

Ciclo
Administración de Sistemas Informáticos en Red

Proyecto
Software MDM (Mobile Device Management)

Alumno
Ernesto Álvarez Siles

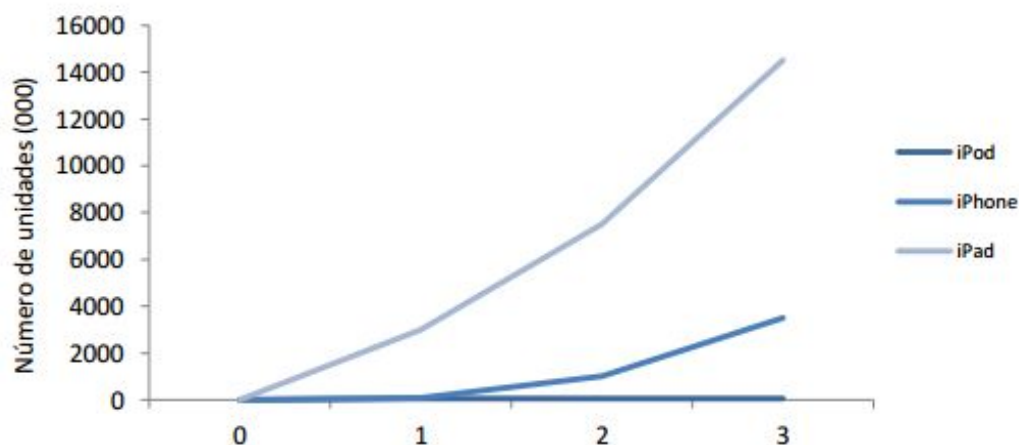
Índice

<u>Introducción y justificación</u>
<u>Objetivos</u>
<u>Análisis del contexto</u>
<u>Desarrollo del contenido</u>
<u>Implantación</u>
<u>Inicialización</u>
<u>Despliegue</u>
<u>Implementación</u>
<u>Operaciones y mantenimiento</u>
<u>Eliminación</u>
<u>Ejemplos de aplicaciones MDM</u>
<u>Instalación Spiceworks MDM (Maas360)</u>
<u>Instalación de la parte del Servidor</u>
<u>Instalación en dispositivos Android</u>
<u>Instalación en dispositivos iOS</u>
<u>Conclusión y valoración personal</u>
<u>Bibliografía y fuentes de consulta</u>

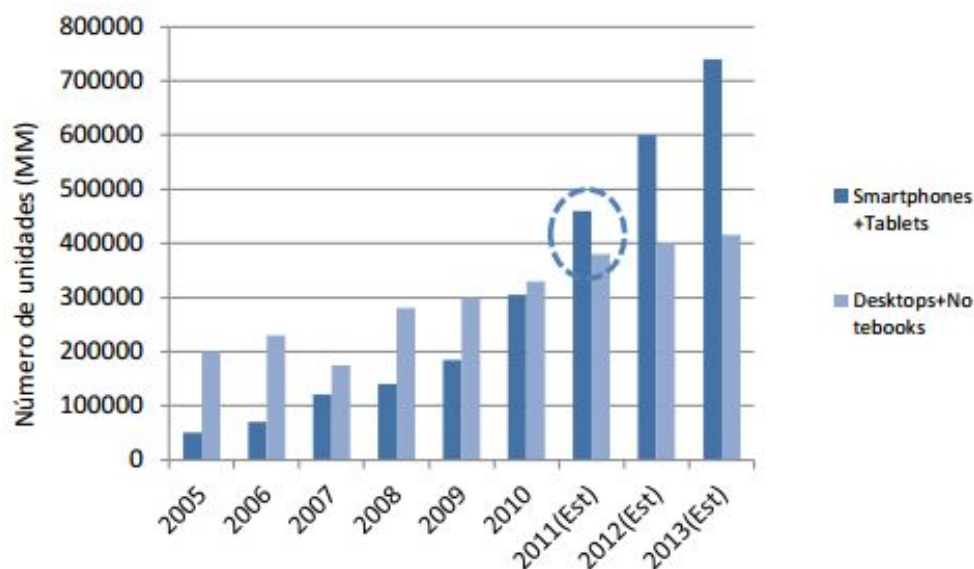
Introducción y justificación

La proliferación y el uso de forma común de dispositivos móviles (teléfonos inteligentes, tabletas...) por parte de la mayoría de la población y la diversidad de aplicaciones que hoy en día existen para dichos dispositivos, permiten darle un uso intensivo por parte de los usuarios en los más diversos escenarios, tanto de ocio como de trabajo o en los estudios.

Los usuarios quieren acceder a Internet independientemente de su localización y del dispositivo que estén usando. El siguiente gráfico muestra la tendencia y aceleración de esta mentalidad: iPad, en un trimestre, llegó al nivel de ventas que a iPhone le costó tres trimestres conseguir (Fuente: Apple).



En el año 2011 la venta de Pc's y notebooks se vió superada por la de smartphones y tablets. Teniendo en cuenta los tiempos de reposición, se estima que en este año el parque desplegado de dispositivos móviles sea superior al de Pc's. (Fuente: Informe KPBC - Top 10 mobile trends).



En el ámbito de la enseñanza han visto en estos dispositivos y sus aplicaciones unas enormes posibilidades educativas y una oportunidad de ayudar a aumentar la productividad de los alumnos. En centros educativos con un número significativo de alumnos que utilicen este tipo de aparatos diariamente, se hace engorrosa la tarea de actualizar dichos dispositivos con nuevas versiones o con nuevas aplicaciones si se hace de uno en uno. Por lo tanto, es imprescindible la ayuda de este tipo de aplicaciones que permiten la actualización e instalación masiva de aplicaciones a distancia y en todos los dispositivos a la vez o a elección del administrador, la monitorización de la actividad de los alumnos en cuanto a su uso, la localización en caso necesario, la seguridad, sincronización de archivos, borrado remoto, etc. , la gestión de las aulas por parte de los profesores y el uso de los dispositivos por parte de los alumnos según los parámetros definidos por el profesor.

Objetivos

El objetivo de este proyecto es analizar las prestaciones de dichas aplicaciones, denominadas MDM (Mobile Device Management), realizar una comparativa teniendo en cuenta varios parámetros y que dicho estudio nos ayude a decidir cuál de ellas nos convendría más usar en nuestro ámbito concreto y según nuestras necesidades. En el caso que nos ocupa, la enseñanza, para cubrir dichas necesidades el software debe permitir o debe cumplir las siguientes especificaciones o prestaciones:

- Administración centralizada de grupos de usuarios (administradores, profesores y alumnos) que se puedan utilizar para asignar políticas de seguridad, reglas de conformidad, ubicaciones, configuración de privacidad y distribuir aplicaciones y documentos.
- Administración centralizada de grupos de dispositivos (aulas, cursos, etc..)
- Distribución de aplicaciones por parte del administrador o los profesores.
- Políticas de seguridad independientes por grupo de dispositivos (), reglas de conformidad (reglas que los dispositivos tienen que cumplir en todo momento), registro de conformidad (registro que indica si efectivamente cumplen las reglas).
- Informes de estado de los dispositivos

Análisis del contexto

En el mercado actual existen una gran cantidad de estas aplicaciones de los tipos más diversos (gratuitas, de pago, con períodos de prueba) y con diferentes prestaciones (geolocalización, selección, instalación y actualización de aplicaciones, sincronización de archivos, etc.). Algunas empresas incluso han aprovechado esta diversificación para sacar sus propias líneas de producto que han denominado EMM (Enterprise Mobile Management). Este tipo de aplicaciones son horizontales, por lo que pretenden abarcar el mayor número de “targets” (objetivos) o clientes potenciales posibles. Esto quiere decir que hay que buscar siempre un compromiso,

válido para el cliente, entre posibilidades del software y la forma de hacer las cosas por parte del cliente.

