Aranda Mobile Device Management

Manual de Instalación y Uso

El uso de dispositivos móviles para mejorar la productividad en las empresas es cada vez más frecuente. Los empleados utilizan celulares y tabletas para acceder a información corporativa, comunicarse con otros empleados, realizar presentaciones, acceder al correo corporativo, ubicar servicios geográficamente, etc. En muchos casos los dispositivos son adquiridos y suministrados por la misma compañía. En otros casos los empleados utilizan su propio dispositivo como herramienta de trabajo, promoviendo así la tendencia conocida como BYOD (Bring your own device / Traiga su propio dispositivo). Todo lo anterior representa un reto de gestión importante para los administradores de IT, ya que en muchos casos deben responsabilizarse de la configuración de estos dispositivos móviles, bien sea para facilitar su ingreso al ambiente empresarial, para instalar las aplicaciones requeridas, para establecer restricciones de uso o para proteger la información corporativa en caso de pérdida o hurto del móvil, entre otras.

Introducción

Prólogo

El uso de dispositivos móviles para mejorar la productividad en las empresas es cada vez más frecuente. Los empleados utilizan celulares y tabletas para acceder a información corporativa, comunicarse con otros empleados, realizar presentaciones, acceder al correo corporativo, ubicar servicios geográficamente, etc. En muchos casos los dispositivos son adquiridos y suministrados por la misma compañía. En otros casos los empleados utilizan su propio dispositivo como herramienta de trabajo, promoviendo así la tendencia conocida como BYOD (Bring your own device / Traiga su propio dispositivo). Todo lo anterior representa un reto de gestión importante para los administradores de IT, ya que en muchos casos deben responsabilizarse de la configuración de estos dispositivos móviles, bien sea para facilitar su ingreso al ambiente empresarial, para instalar las aplicaciones requeridas, para establecer restricciones de uso o para proteger la información corporativa en caso de pérdida o hurto del móvil, entre otras.

¿Qué es AEMM?

Aranda Enterprise Mobility Management EMM es una solución creada para enfrentar los retos de gestión de dispositivos móviles en empresas de cualquier tamaño, de una manera simple y eficiente, desde una consola única de administración. Aranda EMM permite realizar inventarios de software y hardware de los dispositivos móviles usados en la compañía, almacena datos de localización, información de red, históricos de eventos, información de estado (dispositivos rooteados, nivel de batería, espacio disponible, etc.). El administrador de IT podrá enviar a los móviles la configuración inicial requerida para que puedan ser usados apropiadamente: Acceso a redes Wifi, correo electrónico del empleado, aplicaciones necesarias para el trabajo, restricciones para asegurar un buen uso del dispositivo, listados de aplicaciones requeridas/prohibidas, políticas de contraseña, etc.

Aranda EMM permite también aplicar reglas de comportamiento a los móviles, con las cuales se monitorean eventos relevantes como el ingreso o salida de zonas geográficas, estados del móvil, cumplimiento de políticas o desvinculación del sistema. De acuerdo a estas condiciones se ejecutan de forma automática acciones como el envío de correo o cambio de políticas. Se permite el envío de comandos manuales sobre los móviles, como bloqueo, cambio de contraseña, envío de notificaciones de texto y borrado completo. Los dispositivos ingresan al sistema mediante un proceso de vinculación muy sencillo, el cual puede ser monitoreado desde la consola web de administración.

Con Aranda EMM las empresas podrán sacar más provecho de sus recursos de cómputo y podrán brindar a sus empleados un entorno confiable para usar sus dispositivos móviles en el trabajo. Soportando tabletas y teléfonos celulares de sistemas operativos Android y iOS.

Requisitos de Sistema

Servidor de Aplicaciones

Requerimientos	Descripción
Sistema Operativo	Windows Server 2016/2019 Standard Edition o superior, x64, con las últimas versiones de SP Instaladas
Memoria RAM	4 GB
Procesador	Intel Xeon > 3.16 GHz, 4MB Cache, Turbo, HT de 1 Core (o equivalente)
Discos Duros	DD 0 (RAID 10): Partición C: 100 GB (SO) DD 1 (RAID 10): Partición D: 30 GB (App y Web)
Requerimientos Adicionales	- Internet Information Services 8.0/8.5/10/10.0 - Microsoft.NET, Framework 4.8 con las últimas actualizaciones. Certificado SSL emitido por una entidad certificadora reconocida. - Roles Necesarios: **Web Server (IIS)** ° *Web Server*(Common HTTP Features (Default Document, HTTP Errors, Static Content). ° *Health and Diagnostics*(HTTP Logging) ° *Performance*(Static Content Compression). ° *Security*(Request Filtering) ° *Application Development*(.NET Extensiblity 3.5, .NET Extensiblity 4.6, ASP, ASP .NET 3.5, ASP .NET 4.6, ISAPI Extensions, ISAPI Filters, WebSocket Protocol) - Características Necesarias: **NET Framework 3.5 Features** / .NET Framework 3.5 (includes .NET 2.0 and 3.0). **.NET Framework 4.6 Features** / .NET Framework 4.6 / ASP .NET 4.6/ WCF Services (HTTP Activation, Message Queuing, Named Pipe Activation, TCP Activation, TCP Port Sharing)

⚐ **Nota:** - Los discos duros pueden estar dentro del servidor o accesibles a él a través de una SAN (Storage Area Network).

- Se recomienda que los Discos Duros sean SSD o SAS de 15.000 RPM.

⚠ **Advertencia:** En caso de virtualizar este servidor, se recomienda reservar los recursos físicos en relación 1:1 con respecto a los recursos virtuales (Resource Allocation). Esta recomendación aplica para Memoria RAM, Procesador y Discos Duros..

Servidor de Base de Datos

Requerimientos	Descripción
Sistema Operativo	Windows Server 2016/2019 Standard Edition o superior, x64, con las últimas versiones de SP Instaladas
Memoria RAM	6 GB
Discos Duros	DD 0 (RAID 1): Partición C: 100 GB (SO, Transaction Log LDF) DD 1 (RAID 10): Partición D: 10 GB (Data Files MDF)
SQL Server	Microsoft SQL Server 2016/2017/2019 Standard o Enterprise. Instalación con: Full Text Search y Autenticación Mixta. Compatibilidad con Azure SQL.
Requerimientos Adicionales	Garantizar conectividad desde el servidor de aplicaciones hacia el servidor de base de datos.

⚐ **Nota Memoria RAM:** Se debe configurar SQL para que solo consuma 4GB y dejar el resto de la capacidad disponible para el sistema operativo.

⚐ **Nota Discos Duros:**

- Siendo un poco más costosa la opción 1 es la más recomendada, ya que su funcionamiento es mucho más rápido para las operaciones de lecturas y escrituras aleatorias en los MDF y para las lecturas y escrituras secuenciales en los LDF.
- Los discos duros pueden estar dentro del servidor o accesibles a él a través de una SAN (Storage Area Network).

- Para propuestas de Cluster deben contar con un almacenamiento compartido.
- Se recomienda que los Discos Duros sean SSD o SAS de 15.000 RPM.

- El espacio en GB es el requerido y puede ser aumentado en cualquiera de las 3 opciones.

⚠ **Advertencia:** En caso de virtualizar este servidor, se recomienda reservar los recursos físicos en relación 1:1 con respecto a los recursos virtuales (Resource Allocation). Esta recomendación aplica para Memoria RAM, Procesador y Discos Duros En caso de virtualizar este servidor, no se recomienda crear los discos virtuales usando aprovisionamiento Liviano (Thin Provisioning).

Dispositivos Móviles

Sistema Operativo	Versiones
Android	- Vinculación Genérica / Vinculación con Android for Work - Compatible desde 5.0+ / AEMM es compatible desde 5.0+ y brinda soporte desde 9.0+ (próximamente a partir de Android 10+)
Android en Dispositivos Samsung (Knox)	- AEMM es compatible con Android 5.1+ (Knox Standard SDK 5.3, Knox Standard SDK 5.9) - AEMM brinda soporte desde 9.0+ (Knox SDK 3.2.1 - Knox SDK 3.9)
iOS	Compatible con iPad - iPhone AEMM brinda soporte a partir de iOS 10+ (próximamente a partir de iOS 13+)

⚠ **Advertencia:** Aranda Enterprise Mobility Management es compatible con dispositivos que están certificados con Android Enterprise. Si el dispositivo no está certificado con Android Enterprise, se deben

de realizar pruebas sobre dicho dispositivo. Para validar que el dispositivo esta certificado con Android Enterprise, consultarlo en el *listado de dispositivos suministrado por Google*

Navegadores de Internet para consola WEB

- Microsoft Edge 14+
- Microsoft Edge 14+
- Microsoft Edge 14+

REquerimientos de Red

Entorno	Requerimiento	Justificación
Servidor de Aplicaciones	- 1. Puerto 443 TCP (Entrada) - 2. Puertos 389.636 (Salida) - 3. Puertos 25, 587 (Salida) - 4. Puerto 443 (Salida) hacia el dominio arandapush1.arandasoft.com	- 1. Conexión de usuarios de consola y dispositivos móviles - 2. Acceso al servidor LDAP en la Intranet, en el caso de usar la funcionalidad de sincronización con el directorio activo de la empresa. - 3. Acceso al servidores de envío de correo electrónico. - 4. Envío de notificaciones push hacia dispositivos móviles
Todos los Dispositivos	Puerto 443 hacia Servidor de aplicaciones	Conexión a consola de administración
Dispositivos Windows	Salida a los dominios *.notify.windows.com, *.wns.windows.com, *.notify.live.net	Conexión al servicio de notificaciones push para windows
Dispositivos iOS	Puerto 5223 (Salida) hacia direcciones en el formato 17...*	Conexión al servicio de notificaciones push para iOS
Dispositivos Android	Puertos 5228, 5229, 5230 hacia dominios android.googleapis.com, gcm-http.googleapis.com, fcm-http.googleapis.com	Conexión al servicio de notificaciones push para android, tienda de google play y plataforma de Android for Work
Estación de trabajo de usuario de Consola AEMM	- Puerto 443 (Salida) hacia el servidor de aplicaciones - Puerto 443 (Salida) hacia el dominio c.tile.openstreetmap.org	- Conexión a la consola de administración - Presentación de mapas en Open Street Maps

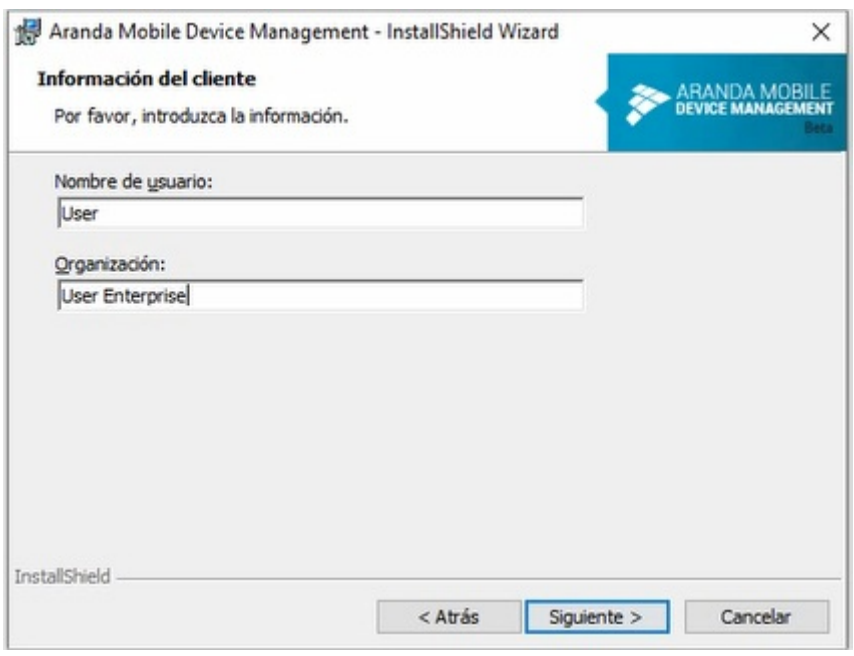
Instalación

Proceso de Instalación

El instalador comienza a extraer los archivos necesarios y a preparar el proceso

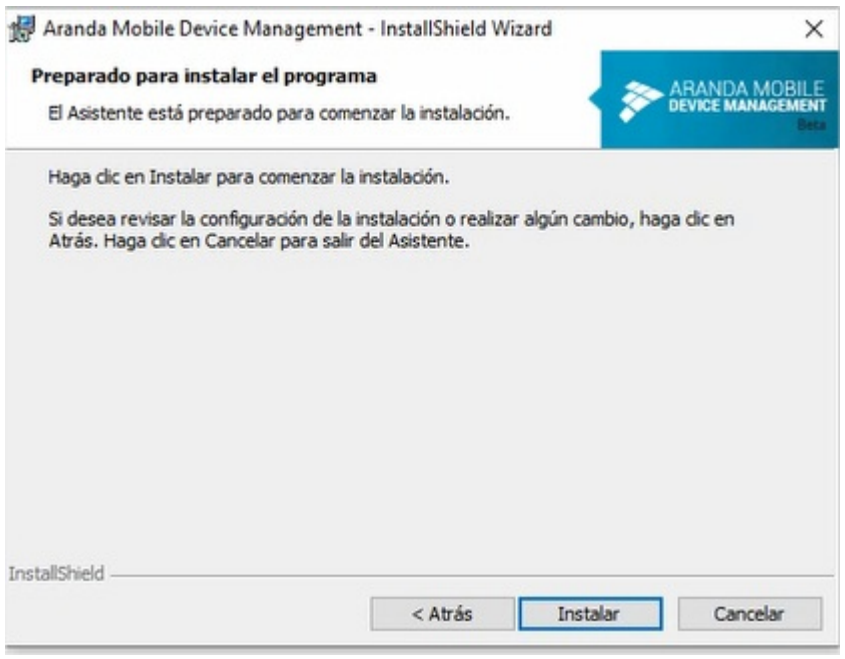
De clic en **siguiente** para continuar con la instalación.

Ingrese el nombre de usuario y la organización. De clic en **siguiente**:

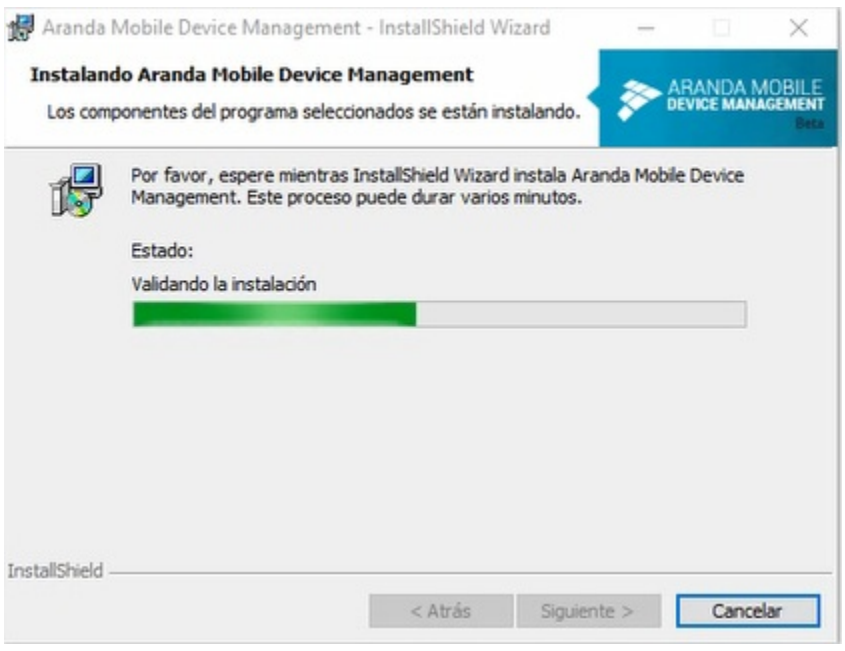


Seleccione el tipo de instalación completa.

De clic en **Instalar**



Espere a que el proceso de instalación se complete



Seleccione finalizar para terminar el proceso de instalación

Configuración de Base de Datos y Servicios Windows

Para la creación o actualización de la base de datos y las respectivas conexiones desde las aplicaciones, así como la gestión de los servicios Windows es necesario utilizar la herramienta **Aranda Database Tools** suministrada por Aranda Software.

