories for my device.
- That Company will only reimburse for mobile device usage in accordance with the Company mobile device policy above.
- That the EMM agent will be installed on the mobile device to provide security and remote management to protect my business/personal data by erasing contents from the device in the event of a security breach or notification from the end-user that the device has been lost/stolen/misplaced.
- That a password on the mobile device must be maintained at all times. After X failed password attempts to log into the device the device will be automatically wiped. Passwords must be kept private. Do not share passwords with anyone, write them down or use them in public or common areas without adequate precautions.
- That Company has the right, at any time and without notice, to suspend or deny access to corporate resources, including email, to mobile devices that fail to meet Company's standards for mobile security and management, including minimum hardware and software versions, password policies, compromised OS, encryption and application restrictions.
- I have the right to opt out of the program and all corporate access and corporate data will be removed from the device. I am also responsible for removing any corporate data from all other locations where it has been copied or replicated.
- To the maximum extent permitted by law, Company will have no liability for the loss, destruction, loss of use, theft or misuse of or damage to the mobile device or any personal data on the mobile device, even if caused by Company's actions or failure to act.
- That Company may change or terminate this program at any time upon thirty (30) days advance notice without further obligation.
- I have read and will abide by the Company Mobile Device Policy.

Device Security Policy

- Only COMPANY approved device models can access corporate resources. The list of approved devices can be found on COMPANY BYOD approved devices.
- All Mobile Devices accessing COMPANY corporate resources must configure and run the EMM agent to allow security policy configuration and device compliance monitoring and control. User is free to disable or uninstall the EMM agent at his own

wish, but it will result in no access to corporate resources.

- All Mobile devices must be protected with passcode and may be preferably encrypted to secure corporate data. The specific requirements are specified below.
- All Mobile Devices automatically check in periodically to the EMM platform for surveillance and configuration updates. The EMM platform will automatically. The EMM platform will block corporate email access if a device has not checked in in 7 days until the next check-in.
- All mobile devices must have an approved AntiVirus security application installed. At the time of this policy, the approved AntiVirus application is avast! Mobile Security.AntiVirus Mobile Security application protects the mobile device against malware and other malicious attacks. The uninstallation of this application by end user is prohibited and detectable by the EMM platform.
- All devices must be encrypted to protect corporate data.The EMM platform can “Wipe” managed mobile devices remotely in case of theft or loss.

Encryption Policy

- All Mobile Devices should be preferably encrypted, if encryption capability available on the device. Native on-device data at rest encryption may be hardware or software based.
- All Mobile Devices accessing the corporate intranet must be encrypted and support certificates for registration, authentication, and data encryption.

PIN Lock Policy

- All devices must be locked with a PIN meeting the following requirements:
- Minimum length of 4 digits (at least 6 for android devices, required for encryption).
- Automatically wipe the device after a maximum of 10 failed login attempts
- Require Mobile Device PIN change every 60 days
- Set idle time-out to 5 minutes maximum (auto-lock)
- Set grace period to 15 minutes maximum (re-enter PIN)

Reporting

- Users must report lost, stolen, missing or replaced devices to the Service Desk. Notification should be immediate, but no later than 24 hours.
- Users must report to IT when a registered device will not be used anymore to access corporate resources in order to deprovision device corporate access..

Application Security Policy

- All installed applications on devices accessing corporate resources must be downloaded from legitimate, official sources (AppStore for iOS, Google Play for android, Marketplace for Windows Phone). Applications obtained outside previously mentioned channels with the exception of enterprise developed apps are considered rogue applications and are not allowed.
- **Cloud-based applications may not be used with corporate data.**
- **SMS and/or Instant messaging applications may not be used to discuss company business.**

- **Third party email applications may not be used to conduct company business.**
- **Password management applications may not be used to store corporate accounts information.**

Mobile OS Patches

- Security relevant updates should be applied within thirty days.

End User Agreement

- Users must sign or otherwise accept the “End User Agreement” Policy before being able to access corporate resources from personal devices.

Data and Internet Roaming Connectivity (applicable only on devices with Corporate SIM Card)

- Data Roaming exchanges are permissible for specific users that require it for work purposes only.
- Mobile Data exchanges can be isolated according to the determined needs of the end user via the EMM and Network Carrier.
- Data Roaming data exchanges should be minimized where possible.

Tethering (applicable only on devices with Corporate SIM Card)

- Tethering is not allowed with corporate mobile devices when the user is outside of the Mobile Device´s registered country. I.e.: When Data Roaming connections are being transmitted.

Rooted/Jailbroken devices

- Rooted or jailbroken devices are not allowed to access COMPANY Corporate resources. These devices will be reported to the EMM platform and access to corporate resources will be disabled.

Privacy Policy

- COMPANY EMM software will not collect any kind of personal data of employee owned devices as SMS, photos or similar data.
- COMPANY EMM will not collect device location information.
- Application inventory information will be collected with the only intention to ensure application policy compliance.
- Remote management and surveillance is solely intended to apply required security policies, control policy compliance and issue a wipe command in case of loss or theft.

BYOD program membership

- Employees are free to unconfigure corporate configuration profiles on personal mobile devices at wish. Opting out of BYOD program should be notified to IT in order to deprovision device corporate access.
- Mobile Device Management agent uninstallation is reported to the EMM platform. COMPANY will 5ssume that an employee has freely unsubscripted from BYOD program if EMM agent is not reinstalled within 7 days.
- Employee-owned devices with access to corporate intranet should be wiped when employee leaves the company or when device is not going to be used for business anymore.

Annex 6.4. App Policy for COPE and BYOD devices

Rogue Apps
Installation of rogue or tricky apps (i.e. rooting or jailbreaking the device, install applications through USB cable…) is prohibited on Company corporate mobile devices. ▪ The approved public mobile application distribution channels are the iOS AppStore (for Apple devices), Google Play (for Android Devices), Windows Phone Martketplace (for Windows Phone devices) and Blackberry App World (for Blackberry devices). ▪ Apps that are obtained outside previously mentioned channels, with the exception of enterprise-developed apps, are considered rogue apps and its installation on corporate mobile devices is prohibited.
Mobile Malware
Mobile Malware is software intended to steal personal information from mobile devices or take control of the device to make calls to pay-per-minute lines, send premium SMS or other malicious activity. Mobile Malware represents a security risk for Company. The malware infection vectors for mobile devices are the following: Mobile Apps, Web Sites, Email attachments, Ringtones, connection based vectors (i.e. SMS, Bluetooth, Wi-Fi, USB, Mobile to mobile connections), Firmware and Physical access to the device. In order to mitigate the risk of mobile malware, users must follow these precautions before using apps: ▪ Always use legitimate, official app stores ▪ Do not open any kind of content (websites, emails, email attachments, SMS…) from untrusted sources. ▪ Be wary of apps that require excessive permissions such as phone or network internet access ▪ Do not install apps from unknown or unauthorized sources via email, web or physical media
Over-privileged Apps
On Android devices, when an application is going to be downloaded, Google Play shows the list of required permissions for the application. User has to review carefully that required permissions by the application are reasonable with application usage. The permissions that pose a risk and to be cautious of accepting are: Make Phone Calls, Send SMS Messages, Modify or Delete SD Card, Read and Write Contact data, Read logs, Full Internet Access, Manage Accounts, Use Credentials, Read/Modify Gmail and Install Packages
Restricted Application Categories (Blacklist)
Company prohibits the installation of the following kind of applications on corporate devices:

- Any application that incurs a cost to the company without prior permission
- Peer to Peer apps (content sharing applications)

Cloud-based applications

Cloud-based applications are applications that store data on third party storage, as Dropbox, Box.Net, Evernote… Installation of these applications is allowed, although, its use to conduct company business is forbidden.

Be aware that using this kind of applications with company business data can represent a high security risk for Company.

Instant Messaging applications

Installation of non-corporate instant messaging applications (i.e. WhatsApp) is allowed, even though, its use to conduct company business is prohibited.

Enterprise Approved Applications

The following applications are defined as corporate and restricted approved software: Avast Mobile Security (Antivirus), WhatsApp (Instant Messaging), LinkedIn (Professional Social Network), OfficeSuite Viewer 6 (Office Reader Suite), OfficeTalk Free (MS Communicator), NitroDesk Touchdown (Optional, requires Purchase Request Approval) and Standard Apps that come default with Smartphone.

ANNEX 7. PHASE 2 COMPARISON CHARTS

Annex 7.1. Mobile devices comparison chart

iPhone 5 | NOKIA Lumia 920 | Samsung GALAXY S IV | BlackBerry Z10 | htc one

Visió General					
Data Publicació	Setembre 2012	Novembre 2012	Abril 2013	Gener 2013	Abril 2013
Sistema Operatiu	iOS 6	Windows 8 Phone	Android Jelly Bean 4.1	BlackBerry 10	Android Jelly Bean 4.2
Interfície d'usuari	iOS	Windows Phone 8	TouchWiz	BlackBerry OS	HTC Sense
Opcions de teclat	Teclat tàctil	Teclat tàctil	Teclat tàctil	Teclat tàctil	Teclat tàctil
Dimensions (mm)	123,8 × 58,5 × 7,6	130,3 × 70,0 × 10,7	136.6 × 69.8 × 7.9	130 × 65.6 × 9	137.4 × 68.2 × 9.3
Pes (g)	112	185	130	135	143

Sensors	Apple iPhone 5	Nokia Lumia 920	Samsung Galaxy S4	Blackberry Z10	HTC One (2013)
Acceleròmetre	✔	✔	✔	✔	✔
Baròmetre	✘	✘	✔	✔	✔
Brúixola Digital	✔	✔	✔	✔	✔
GPS	✔	✔	✔	✔	✔
Giroscopi	✔	✔	✔	✔	✔
Humitat	✘	✘	✔	✘	✘
Termòmetre	✘	✘	✔	✘	✘

Característiques Multimedia	Apple iPhone 5	Nokia Lumia 920	Samsung Galaxy S4	Blackberry Z10	HTC One (2013)
DLNA	✔	✔	✔	✔	✔
FM Receptor	✘	✘	✘	✔	✔
Navegació GPS	✔	✔	✔	✔	✔
Targeta de Vídeo	✔	✔	✔	✔	✔
Reproducció HD	✔	✔	✔	✔	✔
Blaster infrarojos	✘	✘	✔	✘	✘
Micròfon	✔	✔	✔	✔	✔
Chargin Wireless	✘	✔	✘	✘	✘

Pantalla	Apple iPhone 5	Nokia Lumia 920	Samsung Galaxy S4	Blackberry Z10	HTC One (2013)
Mida de la pantalla (")	4	4,5	4,99	4,2	4,7
Densitat dels píxels (PPI)	326	332	441	356	468
Resolució de la pantalla (píxels)	1136 x 640	1280 x 768	1920 x 1080	1280 x 768	1920 x 1080
Tecnologia de pantalla	Retina LCD	LCD	Super AMOLED	Super AMOLED	LCD
Característiques	Sensor llum ambiental, Multi-touch, Sensor proximitat, Vidre resistent a ratllades i Suport a pantalla adicional* (Lumia 920 NO)				

Emmagatzematge i RAM	Apple iPhone 5	Nokia Lumia 920	Samsung Galaxy S4	Blackberry Z10	HTC One (2013)
Emmagatzematge intern	16 Gb	32 GB	16 Gb	16 Gb	64 Gb
Targeta externa (max)	-	-	64 Gb	64 Gb	-
RAM	1Gb	1Gb	2 Gb	2 Gb	2 Gb
Memòria extraïble	-	-	microSD, microSDHC	microSD	-

Especificacions tècniques					
	Apple iPhone 5	Nokia Lumia 920	Samsung Galaxy S4	Blackberry Z10	HTC One (2013)
Velocitat de la CPU	1.2 GHz	1.5 GHz	1.6 GHz	1.5 GHz	1.7 GHz
Nuclis del processador	2	2	8	2	4
CPU	A6 d'Apple	Qualcomm Snapdragon S4 Plus	Exynos 5 Octa	-	Qualcomm Snapdragon 600

Càmera					
	Apple iPhone 5	Nokia Lumia 920	Samsung Galaxy S4	Blackberry Z10	HTC One (2013)
Qualitat càmera davant (Mp)	1.2	1.3	2	2	2.1
Qualitat càmera darrera (Mp)	8	8.7	13	8	4
Resolució màxima de captura de vídeo	1080p	1080p	1080p	1080p	1080p
Opcions de la càmera					
Enfocament automàtic	✔	✔	✔	✔	✔
Mode Burst	✘	✔	✔	✔	✔
Zoom digital	✔	✔	✔	✔	✔
Dual Record Cambra	✘	✘	✔	✘	✘
Càmera Frontal	✔	✔	✔	✔	✔
L'estabilització d'imatge	✔	✔	✔	✔	✔
Flash LED	✔	✔	✔	✔	✔
Panorama	✔	✘	✔	✘	✔
Càmera darrera	✔	✔	✔	✔	✔
Sound & Shot	✘	✘	✔	✘	✘
Enregistrament de vídeo	✔	✔	✔	✔	✔

Bateria					
	Apple iPhone 5	Nokia Lumia 920	Samsung Galaxy S4	Blackberry Z10	HTC One (2013)
Temps de conversa (hores)	8	17	14	10	13
Temps d'espera màxima (hores)	225	400	-	312	-
Capacitat de la bateria	1440 mAh	2000 mAh	2600 mAh	1800 mAh	2300 mAh
Tecnologia	Li Ion	Li Ion	Li Ion	Li Ion	Polímer de Li

Connectivitat					
	Apple iPhone 5	Nokia Lumia 920	Samsung Galaxy S4	Blackberry Z10	HTC One (2013)
Xarxes	3G (HSDPA / CDMA) 4G (LTE / HSPA +) Edge/2G (GSM / GPRS)	3G (HSDPA / CDMA) 4G (LTE / HSPA +) Edge/2G (GSM / GPRS)	3G (HSDPA / CDMA) 4G (LTE / HSPA +) Edge/2G (GSM / GPRS)	3G (HSDPA / CDMA) 4G (LTE / HSPA +) Edge/2G (GSM / GPRS)	3G (HSDPA / CDMA) 4G (LTE / HSPA +) Edge/2G (GSM / GPRS)
Bluetooth	4.0	3.1	4.0	4.0	-
Infraroig	✘	✘	✔	✘	✔
Hotspot Tethering	✔	✔	✔	✔	✔
NFC	✘	✔	✔	✔	✔
WiFi	✔	✔	✔	✔	✔
Connexió de càrrega	Apple Lightning	microUSB, Wireless	microUSB, Wireless	microUSB	microUSB
HDMI	HDMI (Lightning)	-	HDMI (via microUSB)	HDMI	HDMI (via microUSB)
Auriculars	3.5mm	3.5mm	3.5mm	3.5mm	3.5mm

Samsung GALAXY Note 10.1 | Microsoft Surface | ASUS Transformer Pad infinity TF700 | iPad | nexus 10

Visió General

	Samsung Galaxy Note 10.1	Microsoft Surface RT	ASUS Pad infinity TF700	IPad d'Apple (4G)	Samsung Nexus 10
Data Publicació	Agost 2012	Octubre 2012	Juny 2012	Octubre 2012	Novembre 2012
Sistema Operatiu	Android Jelly Bean 4.2	Windows RT	Android Jelly Bean 4.2	iOS 6	Android Jelly Bean 4.2
Dimensions (mm)	256.6 x 172.9 x 8.6	245 x 172 x 9.4	263 x 180.8 x 16.5~18.9	241.2 x 185.7 x 9.4	263.9 × 177.6 × 8.9
Pes (g)	594	680	594	635	603

Sensors

	Samsung Galaxy Note 10.1	Microsoft Surface RT	ASUS Transformer Pad infinity TF700	IPad d'Apple (4G)	Samsung Nexus 10
Acceleròmetre	✔	✔	✘	✔	✔
Baròmetre	✘	✘	✘	✘	✔
Brúixola Digital	✔	✔	✔	✔	✘
GPS	✔	✘	✔	✔	✔
Giroscopi	✔	✔	✔	✔	✔

Característiques Multimédia

	Samsung Galaxy Note 10.1	Microsoft Surface RT	ASUS Transformer Pad infinity TF700	IPad d'Apple (4G)	Samsung Nexus 10
DLNA	✔	✘	✔	✘	✘
Navegació GPS	✔	✘	✔	✔	✔
Targeta de Vídeo	✔	✔	✔	✔	✔
Reproducció HD	✔	✔	✔	✔	✔
Micròfon	✔	✔	✔	✔	✔
Enregistrament de vídeo	✘	✘	✘	✔	✔

Pantalla					
	Samsung Galaxy Note 10.1	Microsoft Surface RT	ASUS Pad infinity TF700	IPad d'Apple (4G)	Samsung Nexus 10
Mida de la pantalla (")	10.1	10,6	10,1	9,7	10
Densitat dels píxels (PPI)	149	148	224	264	299
Resolució de la pantalla (píxels)	1280 x 800	1366 x 768	1920 x 1200	2048 x 1536	2560 x 1600
Tecnologia de pantalla	TFT	HD LCD	TFT	Retina LCD	Real Stripe PLS
Característiques	Pantalla Tàctil, Sensor llum ambiental, Sensor proximitat (Surface i Asus NO), Vidre resistent a ratllades i Suport a pantalla adicional				

Emmagatzematge i RAM					
	Samsung Galaxy Note 10.1	Microsoft Surface RT	ASUS Pad infinity TF700	IPad d'Apple (4G)	Samsung Nexus 10
Emmagatzematge intern	16 GB	64 GB	32 GB	16 GB	16 GB
Targeta externa (max)	32 GB	64 GB	64 GB	-	-
RAM	2 GB	2 GB	1 GB	1 GB	2 GB
Memòria extraïble	microSD	microSDHC	microSD	-	-

Especificacions tècniques					
	Samsung Galaxy Note 10.1	Microsoft Surface RT	ASUS Pad infinity TF700	IPad d'Apple (4G)	Samsung Nexus 10
Velocitat de la CPU	1.4 GHz	1.3 GHz	1.6 GHz	1.4 GHz	1.7 GHz
Nuclis del processador	4	4	4	2	2
CPU	Exynos 4410	NVIDIA T30	NVIDIA Tegra 3	Apple A6X	Samsung Exynos 5250

Càmera					
	Samsung Galaxy Note 10.1	Microsoft Surface RT	ASUS Pad infinity TF700	IPad d'Apple (4G)	Samsung Nexus 10
Qualitat càmera davant (Mp)	1.9	1.2	2	1.2	1.9
Qualitat càmera darrera (Mp)	5	5	8	5	5
Resolució màxima de captura de vídeo	720p	720p	1080p	1080p	1080p
Opcions de la càmera					
Enfocament automàtic	✔	✔	✔	✔	✔
Zoom digital	✔	✔	✔	✔	✔
Càmera frontal	✔	✔	✔	✔	✔
Flash LED	✔	✘	✔	✔	✔
Estabilització d'imatge	✔	✔	✔	✔	✔
Enregistrament de vídeo	✘	✘	✘	✔	✘

Bateria					
	Samsung Galaxy Note 10.1	Microsoft Surface RT	ASUS Pad infinity TF700	IPad d'Apple (4G)	Samsung Nexus 10
Durada de la bateria	8	8	9.5	10	9
Capacitat de la bateria	7000 mAh	8750 mAh	6757 mAh	11560 mAh	9000 mAh
Tecnologia	Polímer de Liti	Polímer de Liti	Polímer de Liti	Polímer de Liti	Polímer de Liti

Connectivitat					
	Samsung Galaxy Note 10.1	Microsoft Surface RT	ASUS Pad infinity TF700	IPad d'Apple (4G)	Samsung Nexus 10
Xarxes	3G (HSDPA / CDMA) 4G (LTE / HSPA +) Edge/2G (GSM / GPRS)	-	3G (HSDPA / CDMA) Edge/2G (GSM / GPRS)	3G (HSDPA / CDMA) 4G (LTE / HSPA +) Edge/2G (GSM / GPRS)	-
Bluetooth	4	4	3	4	3
Hotspot WiFi	✘	✘	✘	✔	✘
USB	✔	✘	✔	✘	✘
WiFi	✔	✔	✔	✔	✔
Connexió de càrrega	Propietari	Propietari	Propietari	Apple Lightning	microUSB
HDMI	-	-	HDMI	HDMI (via Lightning)	HDMI
Auriculars	3,5 mm	3,5 mm	3,5 mm	3,5 mm	3,5 mm

Annex 7.2. OS management capabilities comparison chart

Aprovisionamiento				
	Android	iOS	BlackBerry	WinPhone 8
Por dispositivo	Si	Si	Si	Si
Bulk	Si	Si	Si	Si
Auto aprovisionamiento	Si	Si	Si	Si

Gestión de Activos				
	Android	iOS	BlackBerry	WinPhone 8
Inventario de dispositivo	Si	Si	Si	Si
Detalles del dispositivo	Si	Si	Si	Si
Propiedad	Si	Si	Si	Si
Definir Perdido	Si	Si	Si	-
Definir Encontrado	Si	Si	Si	-
Definir Retirado	Si	Si	Si	Si
Enviar Mensaje	Si	Si	Si	Parcial (email)
Forzar Check-In	Si	Si	Si	-
Re-aprovisionamiento	Si	Si	Si	-
Sincronizar Política	Si	Si	Si	Parcial
Acciones aplicadas a Grupo	Si	Si	Si	Si

Control Protocolo ActiveSync				
	Android	iOS	BlackBerry	WinPhone 8
Inventario Dispositivo	Si	Si	-	Si
Detalles de dispositivo	Si	Si	-	Si
Permitir/Bloquear Acceso correo	Si	Si	-	Si
Borrado	Si	Si	-	Si
Registro	Si	Si	-	-
Gestión políticas ActiveSync	Si	Si	-	Si

Gestión de Aplicaciones				
	Android	iOS	BlackBerry	WinPhone 8
AppStore Empresarial	Si	Si	Si	Si
Biblioteca de Distribución de aplicaciones	Si	Si	Si	Si
Política de gestión de Apps	Si	Si	Si	-
Inventario Apps	Si	Si	Si	-
Instalación Apps	Si	Si	Si	Si

Seguridad				
	Android	iOS	BlackBerry	WinPhone 8
Bloquear	Si	Si	Si	-
Desbloquear	Si	Si	-	-
Borrado	Si	Si	Si (5)	Si
Borrado Selectivo (Correo electrónico)	Si (1,2)	Si	-	Si
Distribución Certificados	Si (2,3)	Si	-	Si (Root)
Cifrado de Políticas (almacenamiento interno)	Si (1)	Si	-	Si
Cifrado de Políticas (SD Card)	Si (1)	N/A	-	-
Política de contraseñas	Si	Si	Si (5)	Si
Política de restricciones	Si (1)	Si	Si (5)	Si
Política de privacidad	Si (4)	Si (4)	Si	-
Bloqueo de registro por SO	Si	Si	Si	Si
Localizar dispositivo	Si	Si	Si	-
Control Adjuntos	Si	Si	-	-
1- Dispositivos SAMSUNG SAFE				
2- Para Exchange, con TouchDown de Nitrodesk				
3- Soportado en Android para el cliente VPN Cisco AnyConect.				
4- La localización y el inventariado pueden ser deshabilitados.				
5- A través de la integración con BES (5.0 o superior).				