En nuestro caso, relacionado con la educación en los institutos de enseñanza secundaria, nos basamos en un contexto “tipo” generalizado, dando por hecho que se ha discutido con el TIC y el personal docente del centro cuáles son las necesidades concretas y qué se espera obtener de la implantación de un sistema de estas características, llegando a las siguientes conclusiones:

- Debe existir un dispositivo por cada alumno, el cual se hace responsable del cuidado del mismo, así como de su carga para garantizar la disponibilidad.
- En cada dispositivo se deberá configurar una cuenta de correo electrónico. En el caso de alumnos de edad inferior a 14 años, se deberá contar con el consentimiento del padre, madre o tutor según el artículo 13 de la LOPD.
- Los usuarios pertenecientes al grupo de administradores del servidor se deberán encargar del registro de los dispositivos en el servidor, altas de usuarios, definición de grupos de usuarios, grupos de dispositivos y distribución de aplicaciones, para lo cual es recomendable una reunión anterior al inicio del curso escolar.
- Los usuarios pertenecientes al grupo de profesores sólo se deberán encargar de verificar el cumplimiento de las políticas de seguridad de los dispositivos (el software cliente se encarga de indicar el grado de cumplimiento de cada dispositivo), distribuir documentos entre dispositivos o bien comunicar a los administradores cualquier cambio posterior en aplicaciones a instalar o eliminar y cambios en las políticas de seguridad.
- Los usuarios pertenecientes al grupo de alumnos son los responsables del mantenimiento de los dispositivos, así como de aplicar los cambios en las políticas de seguridad (sólo hay que seguir los pasos indicados por el cliente de la aplicación), actualizar los contenidos e instalar las aplicaciones. Todo esto lo indica el software cliente y tiene asistentes para realizar estas tareas fácilmente. También hay que tener en cuenta que hoy en día los alumnos,

aunque sean de 13 años, están muy familiarizados con el uso de estos dispositivos.

Todo esto hace que la enseñanza sea más productiva, dinámica, participativa y adaptada a las necesidades de cada clase.

Desarrollo del contenido

La arquitectura de este tipo de software normalmente consiste en un agente, que se instala en cada uno de los dispositivos, un servidor desde el que se realizan las instalaciones, actualizaciones, etc. y una base de datos que almacena toda la información recabada de los dispositivos móviles.

Implantación

Para enfrentarse a la implantación hay que tomarlo como un proyecto con cinco fases:

- Inicialización

Esta fase incluye las tareas que un centro debe realizar antes de diseñar una solución para dispositivos móviles: Identificar las necesidades de dispositivos móviles (cuantos se necesitan) y proporcionar una visión general de cómo debe adaptarse una solución de software a las necesidades del centro, dando forma a las políticas de seguridad y requerimientos funcionales.

- Despliegue

Aquí se especifican las características técnicas del software y sus componentes, incluyendo los métodos de autenticación y cifrado para la protección de las comunicaciones y datos almacenados. También hay que evaluar los distintos tipos de dispositivos y sistemas operativos que van a ser usados y que se verán afectados por las políticas de seguridad definidas. En esta fase se deben elegir los elementos que se usarán en la implementación, tanto hardware como software.

- Implementación

En esta fase se configuran los equipos para que cumplan los requerimientos funcionales y de seguridad, incluidas las políticas de seguridad, instalando y

comprobando el funcionamiento de un dispositivo piloto, incluyendo las restricciones en la navegación definidas por el proxy del centro educativo.

- **Operaciones y mantenimiento**

Esta fase abarca la vigilancia por parte del profesorado del cumplimiento de las políticas de seguridad por parte de los alumnos (instalación y configuración de los dispositivos por parte de los alumnos según las indicaciones del software cliente MDM del dispositivo mediante mensajes push) y funcionamiento e idoneidad de las aplicaciones elegidas para su uso.

- **Eliminación**

Esta fase tiene lugar cuando los dispositivos han finalizado su vida útil y hay que definir las acciones a tomar para el cumplimiento de la legalidad vigente en cuanto a materia medioambiental a la hora de proceder a su destrucción o reciclado.

Ejemplos de aplicaciones MDM

Existen muchas opciones en el mercado. A continuación se nombran las más utilizadas con algunas de sus características más importantes:

- **AirWatch MDM**

Multiplataforma (iOS, Android, Windows Phone).

Licencia de pago. Prueba gratuita 30 días.

Consola de administración única.

Administración de aplicaciones móviles.

Administración de contenido móvil.

Administración de correo electrónico móvil.

Administración de navegación.

- **Manage Engine MDM**

Multiplataforma (iOS, Android, Windows Phone).

Licencia gratuita hasta 1 técnico y 25 dispositivos.

Registro manual o autoregistro con dos niveles de autenticación.

Administrador de aplicaciones.

Administrador de perfiles.

Administrador de seguridad.
Administrador de correo electrónico.
Administrador de inventario.
Auditorías e informes.
Soporta autenticación Active Directory.

– **MobileEther MDM**

Protección de dispositivos móviles y seguridad web en una única solución.
Control de redes sociales.
Administrador de aplicaciones.
Monitorización y seguridad de datos en la nube.
Integración con Active Directory.
Soporta Apple DEP (Device Enrollment Program).
Cumplimiento preciso de políticas de seguridad.

– **SysAid MDM**

Inscripción de dispositivos Android e iOS de forma inalámbrica (OTA), tanto del centro como de los alumnos (BYOD).
Crear, asignar y modificar políticas personalizadas para los dispositivos.
Empleo de configuración WiFi y de correo electrónico creados previamente.
Aplicación de código de acceso que permite resetear, bloquear y borrar los dispositivos.
Trazabilidad de las aplicaciones instaladas con aplicación de monitorización
Protección de datos críticos.

– **Spiceworks MDM (Maas360)**

Este software permite:

- Tener un inventario de todos los dispositivos móviles en un sólo lugar.
Soporta iOS, Android y Windows Phone. Registrando un dispositivo móvil obtiene toda la información del aparato, como tipo de dispositivo, sistema operativo utilizado, etc.
- Monitorear los dispositivos obteniendo información actualizada en tiempo real, pudiendo saber las aplicaciones que se instalan, etc., incluso creando

alertas para dispositivos desactualizados, códigos de acceso deshabilitados, etc.

- Crear informes y estadísticas personalizadas de uso, averías, etc.

La versión de pago (Premium) permite, además de las características anteriores:

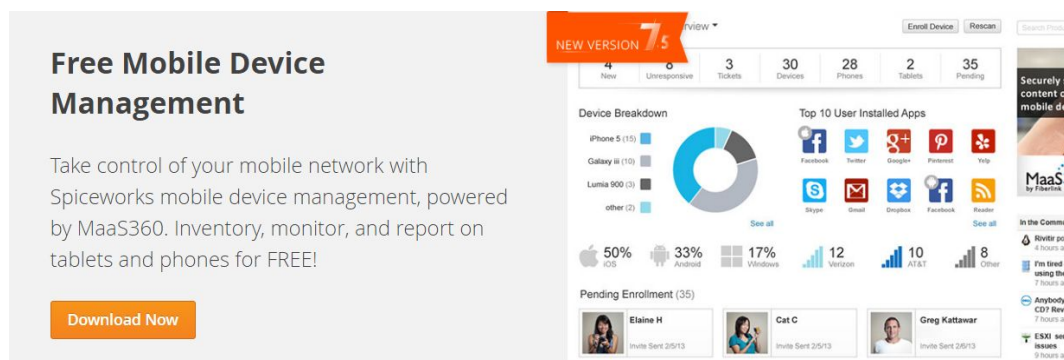
- Bloquea y borra dispositivos perdidos o robados. Además puede usar la característica del portal MaaS360 que permite cambiar los códigos de acceso, gestionar la configuración del dispositivo e incluso establecer un contenedor de correo seguro para proteger los datos de la compañía.
- Autenticar usuarios en Active Directory con códigos de acceso de un sólo uso, configurar políticas de cumplimiento para administrar el comportamiento del usuario, controlar fácilmente cuentas de correo electrónico, acceso WiFi y VPN.
- Acceso a aplicaciones corporativas o aplicaciones aprobadas por el administrador, con la posibilidad de distribuir y administrar fácilmente dichas aplicaciones en todos los dispositivos, incluso creando listas blancas / negras de aplicaciones según sea necesario para satisfacer la política móvil de la empresa.

Como ejemplo de uso vamos a instalar la versión gratuita del software Spiceworks MDM, basado en MaaS360 (desarrollado por Fiberlink, una compañía de IBM), ya que, además de gratuita, parece ser lo suficientemente completa como para satisfacer nuestras necesidades.