Para más información sobre **Aranda Database Tools** dar clic en el siguiente link:

Aranda Database Tools

Configuración de Licenciamiento

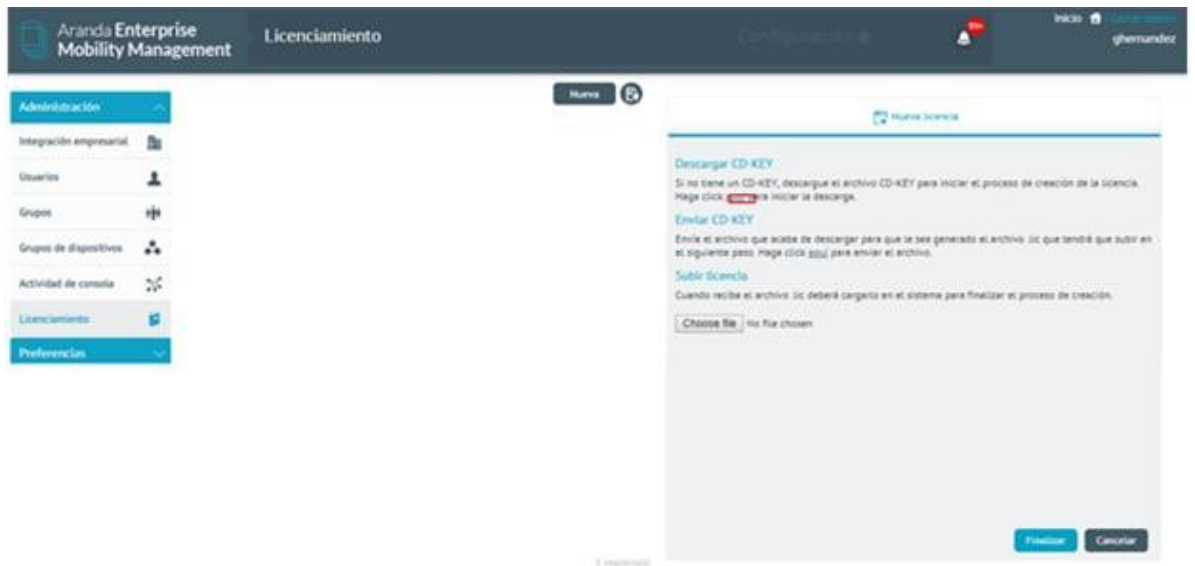
Todos los productos de Aranda Software necesitan de una licencia para su funcionamiento, razón por la cual, la

primera vez que ingrese a Aranda EMM se le solicitará una licencia.

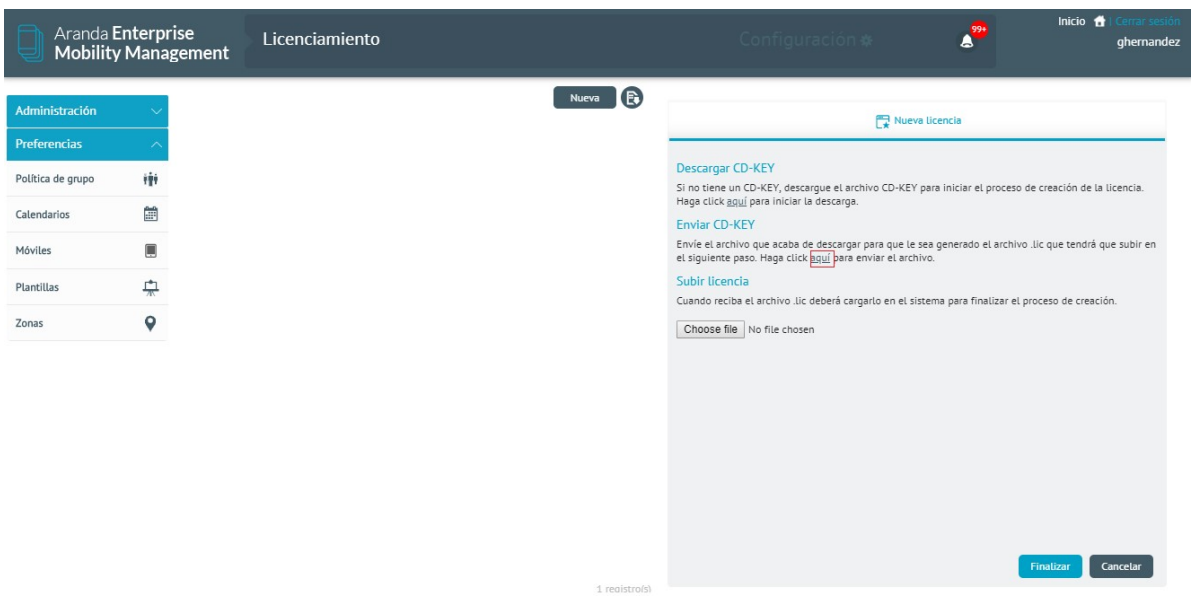
Se explica el proceso a continuación:

De clic en la opción **Nueva**

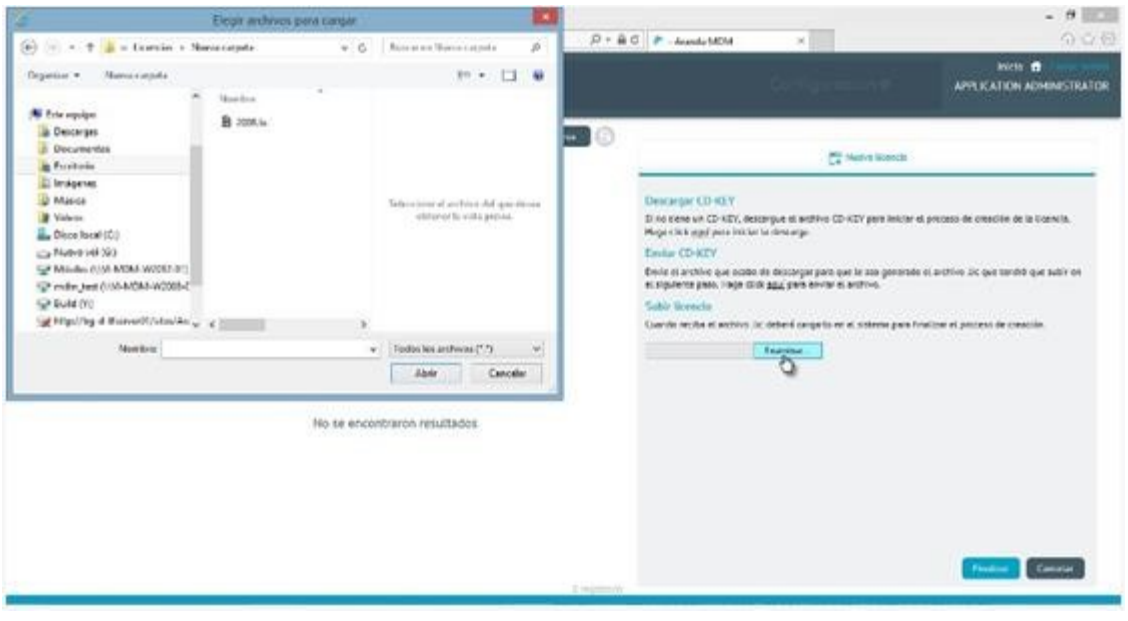
Descargar el Machine – KEY



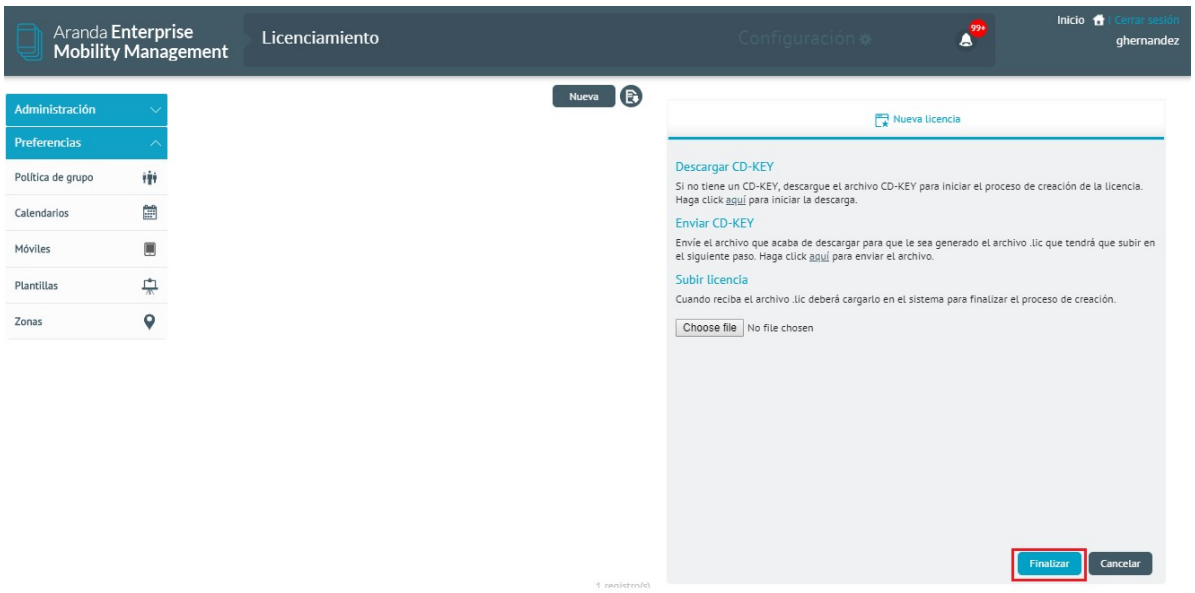
Envíe vía correo electrónico el Maquine -KEY a su representante en Aranda Software



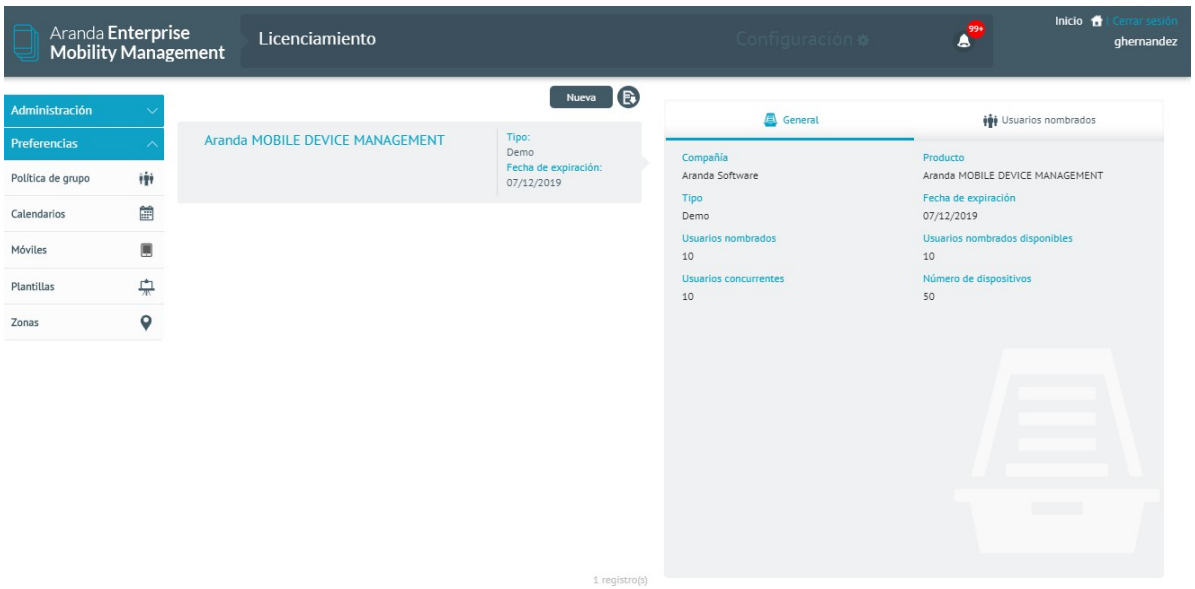
Seleccione la licencia que recibió a través del correo electrónico



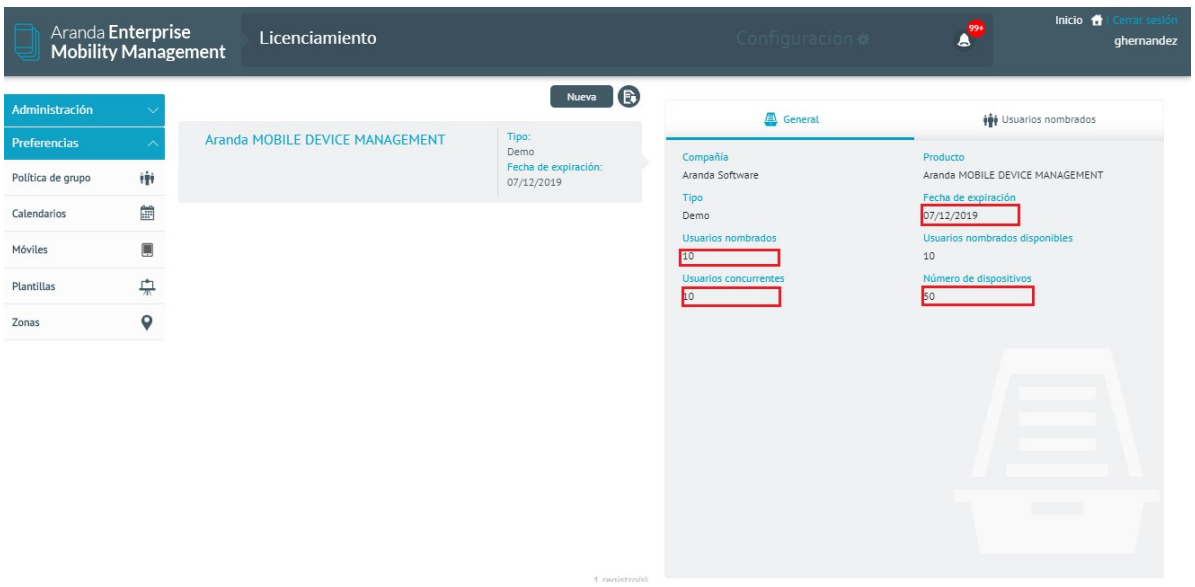
Y de clic en la opción **finalizar**.



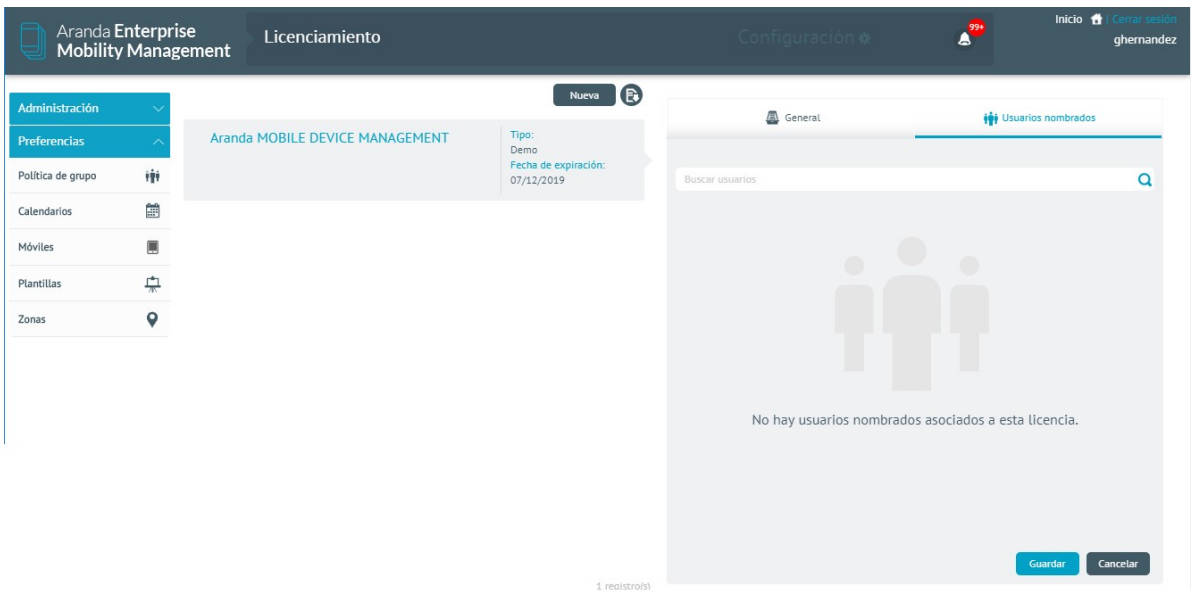
De este modo, la licencia se carga exitosamente



En la licencia se visualizarán la fecha de expiración, usuarios nombrados, usuarios concurrentes y el número de dispositivos permitidos



Los Usuarios nombrados son las licencias que siempre tendrán acceso a la consola. Para agregar este tipo de usuarios se debe ingrese a la pestaña **usuarios nombrados** y adiciónelos.