Acciones de Remediación				
	Android	iOS	BlackBerry	WinPhone 8
Alertas	Si	Si	Si	-
Bloqueo ActiveSync	Si	Si	N/A	-

Gestión de Configuración de Aplicaciones				
	Android	iOS	BlackBerry	WinPhone 8
Exchange	Si (1,2)	Si	N/A	Si
VPN	Si	Si	Si	-
Wi-Fi	Si	Si	Si	-
1- Dispositivos SAMSUNG SAFE				
2- Para Exchange, con TouchDown de Nitrodesk				

Gestión Políticas Gasto				
	Android	iOS	BlackBerry	WinPhone 8
Control Roaming	Si	Si	-	-
Alertas	Parcial	Parcial	-	-

Portal Auto-gestión usuario				
	Android	iOS	BlackBerry	WinPhone 8
Registro Servicio MDM	Si	Si	Si	-
Bloqueo	Si	Si	Si	-
Borrado	Si	Si	Si	Si
Localización	Si	Si	Si	-

Annex 7.3. EMM systems comparison chart

Gestió i registre d'usuaris/dispositius	airwatch	MobileIron	XenMobile
Autoenrollment	✔	✔	✔
Registre per Invitació	✔	✔	✔
Registre per llistat	✔	✔	✘
Registre Vía Web	✔	✔	✔
Usuaris Sinconitzat amb AD	✔	✔	✔
SSO amb serveis Online	✘	✘	✘

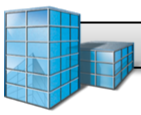
Gestió d'aplicacions	airwatch	MobileIron	XenMobile
Plataformes de desplegamets soportades	Dispositus móbils	Dispositus móbils	Dispositus móbils
Portal d'autoprovisió	✔	✔	✔
Diferenciació apps personal i empresa	✘	✔	✘
Enllaç a Botigues oficials	✔	✔	✔
Distribució d'aplicacions "in-house"	✔	✔	✔
Instalació/Esborrat remot	Android	Android	Android
Distribució d'aplicacions virtualitzades	✘	✘	XenApp

Gestió de configuracions	airwatch	MobileIron	XenMobile
Funcionalitats estàndar	Sincronització de polítiques, Correu corporatiu, VPN, Wi-Fi, Restriccions, Certificats, Contrasenya dispositiu, Web Clips, Accés a Botiga		
Roaming	✔	✔	✔
Sincronització arxius entre diferent dispositius	✘	✘	✘
Accés a serveis virtualitzats	✘	✘	✔

Gestió d'actius i Reporting	airwatch	MobileIron	XenMobile
Gestió d'actius soportats	Dispositus móbils	Dispositus móbils	Dispositus móbils
Funcionalitats estàndar	Inventari dispositiu, Creació de grups, Propietat del dispositiu, Gestió de la privacitat, Estat del dispositiu, Elaboració d'informes personalitzats		

Gestió seguretat i accés	airwatch	MobileIron	XenMobile
Bloqueig/Desbloqueig del dispositiu	✔	✔	✔
Accés recursos interns	✔	✔	✔
App navegador segur	✔	✔	✔
App correu segur	✔	✘	✔
Encriptació adjunts nativa	✘	✔	✘
Contenidor segur informació corporativa	✔	✔	✔
Accés VPN automàtic	✔	✔	✔
Retirada de contigunt corporatiu	✔	✔	✔
Esborrat del dispositiu	✔	✔	✔
Polítiques de xifrat	✔	✔	✔
Política de contrasenya	✔	✔	✔
Política accés al correu	✔	✔	✔
Accés a les aplicacions corporatives	✔	✔	✔

Arquitectura	airwatch	MobileIron	XenMobile
On-Premise	✔	✔	✔
Connected Cloud	✔	✔	✔



Integració amb infraestructura corporativa	airwatch	MobileIron	XenMobile
Directori Actiu	✔	✔	✔
PKI	✔	✔	✔
XenApp	✘	✘	✔
Sharepoint	✔	✔	✔

Impacte econòmic	airwatch	MobileIron	XenMobile
Cost llicenciament anual	50$	60$	75$
Tipus llicenciament	Per dispositiu	Per dispositiu	Per dispositiu
Infraestructura servidora	Infraestructura dedicada (min. 2 servidors)	Infraestructura dedicada (min. 2 servidors)	Infraestructura dedicada (min. 2 servidors)
Servei de manteniment i operació	Exclusiu per a plataforma mobilitat	Exclusiu per a plataforma mobilitat	Exclusiu per a plataforma mobilitat

Annex 7.3.1.1. Conclusions

For all the solutions there are a common set of features for all solutions that can be group as follows:

- Registration of new devices/users: Per device/user, By list of devices/users and By invitation (registration is made by the user).
- Administrative management: Device inventory, Detailed overview of devices, Device status (active, lost, quarantine, retired, etc.), Policies synchronization, Creation of groups and Custom views.
- Security: Lock/Unlock Device, Wipe device, Distribution of certificates, Encryption policies, Password policy and number of attempts, Localization and Mail Access Policy.
- Access Control: Mail Access (Activesync), Access to corporate applications and Access to internal resources.
- Application Management: Application Distribution Portal, Application control by user, Inventory, Remote installation and Remote app wipe.
- Device configuration: Corporate mail, VPN, Wi-Fi, restrictions, SCEP, device password and web clips.

On the other hand, there are some advanced functionalities which only can be available with a specific solution. A summary is shown in [**¡Error! No se encuentra el origen de la referencia.**]:

Annex Tab. 14 EMM Systems summary comparison chart

	MOBILEIRON	AIRWATCH	XENMOBILE
Mobile Device Management (MDM)	✓	✓	✓
Architecture:			
• On Premise	✓	✓	✓
• Integrated Cloud	✓	✓	✓
• Cloud	✓	✓	✓
Virtual environments:			
• Virtual desktop acces	✗	✗	✓
• Virtual app acces	✗	✗	✓
Safe Browsing:			
• Own APP	✓	✓	✓
Safe Email:			
• Own APP	✗	✓ Android	✓
• Email Attachments encryption	✓	✗	✗
Mobile Aplication Management (MAM)	✓	✓	✓
Mobile Content Management(MCM):			
• MCM Client on device	✓	✓	✓
• Wrapping for Apps in-house	✓	✓	✓
• Wrapping Apps AppStore "Partners"	✓	✗	✗
Remote Wipe of Coporate Data	✓	✓	✓
Corporate Network Acces:			
• VPN	✓	✓	✓
• AppTunnel or microVPN (SSL-VPNs)	✓	✓	✓
License per device and year	60 €	45€	75 €

ANNEX 8. PHASE 3 TECHNICAL REFERENCES

Annex 8.1. iOS MDM protocol

- *All the data below has been recollected and summarized from [28], [29] and [30].*

Annex 8.1.1. What is iOS MDM

In 2010, Apple introduced Mobile Device Management (MDM) services for iOS, a solution to the problem of iOS MDM, targeted at the enterprise. This system features remote installation of profiles, querying of device settings, and certain remote controls: lock, unlock, and remote wipe of a device.

iOS MDM allows for a much more robust and complete manner of managing iOS devices. A key feature of MDM is that it allows administrators to push profiles to the device without any manual intervention. The benefits include:

- Background management of the device for policy enforcement, policy updates and immediate management actions.
- Richer set of device details including applications installed, encryption status, configuration status, and so on.

Annex Tab. 15 EMMS Capabilities with or without iOS MDM

EMMS Capabilities	Without iOS MDM	With iOS MDM
Create configuration profiles and push settings	YES	YES
Distribute configurations securely using SCEP	YES	YES
Make changes to configurations/settings without user intervention	NO	YES
Provide inventory (user, phone #, and so on) information for device	YES	YES
Gather application inventory	NO	YES
Gather security posture (for example, data protection enabled)	NO	YES
Selectively wipe e-mail, calendar, contact data	NO	YES
Provision certificates	YES	YES
Automatically renew certificates if expired	NO	YES
Distribute provisioning profiles to enable enterprise applications	YES	YES
Recommend App Store applications	NO	YES
Alert if device is internationally roaming	NO	YES

Annex 8.1.2. How it Works

The MDM service essentially consists of three elements:

- The device being managed (iOS devices)
- The server doing the management (EMMS)
- A method by which the server wakes up the device (APNS)

Annex 8.1.2.1. Enrollment

EMMS support over-the-air (OTA) enrollment, and can implement various challenge and response systems, both to authenticate the user and to ensure that only desired devices are enrolled in the system. However, the OTA system relies on a Simple Certificate Enrollment Protocol (SCEP) server.

During enrollment, the device provides unique identifying information to EMMS, which is used by the EMM Core to send messages through the Apple Push Notification Service. Long-term connections from EMMS to client, or vice versa, do not exist with the design of iOS MDM protocol, only connection to APNS.

After enrollment, each interaction between client devices and the MDM server consists of four elements [see also diagram on the next page]:

- 1. Server requests push notification through Apple
- 2. Apple pushes notification to device
- 3. Device connects to server
- 4. Server and client exchange commands and responses

Annex 8.1.2.2. Push Notification

When the EMMS needs to communicate with a device, it queues up the desired command, and then sends a very simple push notification message through APNS. No information other than an identifying token is present in this message. Upon receipt of the notification, the device contacts the server, which then provides the queued command to the client. Upon completion of the command, the client responds with an appropriate acknowledgment, and the connection between client and server is closed.

Annex 8.1.2.3. Client / Server Interaction

The device interacts with the server by connecting to a designated URL and exchanging XML formatted data in the form of an Apple Property List (.plist) file.

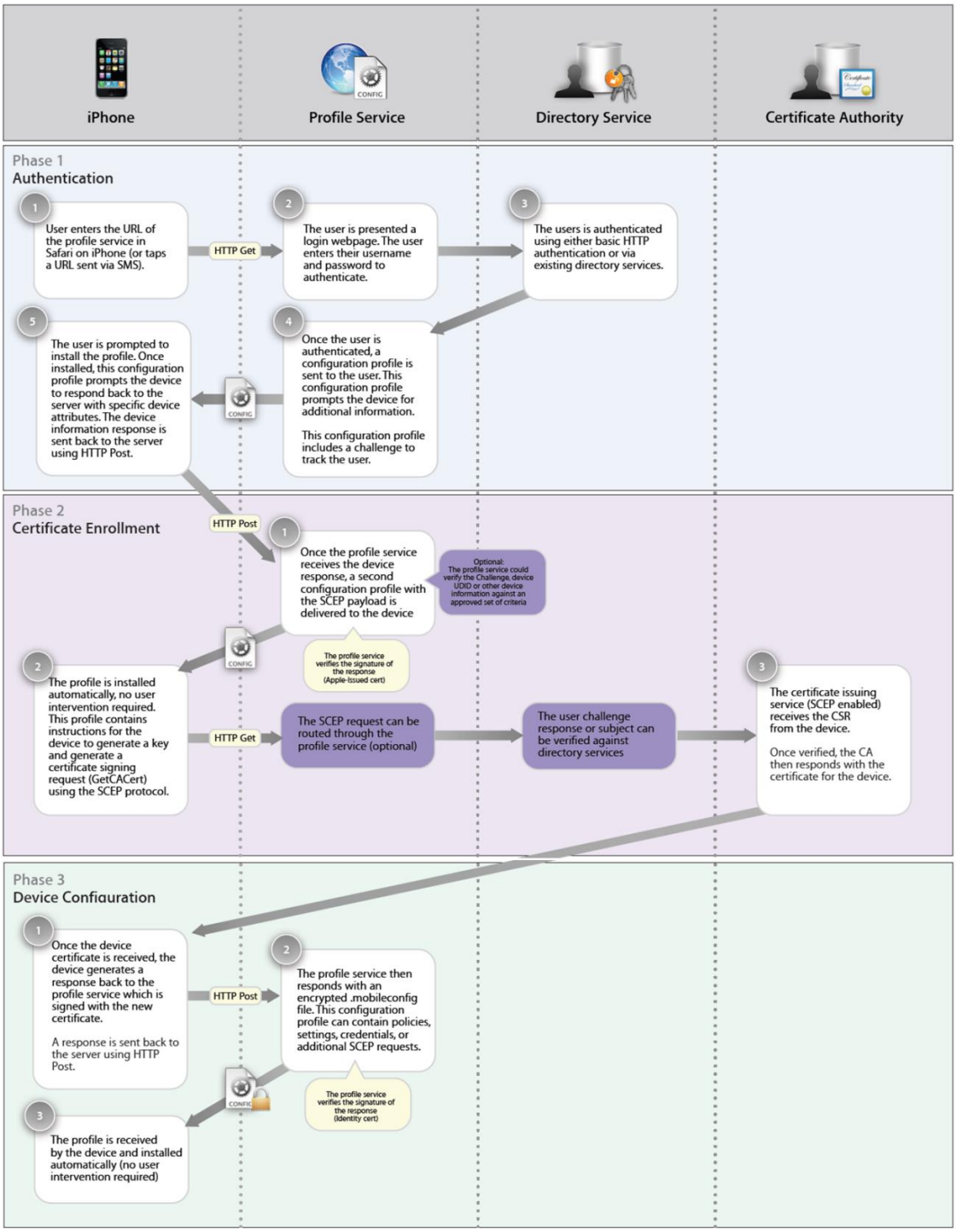
The first message a client sends upon connecting to the server is a simple “Status: Idle” notification, indicating that the device is ready to receive commands from the MDM server.

Upon receipt of this message, the server sends whatever command may be waiting for that device. This command is also presented as an XML formatted .plist file, and can be only a simple command (Clear Passcode, Wipe, Block, etc.) or a device setting, called Configuration Profile.

A configuration profile is an XML file that allows you to distribute configuration information. If you need to configure a large number of devices or to provide lots of custom email settings, network settings, or certificates to a large number of devices, configuration profiles are an easy way to do it.

A configuration profile contains a number of settings that you can specify, including: Restrictions on device features, Wi-Fi settings, VPN settings, Email server settings, Exchange settings, LDAP directory service settings, CalDAV calendar service settings, Web clips and Credentials and keys.

The device acts upon the command, and may then respond with another .plist, providing either a simple acknowledgement of the command, an error message, or a detailed response (in the case of device inventories and similar commands).



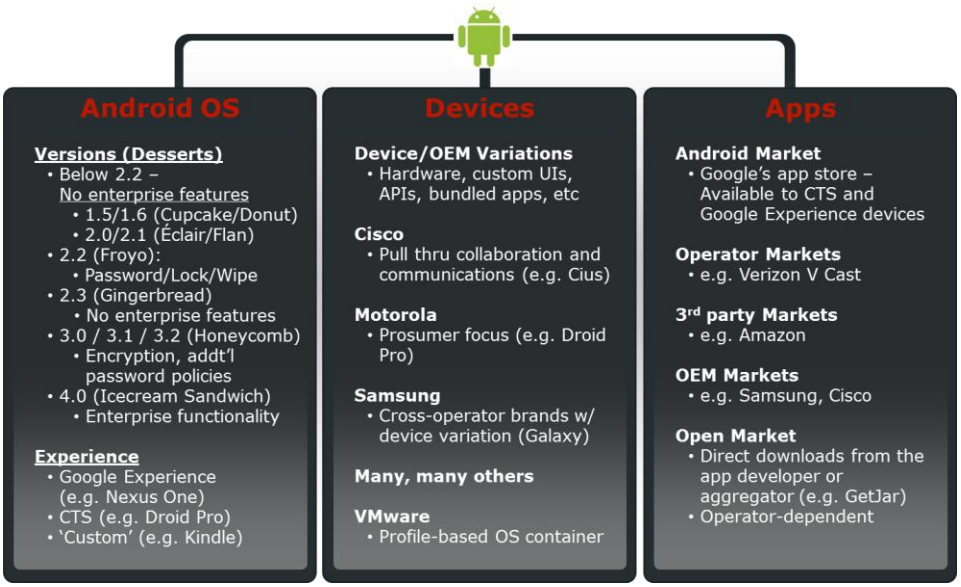
Annex Fig. 11 iOS Enrollment

Annex 8.2. Android MDM solutions

- *All the data below has been recollected and summarized from [31], [32], [33] and others.*

Annex 8.2.1. Android Management Landscape

Android platform represents a challenge to Mobile IT. Unlike the homogenous experience of iOS where there is a single Appstore and the same look and feel across different devices, Android feels fragmented. Enterprise-friendly features found their way into version 2.2, and although there have been several versions since, a lot of Android devices don't supports it.

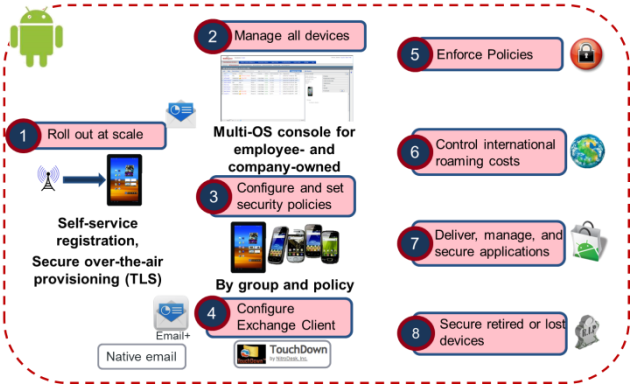


Annex Fig. 12 Android Overview

The open operating system promotes those more than 40 manufacturers improving the OS with each OEM's own unique variations. For sure, also feature support varies across OEMs. Moreover, beyond Google Play, there are many other locations where devices may "side load" apps.

Annex 8.2.2. Android Lifecycle management

Managing Android devices begins with registering devices over the air. Once registered, Androids are managed along with iOS from the same management console.



EMMS leverages to deliver policies and settings such as ActiveSync mail by groups. There is also a storefront which allows recommending and subsequent management of apps. Finally, Android devices also may be retired, wiped, locked and otherwise remotely managed from the EMMS.

Annex Fig. 13 Android Lifecycle management

Annex 8.2.3. Samsung SAFE

While native Android provides basic device management capabilities, there are still some key management features missing for the EMM. Moreover, organizations demanding the highest levels of mobile security may require more out of their mobile platform. Some missing EMM features are full-device encryption, Wi-Fi, VPN, and ActiveSync management may all be mitigated by these means.

In those cases, EMMS need to use vendor-purchased apps or manufacturer APIs directly to ensure capabilities to at least respective devices. For example, EMMS uses Samsung own APIs, Samsung For Enterprise (SAFE), extending the capabilities of select Android devices to provide these advanced device management capabilities.

Annex Tab. 16 Samsung SAFE Capabilities

Samsung SAFE Capabilities		
• Application Management	**• Remote Bluetooth Configuration**	**• Kiosk Mode**
- Silently Push/Remove Applications	- Enable/Disable Discoverability	- Disable HW and Soft Keys
- Control Application Store Access	- Blacklisting and Whitelisting	- Add/Remove Applications
- Blacklisting and Whitelisting Control	Management for BT Devices	and Widgets
for Applications	and Profiles	- Control Notification Bar and
• Enable/Disable	**• Remote Microsoft® Exchange**	- Home Screen
- Bluetooth®	ActiveSync® Configuration	**• Security Management**
- Camera	**• VPN Configuration**	- Enforce Password Settings
- Wi-Fi®	- Cisco AnyConnect® VPN	- Certificate Installation
- Tethering	- Legacy Android™ VPN	- Remote Lock and Full/Selective Wipe
- Voice Recording	**• Asset Tracking**	- Device/SD Card Encryption
- Screen Capture	- Device Info	**• Email extended capabilities**
- Use of SD Card	- Network Info	Out-of-Office Assistant
- Desktop Sync	**• Expense Management**	- Follow-Up Flags
- OTA Firmware Upgrade	- Enforce Roaming Policies	- High-Importance Status
• Wi-Fi Profile Configuration	- Apply Voice Calling and SMS Limits	- Partial Download
- SSID (Network Name)	**• Location Management**	- Conversation View
- Security Parameters	- Turn On/Off GPS	- Free/Busy Lookup
- Blacklisting and Whitelisting		- Propose New Meeting Time

Annex 8.2.4. Samsung KNOX

The KNOX container essentially provides a secure work environment where work-related apps, corporate email, business contacts and other sensitive data rests. Apps inside this container are identified with the KNOX secure badge and are password protected. On the personal side, personal email, media, games, social apps and other content is always accessible.

Samsung KNOX features include TrustZone-based Integrity Monitoring (TIMA) for protecting the kernel, secure boot, Security Enhanced (SE) Android, a secure application container for apps and data and Single Sign On (SSO).

Annex Fig. 14 Samsung KNOX

EMMS supports KNOX with the following functions: Create and destroy the secure container and enable or disable a container for a device. Further it can configure the container's password policy, point to an exchange and browser app setting and also support the installation and removal of apps within the container.

Annex 8.3. PKI, certificates and SCEP

Annex 8.3.1. What is a PKI

A PKI (public key infrastructure) enables users of a basically unsecure public network to securely and privately exchange data through the use of a public and a private cryptographic key pair (Public Key and Private Key). Both are obtained and shared through a trusted authority called Certificate Authority (CA).

The PKI provides digital certificates that can identify an individual or an organization and also provides directory services that can store and revoke the certificates if was necessary.

The PKI assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message. It works as follows:

- When you encrypt something with the public key of a person, only the private key can decrypt it (confidentiality).
- When you encrypt something with the private key of a person, anyone with the public key can read it. As private key is unique and is held by single person the message only can have been made by him (authentication and non-repudiation).

Annex 8.3.2. Why use client identity certificates

The main reasons for use client identity certificates are:

- Enhance security of devices: Certificates enable Multi-factoring access or creating higher-level mechanisms for corporate services access.
- End-user ease of use: Certificates gives users an authentication scheme where there is nothing to enter and no worrying about passwords being saved on devices.
- Less support needed: Users do not have to remember passwords or accidently lock their accounts because certificates authenticate them.
- Advanced features: Some advanced technologies, such as VPN on-demand, require the use of certificates for authentication.

Annex 8.3.3. Why use SCEP for client certificates

When you decide to use certificates in your environment, you must think about the distribution of those certificates. There are many ways to distribute certificates, including the Simple Certificate Enrollment Protocol (SCEP). SCEP is a medium that enables the distribution of dynamically created user certificates. The benefits of SCEP are:

- SCEP automates certificate distribution and requires little cost to implement.
- Without SCEP, distribution of certificates means manually distributing each individual certificate to a user's device. Depending on how many users and devices you have in your system, this may be unmanageable.

Annex 8.3.4. SCEP/NDES protocol

➢ *All data of this section have been summarized from [34].*

SCEP enables network devices (for example, routers) that do not run with domain credentials to enroll for x509 version 3 certificates from a Certification Authority (CA).

At the end of the transactions defined in this protocol, the network device will have a private key and associated certificate that is issued by a CA. Applications on the device may use the key and its associated certificate to

interact with other entities on the network. The most common usage of this certificate on a network device is to authenticate the device in an IPSec session.

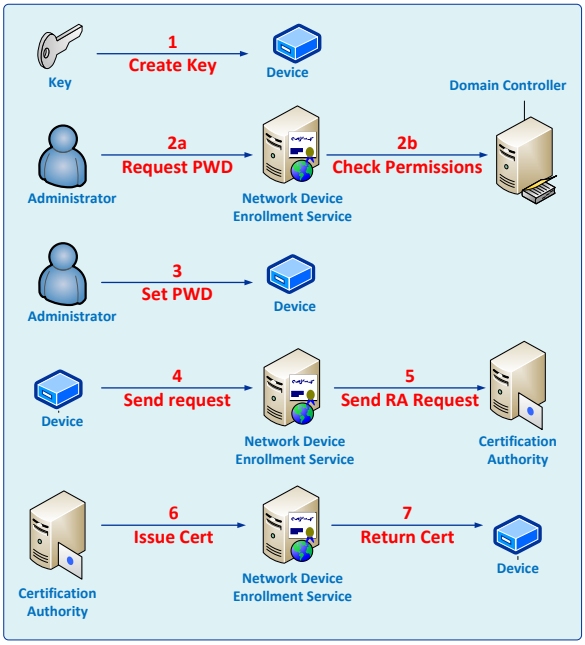
Annex 8.3.4.1. Entities

The following entities are involved in SCEP.

- Device (client.) This is the actual client for this protocol.
- Device Administrator. This entity is responsible for the administration of the device or client.
- Network Device Enrollment Service. This is the service that corresponds to the server in the SCEP. This service might be referred to as the RA.
- CA server. This is the server that runs Certificate Services. The CA issues client certificates.
- CA administrator. This user has administrator rights on the CA server and can modify its policy settings.
- Domain Controller (DC). This is the server that runs Microsoft Active Directory Domain Services. It is used as a central repository for certificate templates to enforce certificate issuance policies across the domain.

Annex 8.3.4.2. Enrolment Process

It illustrates the various steps for enrolling certificates through the Network Device Enrollment Service.



Annex Fig. 15 SCEP Enrollment

The enrollment process includes the following steps.

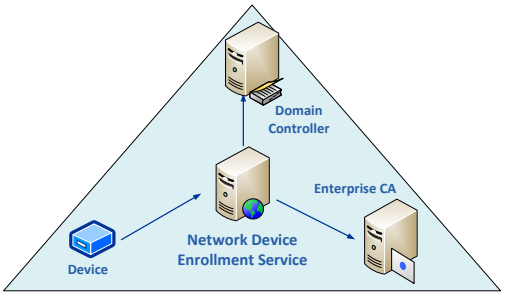
- The device generates an RSA public-private key pair on the device.
- The administrator obtains a password from the Network Device Enrollment Service.

  The administrator browses to the administration Web page.

  The service verifies that the administrator holds the required permissions for the configured certificate templates.
- The administrator sets the device with the password and sets it to trust the enterprise PKI.
- The administrator configures the device to send the enrollment request to the Network Device Enrollment Service.
- The Network Device Enrollment Service signs the enrollment request with its Enrollment Agent certificate and sends it to the CA.
- The CA issues the certificate and returns to the service.
- The device retrieves the issued certificate from the service.