Instalación Spiceworks MDM (Maas360)

Instalación de la parte del Servidor

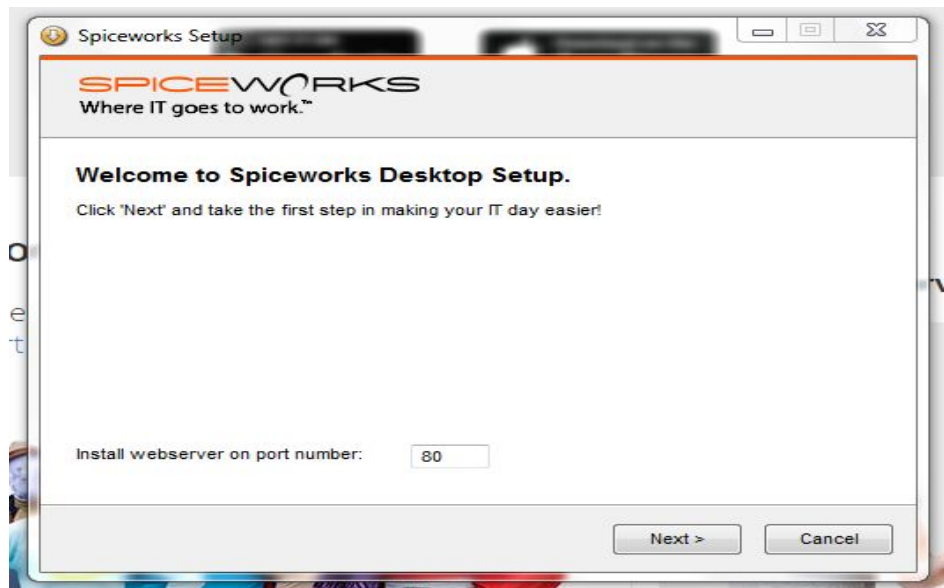
La descarga de la parte correspondiente al servidor de la aplicación se puede realizar desde el siguiente enlace: <http://www.spiceworks.com/download/app/>



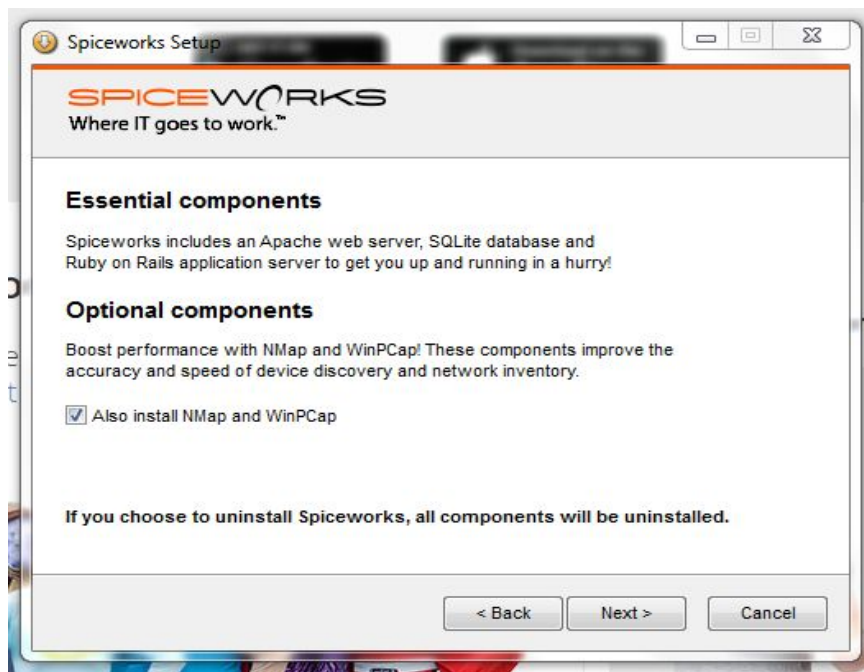
Antes de iniciar la descarga debemos crear una cuenta de administrador, que no es otra cosa que crear una cuenta en Spiceworks para poder descargar el software.

The image shows a screenshot of the 'Create your admin account' form. The form has an orange header with the text 'Create your admin account. We'll set you up with app access and notifications.' Below this, there are two input fields: 'Email (This will be your username)' and 'Password (Create a strong password)'. A 'Start App Download' button is located below the password field. At the bottom, there's a link that says 'Already have a Spiceworks account? Log In'.

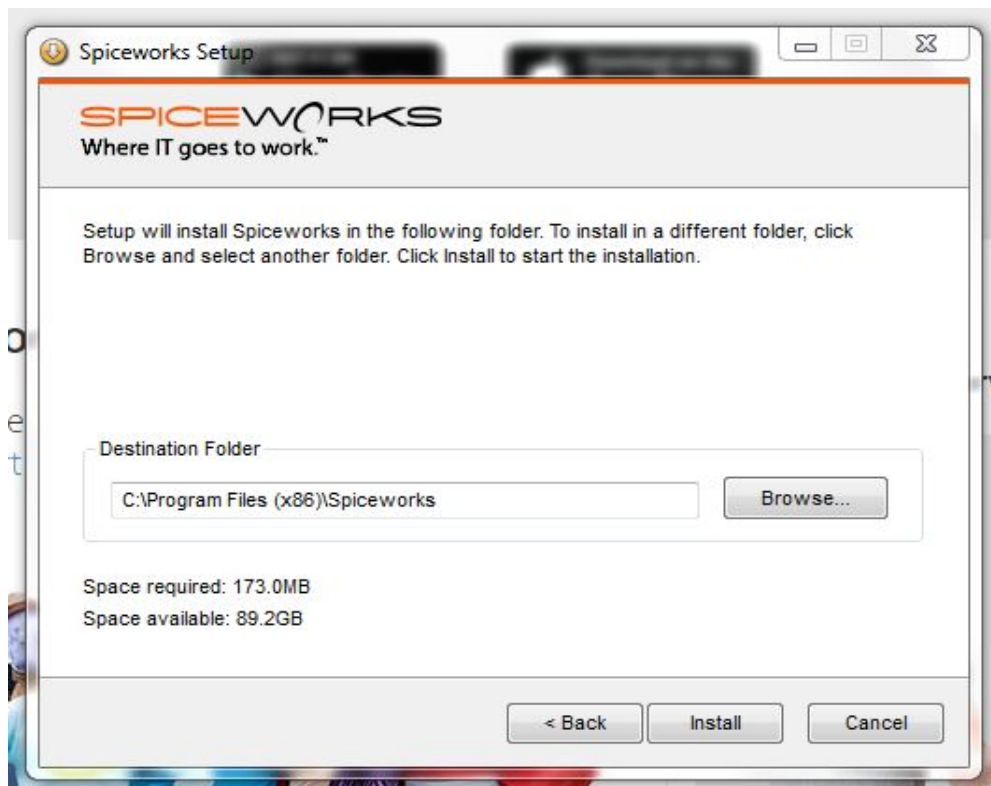
Después de crear la cuenta y descargar el paquete de software, comenzamos con la instalación que es muy simple y se realiza en pocos pasos.