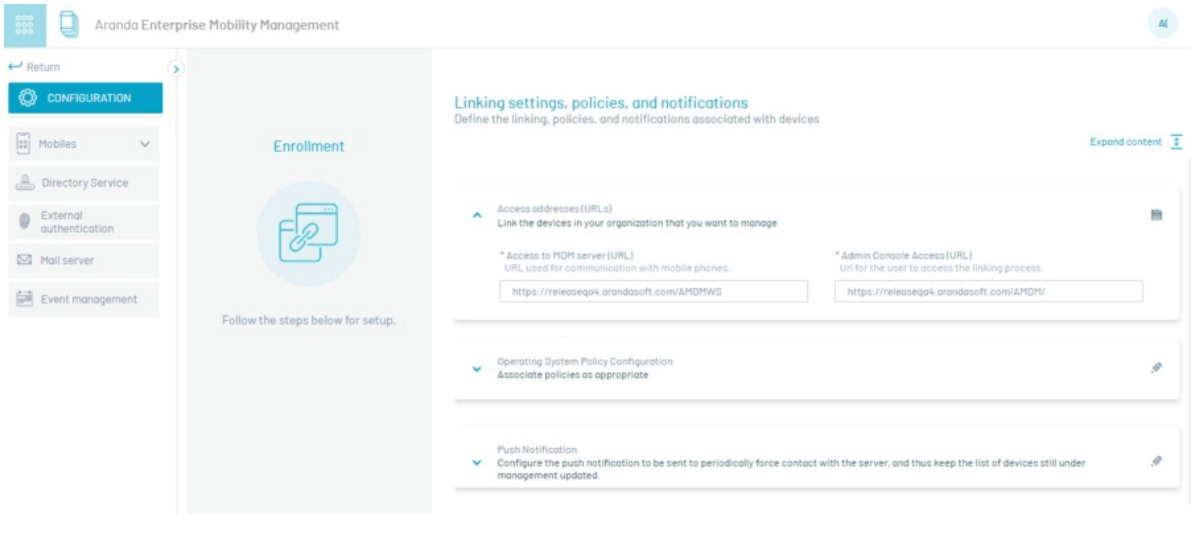


Configuración Inicial

Para configurar Aranda EMM es necesario tener en cuenta lo siguiente:

Configuración de las URLS para acceso a la consola y el servidor.

- URL de acceso al servidor MDM: Se utiliza para la comunicación con los dispositivos móviles.
- URL de la consola de administración: Permite que el usuario acceda al proceso de vinculación desde el dispositivo y pueda gestionar su vinculación. (Para más información. Ver Sección Vinculación de Dispositivos)



Configuración Addons

Paquete instalable que el agente genérico usa para extender la funcionalidad de control y requerimientos, para los proveedores disponibles LGE y Cyrus.

- Configuración: Se debe realizar la configuración al servidor de almacenemiento donde se van alojar los adons, está configuración se realiza desde la base de datos en la tabla afw_settings, como se muestra a continuación:


```
select *

from afw_settings

where sett_key ="AdonsContainer"
```

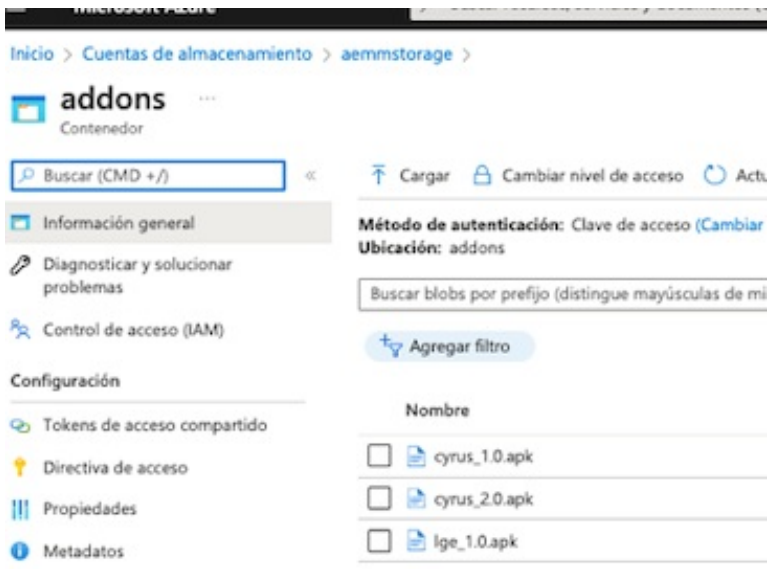
En el campo sett_value encontrará un json el cual aloja los siguientes datos:

Campo	Descripción
Variables	Descripción
type	Tipo
Camconnectionstring	Conexión al storage
containername	Nombre de la carpeta
Campo	Descripción

Ejemplo:

```
{
"type":"1",
"connectionstring":"DefaultEndpointsProtocol=https;AccountName=aemmstorage;xxx",
"containername":"addons"
}
```

Campo	Descripción
Type	Debe tener en cuenta que el tipo de almacenamiento es igual a uno (1), como lo muestra en el ejemplo anterior.
Connectionstring	El endpoint lo encuentra en la cadena de conexión configurada en su cuenta de almacenamiento. En el ejemplo anterior muestra que la configuración fue realizada desde un block storage de azure, el dato de la variable la encontramos en claves de acceso-> Cadena de conexión.
Containername	El nombre de la carpeta donde se encuentran alojados los addons en la cuenta de almacenamiento. Recuerde que para guardar los addons el nombre debe cumplir con los siguientes parámetros: nombre_versión.extensión (lge_1.0.apk)



- Cuando la herramienta obtenga conexión con la cuenta de almacenamiento remoto unificado, este devuelve un listado de addons, el cual almacenará y actualizará el cache local del listado de addons, lo podemos validar en la tabla AMDM_MOBILEADON, esta tabla sólo guardará la última versión de los addons.

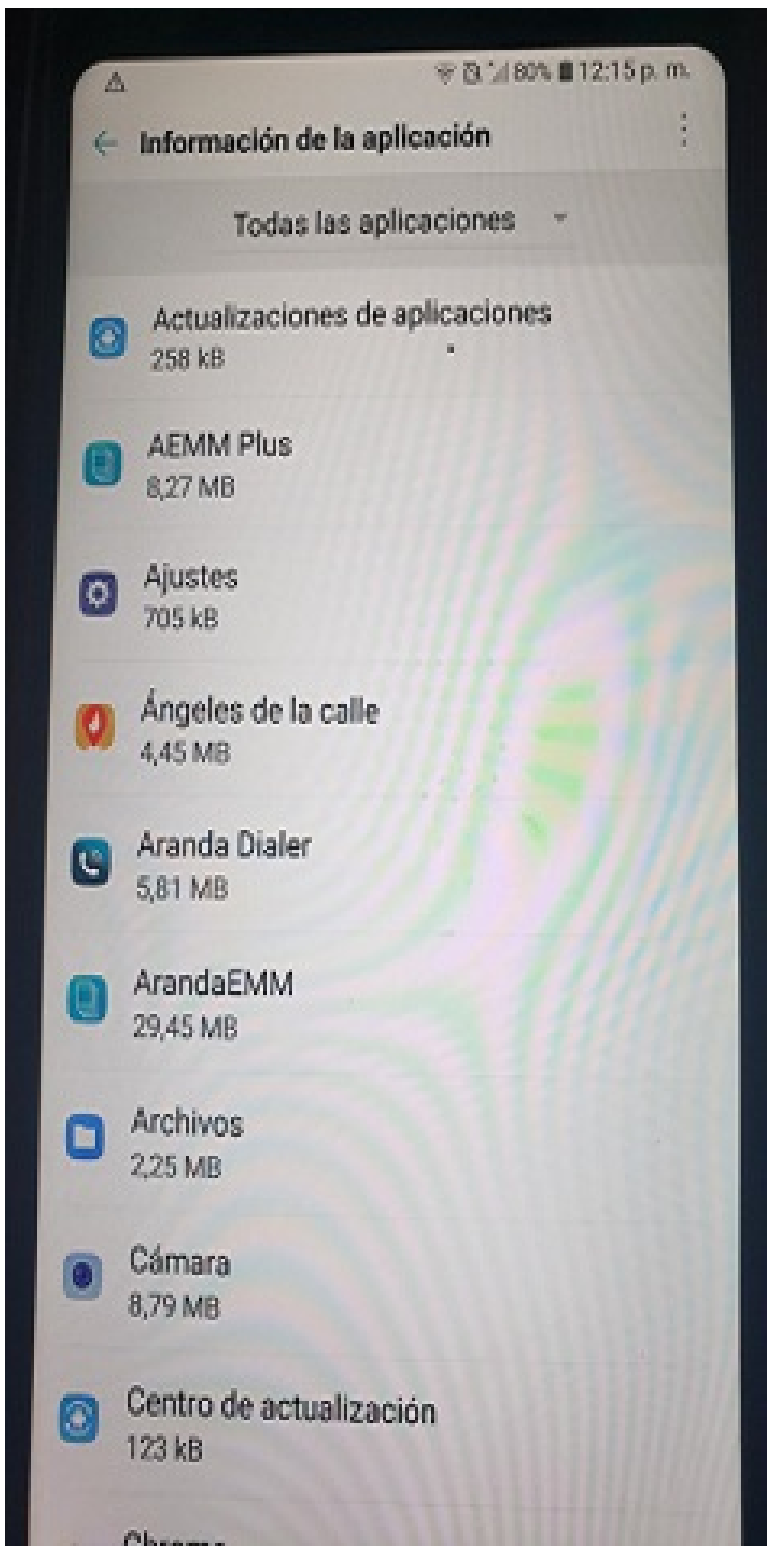
- De igual forma tiene configurado una tarea que se ejecuta periódicamente para actualizar el listado de addon la cual encontramos en la tabla afw_scheduler; esta tabla se ejecuta cada 720 min, es decir 2 veces al día actualizando el cache local del listado de addons.

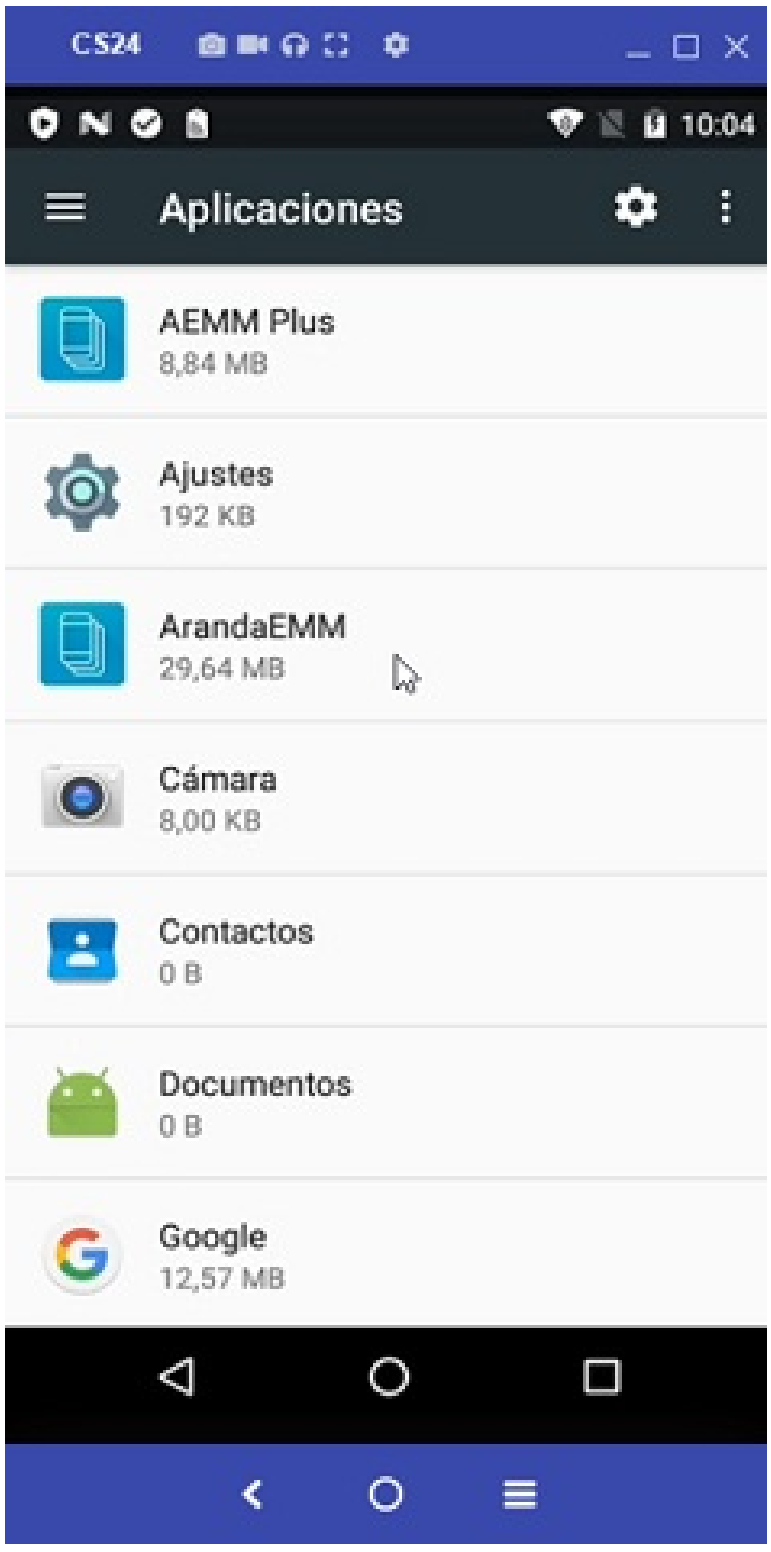
```
20  select *
21  from afw_scheduler
22  where sche_task_id = 33066
23
```

Results | Messages

	sche_id	sche_name	sche_description	sche_frecuency_type	sche_recurse_every	sche_weekdays
1	73	AMDM_SynchronizeAdonsListTask	AMDM Sincronización de listado local de Adons de...	Interval	720	0

- Dispositivos: Cuando se realice la configuración correspondiente en consola y el dispositivo cuente con el agente genérico que incluya está característica, se enviará a instalar automáticamente en los dispositivos el ADDON correspondiente de acuerdo al fabricante al cual pertenece (LG- Cyrus). Recordemos que el addon no tiene launcher sino que se podrá visualizar en ajustes de android-> aplicaciones-> podemos observar el agente instalado ArandaAEMM y el launcher AEMM PLUS

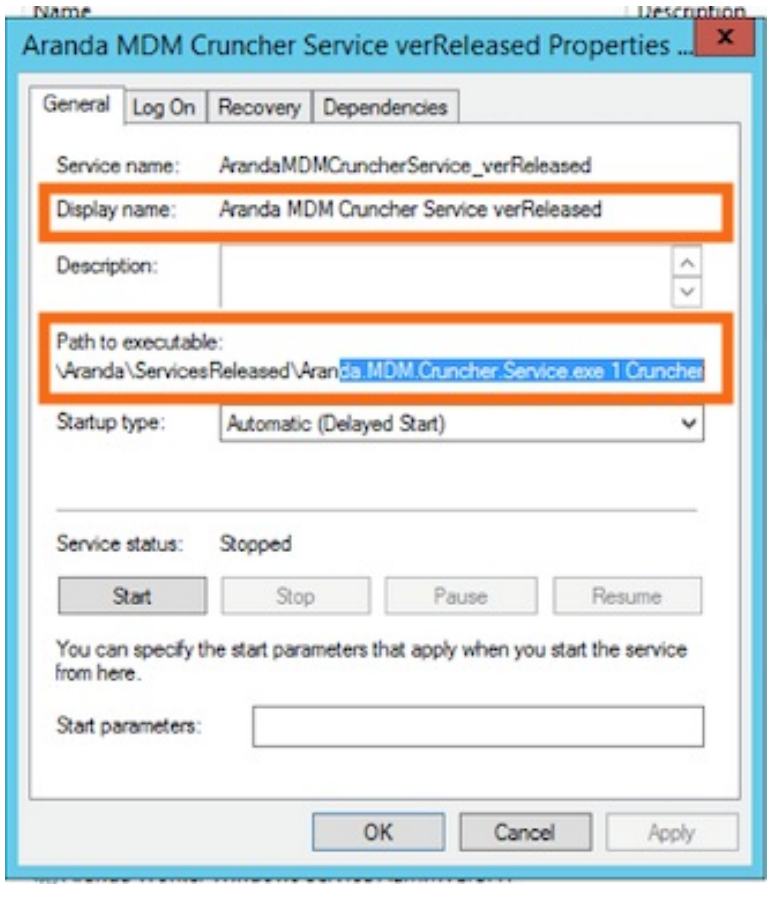




Configuración Cruncher

Este es el servicio que procesa archivos de alta demanda.

Multi Instancias para el cruncher: Se mejora la capacidad del cruncher de trabajar en paralelo sobre un mismo tenant, con el fin de optimizar el proceso de colas, estos cruncher se pueden crear a demanda.