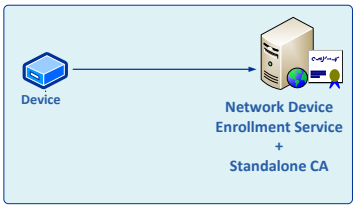
Annex 8.3.4.3. Scenario Deployments

- In an enterprise scenario deployment, the service will use an existing Enterprise CA.
- Since the CA computer has access to the CA key, it is recommended to reduce the attack surface of the computer hosting the CA by not enabling additional services. Therefore, the recommended setting is to install the Network Device Enrollment Service on a different computer than the one hosting the CA service.



Annex Fig. 16 Enterprise CA

- In this deployment scenario, all permissions will be based on permissions set on certificate templates published in the DC. In addition, the certificate requests sent to the CA will be based on certificate templates.



- In standalone scenario, the service will not use an existing Enterprise CA. Instead, it will use a stand-alone CA. It is recommended that the stand-alone CA will be deployed on the same computer as the Network Device Enrollment Service and will be used to issue device certificates only.

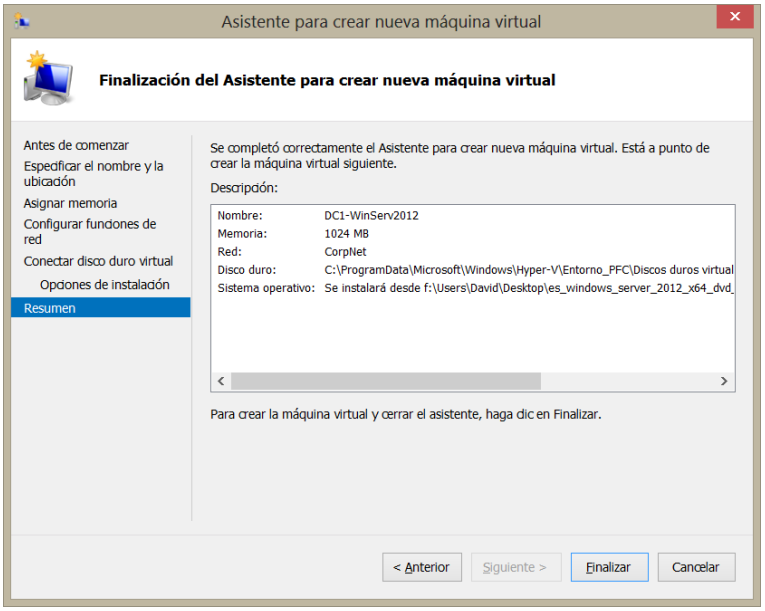
Annex Fig. 17 Standalone CA

ANNEX 9. PHASE 3 ON-PREMISE LAB ENVIRONMENT SETUP

Annex 9.1. Base Server Configuration

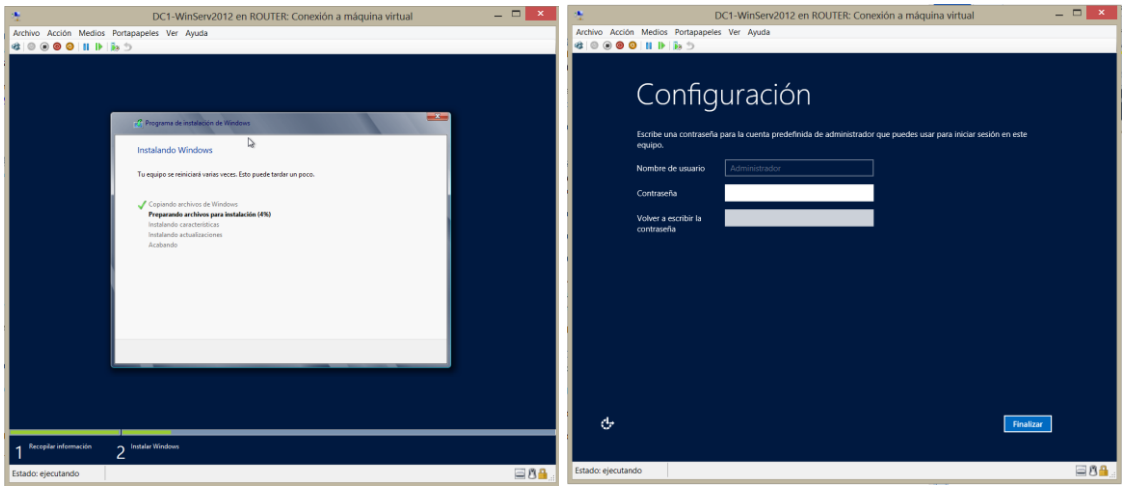
Annex 9.1.1. Provisioning the Virtual Machine

- Define Name, virtual machine and hard drive path, RAM memory, network connection and ISO for installation.



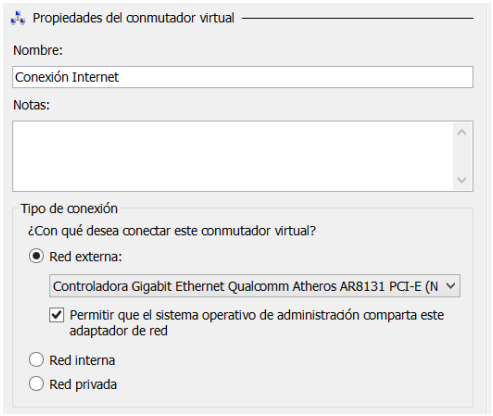
Annex 9.1.2. Installing the Operative System

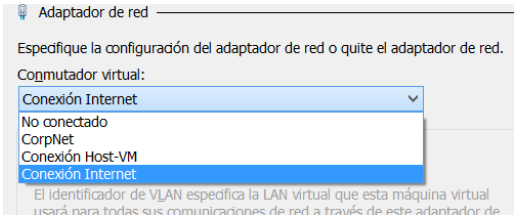
- Instructions are followed to complete the installation and a strong password for the local Administrator account is defined.



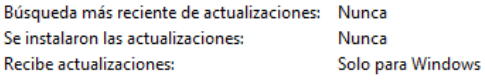
Password: Admin@Local01

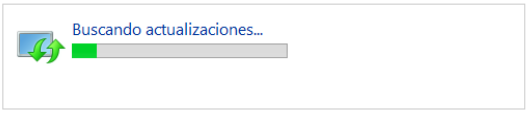
- Creating an internet virtual switch and connecting VM to it.

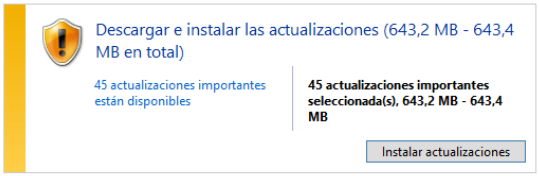


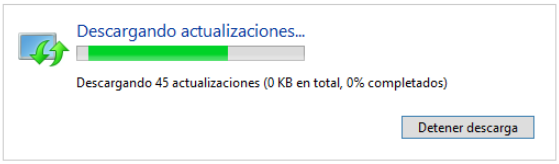


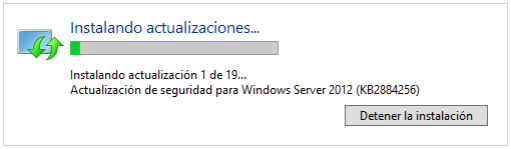
- Run upgrade program, download and install the latest OS features

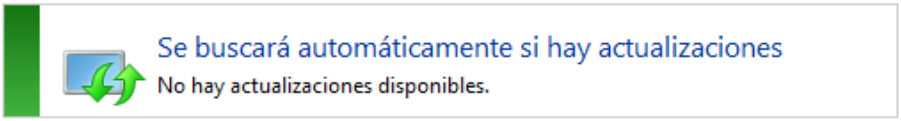






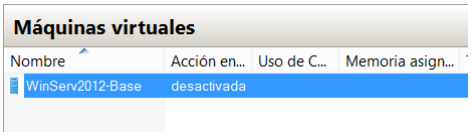


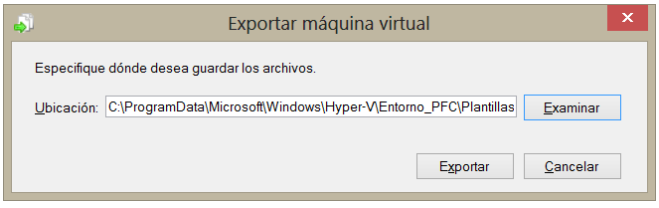


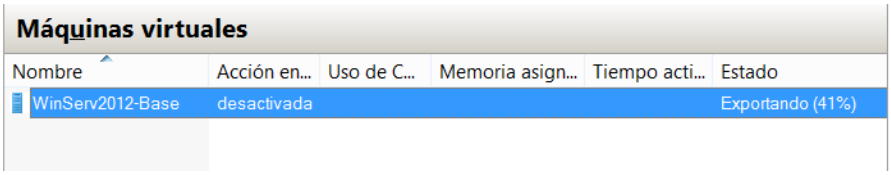


Annex 9.1.3. Creating a Virtual Machine Template

- Select the upgraded base-VM and export it as a template.

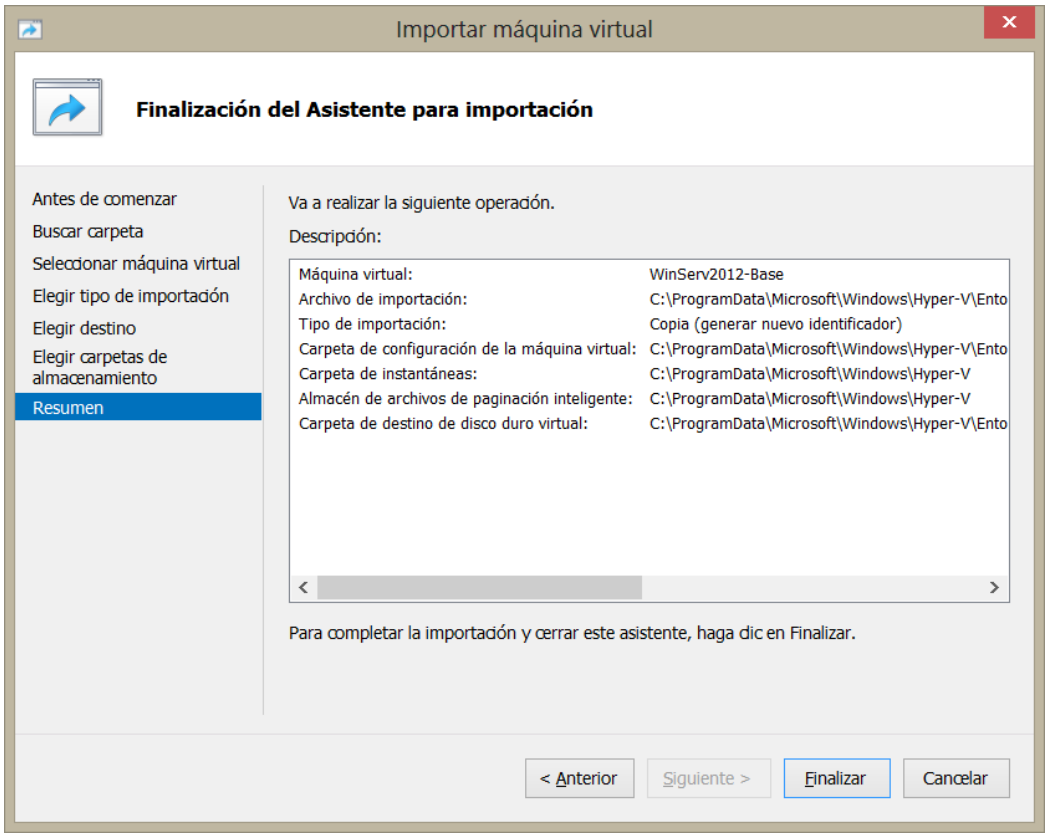






Annex 9.1.4. Creating other VM through template

Import the template with the wizard: select VM template, importation type (new identifier-no duplication) and select data folders.



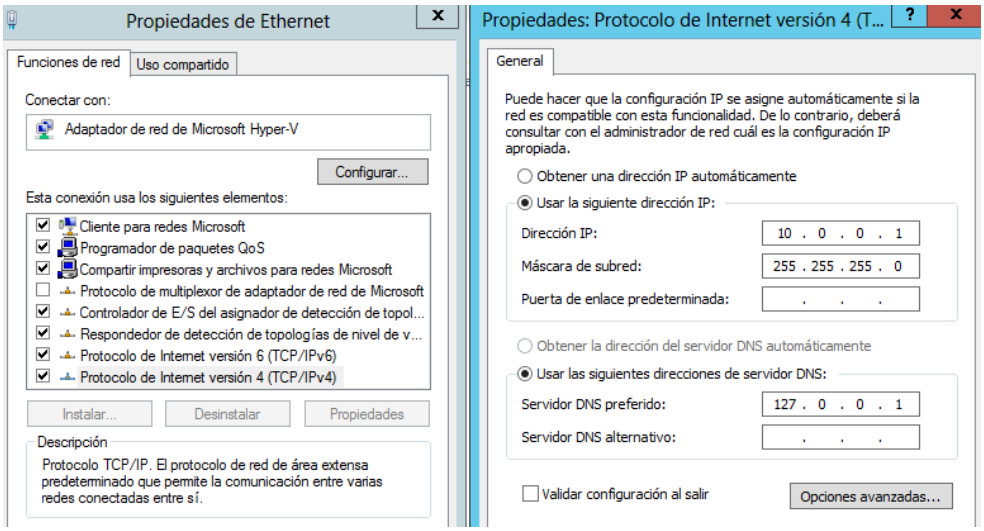
Annex 9.2. Configuring corporate directory services

The Virtual Machine DC1 will provide the following services:

- A domain controller for the corp.contoso.com Active Directory Domain Services (AD DS) domain
- A DNS server for the corp.contoso.com DNS domain
- A DHCP server for the Corpnet subnet

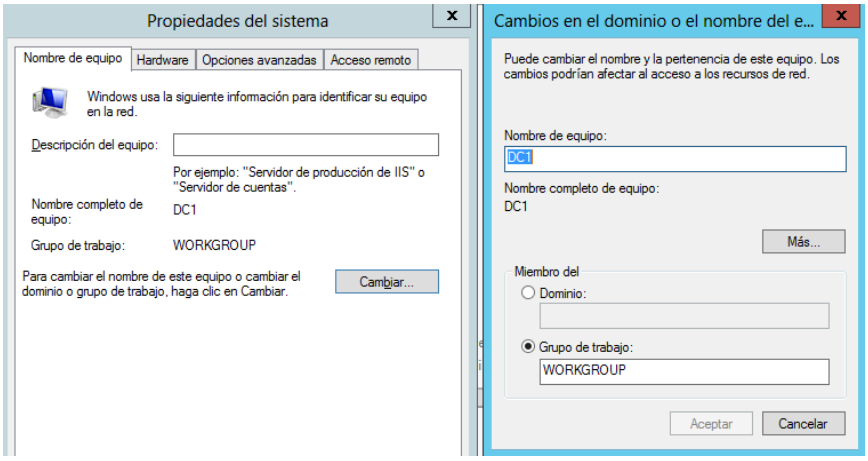
Annex 9.2.1. Configuring network settings and Server name

Configure the TCP/IP parameters for the DC1 at CorpNet. The settings will be a static IP address of 10.0.0.1 and the subnet mask of 255.255.255.0.



Annex 9.2.1.1. Server Name

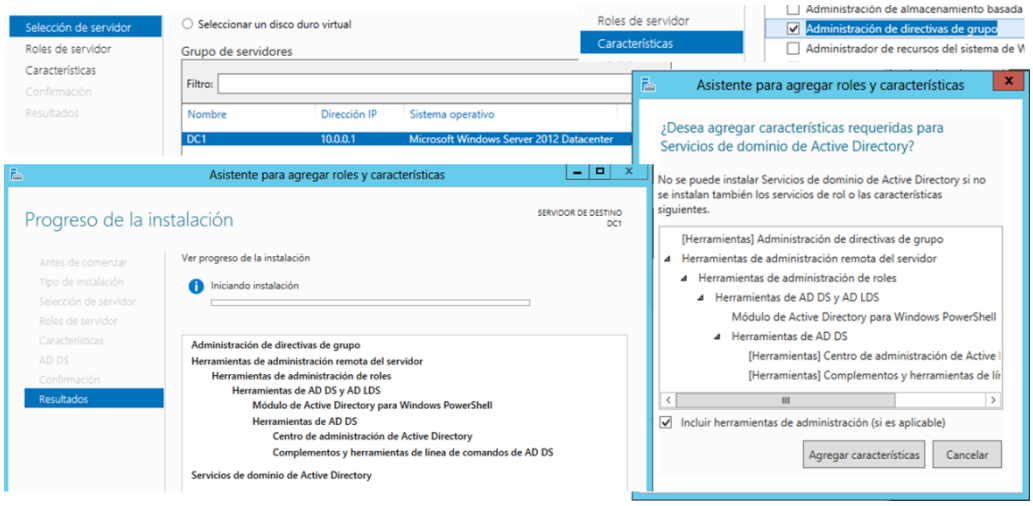
Changing the **Computer Name on** tab of the System Properties, **Change** it to **DC1**, and then restart the computer.



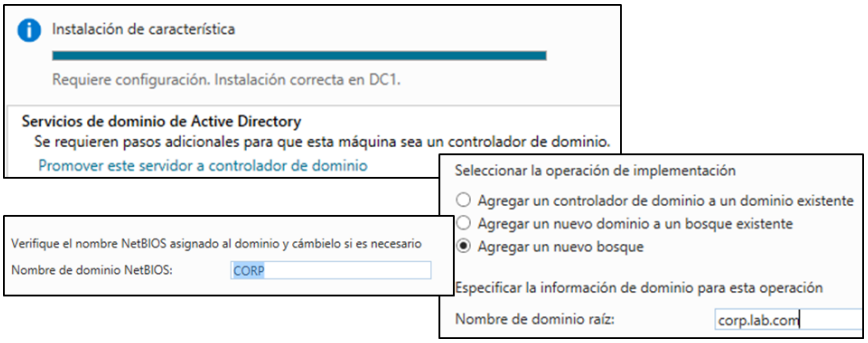
Annex 9.2.2. Installing Domain Controller and DNS roles

- Launch the Server manager and click on “Add roles and features” option

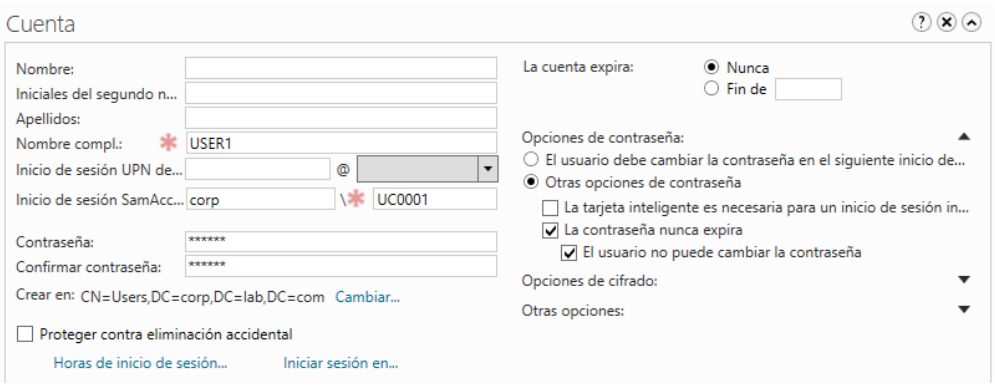
- Select the server where the role will be installed and the role select Active Directory Domain Services



- Once installation is finished, Server shloud be promoted to “Domain Controller”. In this process will be defined the domain name and other details.

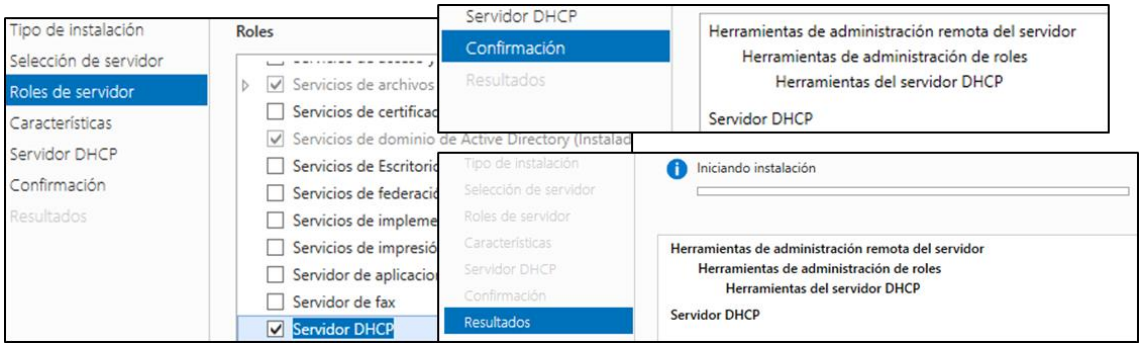


- In the **Prerequisites Check** dialog, since this is the first DNS server deployment in the forest, all warnings regarding DNS delegation can be ignored.
- In order to test the new configuration a user will be created.

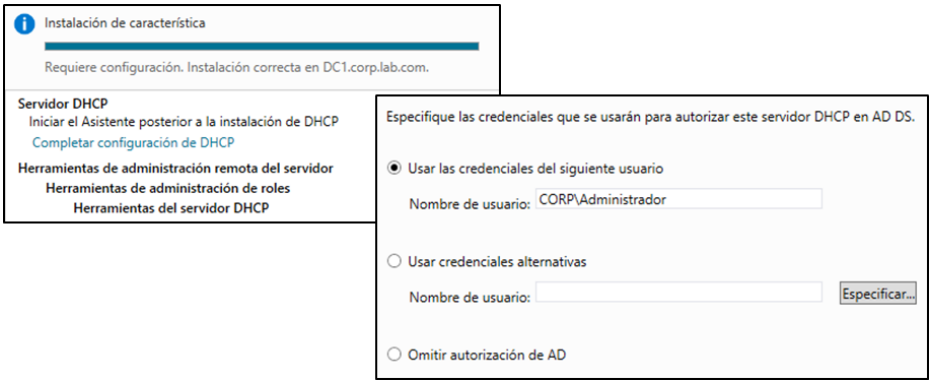


Annex 9.2.3. Installing DHCP role

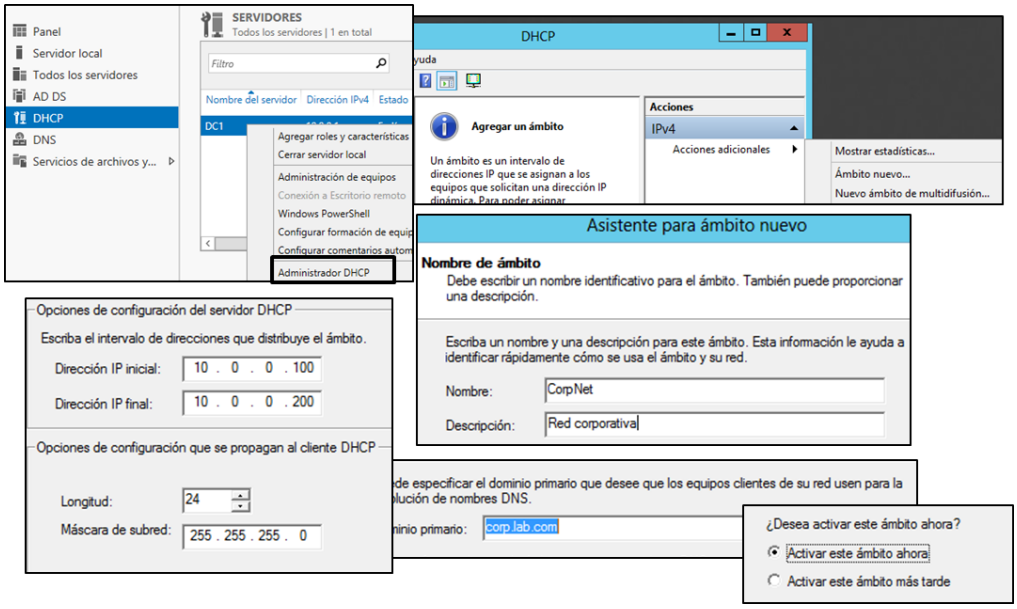
- As in previous case, installation starts with add roles wizard.



- Once the role is installed, some configurations are needed.



- Finally, it will be configured a new DHCP scope.