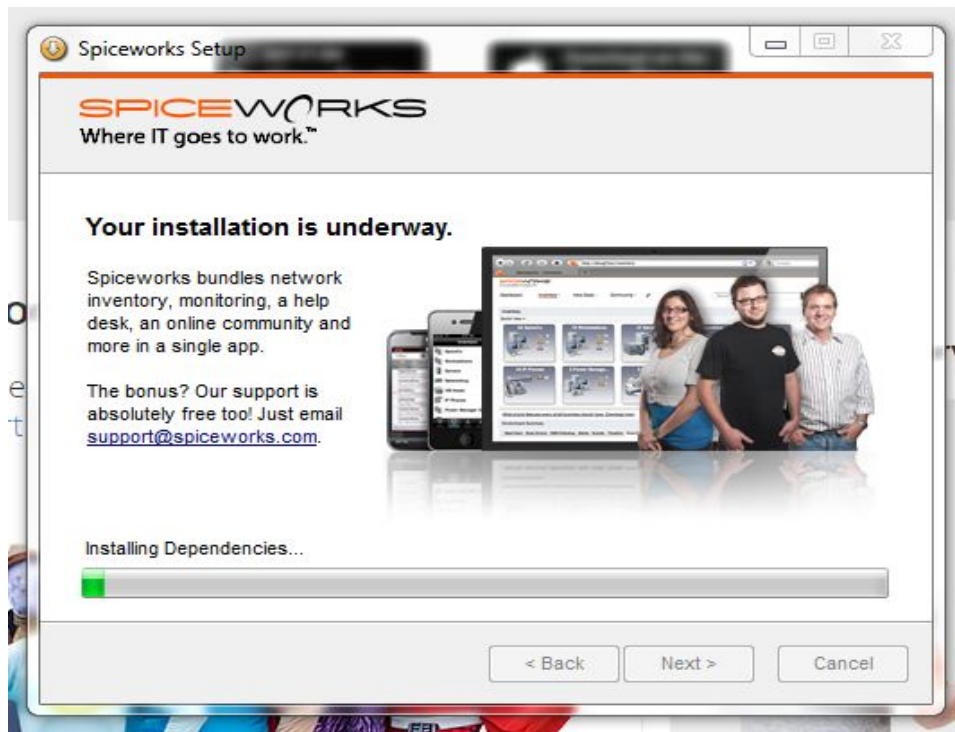
En la siguiente pantalla nos da a elegir los componentes que queremos instalar.



En el siguiente paso elegimos en qué carpeta queremos instalar el programa.



Y eso es todo. En la siguiente pantalla podemos ver el progreso de la instalación.



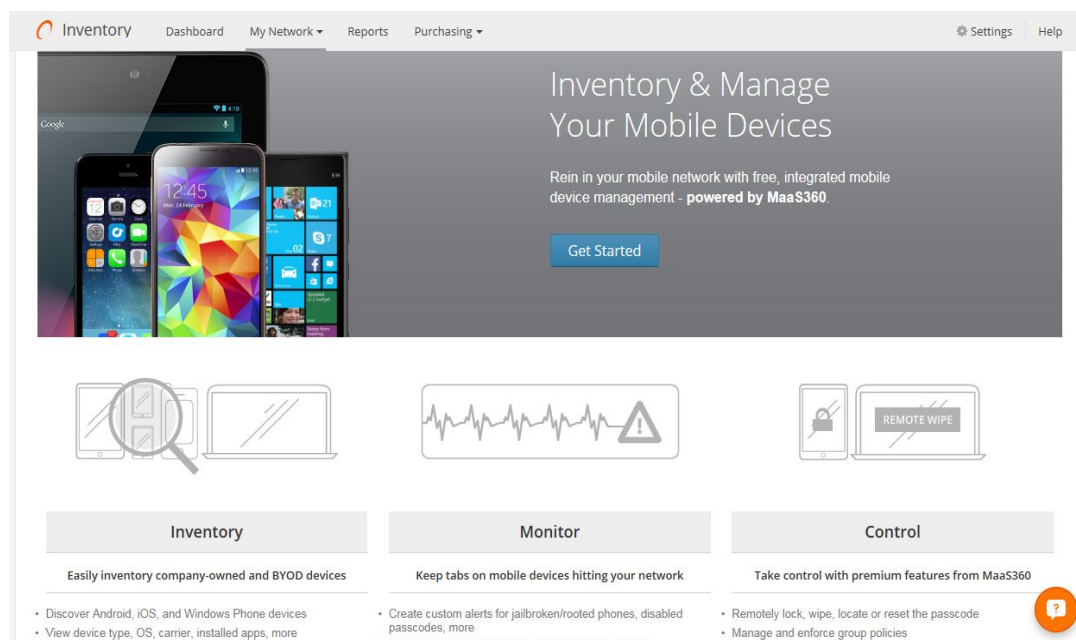
Una vez finalizada la instalación, en la siguiente pantalla nos solicitan nuestros datos para personalizar dicha instalación.

A screenshot of the "Personalize this install of Spiceworks." form. The title bar says "Personalize this install of Spiceworks." and the subtitle says "Tell us a bit about yourself." The form has the Spiceworks logo at the top. It contains four input fields: "What's your name?" with two text boxes containing "Ernesto" and "Alvarez"; "Where do you work?" with a text box containing "Melilla"; "Where should we send monitoring and alert emails?" with a text box containing "eas1701@gmail.com"; and "In what industry is your company?" with a dropdown menu showing "IT Service Provider". At the bottom of the form is a "Save" button.

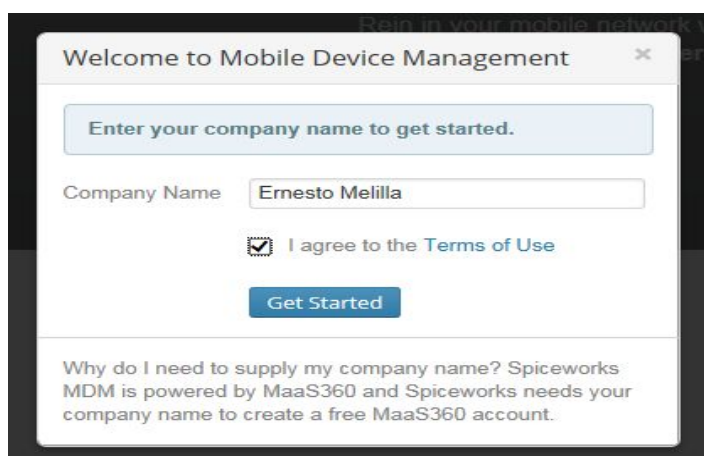
Con esto ya hemos terminado. Nos crea un icono de acceso directo en el escritorio, y al hacer doble click sobre él, se nos abre el navegador que tengamos

configurado por defecto (el programa se ejecuta en entorno web) y carga la página inicial de bienvenida donde podemos ver las opciones que tenemos en la aplicación.

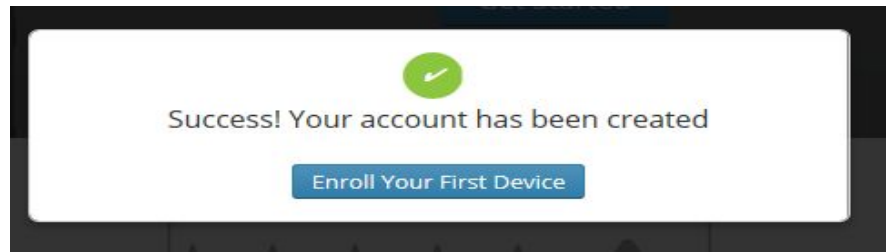
El siguiente paso sería configurar el MDM (Set Up MDM). En la siguiente pantalla debemos hacer click para continuar en el botón Get Started para inventariar y administrar los dispositivos móviles.



A continuación nos solicita el nombre de la empresa para la creación de un cuenta gratuita en MaaS360.



Tras esto debería salir una ventana como la siguiente, indicando que la cuenta ha sido creada satisfactoriamente e invitándonos a registrar nuestro primer dispositivo.



En la pantalla de registro de nuestro primer dispositivo nos pregunta quién es el propietario. Después de esta primera alta en la base de datos, se podrán registrar múltiples dispositivos a la vez.

A screenshot of a device enrollment screen. At the top, there is a light blue banner with the text: "Let's start by enrolling your first mobile device. Choose who this device belongs to. After the initial set-up, you'll be able to enroll multiple devices at once." Below the banner, there are three main sections separated by vertical lines. The first section is titled "Yourself" and shows a user card for "Ernesto Alvarez" with email "eas1701@gmail..." and role "IT". Below the card is a blue "Choose" button. The second section is titled "An Existing User" and has a dropdown menu labeled "Select a user". Below it is a user card for "Spice Rex" with email "spicerex@spice..." and role "IT". Below the card is a blue "Choose" button. The third section is titled "Create a New User" and contains three input fields: "First Name", "Last Name", and "Email". Below these fields is a blue "Choose" button. The screen also has a search icon, a list icon, and a close icon at the top.

Elegimos la opción de la izquierda que somos nosotros mismos y a continuación se nos abre otra ventana para que elijamos el tipo de dispositivo según su sistema operativo.

What type of device are you trying to enroll?