Administración

Configuración Conexión con CMDB

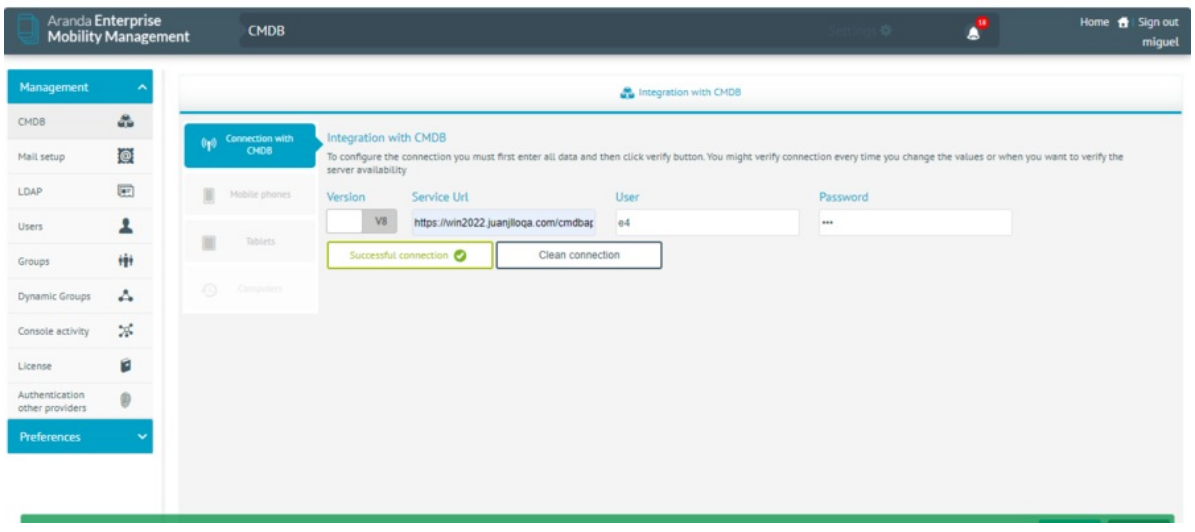
Para configurar la conexión con CMDB, ingrese a la consola de inicio de AEMM, en la sección de **administración** del menú principal, seleccione la opción **CMDB** y en la vista de información podrá completar los datos para conectar con la CMDB deseada.

Versión 8

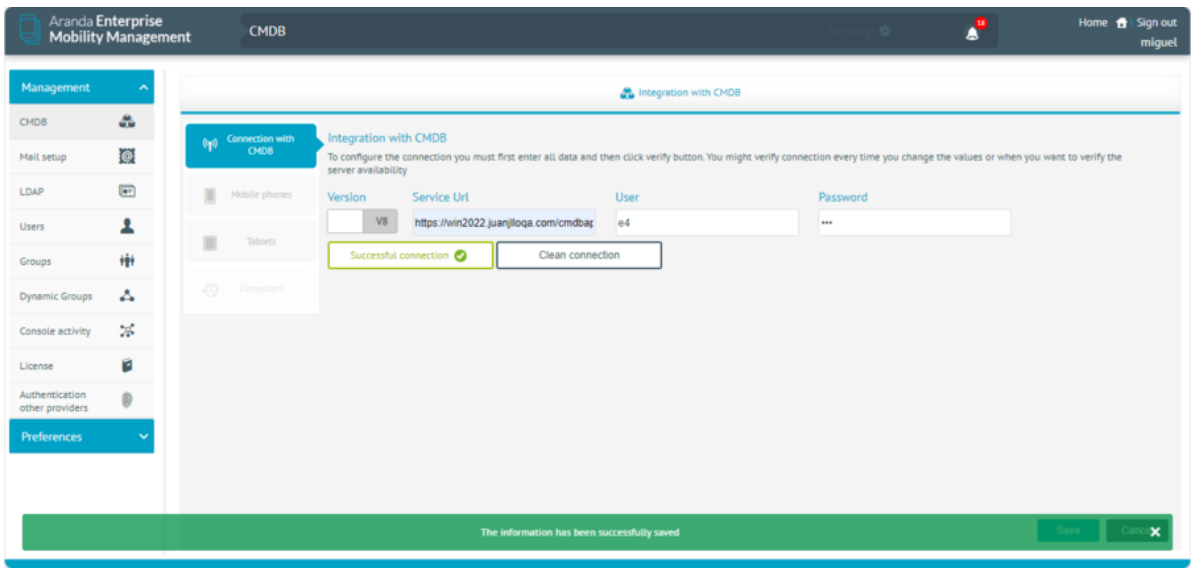
Para conectarse con esta versión en específico, debe ingresar los siguientes datos:

- Url: Dirección url donde está alojada el API CMDB.
- Usuario: El usuario de ingreso a la CMDB.
- Contraseña: El password asociado al usuario de CMDB.

1. De clic en la opción **Verificar Conexión** para poder habilitar la opción de guardar.



2. Después de haber validado la conexión, seleccioné el botón **Guardar**.



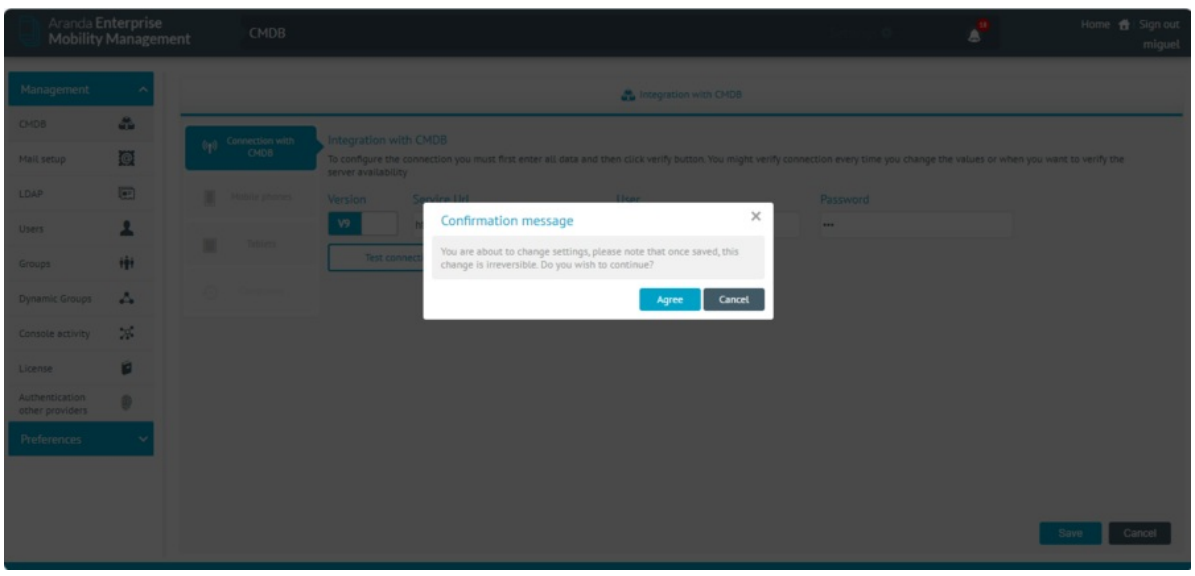
3. En la vista de Información se habilitarán las opciones de conexión CMDB. Seleccione los campos de los activos (CIs) que desea mapear y realice el mapeo de los campos adicionales de la CMDB con los de Aranda EMM.

Versión 9

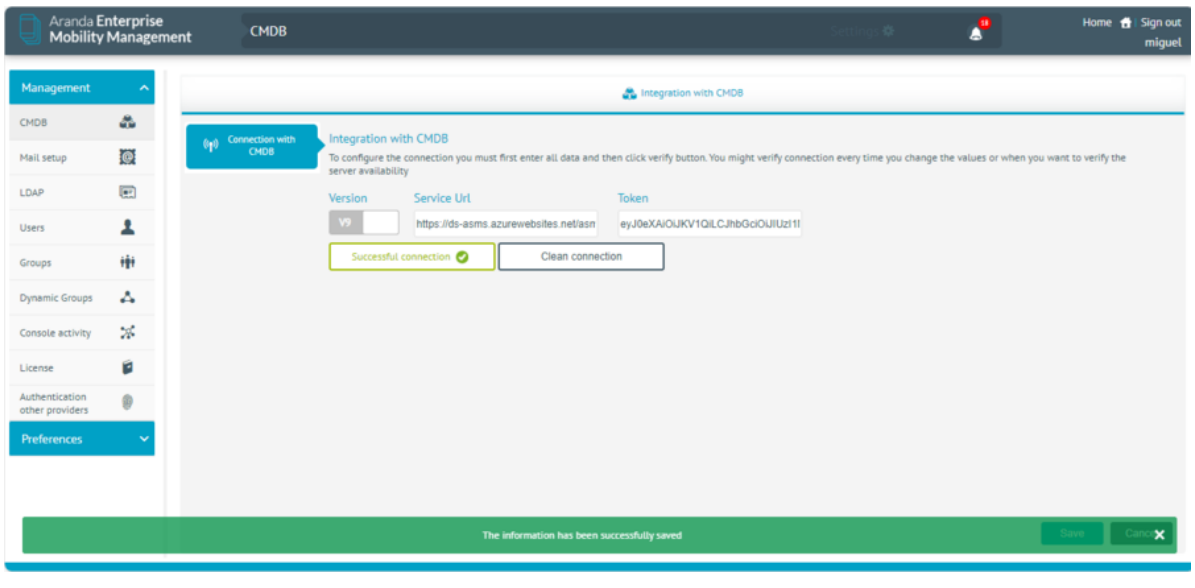
Para poder conectarse en la versión 9 de CMDB debe llenar los siguientes datos:

- Url: Dirección url donde está alojada la API CMDB.
- Token: Token de conexión que remplaza las credenciales del usuario y contraseña

1. De clic en el switch de versiones para poder configurar esta versión, allí aparecerá una ventana de confirmación indicándole que la acción que va a ejecutar va a ser irreversible.



2. Similar como en la versión 8 de clic en la opción de **Verificar Conexión**, y luego puede oprimir el botón de **Guardar**.

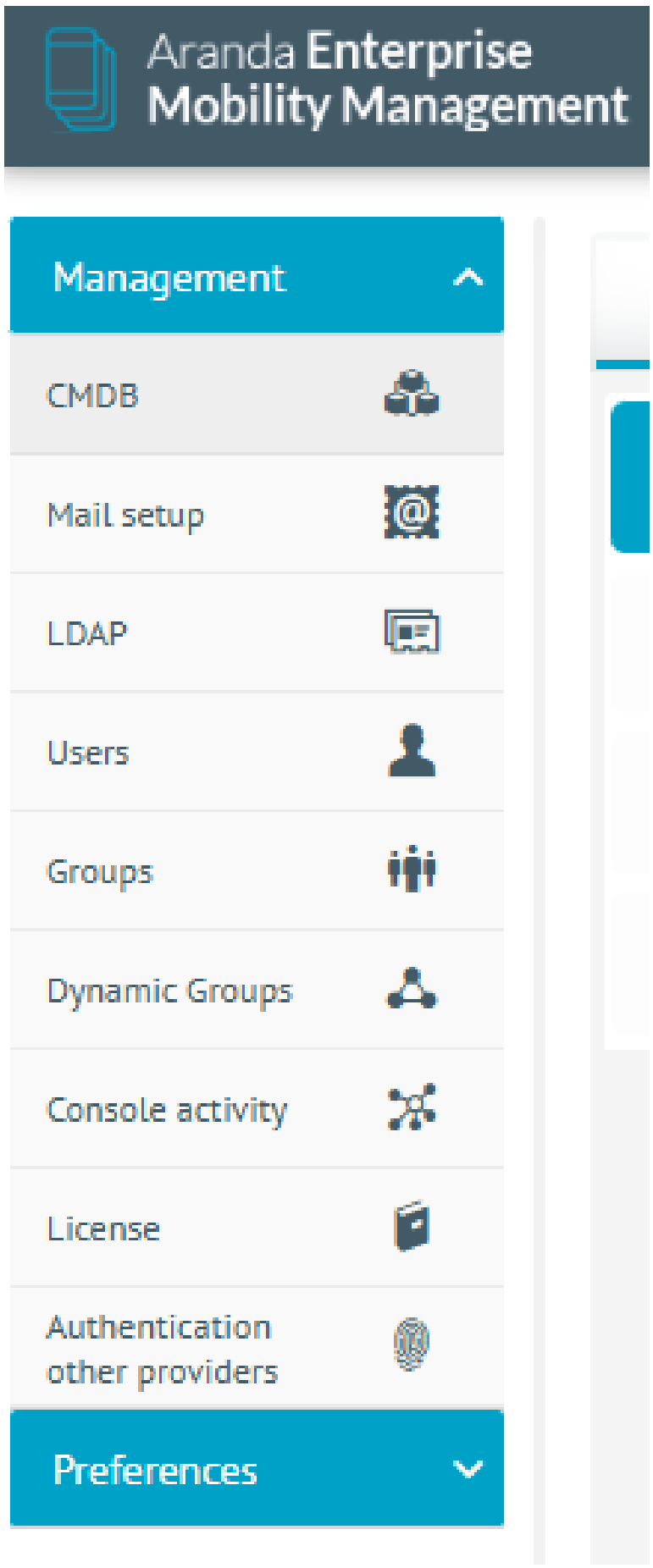


⚐ **Nota:** Tener en cuenta que después de configurar una conexión con CMDB versión 9, no podrá volver a configurar conexiones con versión 8..

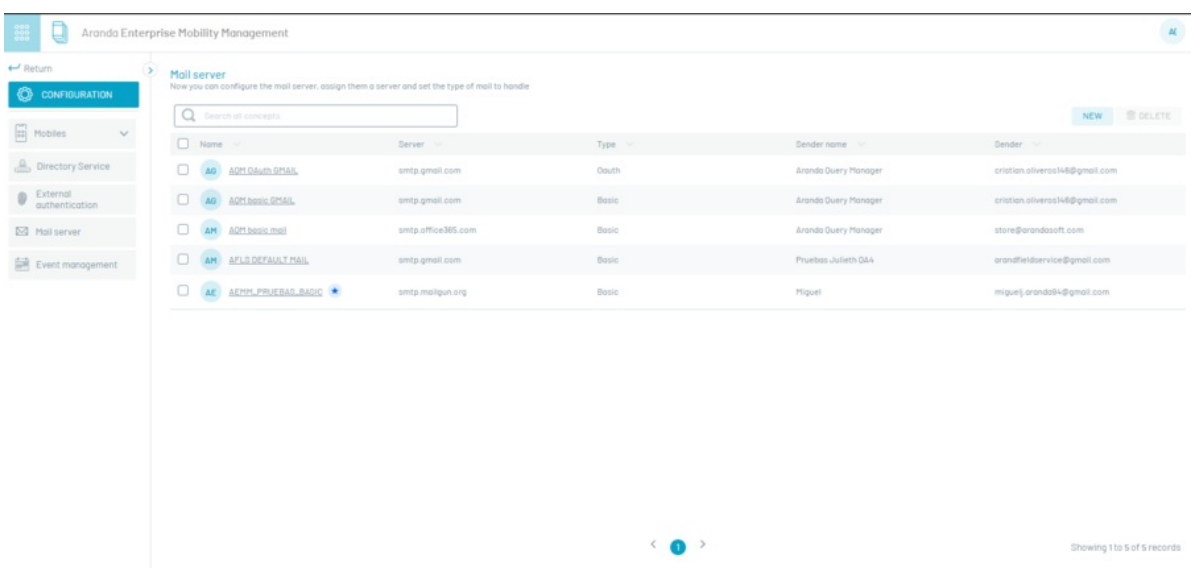
Configuración de Correo

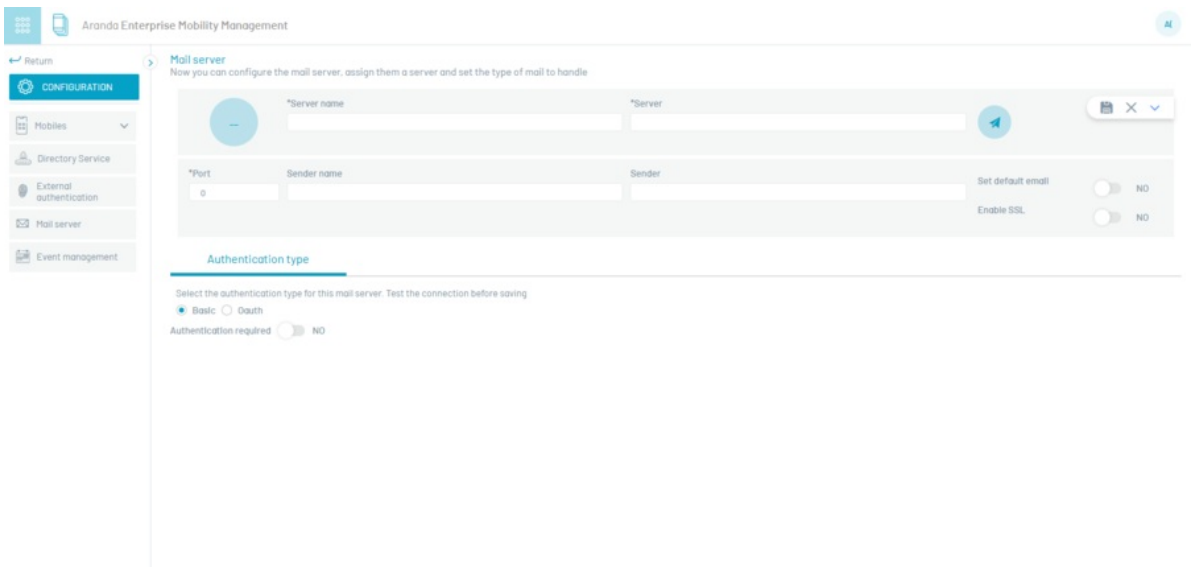
Este módulo permite configurar los dominios de autenticación que estarán disponibles en la consola. El detalle de los pasos necesarios para la configuración lo encontrar.