Annex 9.3. Configuring Web server

The Virtual Machine APP1 will provide the following services:

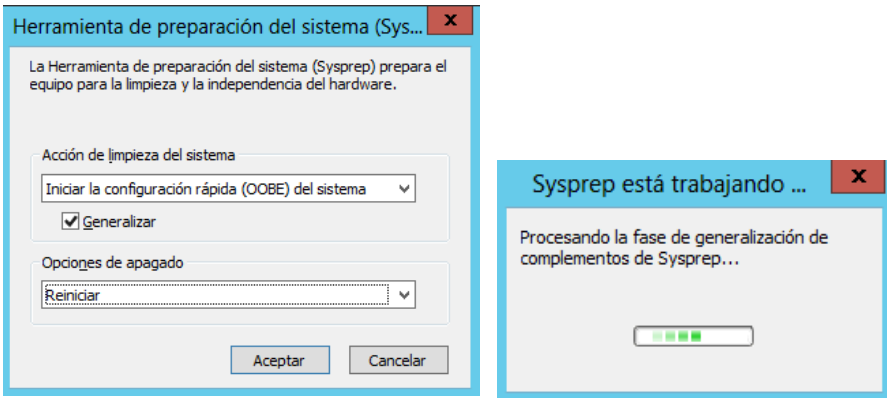
- IIS role provides web and file sharing services.
- Basic PKI role composed by an Enterprise CA.
- SCEP service for mobile devices certificates.

APP1 is a new server so, according to previous chapter, a new VM has been provisioned through Base Server Template. After that, the configuration continues as follows

Annex 9.3.1. Changing SID of VM

In order to avoid errors caused by Server ID duplicated due to VM clone, first of all is needed to execute the command below:

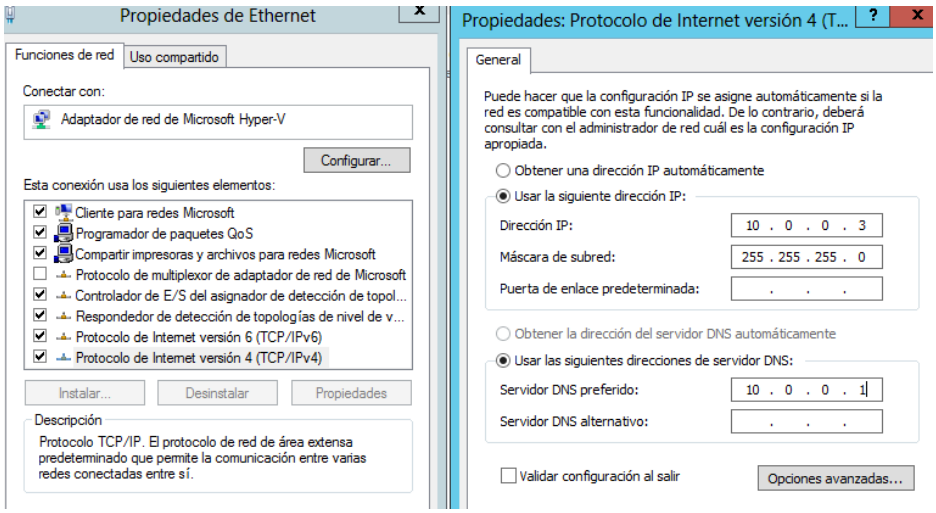
C:\Windows\system32\sysprep\sysprep.exe



Once the server is restarted, we can start with the configuration.

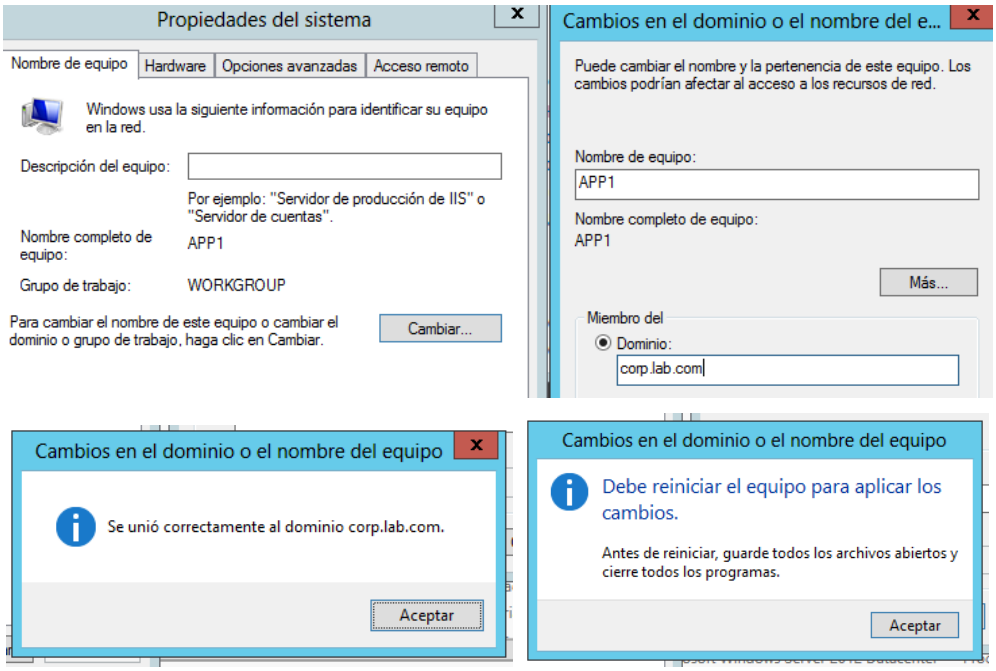
Annex 9.3.2. Configuring network settings and Server name

Configure the TCP/IP parameters for the APP1 at CorpNet. The settings will be a static IP address of 10.0.0.3 and the subnet mask of 255.255.255.0.



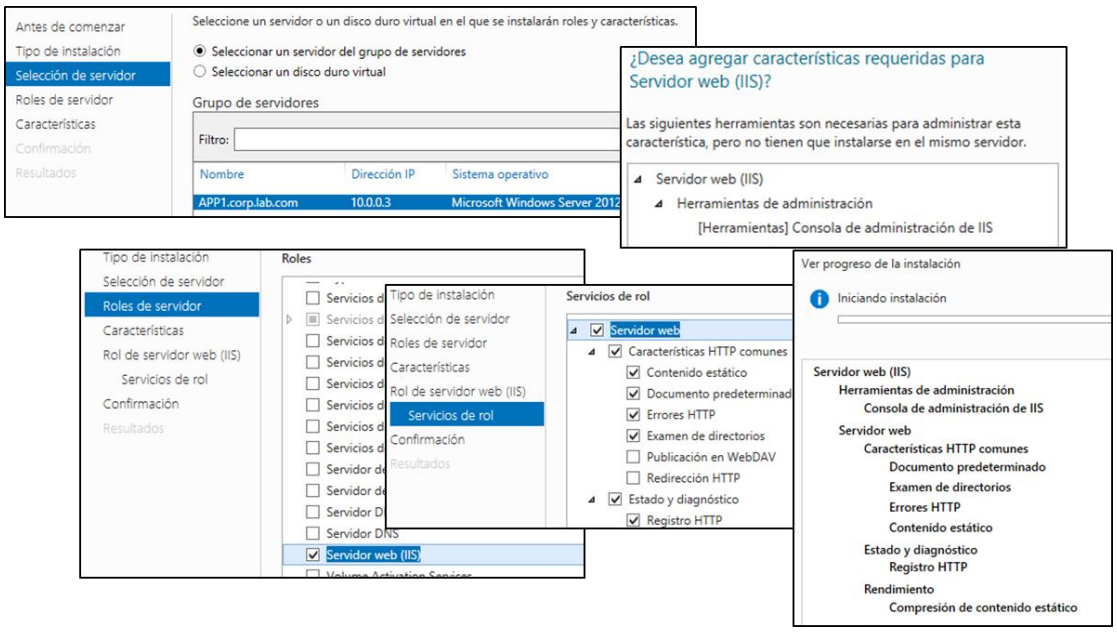
Annex 9.3.2.1. Server Name and Domain Join

Changing the **Computer Name on** tab of the System Properties, **Change** it to **APP1, adds it to corp.lab.com domain** and then restart the computer.



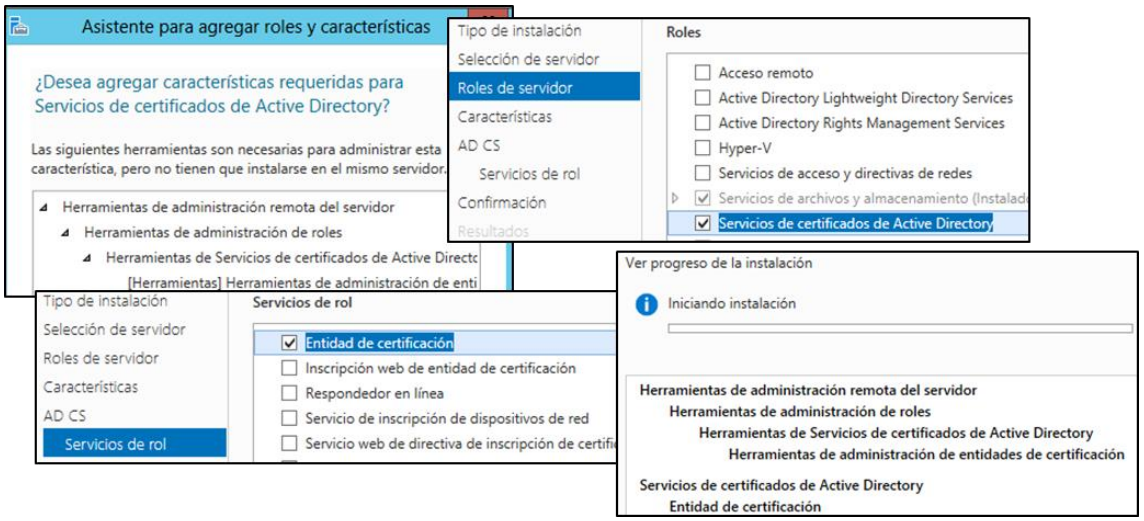
Annex 9.3.3. Configuring IIS role

- As in previous cases, through “Add role” wizard the IIS installation is launched.

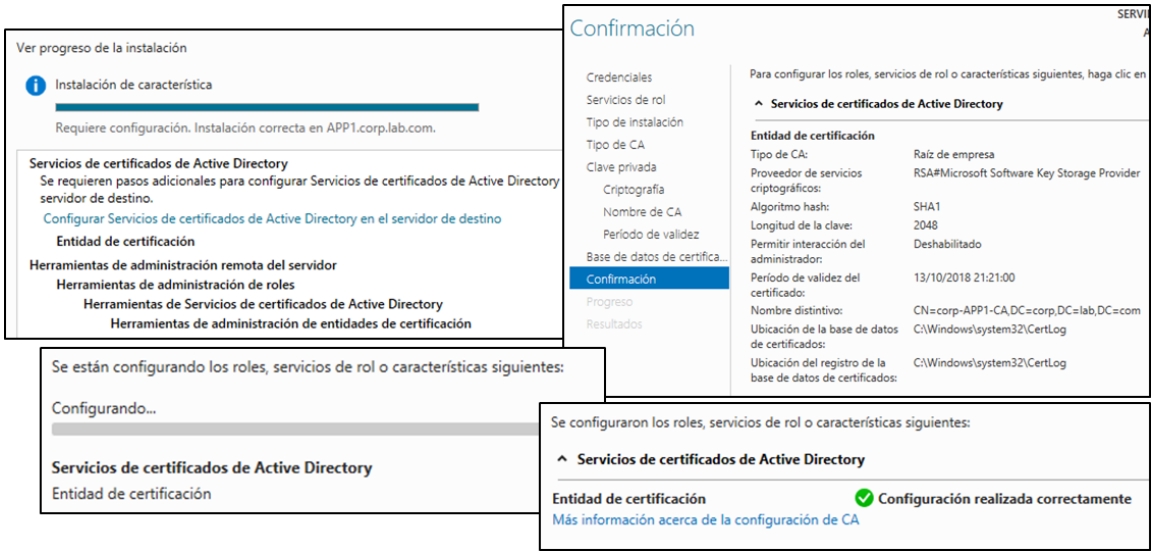


Annex 9.3.4. Configuring basic PKI

- As in other cases, the first steps are done with “add role” wizard.



- Once the installation is finished, some additional configuration steps are required: Services, private key, type of CA, cryptography details, CA validity time, CA Name and other settings.



Annex 9.3.5. Configuring NDES service

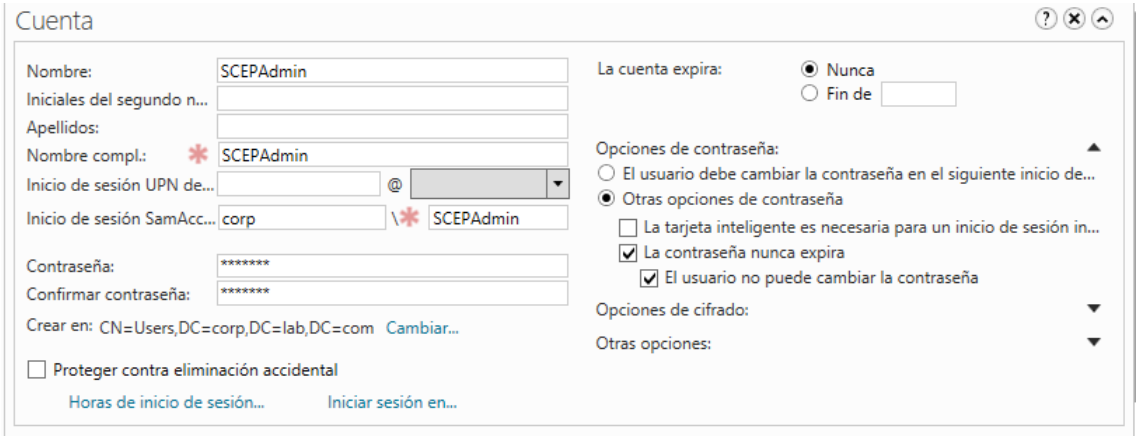
For more information about Network Device Enrollment Service, theoretical base can be consulted at [Annex 8.2.1].

Annex 9.3.5.1. Creating service users

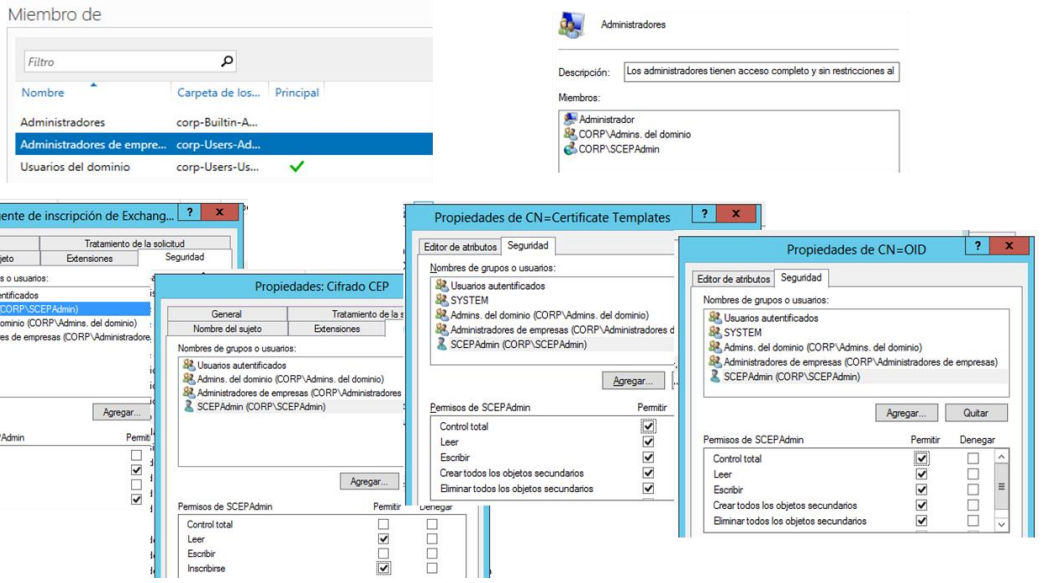
There are three roles related to setting up and running the service.

- **Service Administration user – SCEPAdmin**

Service Administrator The user who logs on the service machine and installs the Network Device Enrollment Service. This user is referred to as SCEPAdmin.

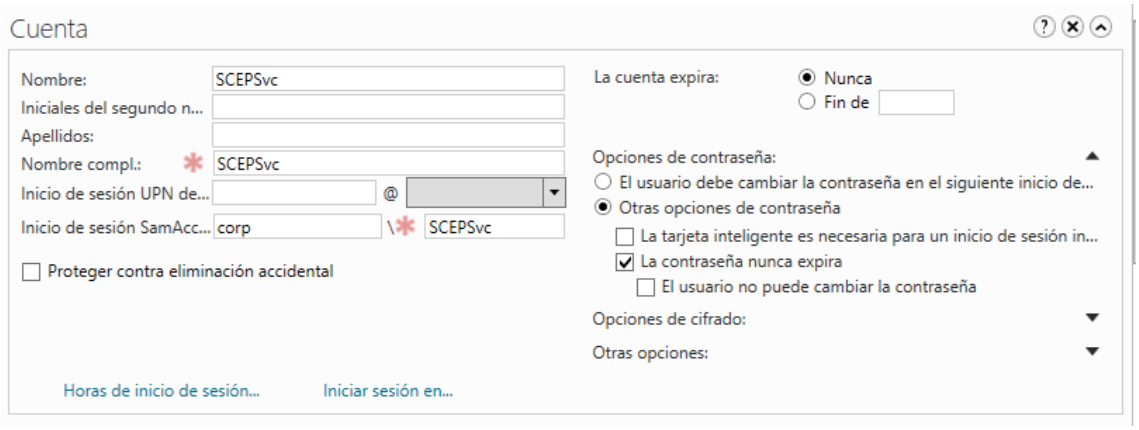


- Must be a member of the Enterprise Admins group (this is just required for installation and not for ongoing administration).
- Must be VM Local administrator
- Must have Enroll permission on the “Exchange Enrollment Agent (Offline request)” and “CEP Encryption” templates.
- Must have permissions to add templates to the selected CA.

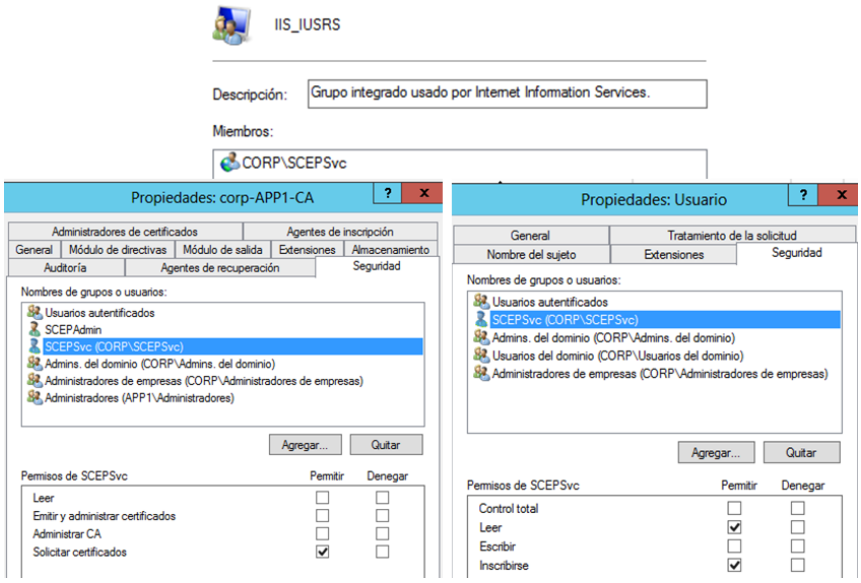


- **Service Account user – SCEPSvc**

The credentials which will be used to run the service. This user is referred as SCEPSvc.

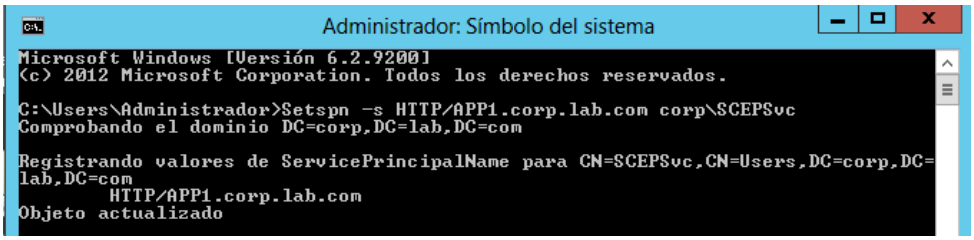


- Must be IIS_IUSRS Local Administrator
- Must have request permission on the configured CA.
- Must be a domain user account and have **Read** and **Enroll** permissions on the configured templates.



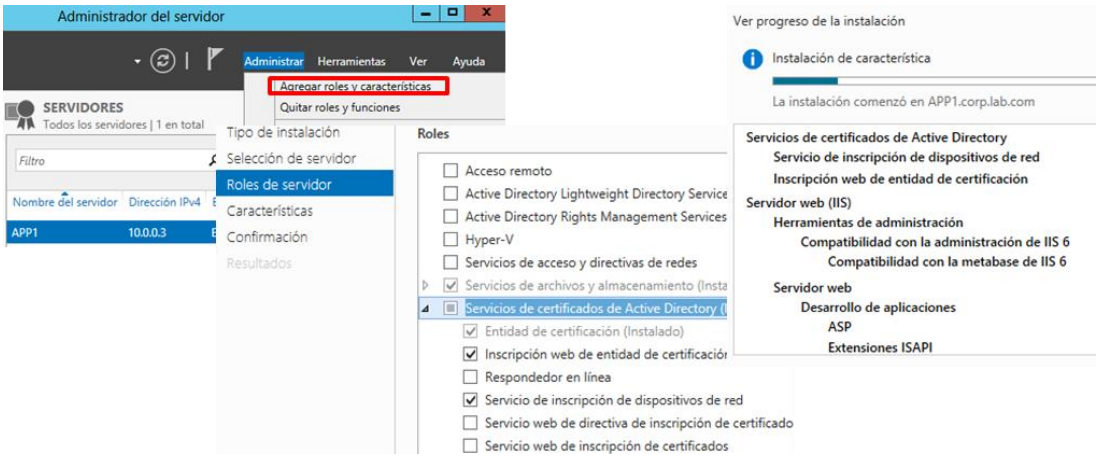
- Must have SPN set in Active Directory.

To do so, use the Setspn command syntax of: **Setspn -s HTTP/***computerFQDN domainname******accountname*.

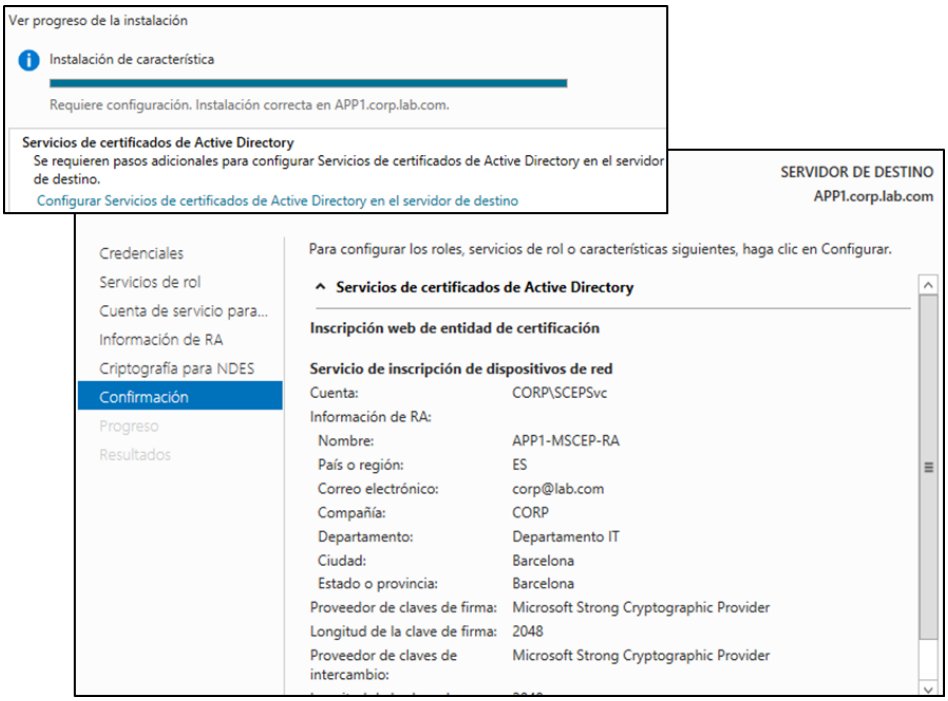


Annex 9.3.5.2. Configuring NDES Role

- As in other cases, “Add roles” wizard is used for first steps



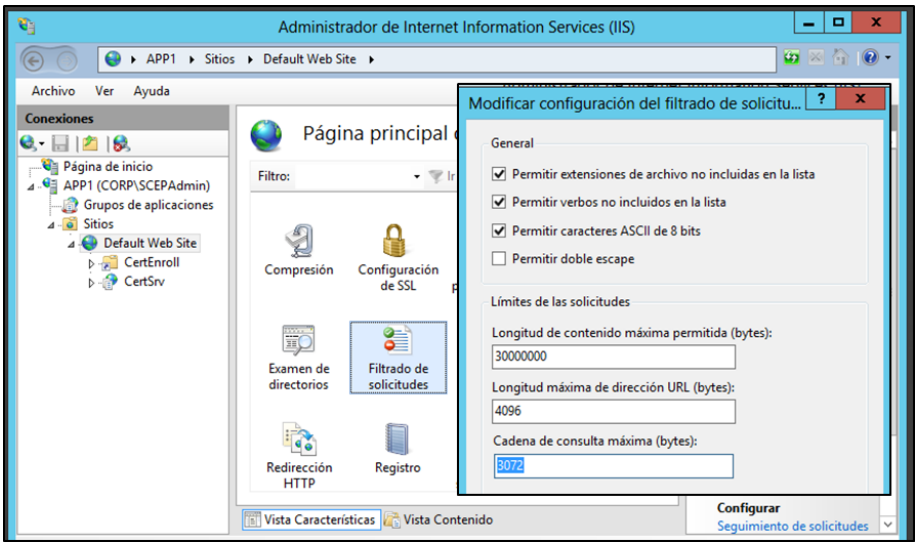
- Once the role is installed, additional settings must be configured: Role account, which role services, NDES service account, Registry authority definition, cryptography details and other settings.