☐ Android Tablet or Phone
 ☐ Apple iOS Tablet or Phone*
 ☐ Windows Phone

Or Or

*Requires additional setup

Previous Next

Para simplificar el primer registro, elegimos que es un teléfono o tableta android, ya que registrar un dispositivo iOS requiere de pasos adicionales que veremos más adelante cuando registremos uno de estos dispositivos. Pulsamos en “Next” para continuar.

En la siguiente ventana nos sale otro botón para que enviemos un correo al propietario del dispositivo para que proceda a su registro. El propietario recibirá un correo de Maas360 indicando los pasos para el registro del dispositivo. La persona en cuestión debe completar el proceso de registro e instalar la aplicación en su teléfono o tableta usando el enlace facilitado en el correo. Una vez registrado, el dispositivo estaría visible en el servidor en aproximadamente 15 minutos.

Congratulations! Now you are ready to send your first enrollment request email

*Before sending we recommend you backup your device

Ernesto Alvarez
 eas1701@gmail...
 Admin IT

Send Request

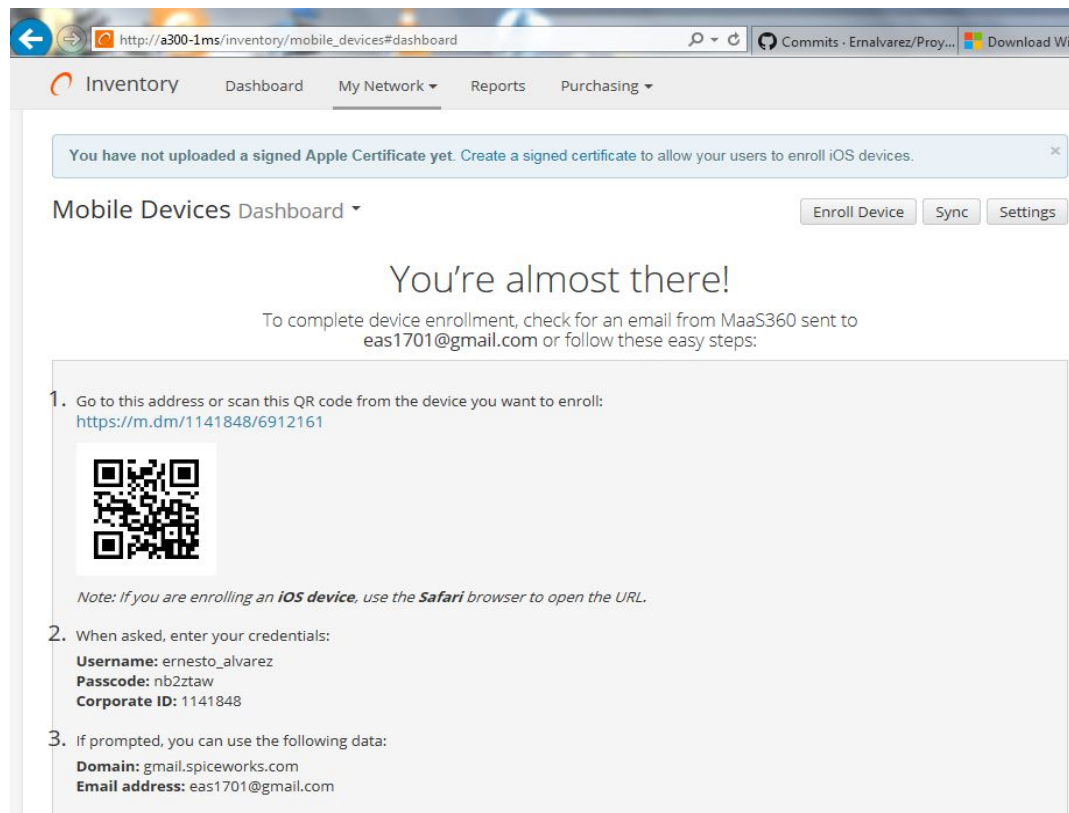
Here's what happens next...

The person you are enrolling will receive an email from Maas360 that provides the steps to enroll.

The person must complete the enrollment process and install the app to their phone using the links in the email.

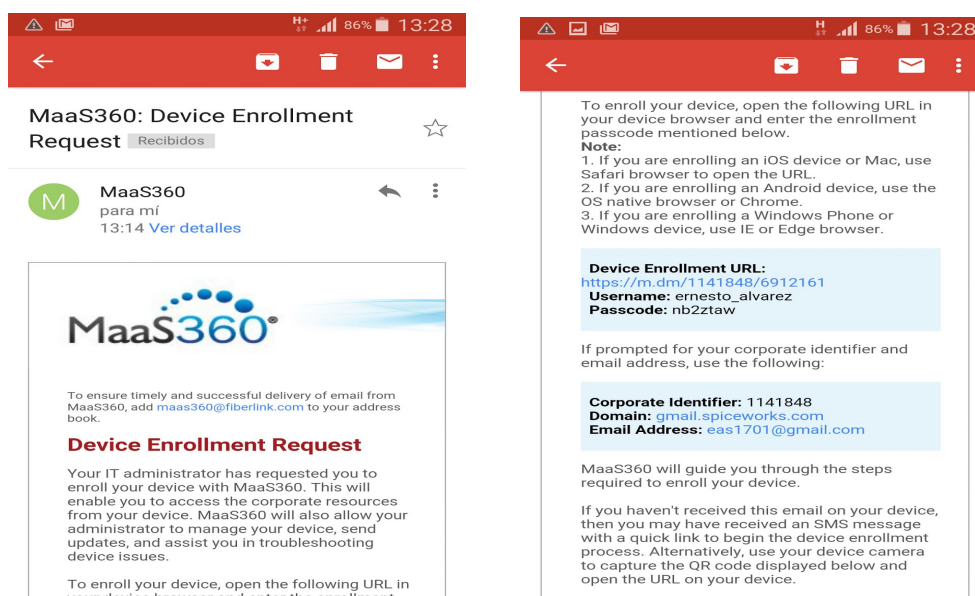
Once enrolled, you should be able to view this device in your Mobile Overview in about 15 minutes.

La siguiente ventana nos indica que los pasos a seguir para el registro están en el correo enviado, o que se pueden seguir los indicados allí.