1. Para realizar la configuración del correo, ingrese a la consola de inicio de AEMM, en la sección de **Administración** del menú principal, seleccione la opción **Configuración de correo**.

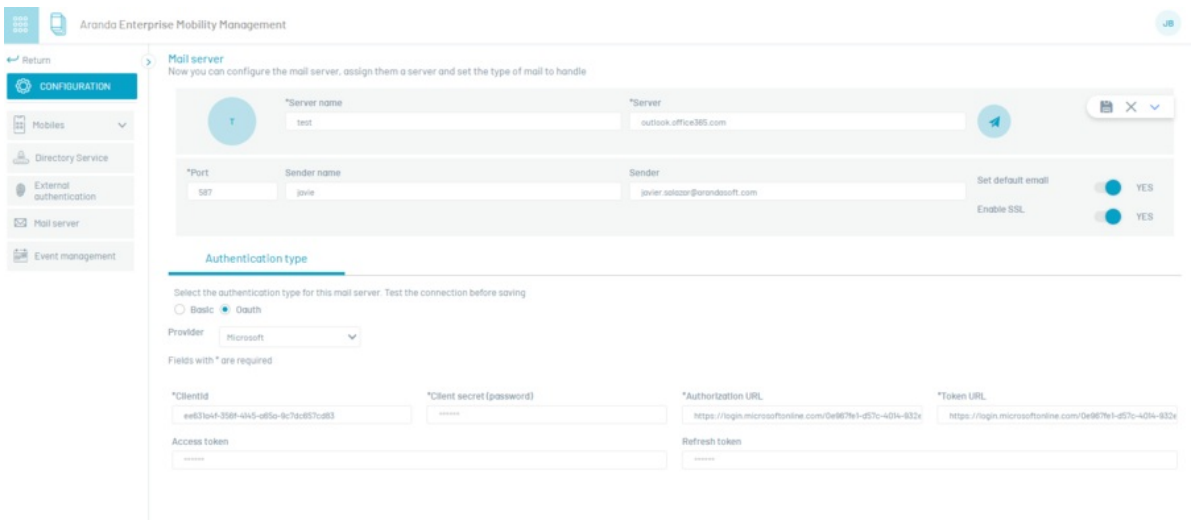


En la vista de información, seleccione el botón **NUEVO** y en la Vista Detalle podrá completar la información requerida del servidor.

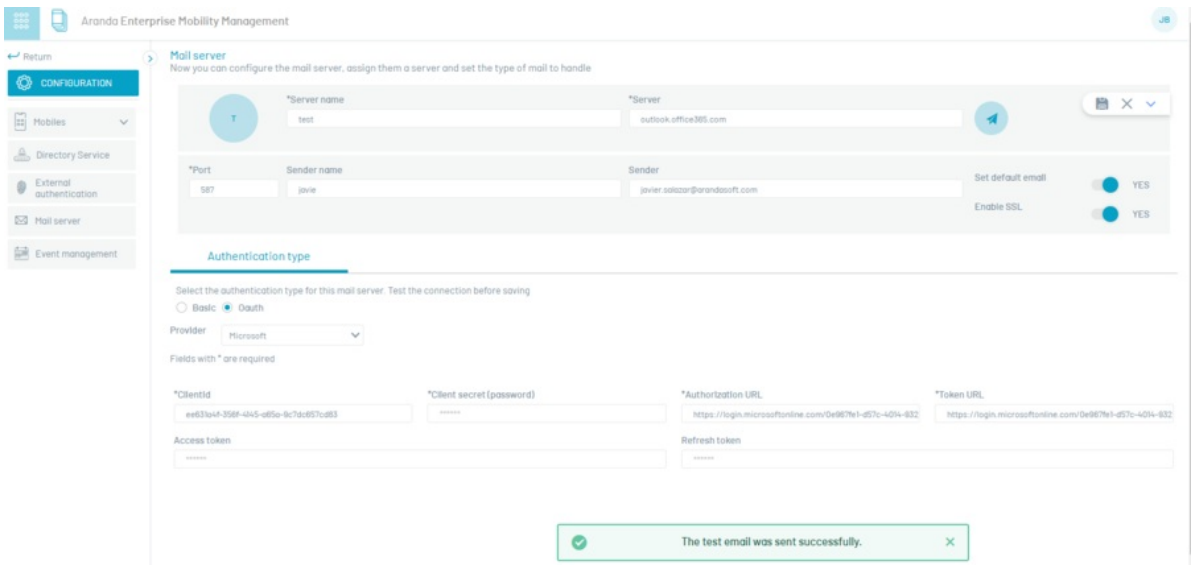




Campo	Descripción
Nombre del servidor	Nombre de la configuración que está creando.
Servidor	Nombre del servidor que permite el transporte del email en la Internet.
Puerto	Número de puerto por el que se conectara al servidor.
Nombre del remitente	Nombre que aparecerá en las notificaciones de correo.
Remitente	Dirección de correo electrónico para enviar las notificaciones.
Establecer correo predeterminado	Activa/Desactiva la opción de configurar el registro por defecto para el envío de correos de la consola de AEMM.
Habilitar SSL	Activar/Desactivar la opción del certificado SSL.
Tipo de autenticación	En esta opción se selecciona y se configura el tipo de autenticación para el servidor de correo, se visualizan las siguientes opciones: - **Básica**: Solicita los campos obligatorios de: Usuario (nombre de usuario utilizado para para conectar con el SMTP) y Contraseña (contraseña para conectar al SMTP.). - **OAuth**: Solicita los campos obligatorios de ID Cliente, Secreto del cliente (Contraseña), URL de autorización, URL de token, Token y Access Token . **Nota:** En el portal de configuración de Microsoft se debe configurar en la opción URI de redirección la URL de la aplicación. Por ejemplo: https://localhost/smtp . - Para obtener los datos anteriores remítase al siguiente documento.

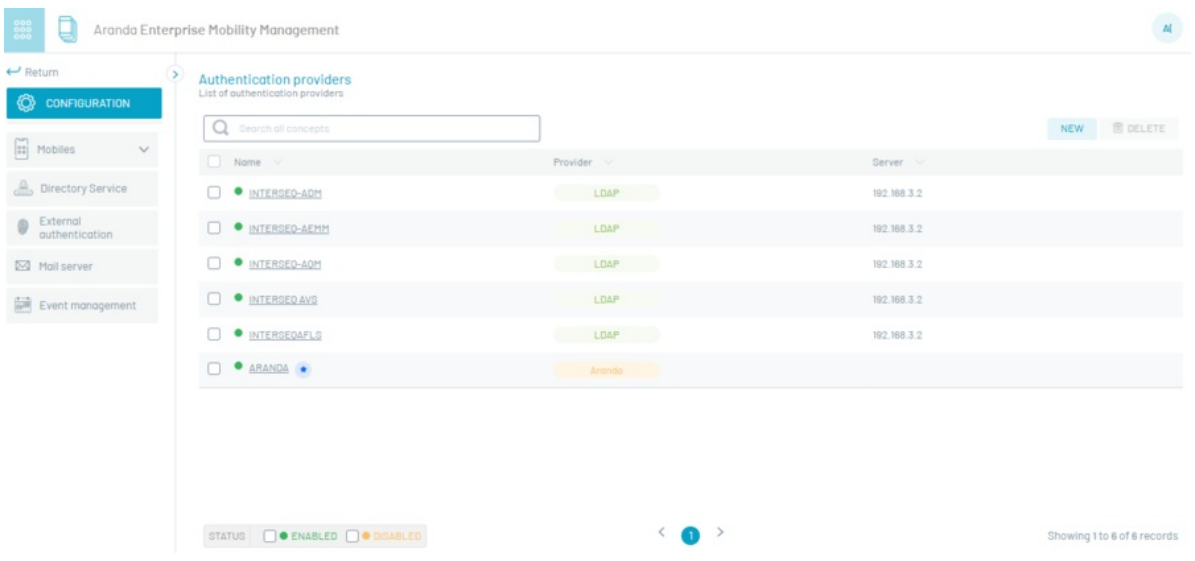


2. En la Vista detalle de correo en la consola de inicio de AEMM, haga clic en el botón **Enviar correo de prueba**. Al dar clic al botón, se recibirá un correo de prueba enviado desde el servidor AEMM al buzón de entrada del destinatario.



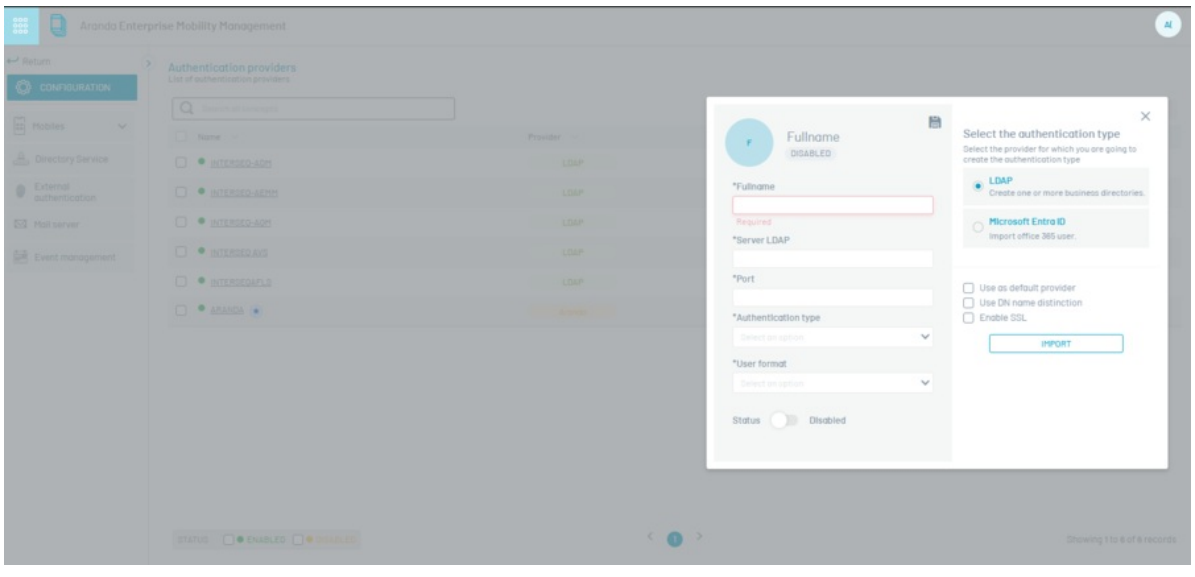
3. Después de comprobar que la configuración es correcta seleccionar el botón **Guardar**.

Servicio de directorio (LDAP)

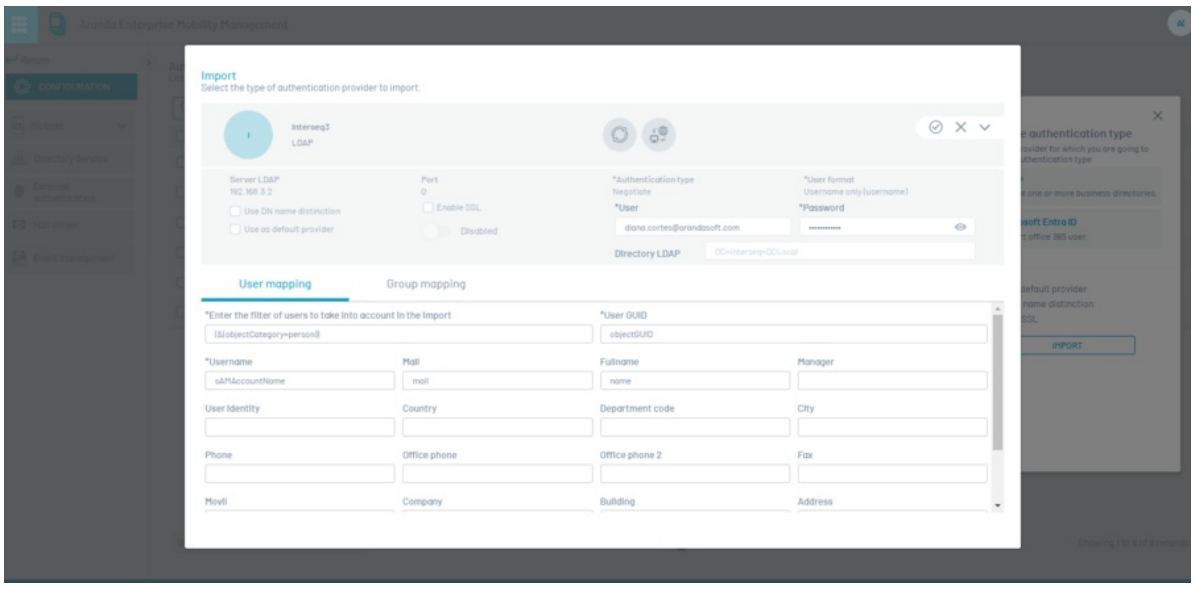


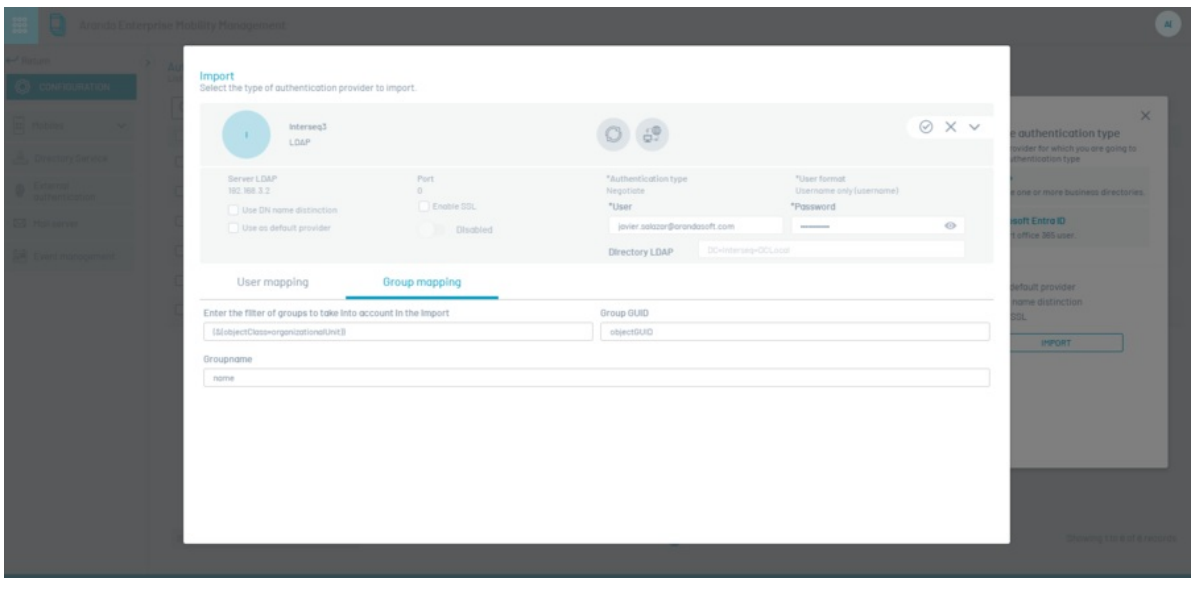
Este módulo permite configurar los dominios de autenticación que estarán disponibles en la consola.