Annex 9.3.6. NDES additional configuration for mobile devices

Annex 9.3.6.1. IIS request max length

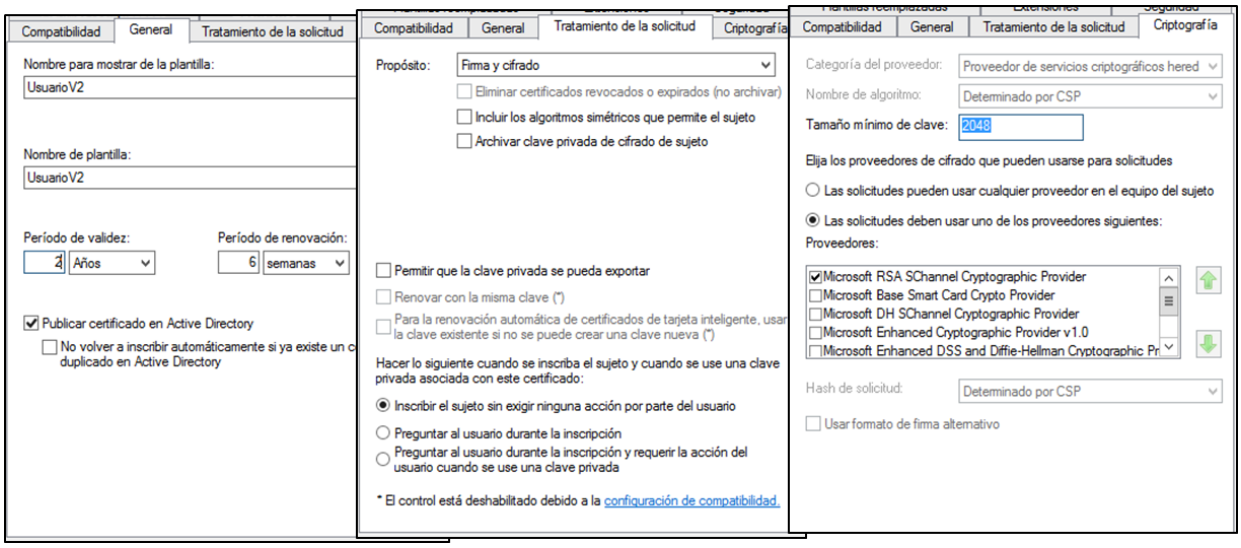
In a mobile devices scenario, the device (e.g. iPad) was sending a string over 2700 characters, but the default size allowed by the request filtering is 2048. it means that the amount of data being sent in the HTTP URL is larger than what is allowed by default. Hence is needed to change it.

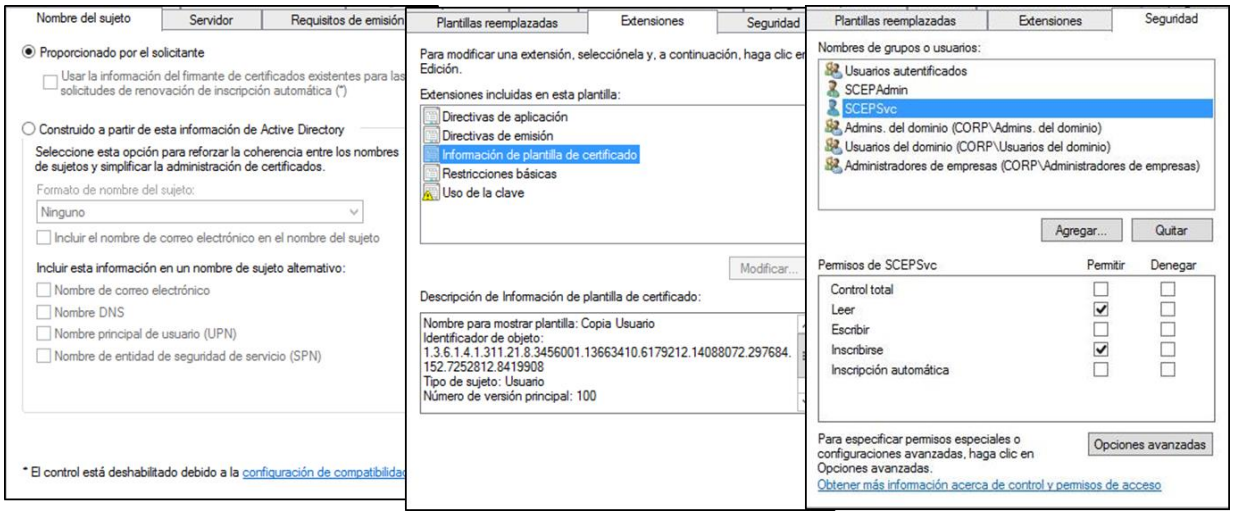


Annex 9.3.6.2. Mobile devices custom certificate template

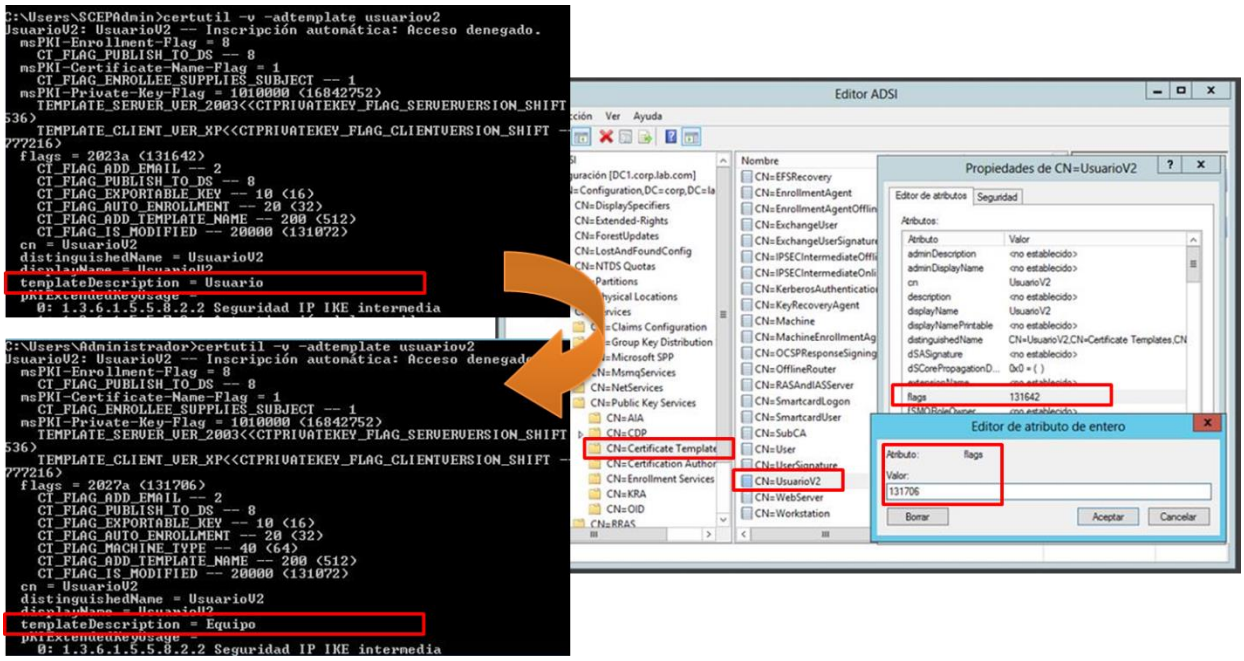
Network Device Enrollment Service (NDES) does not support user templates. As a result, a new the user template should be created and next it has to be changed from user to computer template.

- **Creating the new userV2 template**

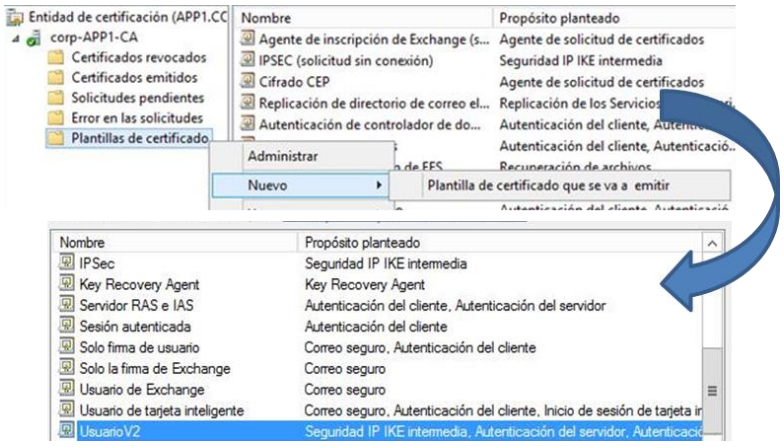




- **Changing the template type to computer**

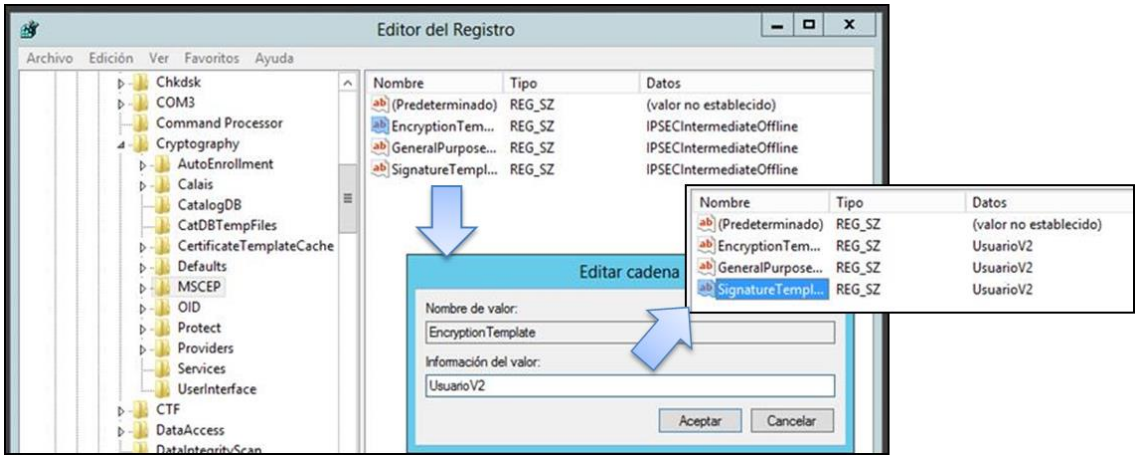


Annex 9.3.6.3. Publishing the certificate to the Certification Authority



Annex 9.3.6.4. Changing default NDES template

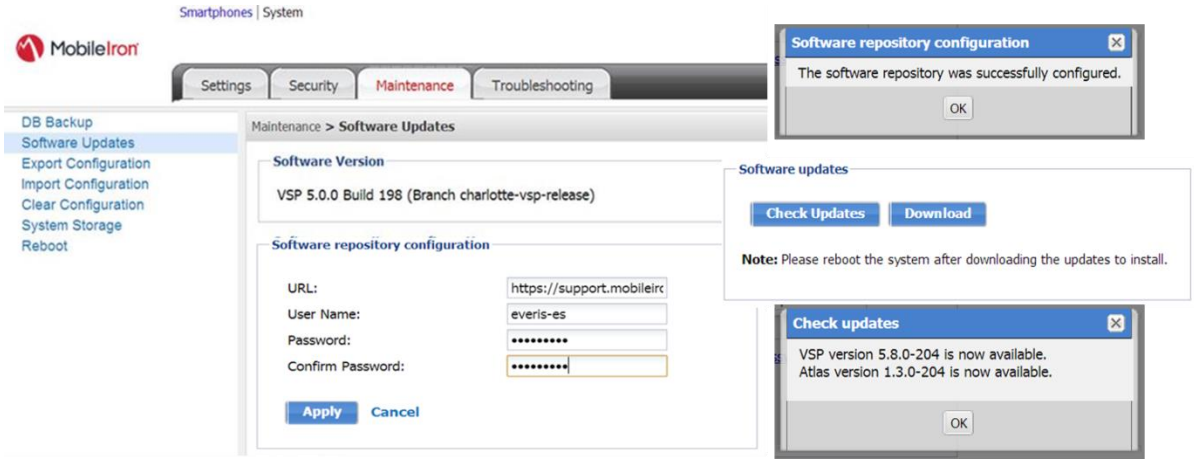
Finally, it is needed to configure the Network Device Enrollment Service (NDES) to issue certificates based on the certificate template created. Hence we have to edit the following registry key:



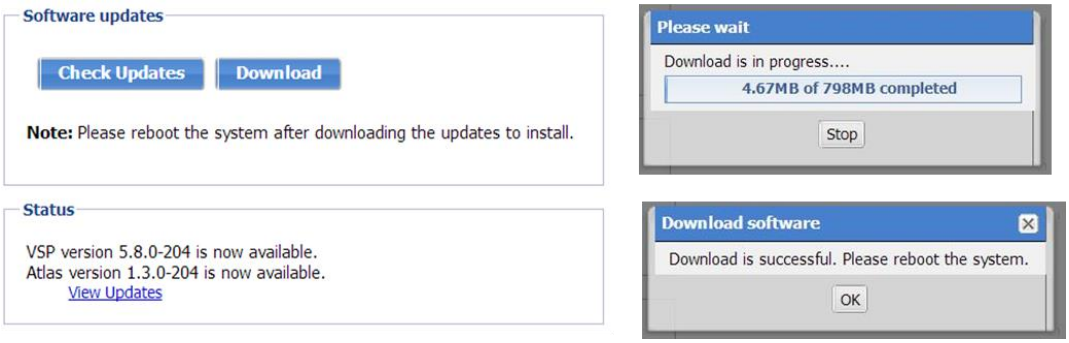
ANNEX 10. PHASE 3 CLOUD-BASED LAB ENVIRONMENT SETUP

Annex 10.1. Cloud EMM Core upgrade

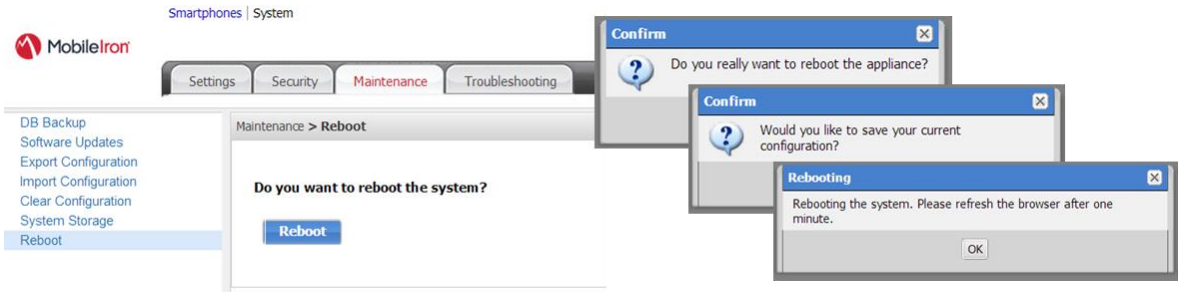
- **Configuring repository for software download.**



- **Downloading EMM Core ISO.**



- **Rebooting the virtual appliance for upgrade.**



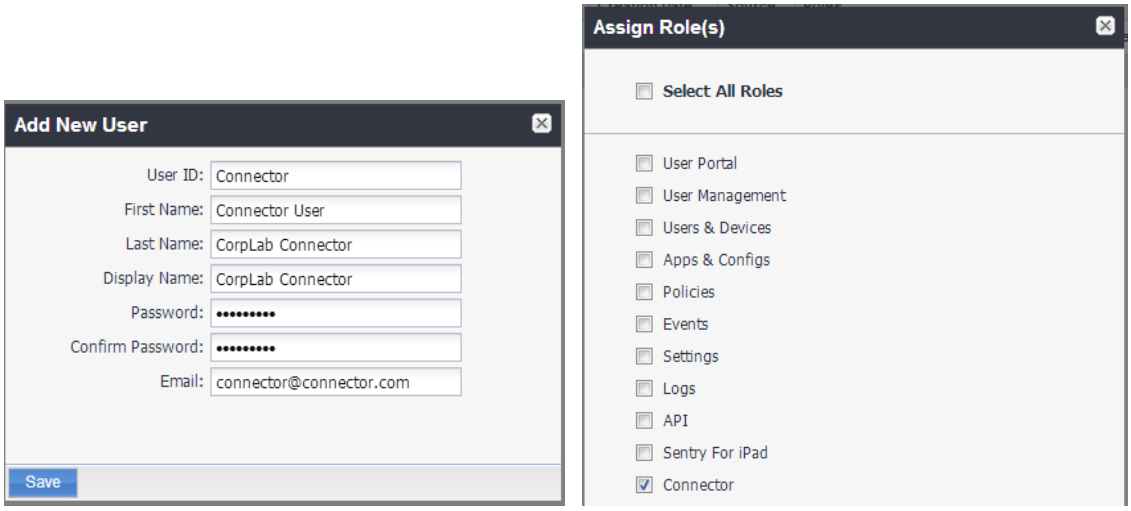
Annex 10.2. Enterprise Connector setup

There are several tasks that need to be completed on the EMM Core prior to Connector installation. This section describes these tasks.

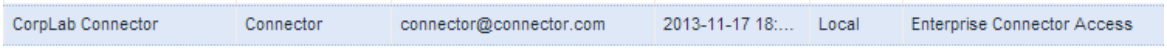
Annex 10.2.1. Assigning the Connector role

Each Connector authenticates to the EMM Core with an authorized local user account. It is recommended create a user and assign only the Connector role to authenticate through EMM Core.

- Add Local User (PSW: Connector01) and assign Connector role:

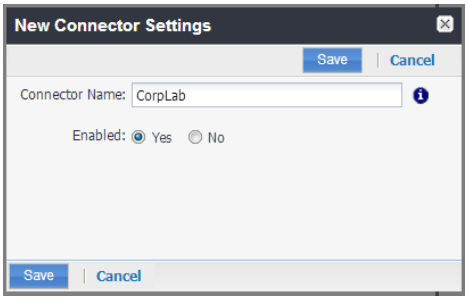


- If all Works fine, It will be shown something similar to this:

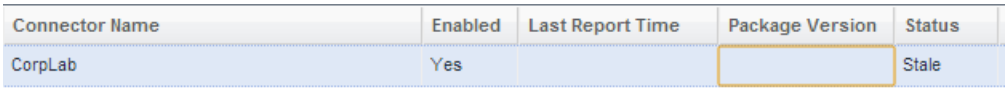


Annex 10.2.2. Adding Enterprise Connector to EMM Core

- Adding connector in Settings > Connector and enable it:

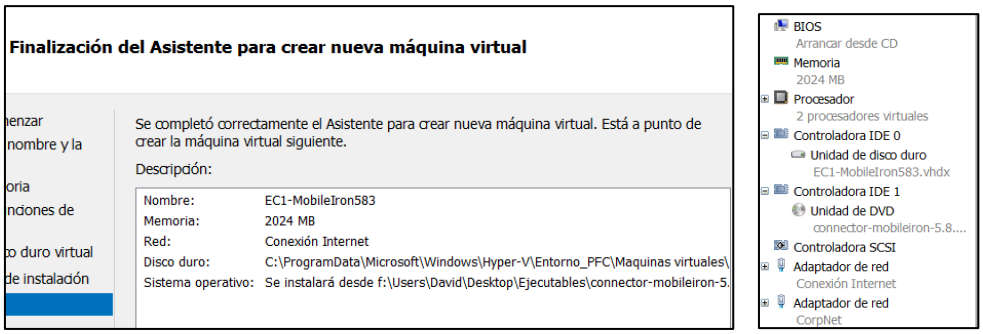


- After add this connector, it remains in “Stale” status until EMM Core and Connector establishes the first connection. At “Connector Details, it will find the URL (https://de.mobileiron.net/teveris/ec) for connection.

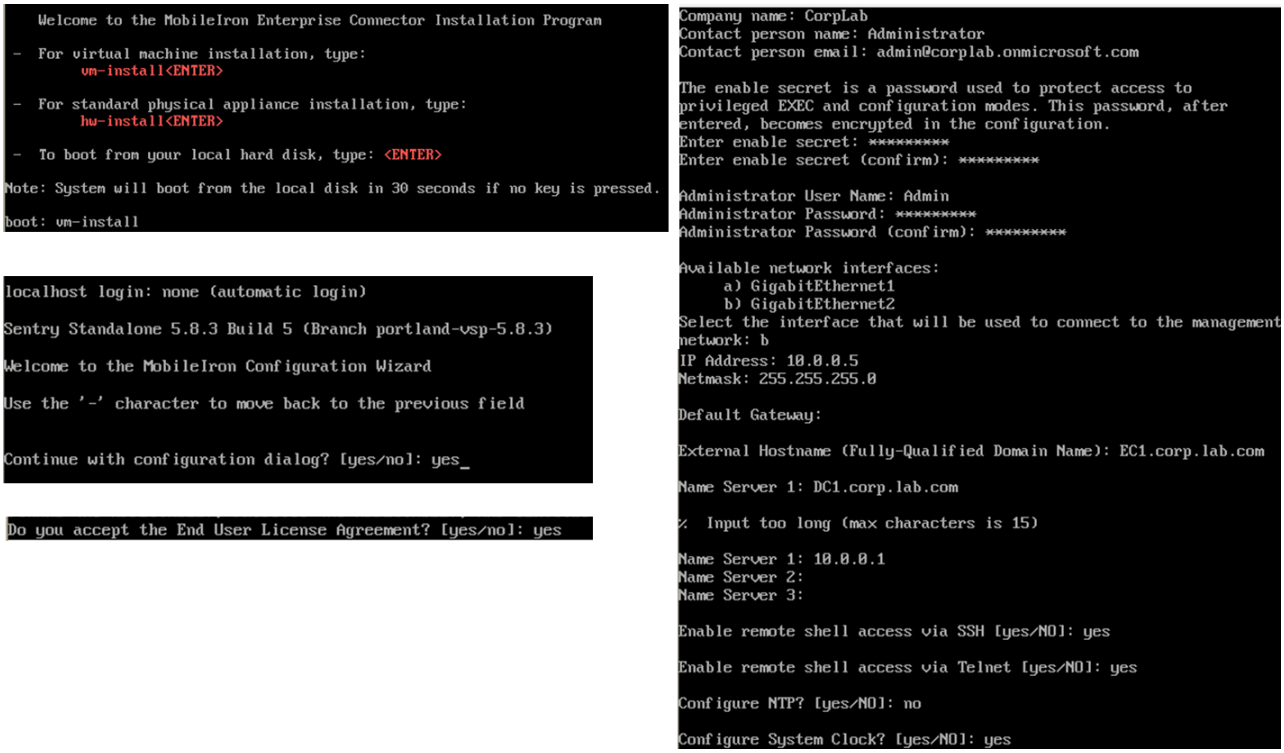


Annex 10.2.3. Installing Connector virtual appliance

Annex 10.2.3.1. Provisioning the virtual machine



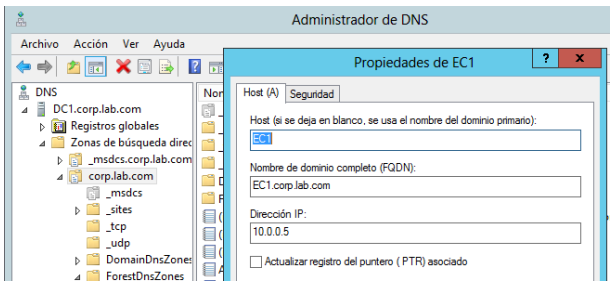
Annex 10.2.3.2. Installing the connector ISO



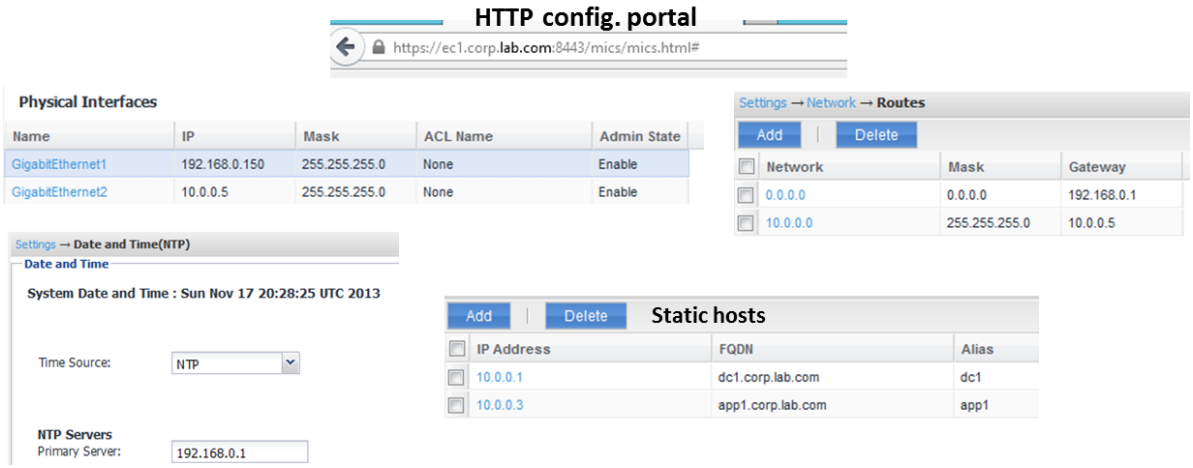
Annex 10.2.3.3. Configuring Enterprise Connector

Once Enterprise Connector is installed, it needs some configurations in order to be able to reach Cloud EMM Core.