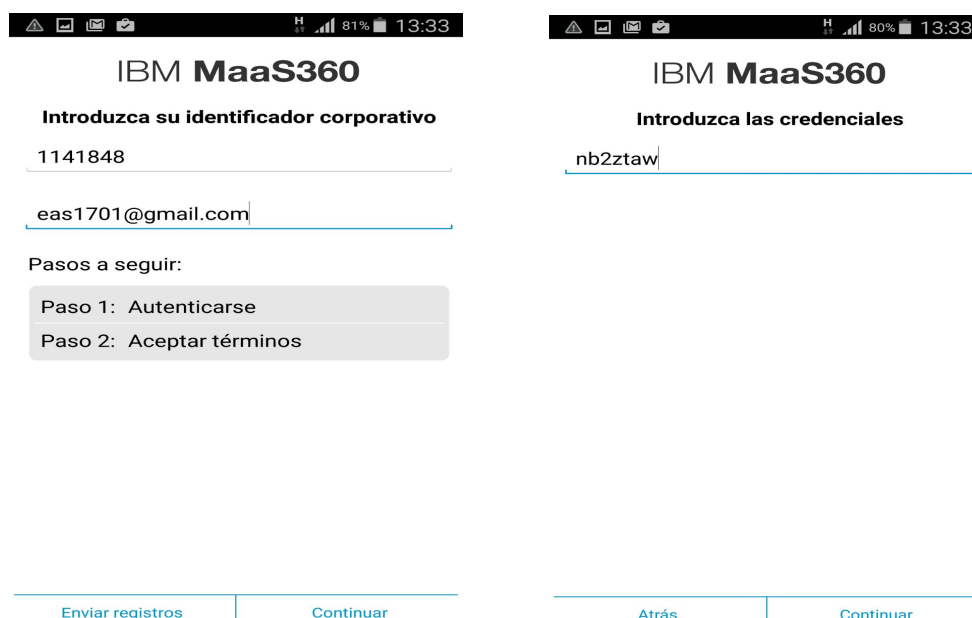


Instalación en dispositivos Android

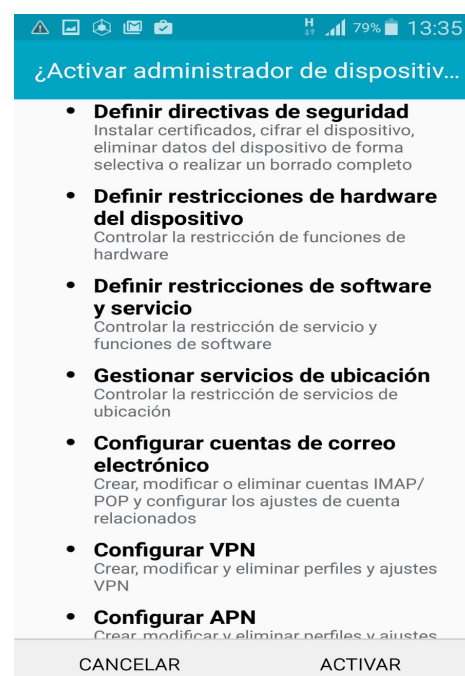
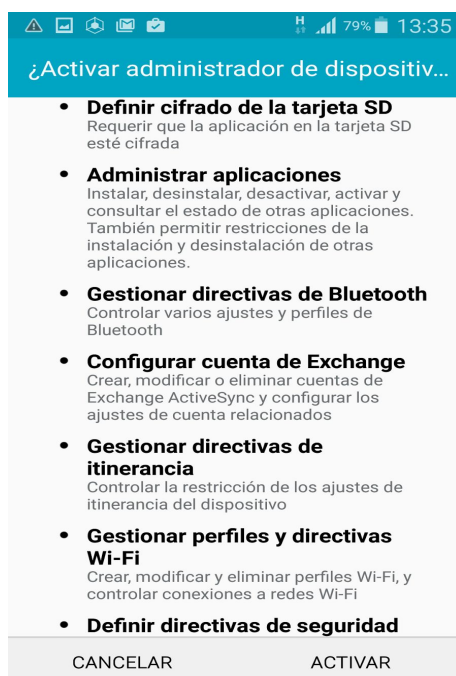
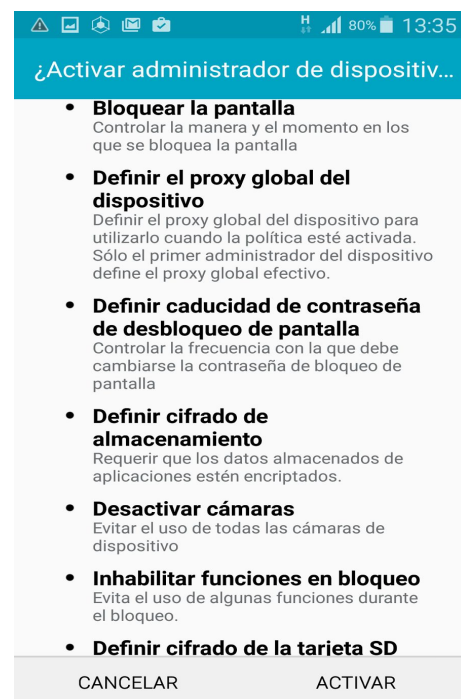
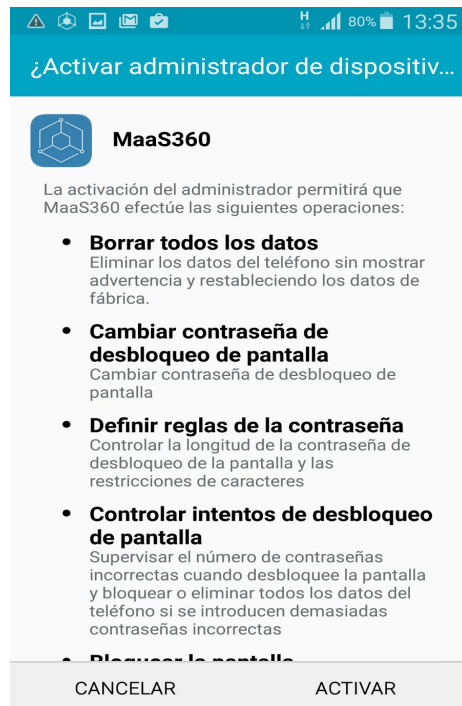
El siguiente paso sería instalar la aplicación cliente en el dispositivo móvil siguiendo las instrucciones del correo electrónico recibido.



Pulsando el link a la URL, nos envía a una página con en enlace a la descarga de la aplicación en Google Play. Una vez instalada nos crea un icono de acceso directo que debemos pulsar para acceder a la aplicación, la cual nos solicita las credenciales de acceso facilitadas en el correo electrónico.

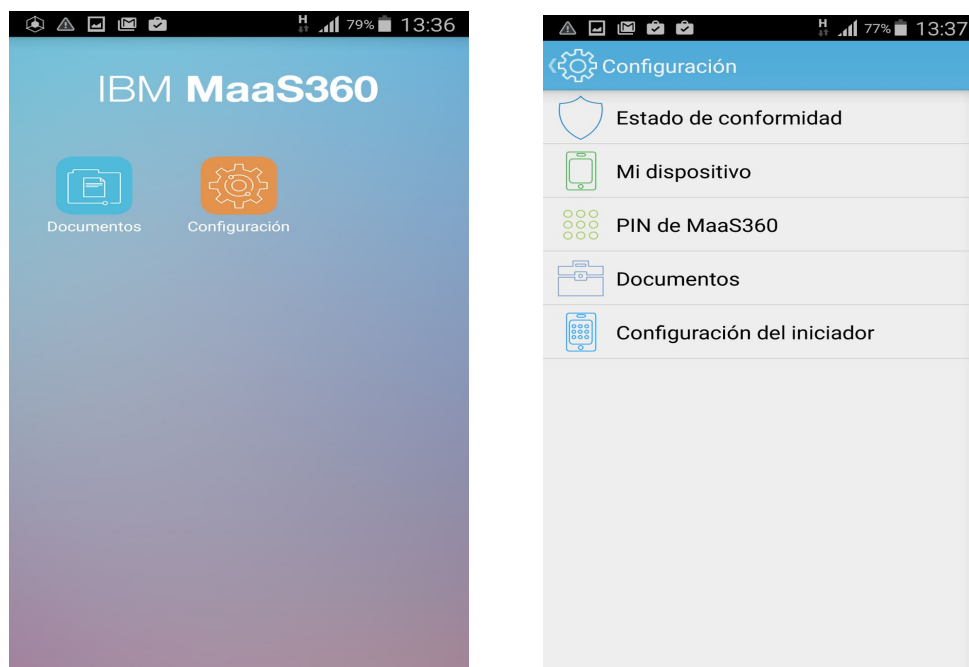


Una vez autenticados, nos pregunta si queremos activar el administrador indicando las operaciones que permitirá realizar a MaaS360 sobre el dispositivo móvil. A continuación inserto capturas de pantalla del dispositivo para que podamos ver cuáles son esas operaciones autorizadas, que son muchas y muy interesantes.

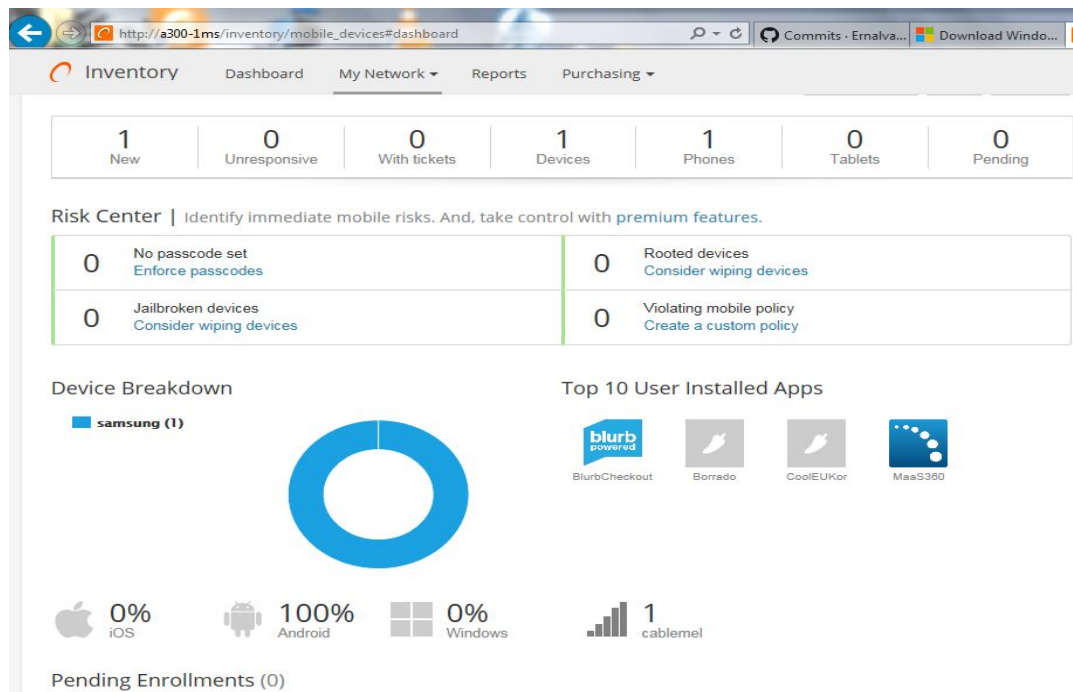




Una vez activado el administrador, ya accedemos a la página principal de la aplicación móvil.