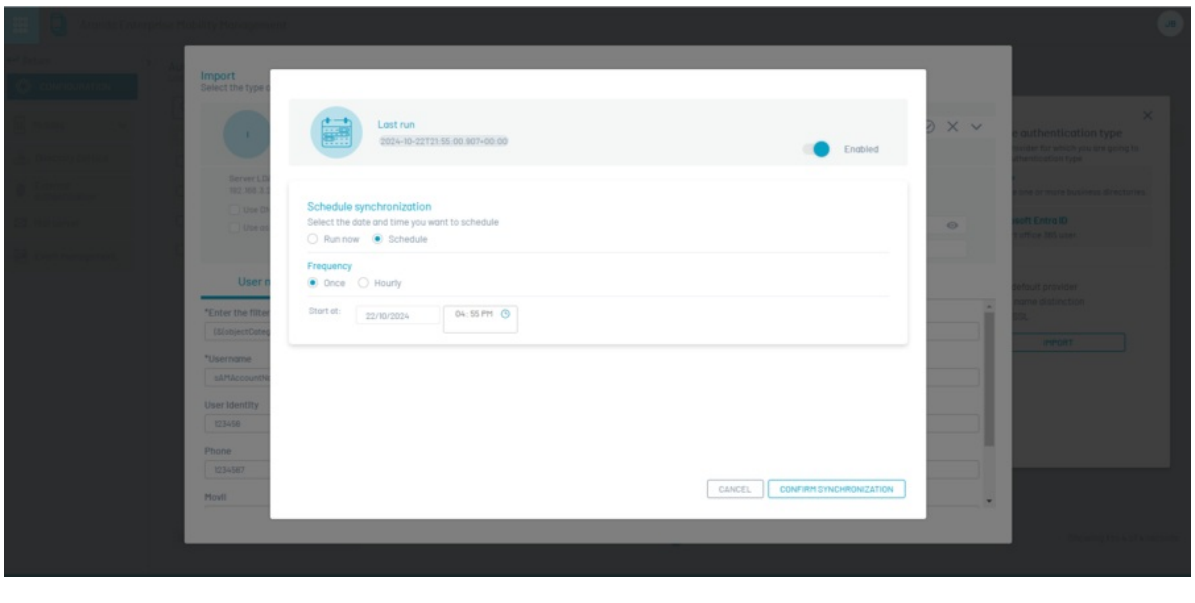
Para agregar un nuevo dominio haga clic en el botón **NUEVO**



Luego de que llene la información marcada con asterisco (*), puede configurar las opciones que están en el botón IMPORTAR:

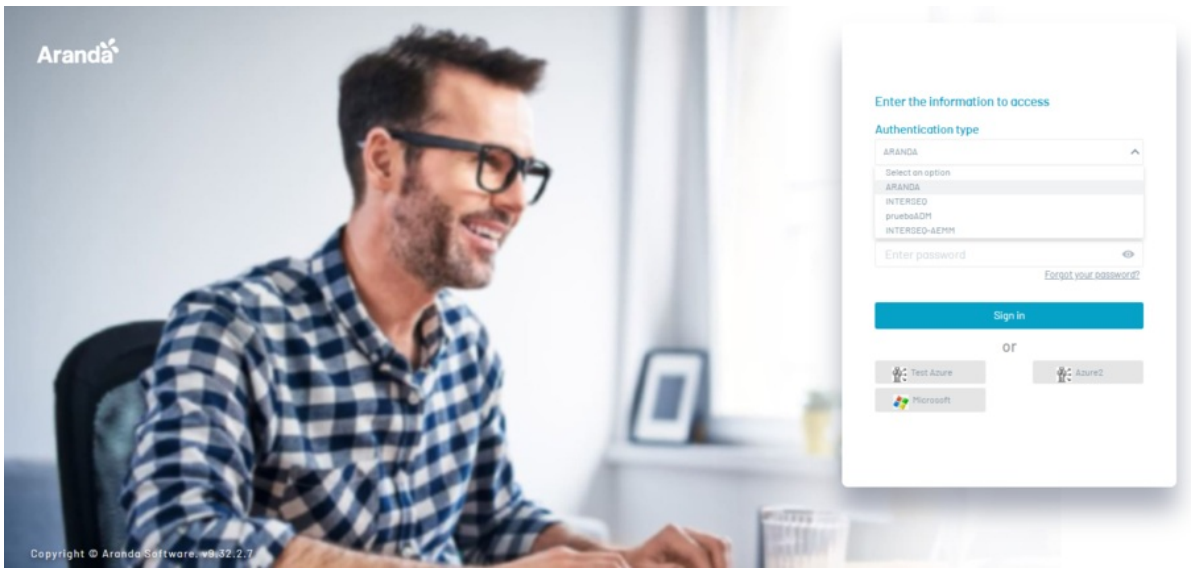






Cuando estén diligenciados todos los datos haga clic en **Guardar** para persistir el nuevo dominio.

Luego de agregar el dominio se sincronizará y estará disponible en el combo de dominios de autenticación presentado en la pantalla de inicio de sesión.

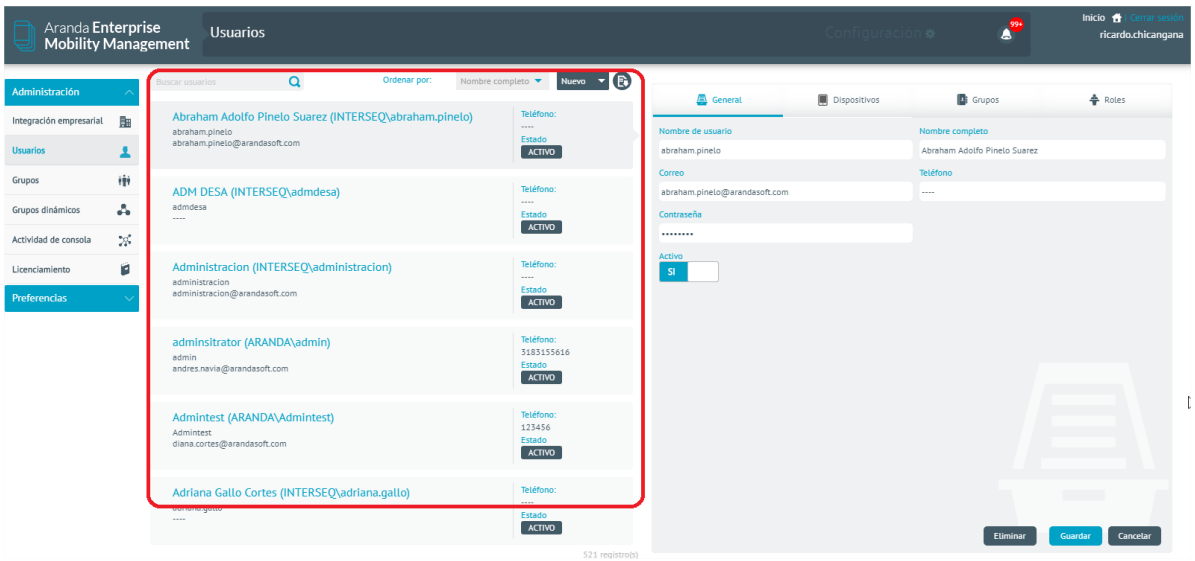


Usuarios

Se conocen dos tipos de usuarios en AEMM; los de consola y los usuarios móviles. Los usuarios de consola son aquellos que ueden intervenir y monitorear los dispositivos móviles que se registren en la consola y los usuarios móviles son los que se vinculan en la consola con su dispositivo móvil pero nunca tienen una administración directa en la consola.

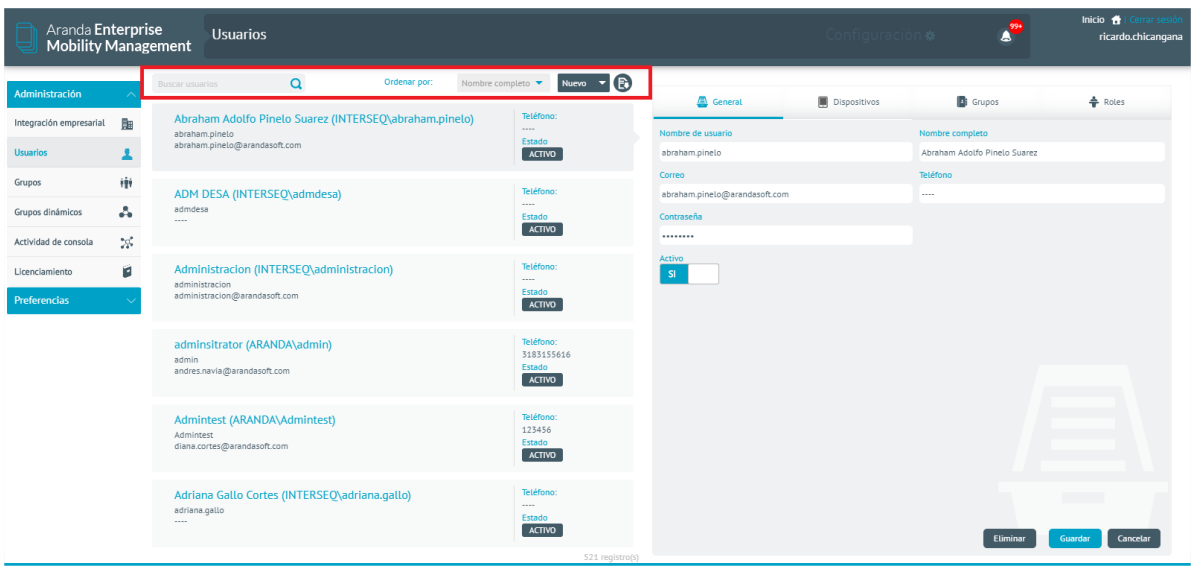
Listado de Usuarios

Al acceder a la sección de usuarios se presenta un listado paginado con scroll infinito de los usuarios existentes en el sistema.



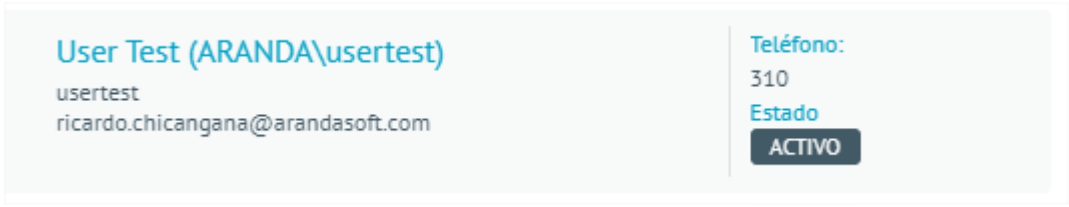
En la parte superior del listado se presentan los siguientes controles:

Controles	Descripción
Búsqueda:	Permite la búsqueda básica de usuarios, por su nombre de usuario o su nombre completo.
Ordenación:	Permite ordenar el listado por los campos; nombre completo, nombre de usuario y correo; de manera ascendente y descendente.
Nuevo:	Permite la creación e importación de nuevos usuarios.
Exportación:	Permite la exportación del listado a archivo Excel descargable.



Por cada usuario se presenta un registro en el listado que contiene la siguiente información:

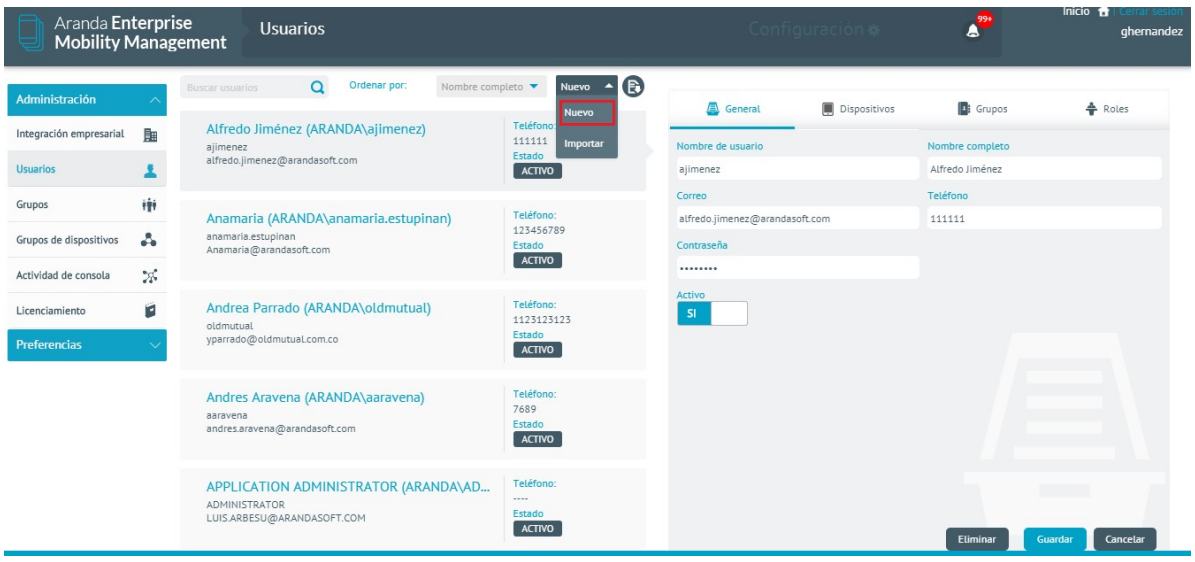
Campos	Descripción
Nombre completo:	Nombre completo del usuario
Nombre de usuario:	Nombre de usuario usado para autenticarse ante el sistema.
Correo:	Correo electrónico del usuario, usado para el envío de notificaciones del sistema.
Teléfono:	Número telefónico del usuario.
Estado:	Estado el usuario ante el sistema, puede ser Activo o Inactivo.



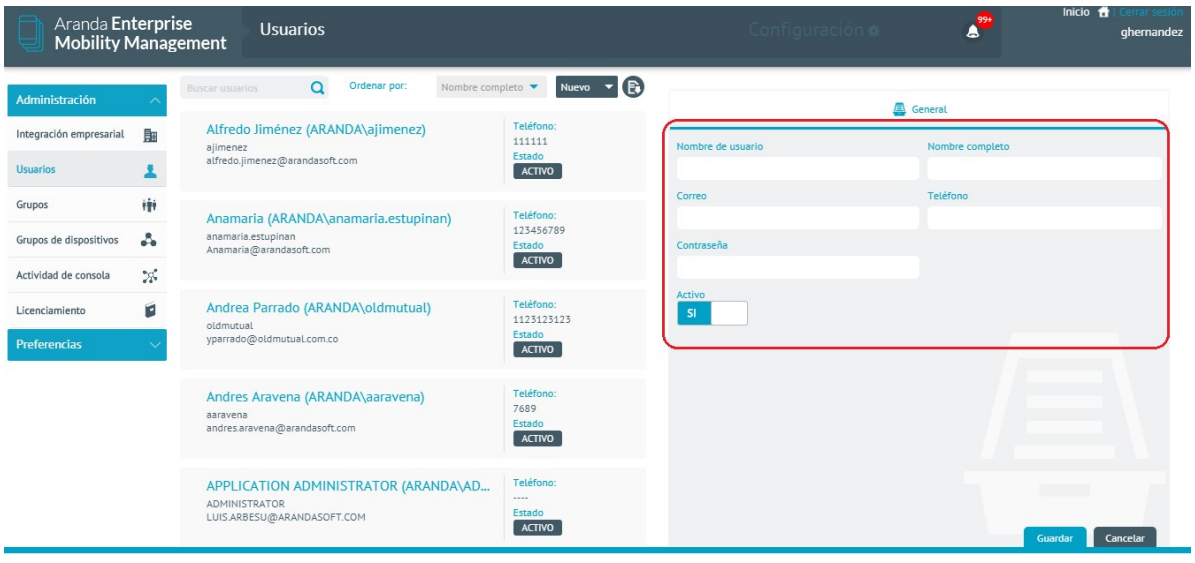
Creación de usuario nuevo

Los usuarios de consola son creados como usuarios locales y se hacen necesarios cuando estos no se obtienen del directorio activo, a este tipo se usuarios les es permitido realizar modificaciones a su información.