- Enterprise Connector DNS record setup



- Configuring Enterprise Connector connectivity

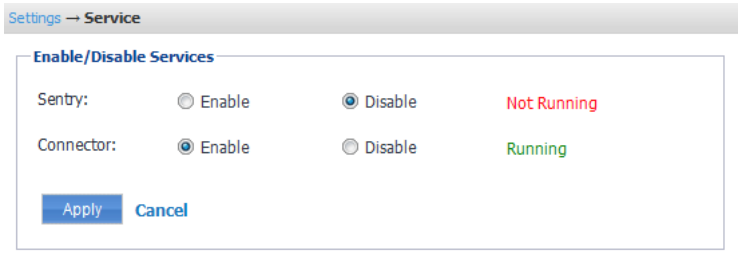


Annex 10.2.4. Establishing connection EMM Core-Connector

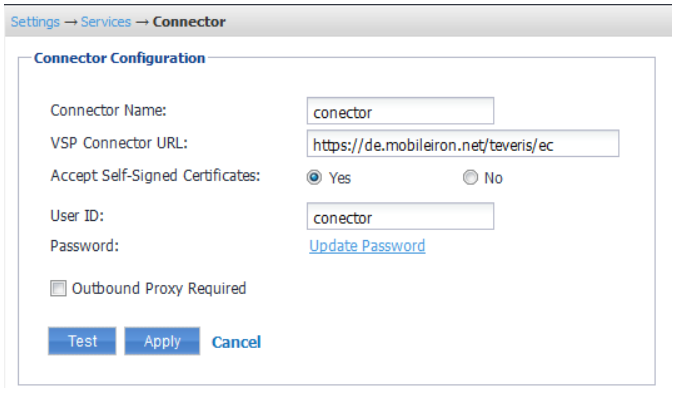
After the Enterprise Connector is installed and configured on the EMM Core, next step is to establish the connection in between.

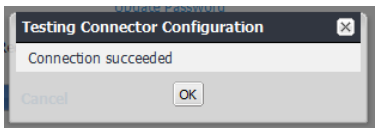
- Disabling Sentry service from connector configuration web portal.

https://EC1.corp.lab.com:8443/mics

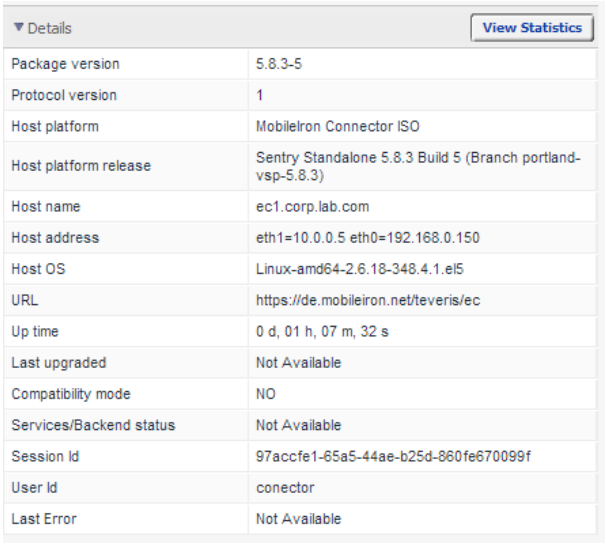


- Establishing relation EMM Core – Enterprise connector: Specify the *Connector Name* (must match what was configured on the Cloud EMM Core), *EMM Core Connector URL and ID data.* Next, test the connection.





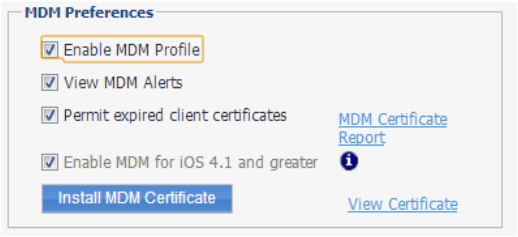
Connector Name	Enabled	Last Report Time	Package Version	Status
conector	Yes	2013-11-22 21:21:23	5.8.3-5	Connected



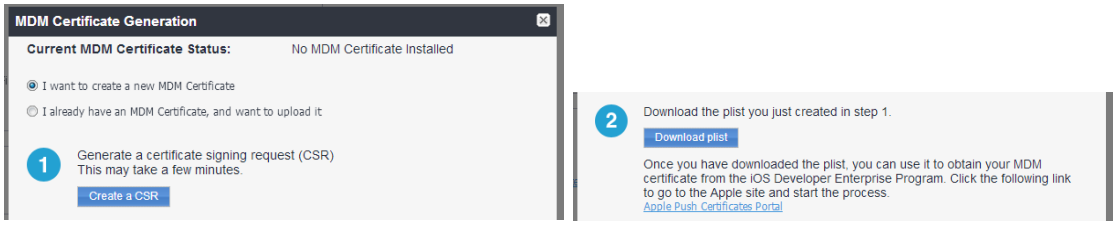
Details	View Statistics
Package version	5.8.3-5
Protocol version	1
Host platform	MobileIron Connector ISO
Host platform release	Sentry Standalone 5.8.3 Build 5 (Branch portland-vsp-5.8.3)
Host name	ec1.corp.lab.com
Host address	eth1=10.0.0.5 eth0=192.168.0.150
Host OS	Linux-amd64-2.6.18-348.4.1.el5
URL	https://de.mobileiron.net/teveris/ec
Up time	0 d, 01 h, 07 m, 32 s
Last upgraded	Not Available
Compatibility mode	NO
Services/Backend status	Not Available
Session Id	97accfe1-65a5-44ae-b25d-860fe670099f
User Id	conector
Last Error	Not Available

Annex 10.3. Enable iOS MDM support

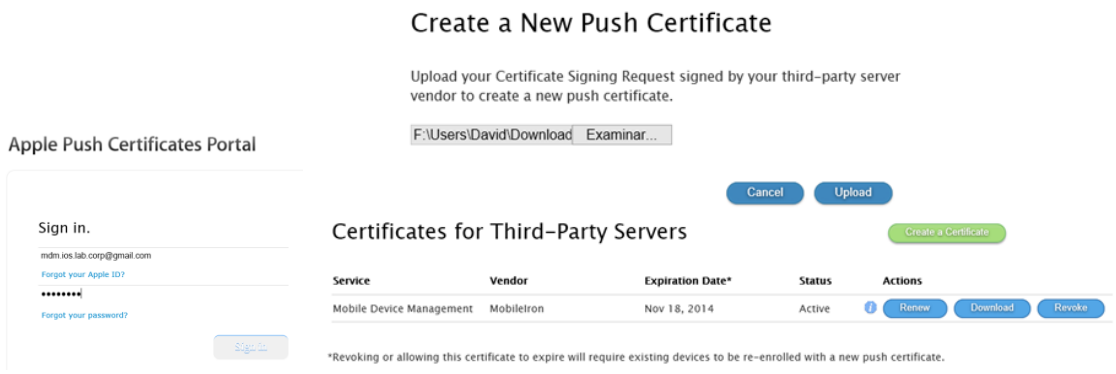
- **Enable MDM profile at EMM Core**



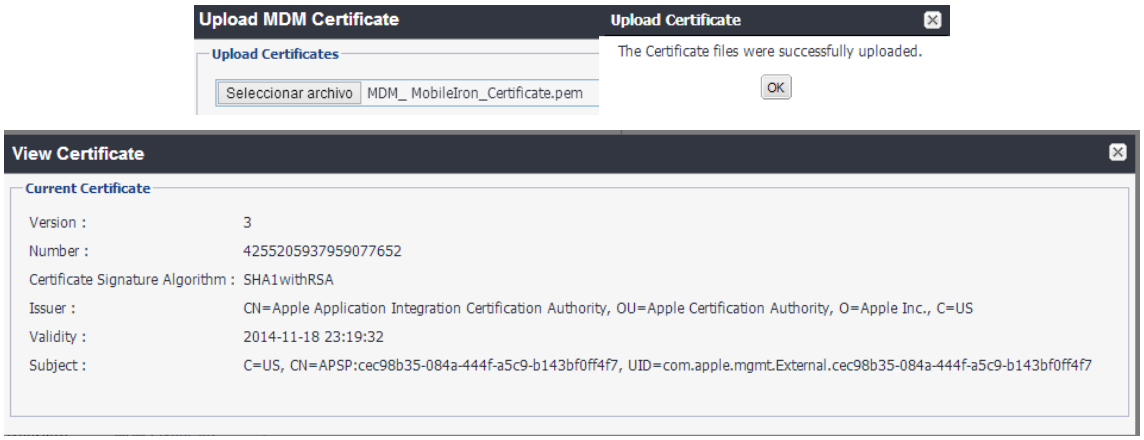
- **Generate a Certificate Signing Request (CSR)**



- **Access to Apple Push Certificates Portal, upload CSR and download the MDM certificate**

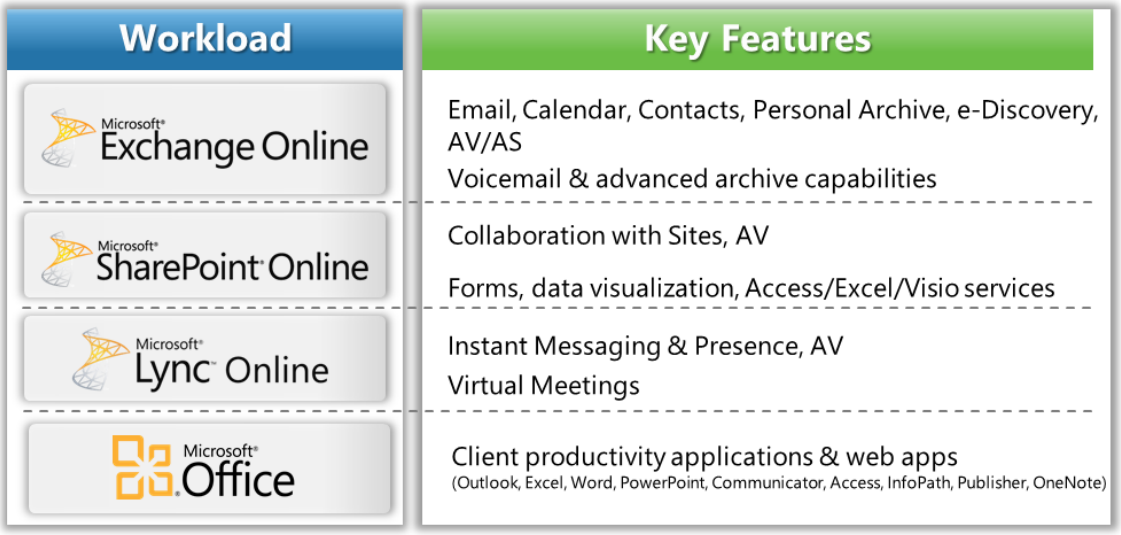


- **Upload MDM certificate to EMM Core**



Annex 10.4. Office 365 Setup

In order to provide email, document repositories, instant messaging and office tools, an Office 365 trial account has been setup

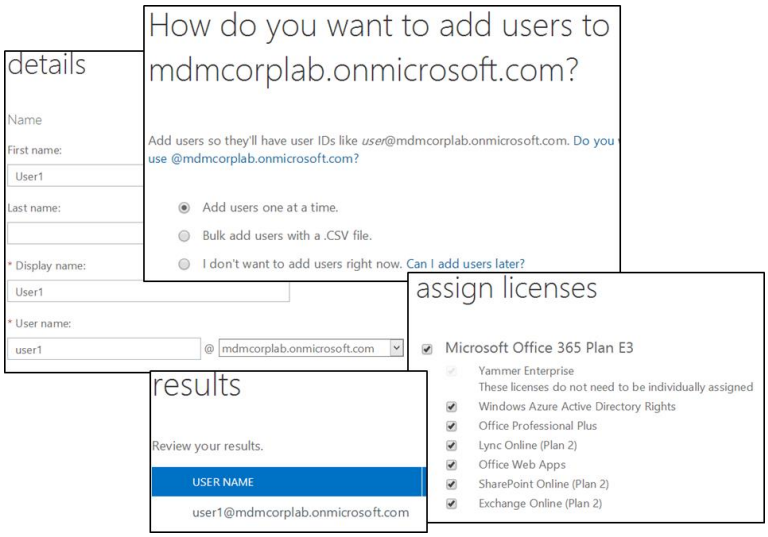


Annex 10.4.1. Register in Office 365 trial

The first step is to register in Office 365 program. To do this, go to the site and fill the form.

Annex 10.4.2. Adding Users

Finally, up to 25 users can be added for use the different services.

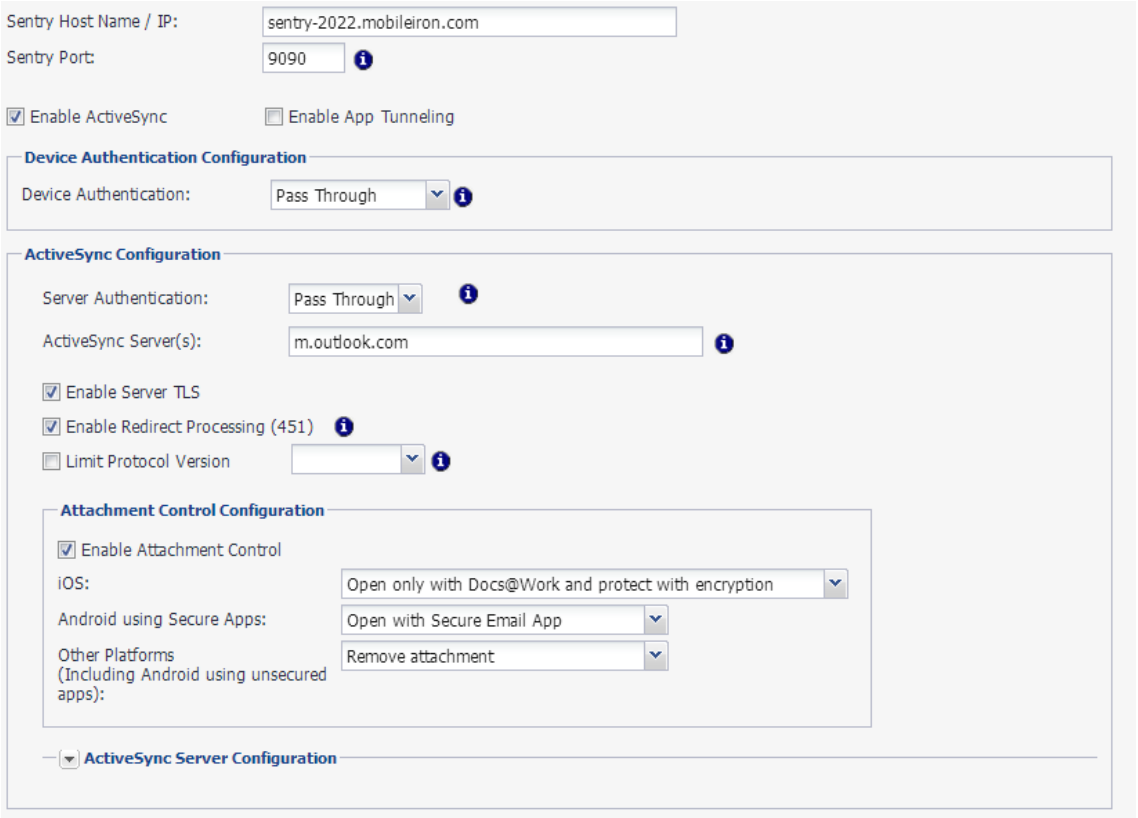


Annex 10.5. Enterprise services integration

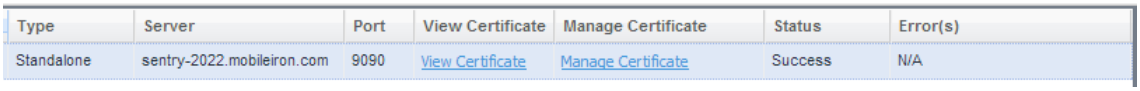
Annex 10.5.1. Adding Email Gateway to EMM Core

- *All the steps referred below, has been done according vendor's guide. [35]*

Email gateway should be added to the EMM Core for establish an email control policy. In order to do this, in EMM admin portal, Settings > Sentry > Add New, some information is needed: Gateway host and port, App or Email gateway type and some configuration about ActiveSync server).



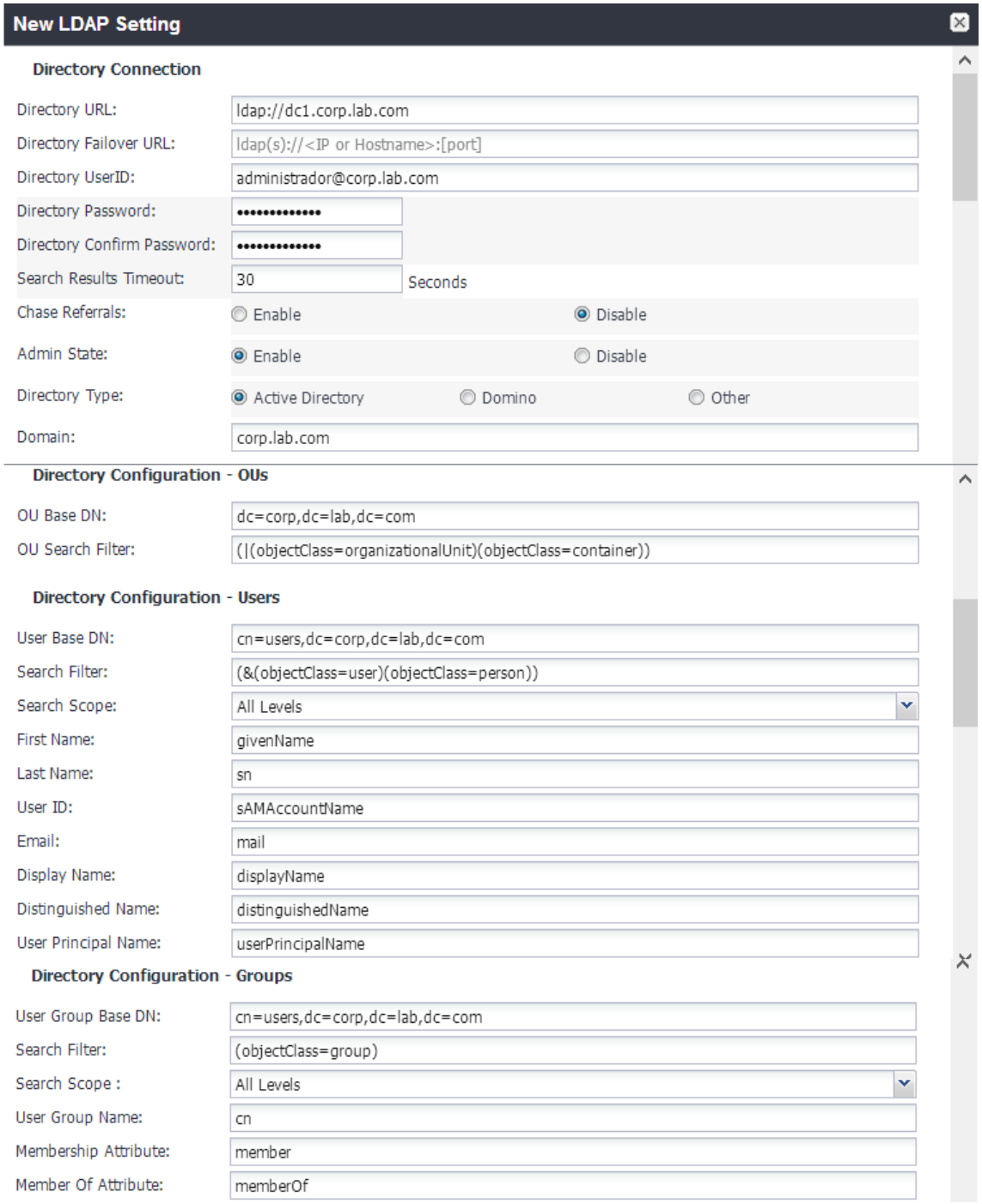
Once the Email Gateway has been added correctly, EMM Core will show gateway data and connection status.



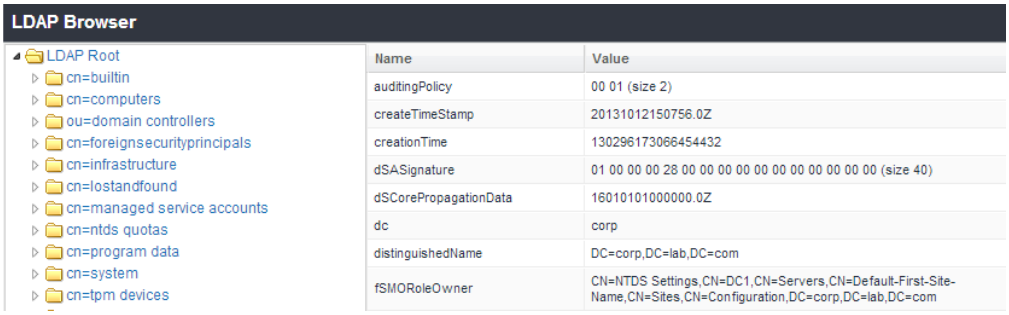
Type	Server	Port	View Certificate	Manage Certificate	Status	Error(s)
Standalone	sentry-2022.mobileiron.com	9090	View Certificate	Manage Certificate	Success	N/A

Annex 10.5.2. Adding LDAP Sync

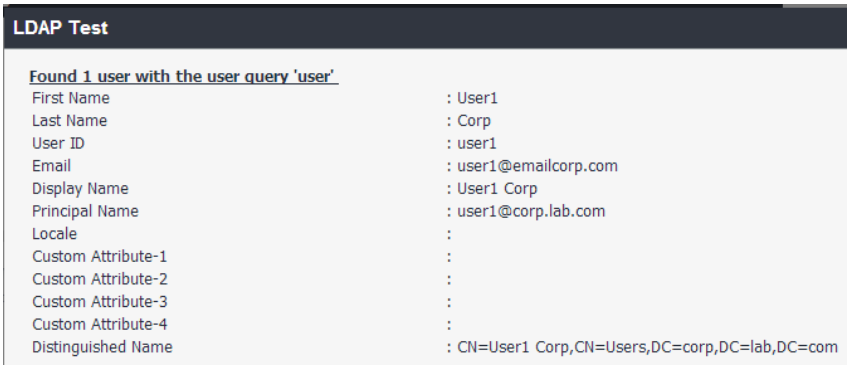
- In EMM Core admin portal, you can add a LDAP server, from Settings> LDAP>Add new. It has been provided Direcotry URL, user ID and password to establish the connection and other directory data like OU Base DN and User Base DN.