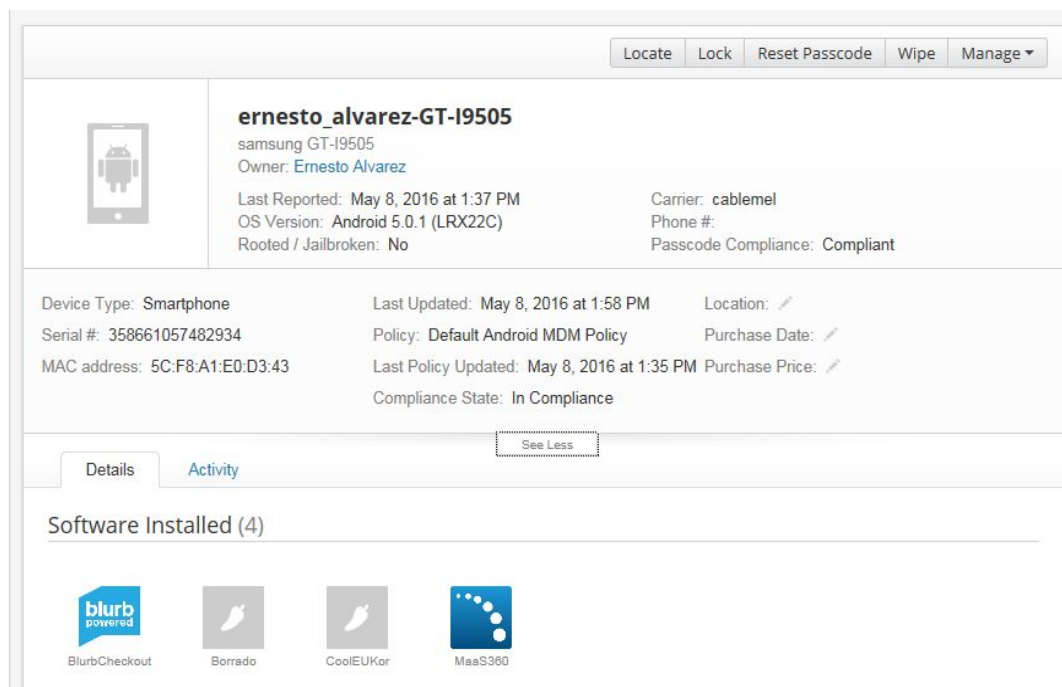


Una vez instalada la aplicación cliente en el dispositivo móvil, nos vamos a la aplicación servidor y podemos ver que ya existe un dispositivo registrado en el inventario de dispositivos móviles.



En la ventana podemos ver además un centro de riesgo donde nos advierte de los dispositivos que pueden estar en riesgo. Si damos click en “premium features”, activamos una versión de prueba de 30 días con todas las características premium activadas.

Si pulsamos sobre el dispositivo, accedemos a una página que nos muestra gran cantidad de datos y las acciones que podemos realizar sobre el mismo, como localizar, bloquear, borrar, etc.






ernesto_alvarez-GT-I9505
samsung GT-I9505
Owner: Ernesto Alvarez

Last Reported: May 8, 2016 at 1:37 PM
OS Version: Android 5.0.1 (LRX22C)
Rooted / Jailbroken: No

Carrier: cablemel
Phone #:
Passcode Compliance: Compliant

Device Type: Smartphone
Serial #: 358661057482934
MAC address: 5C:F8:A1:E0:D3:43

Last Updated: May 8, 2016 at 1:58 PM
Policy: Default Android MDM Policy
Last Policy Updated: May 8, 2016 at 1:35 PM
Compliance State: In Compliance

Location: 
Purchase Date: 
Purchase Price: 

See Less

Details Activity

Software Installed (4)

blurb powered
BlurbCheckout

Borrado

CoolEUKor

MaaS360

Instalación en dispositivos iOS

Para la instalación en dispositivos iOS, es necesario subir un certificado apple válido al servidor. Para crear un certificado firmado, tenemos que hacer click sobre “Create a signed certificate”.

You have not uploaded a signed Apple Certificate yet. [Create a signed certificate](#) to allow your users to enroll iOS devices.

Si intentamos crear el certificado con Internet Explorer, no sale un mensaje indicando que debemos utilizar otro explorador, ya que IE no es compatible con ese proceso.

MaaS360 Account Information

Company name: Ernesto Melilla
Billing ID: 1141848

The Apple Certificate process is not compatible with Internet Explorer. Please use a different browser to complete the process. You can use Internet Explorer again once you're done.

Para obtener el certificado, hay que seguir los pasos indicados en la página que se muestran a continuación: Tener una ID de Apple válida, descargar la solicitud del certificado de Apple, subir la solicitud a Apple y por último importar el certificado al servidor de Spiceworks.

Inventory Dashboard My Network Reports Purchasing



MaaS360 Account Information
Company name: Ernesto Melilla
Billing ID: 1141848

Apple Certificate
Certificate Status: No certificate found, please create and upload one below.

Enter your company Apple ID or create a new one


Save your Certificate Signing Request

3 Upload your CSR to Apple



Upload your CSR to Apple

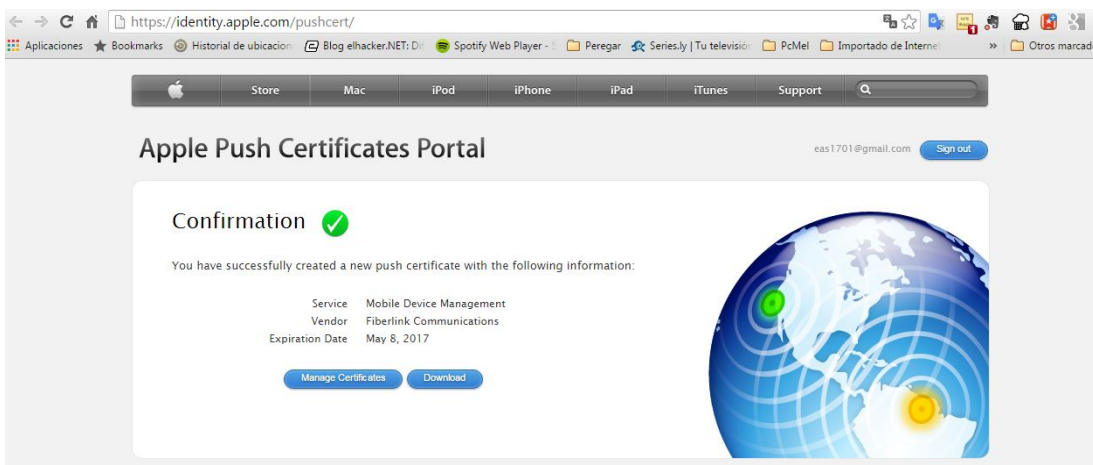
After uploading your CSR, you need to download your certificate, see example below:



Previous Next

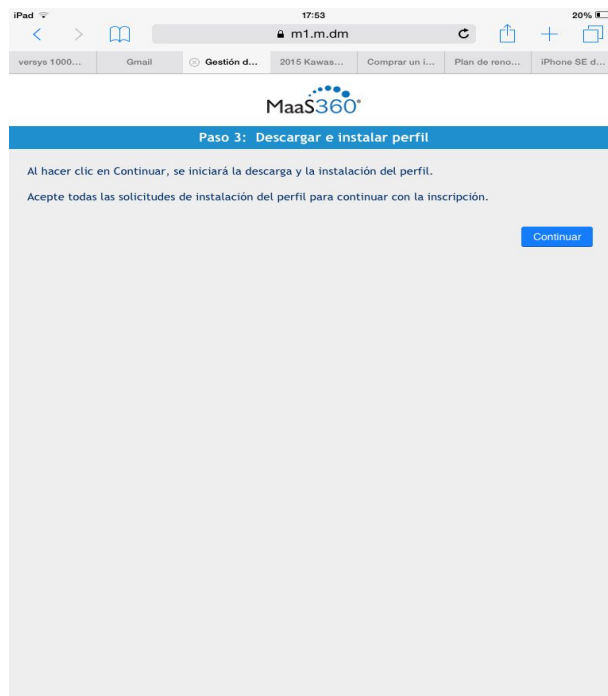
4 Import your Apple Certificate to Spiceworks

A continuación se muestra la página para la obtención del certificado:



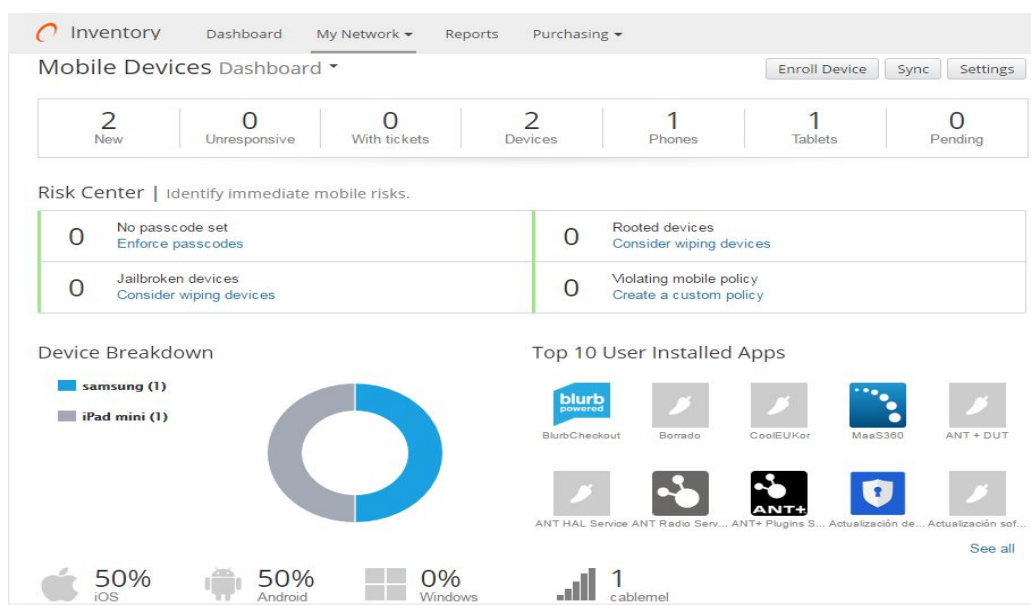
Descargamos el certificado obtenido en esta página y se importa en Spiceworks. El certificado tiene una validez de un año.

Para registrar ahora un dispositivo apple, procedemos como con cualquier otro dispositivo, pulsamos "Enroll device", elegimos el propietario y enviamos una solicitud de registro por correo electrónico. Abrimos el correo electrónico en el dispositivo Apple y seguimos las instrucciones. Se descarga el perfil en el dispositivo Apple y nos solicita insertar las credenciales al igual que en el dispositivo android.

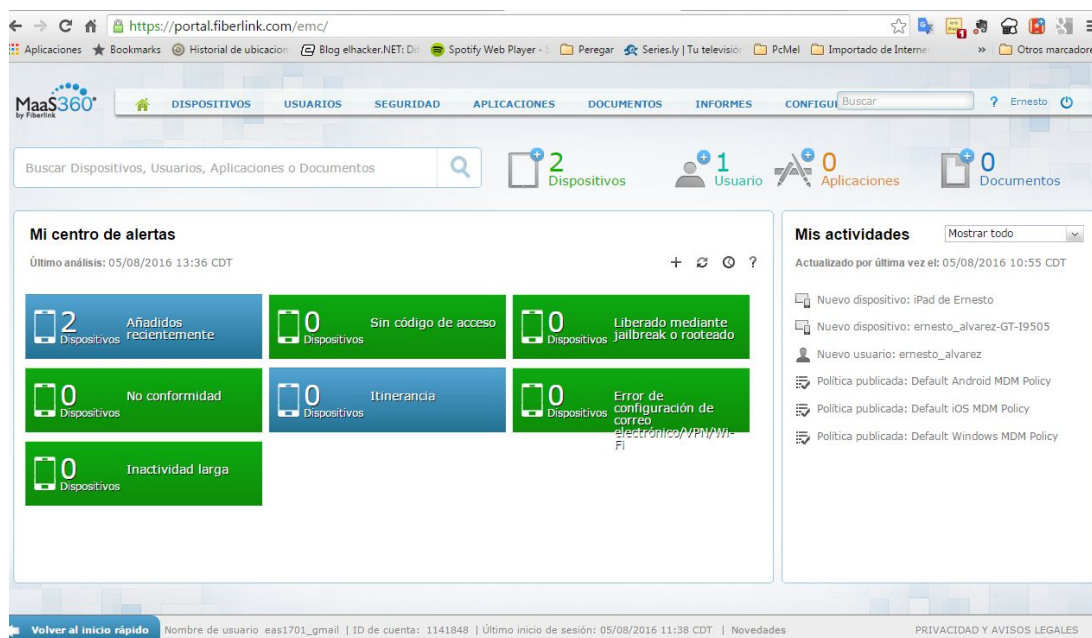


Después de la instalación nos pregunta si confiamos en la fuente del perfil para la administración remota del iPad. Si respondemos afirmativamente, el perfil queda instalado y verificado en el dispositivo.

Al igual que con cualquier otro dispositivo, al rato podemos verlo reflejado en la página de registro y administración.



También existe la posibilidad de iniciar sesión y manejar los dispositivos desde el portal de Maas360, donde también podemos cambiar el idioma.



En definitiva vemos cómo la versión de pago de estas aplicaciones nos permiten tomar un control total de los dispositivos registrados.

Conclusión y valoración personal

La digitalización de la educación es un hecho desde hace unos años. El propio Ministerio de Educación ha invertido muchos recursos en su programa Escuela 2.0, un proyecto de integración de las Tecnologías de la Información y Comunicación en los centros educativos, creando las aulas digitales dotando de recursos TIC a los alumnos y profesores (ordenadores personales, pizarras digitales interactivas, etc), garantizando la conectividad a Internet, y promoviendo la formación del profesorado. La inclusión de las tabletas en el aula gestionadas por un software MDM sería el siguiente paso lógico para la digitalización de la educación, que aunque todavía hay pocos proyectos en marcha, cada vez son más las empresas que ven en esta parcela de mercado una oportunidad de negocio debido a la expansión que se puede prever en la implantación de estas soluciones en los centros educativos.

Bibliografía y fuentes de consulta

https://es.wikipedia.org/wiki/Mobile_device_management

<http://www.telecomunicacionesparagerentes.com/10-soluciones-de-gestion-de-dispositivos-moviles-mdm-para-entornos-byod-i/>

<http://www.spiceworks.com/free-mobile-device-management-mdm-software/>

<https://portal.fiberlink.com/emc/>

<https://www.air-watch.com/es/soluciones/administracion-de-dispositivos-moviles>

<https://www.manageengine.com/mobile-device-management/>

https://resources.iboss.com/mobile_security/mdm_mobileether.html

<https://www.sysaid.com/es/it-service-management-software/it-asset-management/mobile-device-management>

<http://atsistemas.com/expresat/2013/02/como-implantar-sistema-de-gestion-de-dispositivos-moviles-mdm/#>

<http://www.ite.educacion.es/escuela-20>