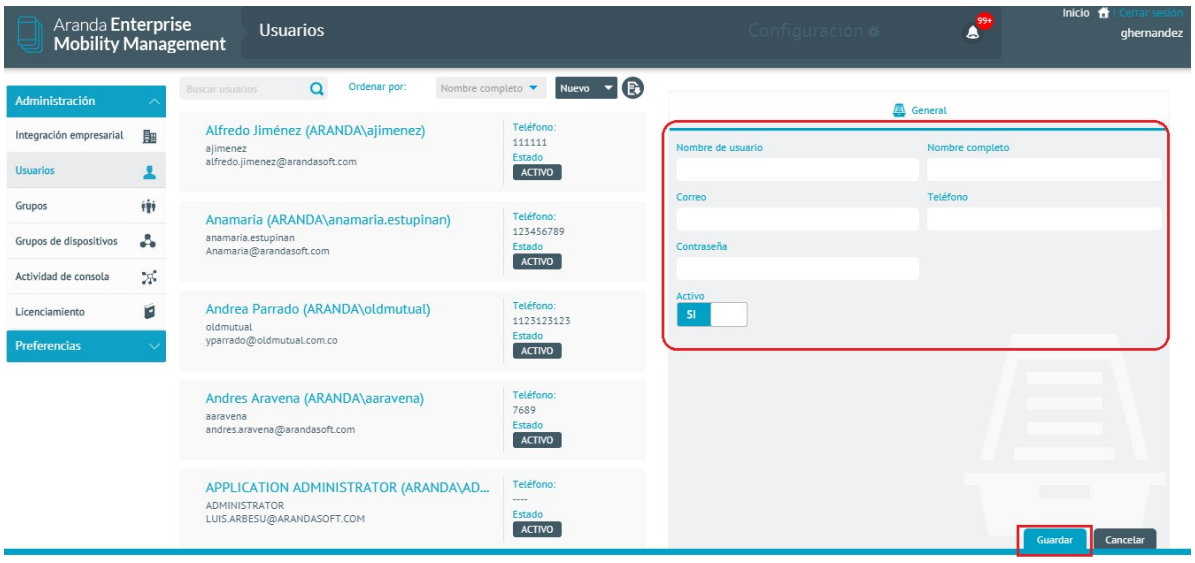
Para crear un usuario ingrese a **configuración** > luego a **usuarios** y dé clic en **Nuevo**



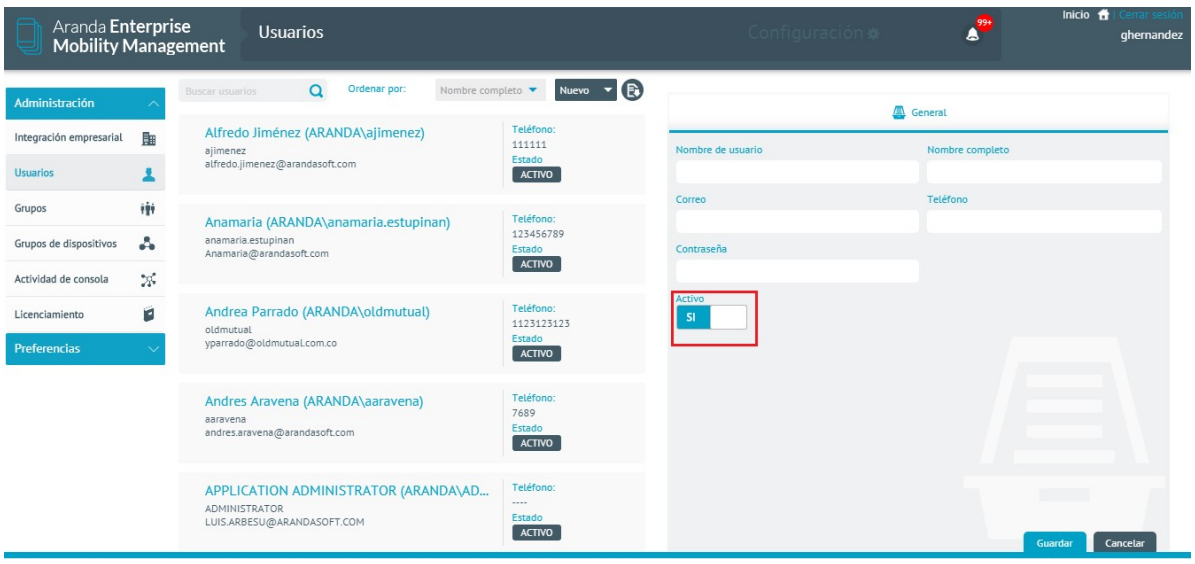
Ingrese la información requerida:



De clic en **Guardar**



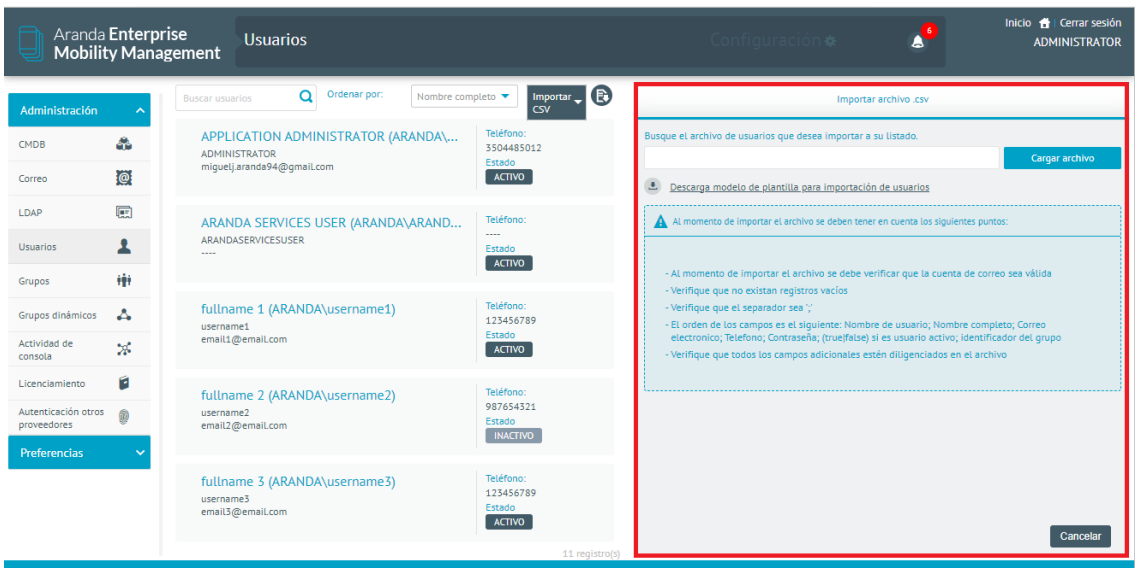
Los usuarios se pueden almacenar como activos e inactivos. (Si el usuario se encuentra inactivo no tiene interacción con ningún proceso)



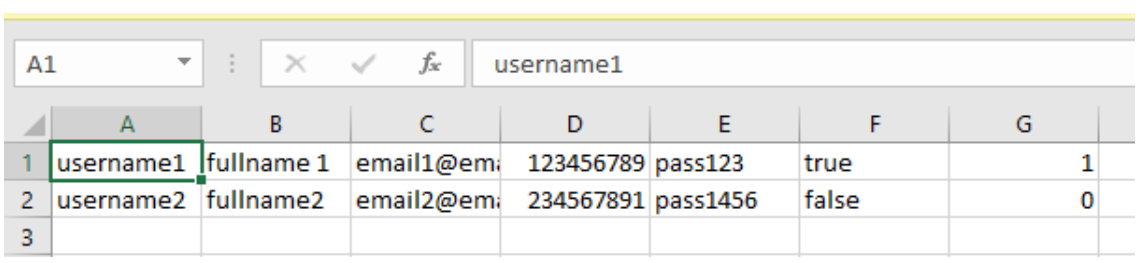
En el detalle de cada usuario se pueden encontrar las secciones de General, Dispositivos, Grupos y Roles que se describen a continuación.

Creación masiva de usuarios

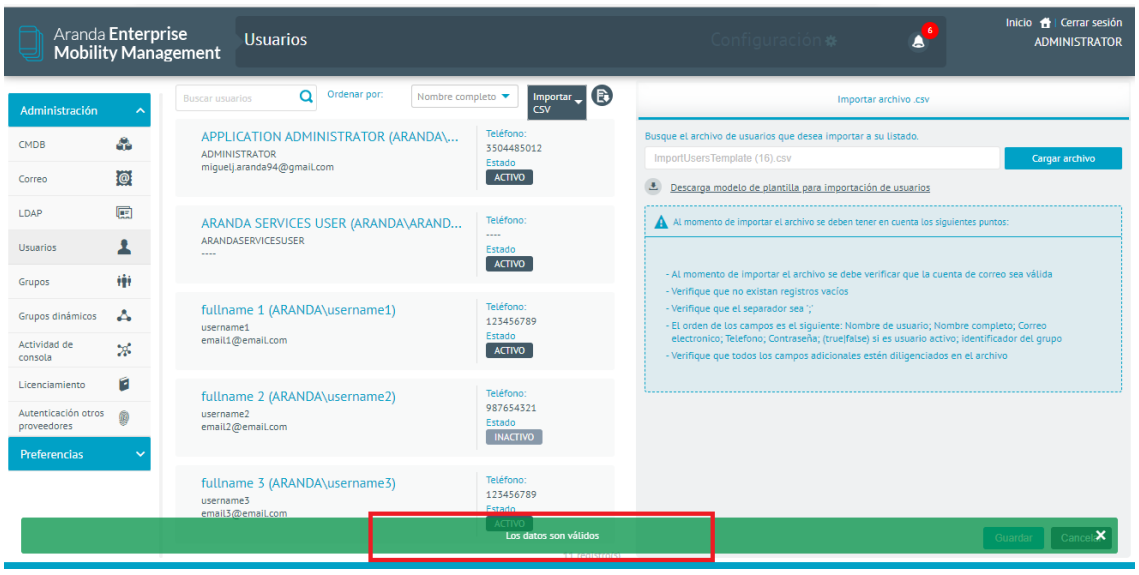
1. Para la creación masiva de usuarios, ingrese a la consola de administración de AEMM, en la sección de Administración del menú principal, seleccione la opción Usuarios; en la vista de información, seleccione el botón **Importar CSV**.



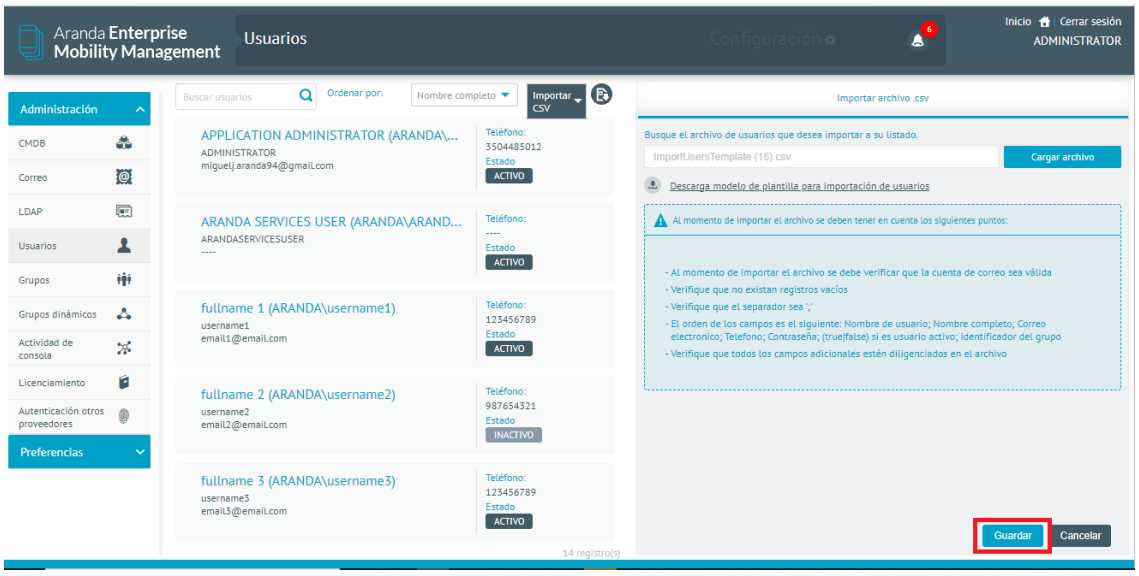
2. Esta acción descarga un archivo .csv que servirá como plantilla de guía para completar la información requerida para la importación.



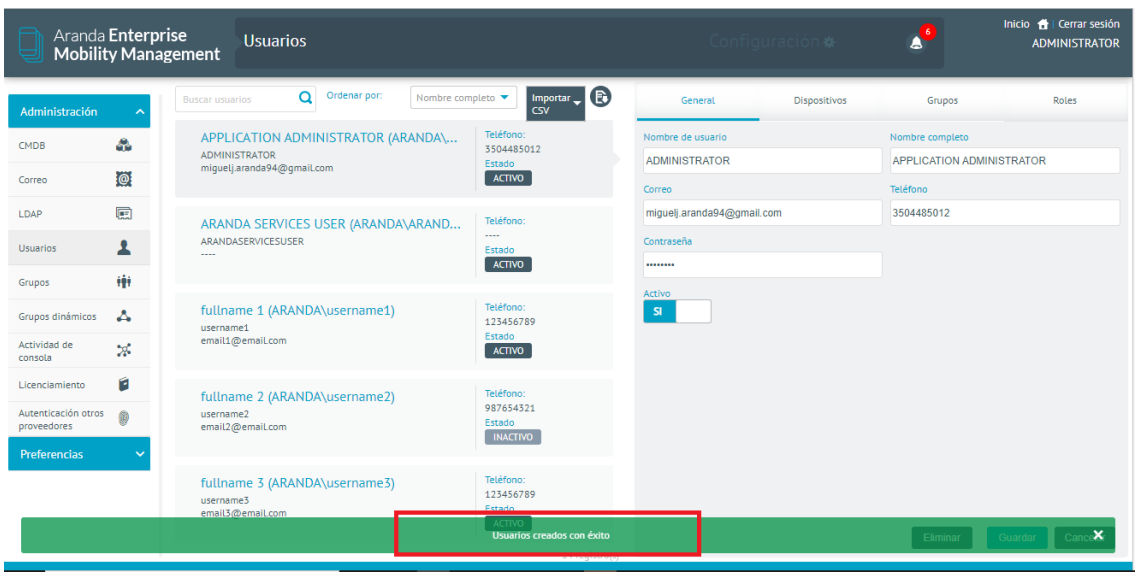
3. En la vista detalle de importar usuarios seleccione el botón Cargar Archivo para subir el archivo actualizado.



4. Después de validado el archivo haga clic en el botón guardar.

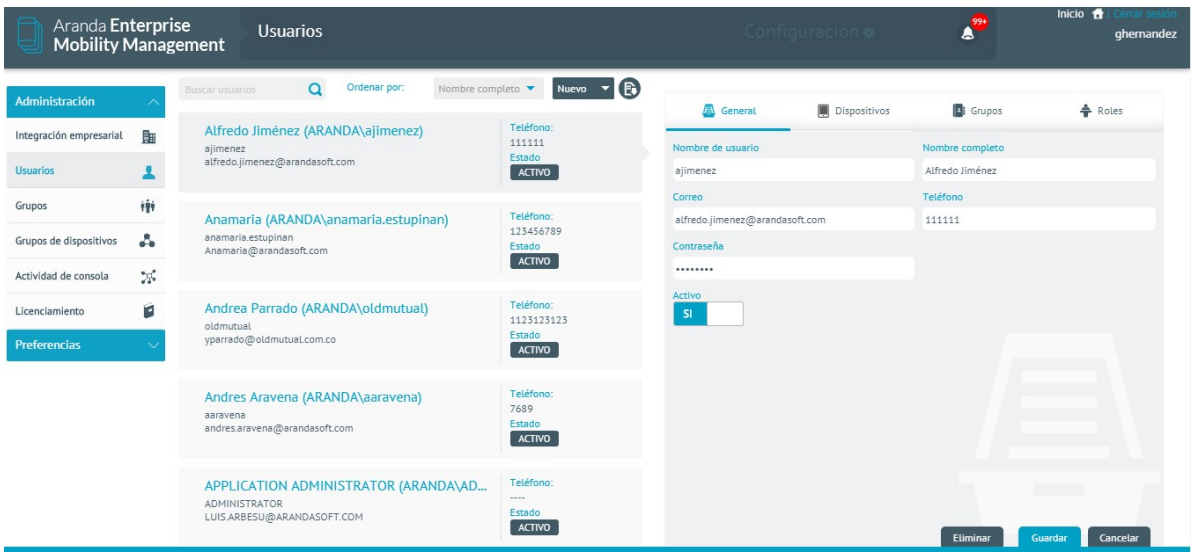


5. Al finalizar el proceso podrá visualizar un mensaje indicando el éxito del proceso.



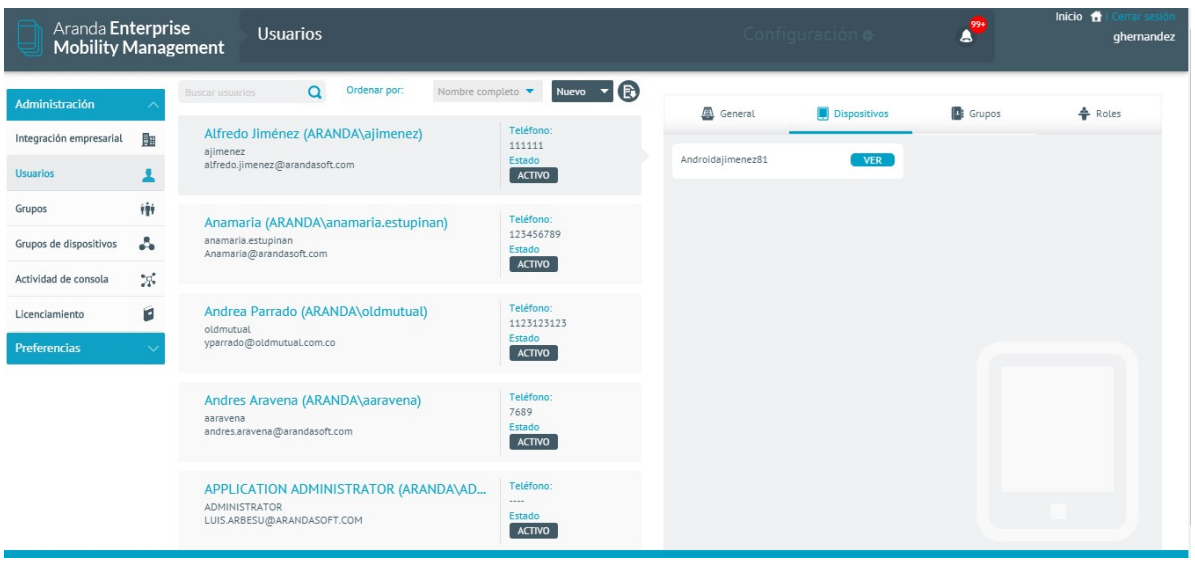
General

Se gestiona información como nombre de usuario, nombre completo, correo, teléfono, y contraseña. El usuario solo se puede eliminar si este no se encuentra asociado a grupos.