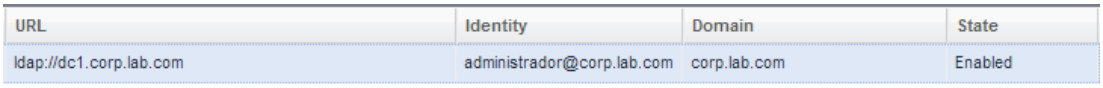
- Once all data is added, you can try to reach LDAP tree from the LDAP browser of admin portal.



- If previous step works fine, in order to test the service you can add some LDAP users and see if all the directory data is added.



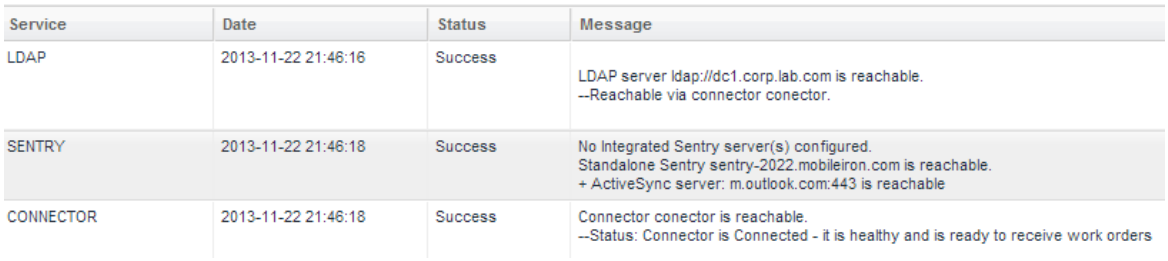
- Finally, you can save the preferences and see the LDAP server data and connection status form Admin Portal.



URL	Identity	Domain	State
ldap://dc1.corp.lab.com	administrador@corp.lab.com	corp.lab.com	Enabled

Annex 10.5.3. Verifying all services are working

With the aim of check that all the services are running in the correct way, a verify process from admin portal can be done.



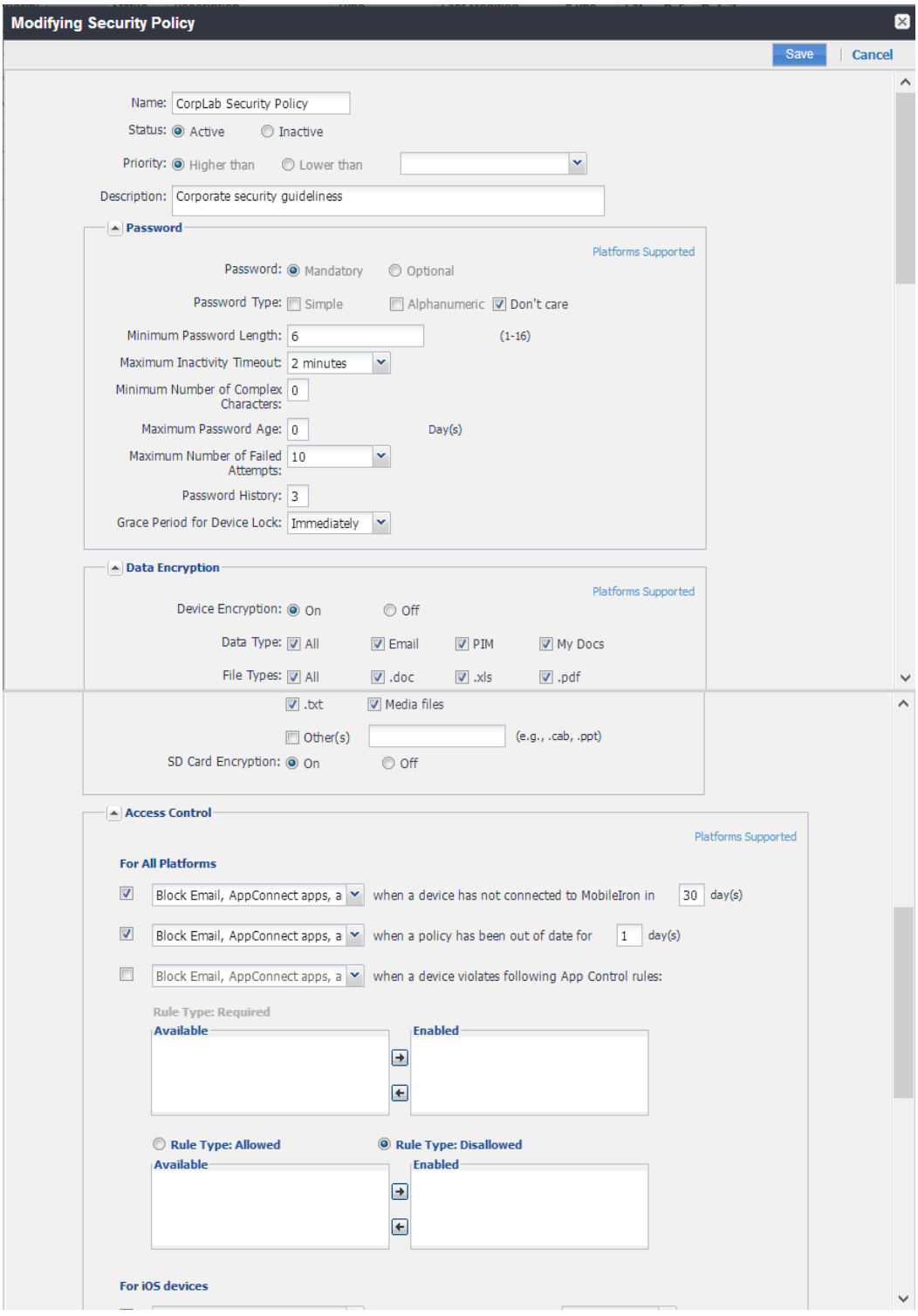
Service	Date	Status	Message
LDAP	2013-11-22 21:46:16	Success	LDAP server ldap://dc1.corp.lab.com is reachable. --Reachable via connector conector.
SENTRY	2013-11-22 21:46:18	Success	No Integrated Sentry server(s) configured. Standalone Sentry sentry-2022.mobileiron.com is reachable. + ActiveSync server: m.outlook.com:443 is reachable
CONNECTOR	2013-11-22 21:46:18	Success	Connector conector is reachable. --Status: Connector is Connected - it is healthy and is ready to receive work orders

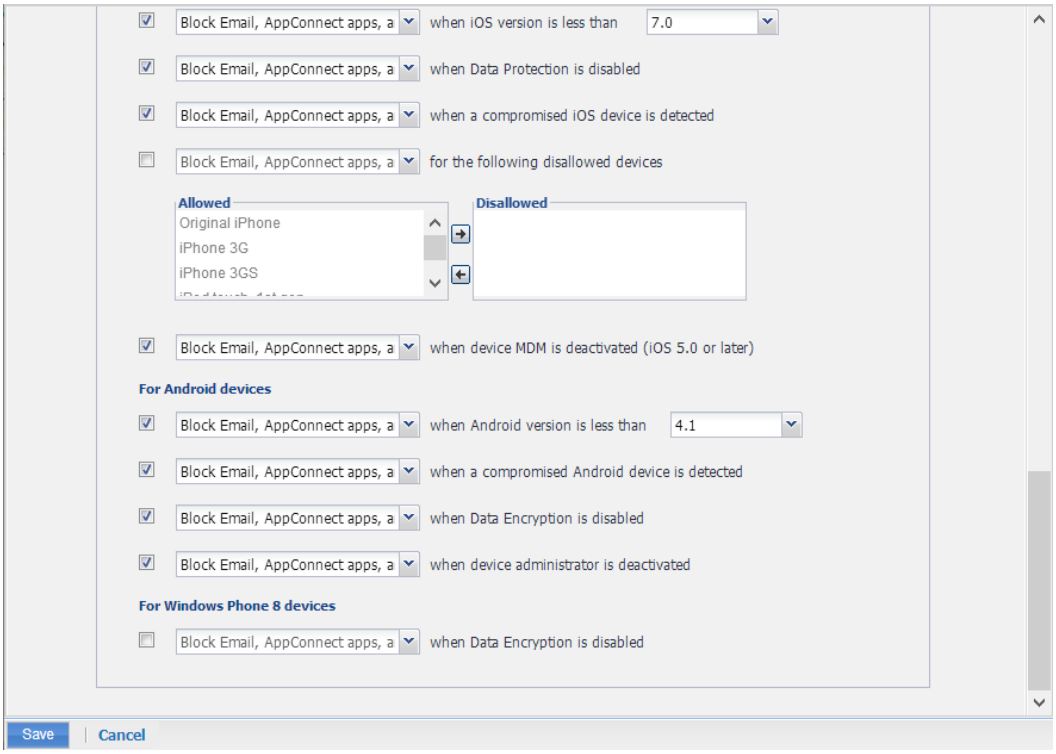
If LDAP, Email gateway and Connector are running the results will show a “Success” status.

ANNEX 11. PHASE 3 DETAIL OF POLICIES AND SETTINGS CONFIGURED

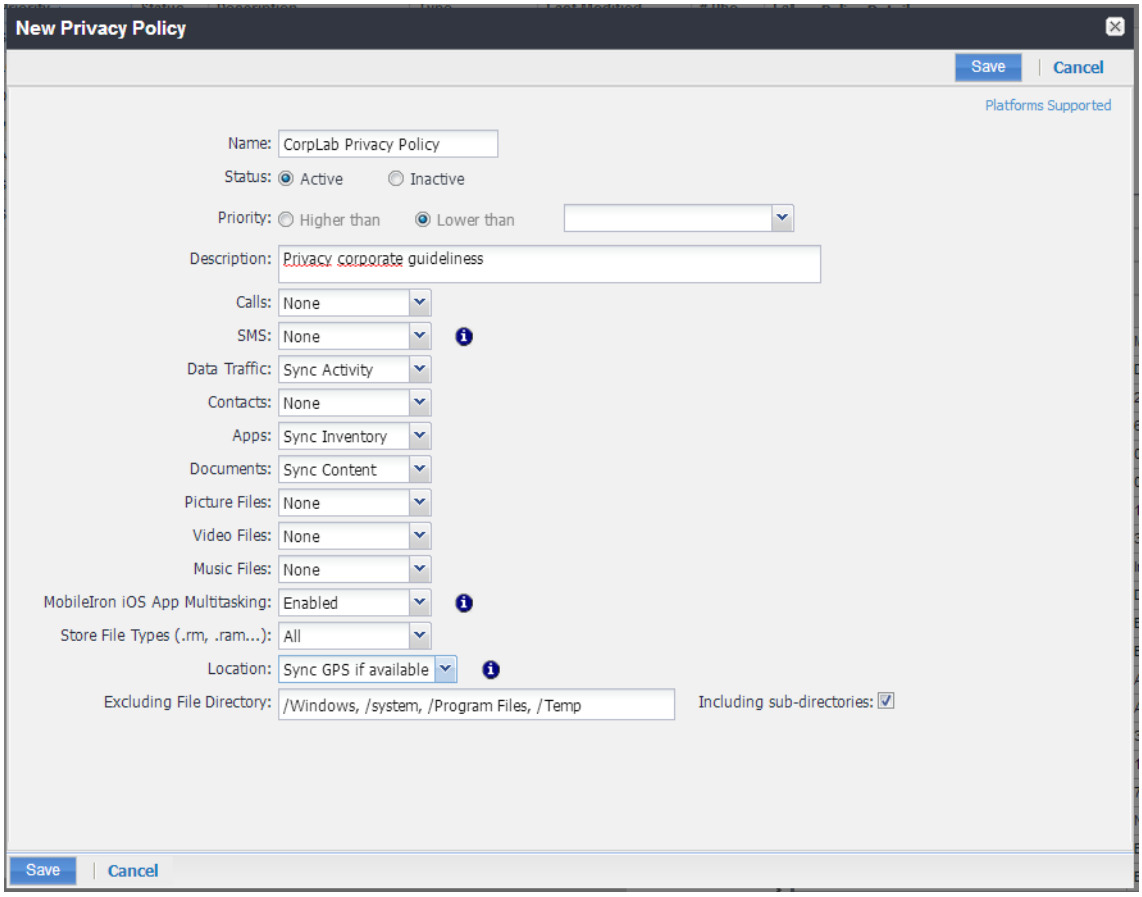
Annex 11.1. Policies details

Annex 11.1.1. Security Policy

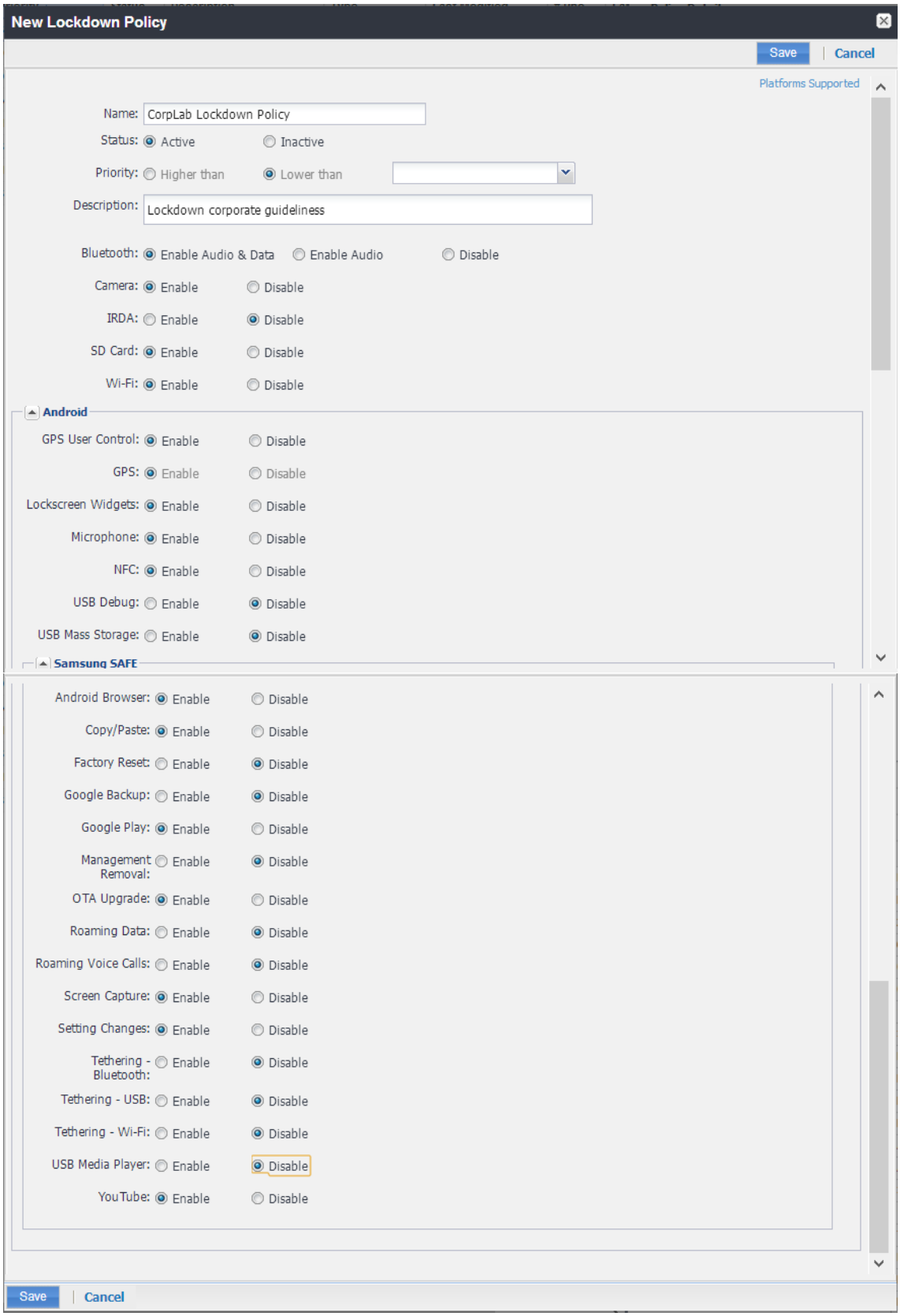




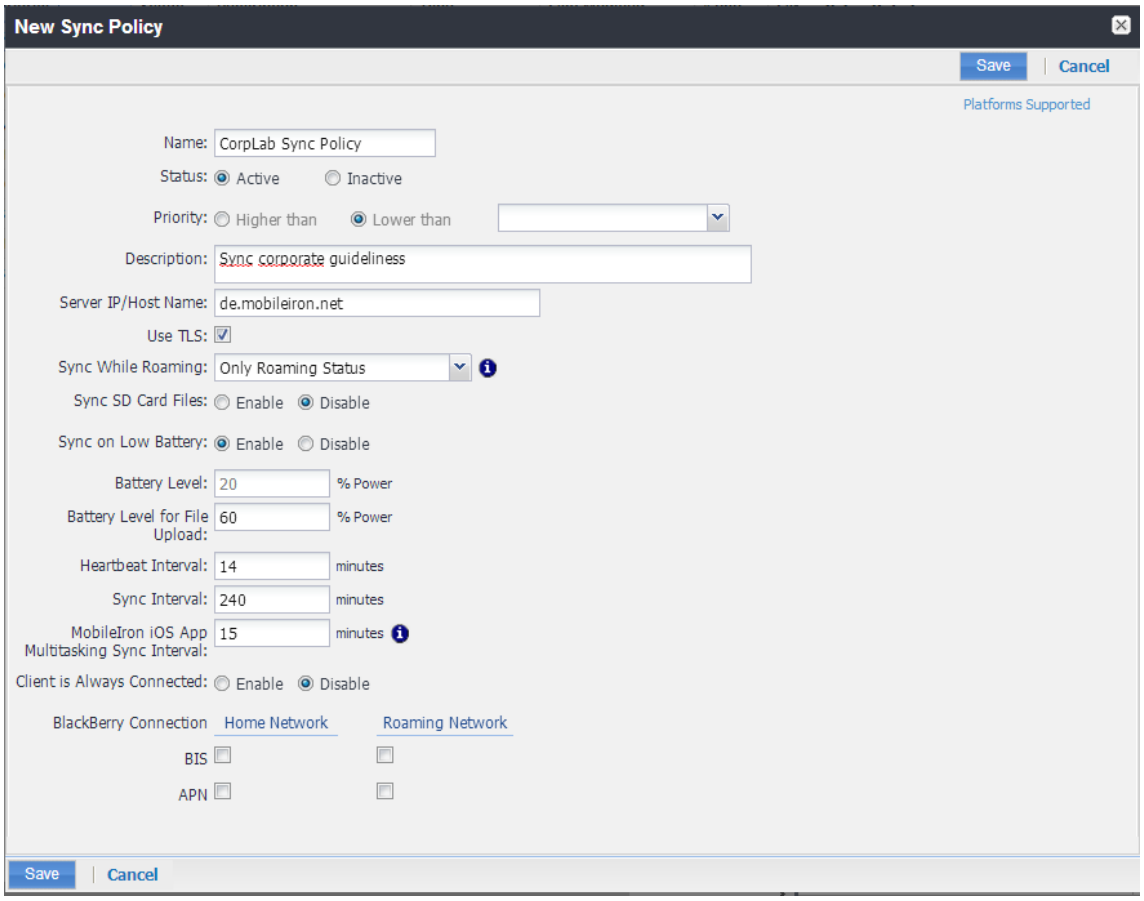
Annex 11.1.2. Privacy Policy



Annex 11.1.3. Lockdown Policy

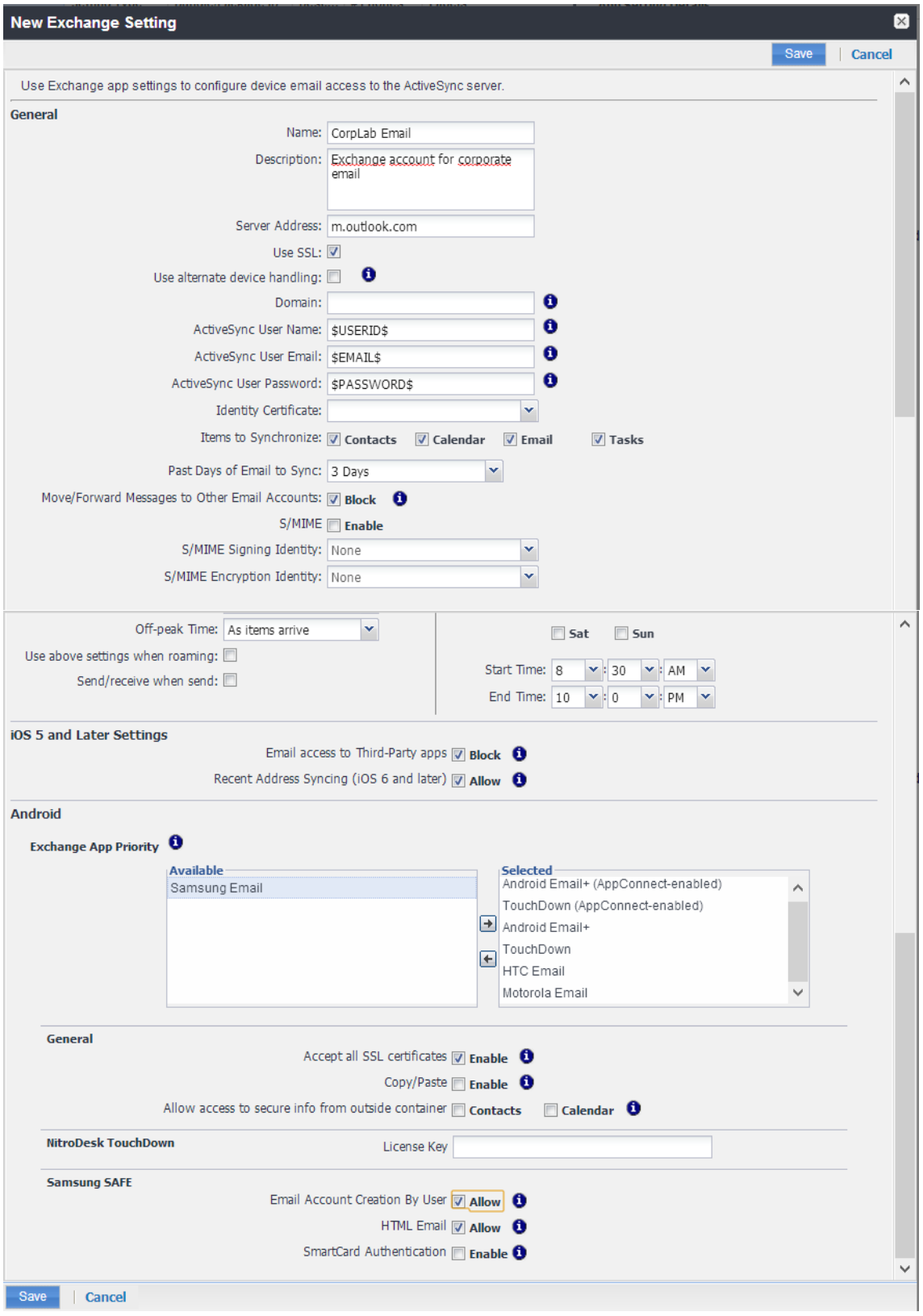


Annex 11.1.4. Sync Policy

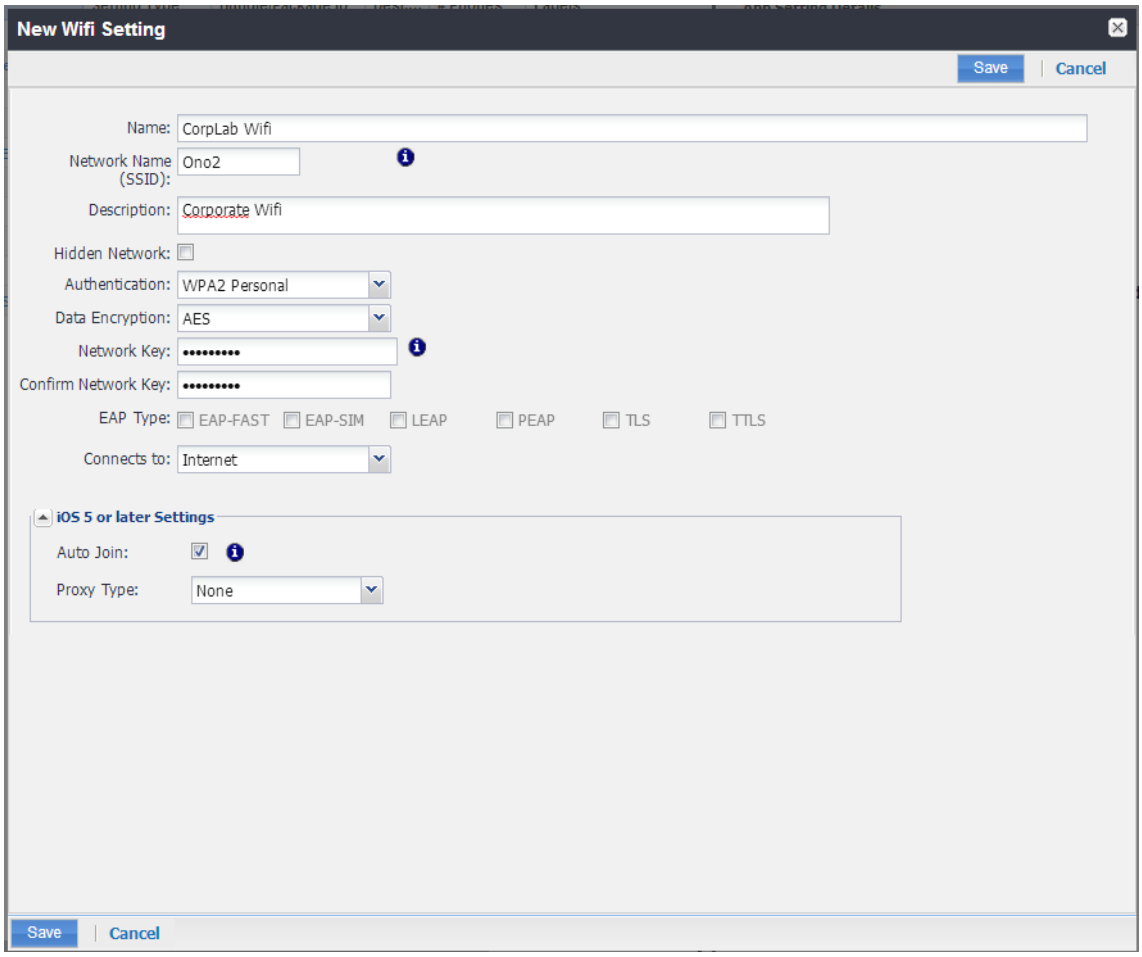


Annex 11.2. Settings details

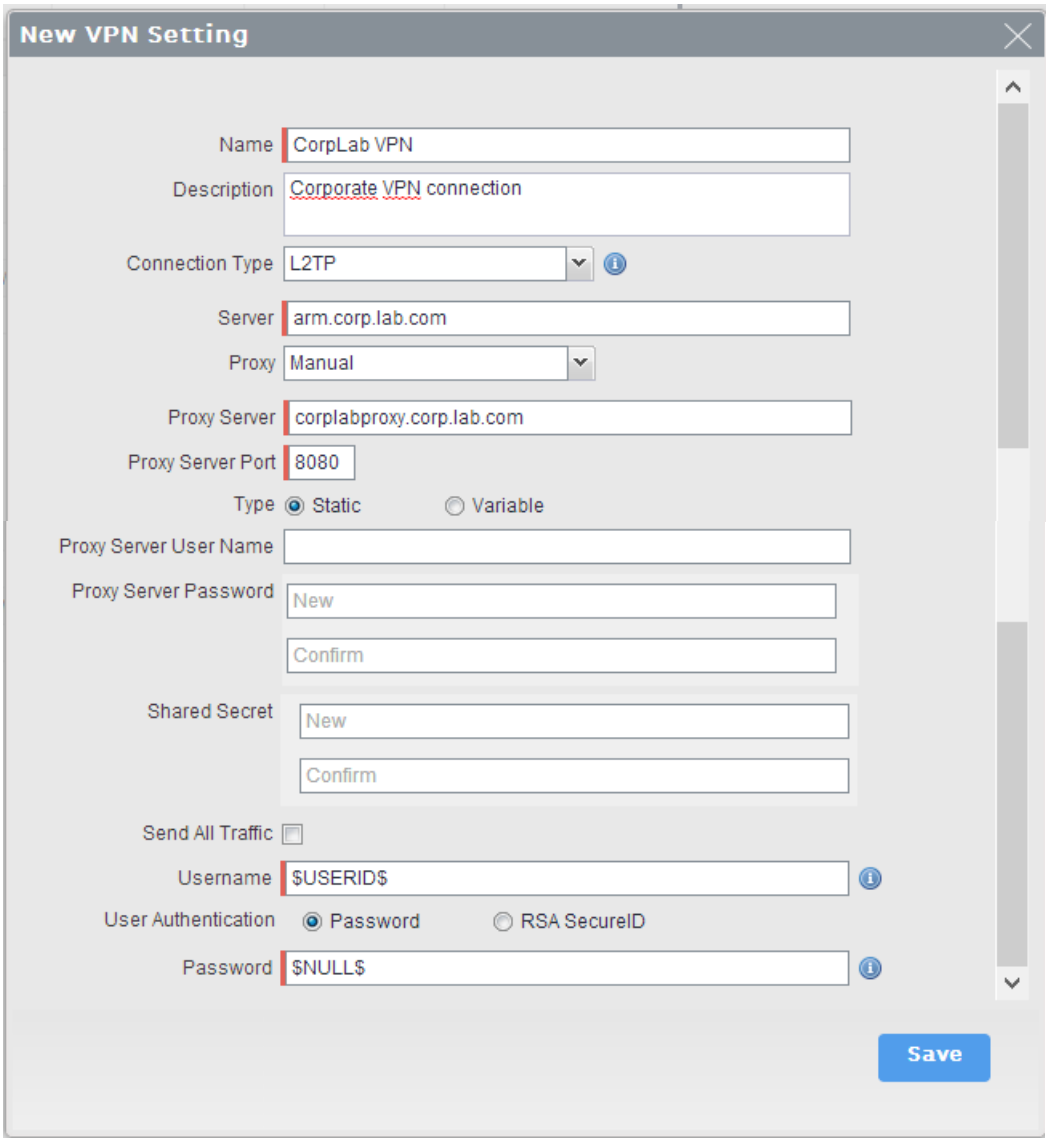
Annex 11.2.1. Exchange settings



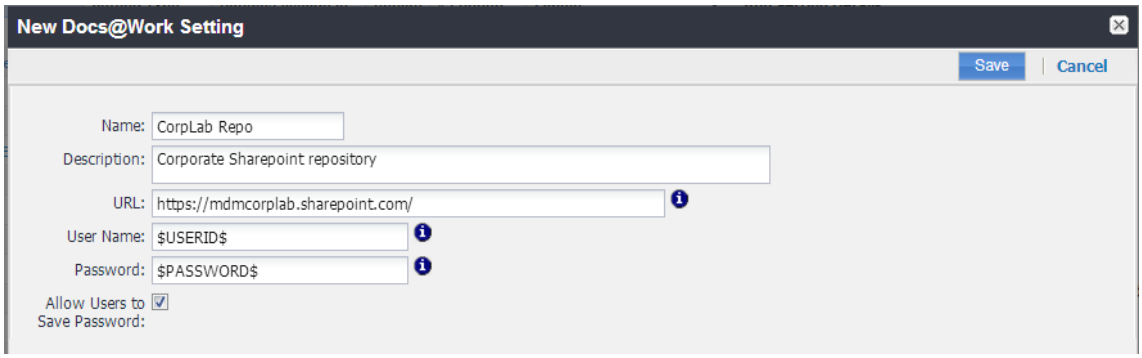
Annex 11.2.2. WiFi settings



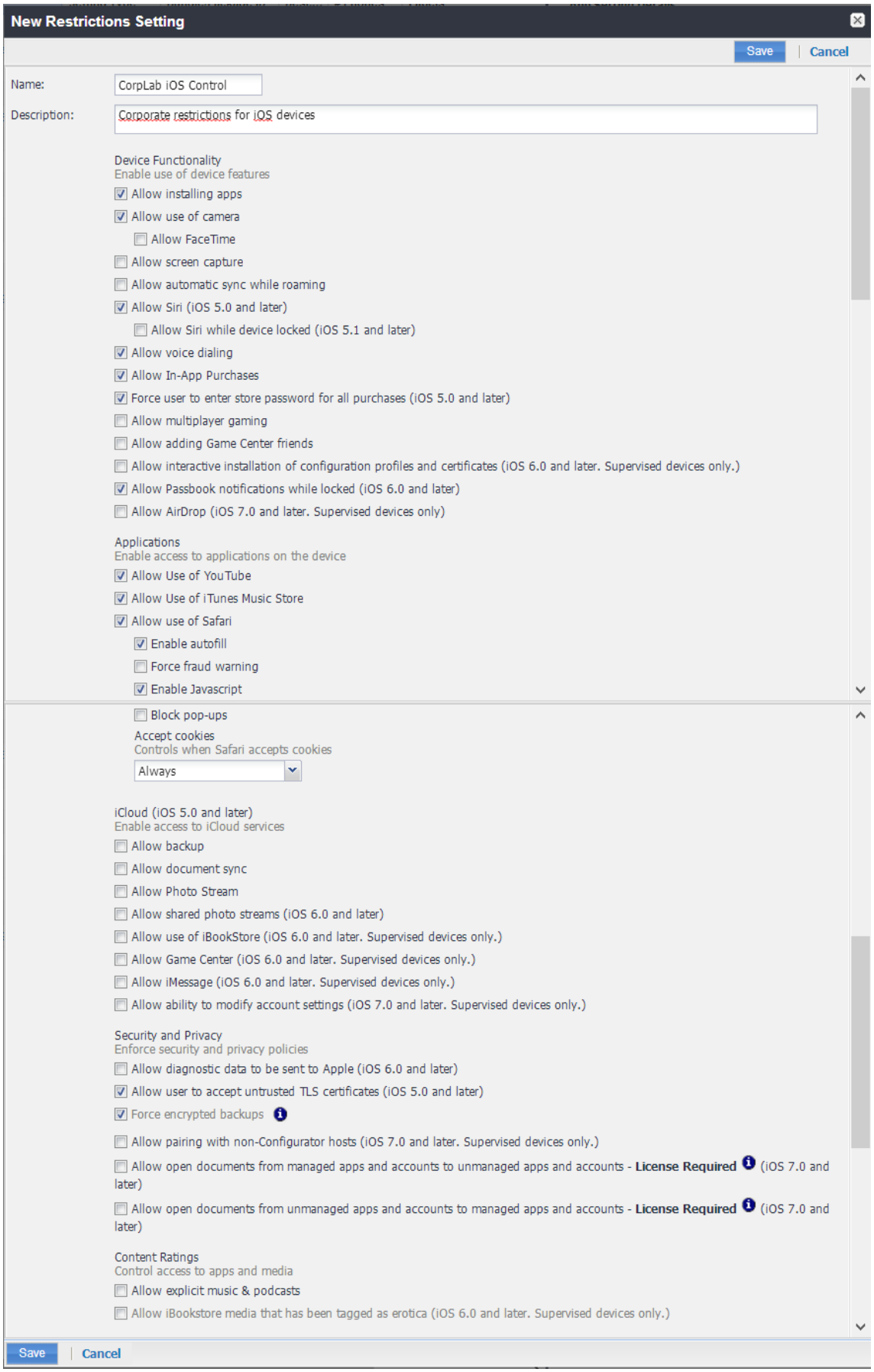
Annex 11.2.3. VPN settings



Annex 11.2.4. Documents container settings

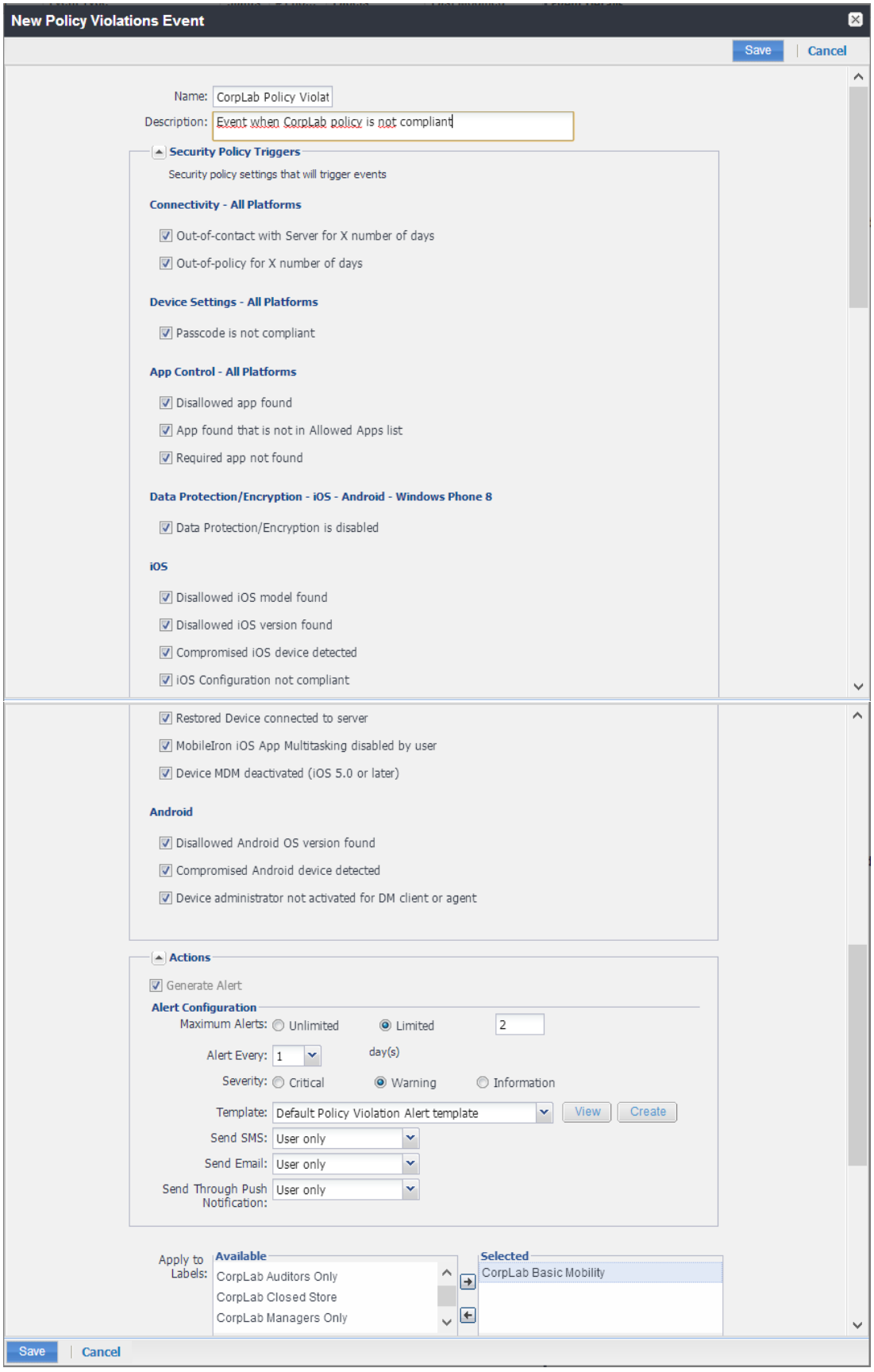


Annex 11.2.5. iOS restriction settings

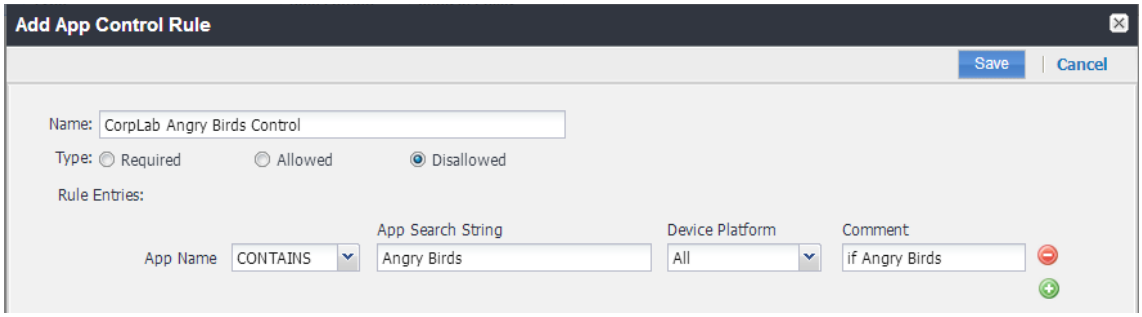


Annex 11.3. App Management control

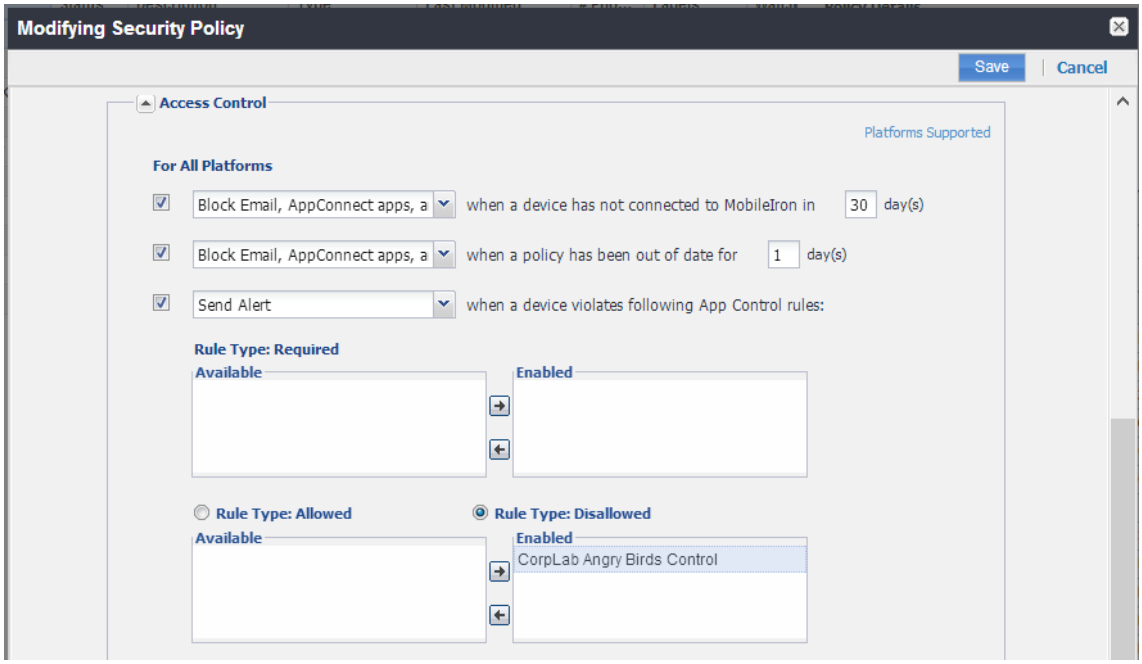
- **Step 1: Configure Alerts (not only for apps!)**



- **Step 2: Define Rules**

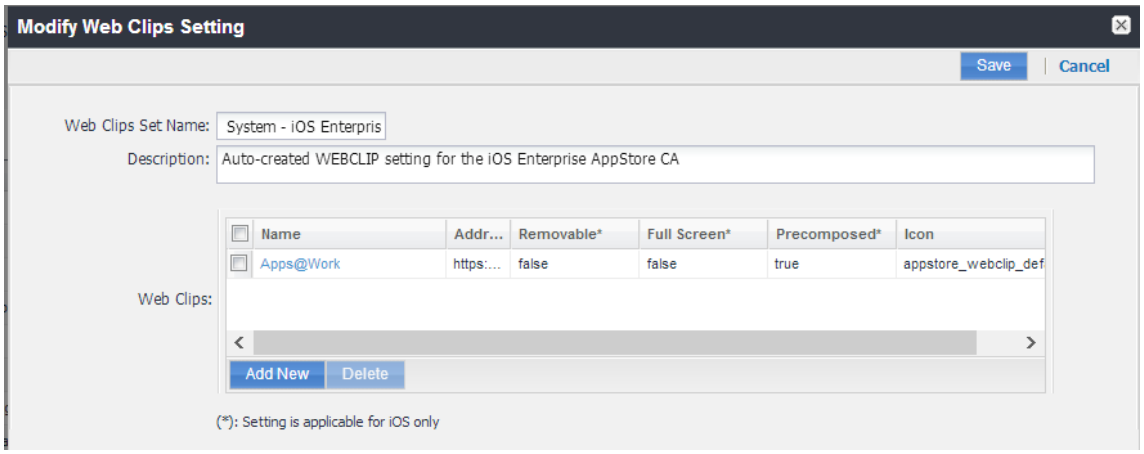


- **Step 3: Activate Rules**

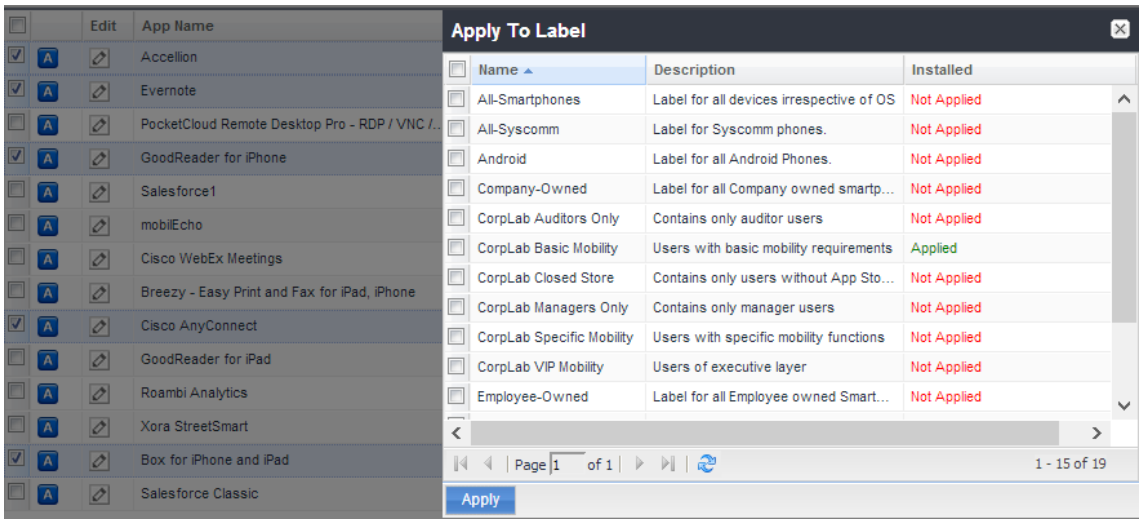


Annex 11.4. Enterprise App Storefront

- Enable WebClip for App Storefront



- Select apps for Store and apply to label


Edit
App Name
Accellion
Evernote
PocketCloud Remote Desktop Pro - RDP / VNC /...
GoodReader for iPhone
Salesforce1
mobilEcho
Cisco WebEx Meetings
Breezy - Easy Print and Fax for iPad, iPhone
Cisco AnyConnect
GoodReader for iPad
Roambi Analytics
Xora StreetSmart
Box for iPhone and iPad
Salesforce Classic
Apply To Label
Name
Description
Installed
All-Smartphones
Label for all devices irrespective of OS
Not Applied
All-Syscomm
Label for Syscomm phones.
Not Applied
Android
Label for all Android Phones.
Not Applied
Company-Owned
Label for all Company owned smartp...
Not Applied
CorpLab Auditors Only
Contains only auditor users
Not Applied
CorpLab Basic Mobility
Users with basic mobility requirements
Applied
CorpLab Closed Store
Contains only users without App Sto...
Not Applied
CorpLab Managers Only
Contains only manager users
Not Applied
CorpLab Specific Mobility
Users with specific mobility functions
Not Applied
CorpLab VIP Mobility
Users of executive layer
Not Applied
Employee-Owned
Label for all Employee owned Smart...
Not Applied
Page 1 of 1
1 - 15 of 19
Apply