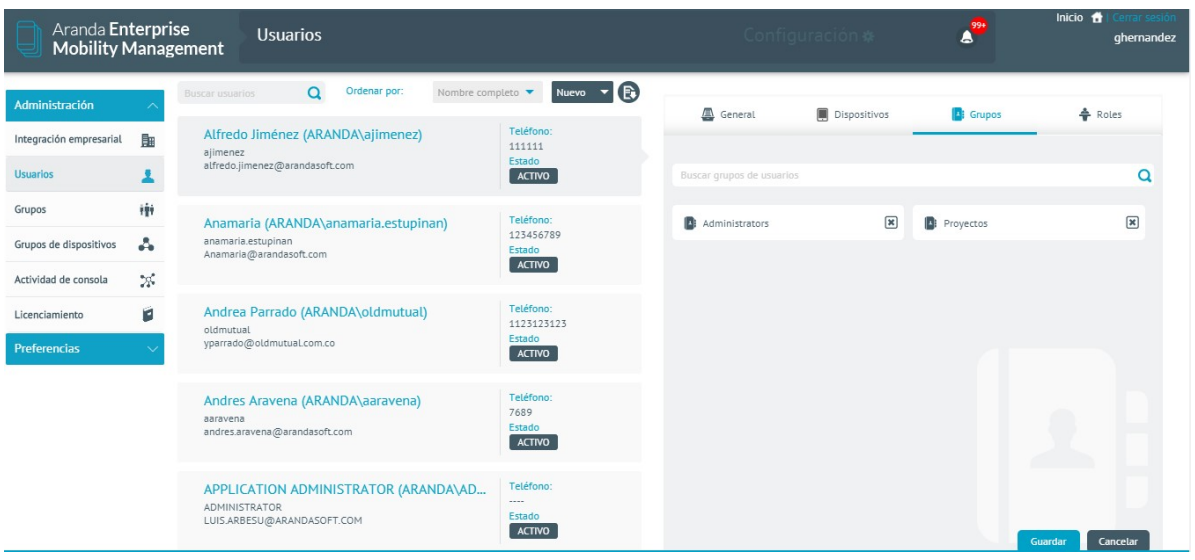
Dispositivos

Se visualizan los dispositivos que el usuario tiene vinculados.



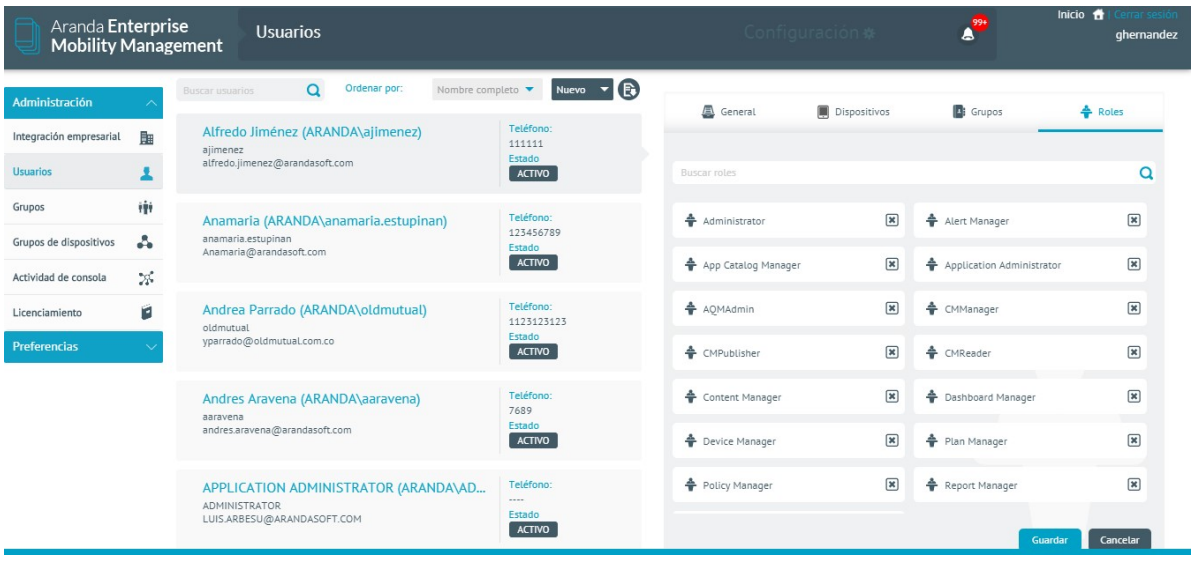
Grupos de usuarios

Contiene los grupos a los cuales se encuentra asociado el usuario.



Roles

Indica los roles o permisos que tiene el usuario para el acceso a la consola. Existen 11 tipos de roles.



Los usuarios también se pueden clasificar como usuarios locales y de directorio activo (Para más información diríjase al apartado **¡Error! No se encuentra el origen de la referencia.** Configuración del directorio empresarial).

Seguridad y control de acceso usando roles

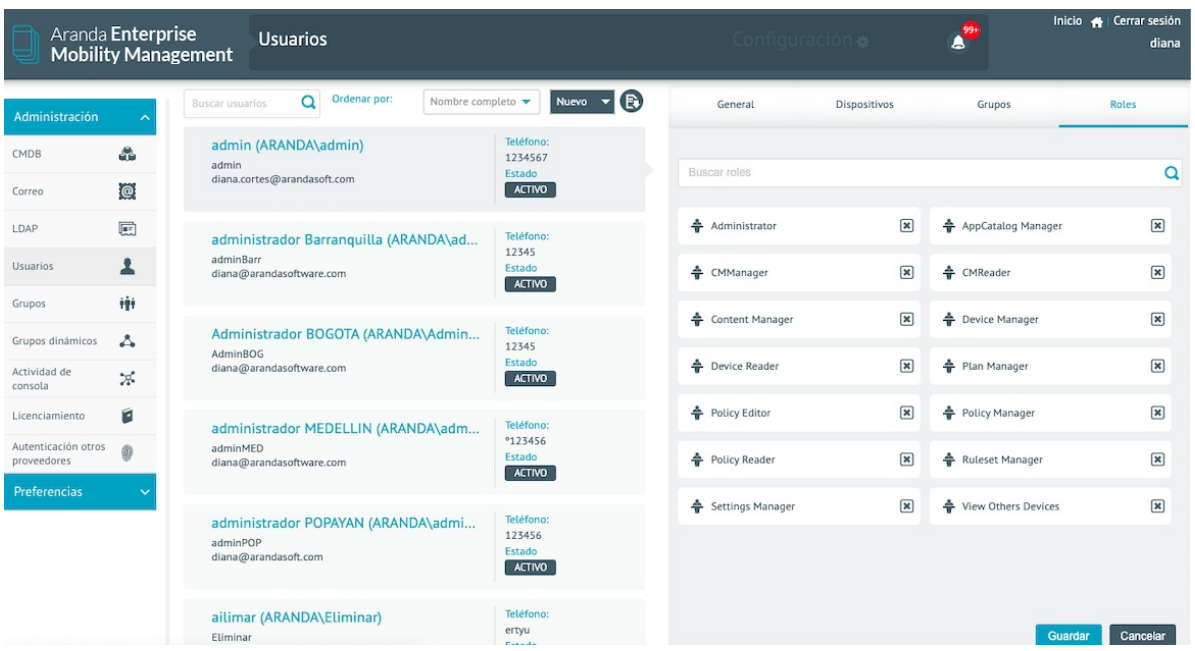
Descripción de los distintos tipos de Roles

Descripción

Para el uso y administración de la consola web se han establecido un conjunto de roles por defecto que permiten segmentar las diferentes funcionalidades disponibles dentro de la consola, creando la posibilidad de permitir o restringir el acceso a cada una de ellas. Existen 12 tipos de roles:

Roles	Descripción
Device Manager:	Gestor de dispositivos, tiene permisos para ver, editar y enviar comandos a dispositivos.
Device Reader:	Visualizador de dispositivos, tiene permisos para ver información sobre dispositivos.
Policy Manager:	Gestor de Políticas, tiene permisos para crear, ver, editar, eliminar y aplicar políticas.
Policy Editor:	Editor de políticas, tiene permisos para ver y editar políticas.
Policy Reader:	Visualizador de Políticas, tiene permisos para ver información de políticas.
Ruleset Manager:	Gestor de conjuntos de reglas, tiene permisos para crear, ver, editar y eliminar conjuntos de reglas.
AppCatalog Manager:	Gestor de catálogo de aplicaciones, tiene permisos para importar, ver y eliminar aplicaciones del catálogo.
Content Manager:	Gestor de contenidos, tiene permisos para crear, ver, editar y eliminar contenidos.
Plan Manager:	Gestor de planes de consumo, tiene permisos para crear, ver, editar, eliminar y aplicar planes de consumo.
Settings Manager:	Gestor de configuraciones, tiene permisos para editar y aplicar configuraciones del sistema.
Administrator:	Administrador general de la aplicación, tiene todos los permisos de los roles anteriores.
View Others Devices:	Permiso que permite al usuario visualizar todos los dispositivos o únicamente al grupo asociado; con este rol puede listar todos los dispositivos asociados al grupo/usuario o segmentar la visualización de la data si es requerida, aplicando acciones de administración específicas a cada uno de ellos. Para hacer uso de este rol, consulte la *Configuración de View Other Devices*.

Cada rol tiene asignado un conjunto de permisos que restringen o permiten el acceso a cada funcionalidad, la forma de asociar estos comportamientos a los usuarios de la plataforma es a través de la relación que se puede establecer entre los usuarios y los roles, o entre los roles y los grupos de usuarios (los cuales a su vez están integrados por usuarios que heredan los roles del grupo o grupos al que pertenecen).

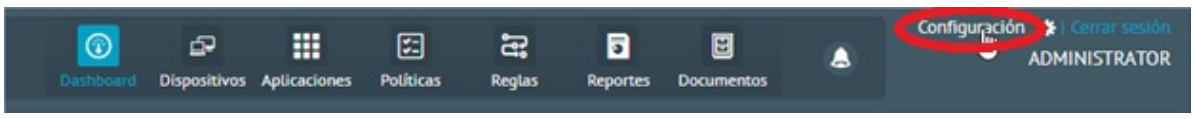


Para la asignación o modificación de los roles que un usuario tiene existen 2 formas:

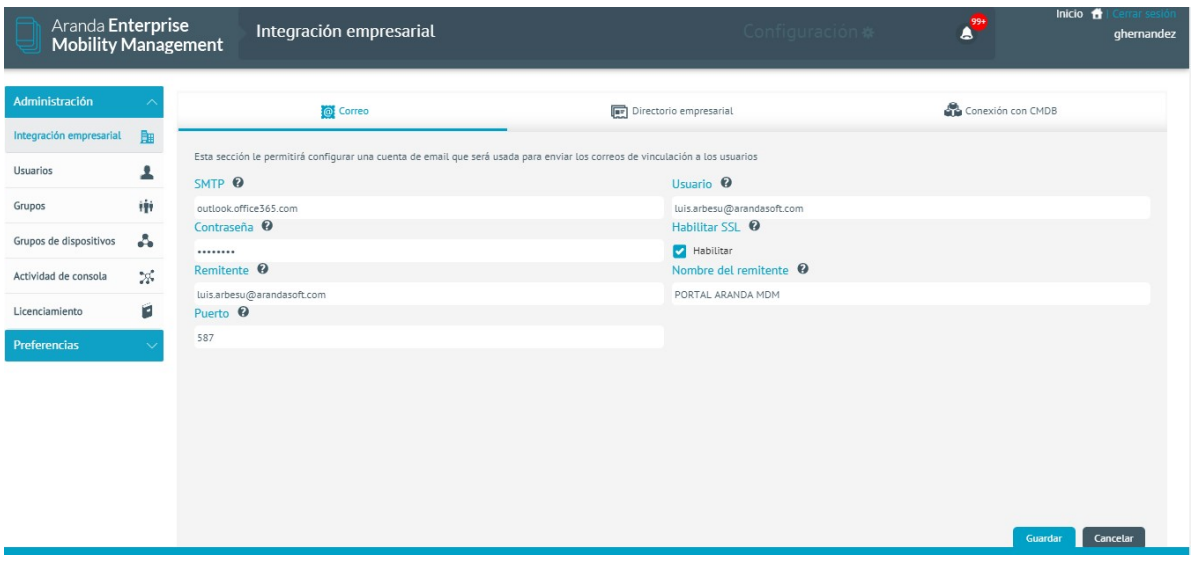
Asígnelos al usuario directamente o asígnelos a un grupo de usuarios y haga que el usuario pertenezca al grupo.

Asignación de roles a un usuario

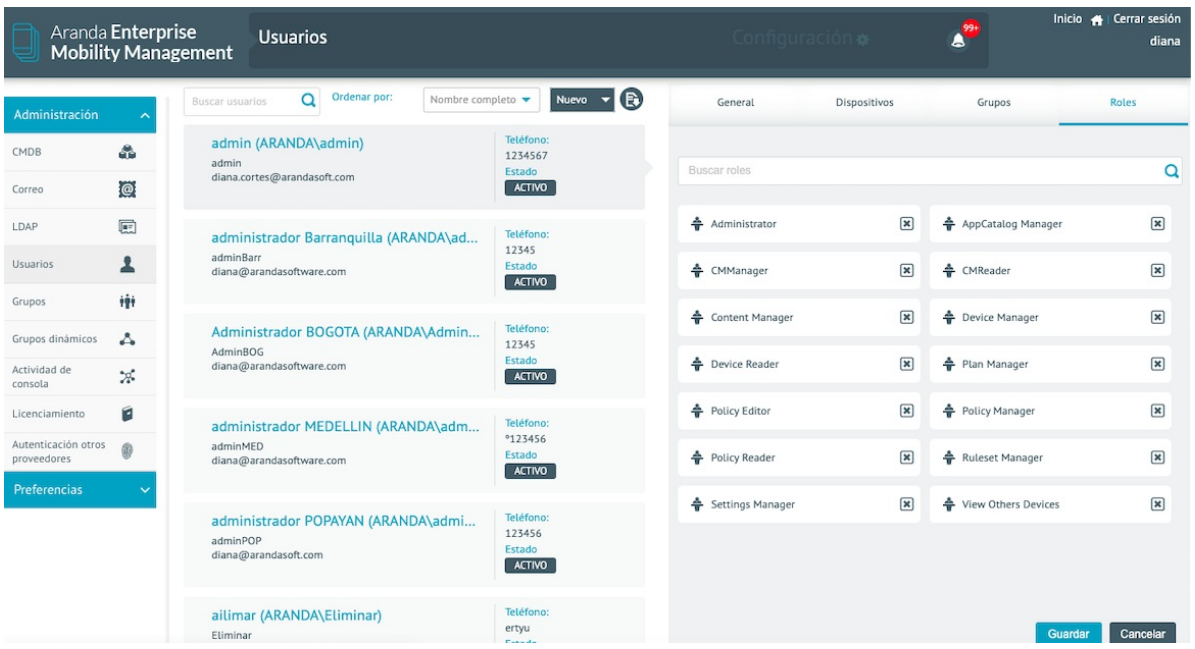
Ingrese a la sección de **configuración** en la parte superior derecha de la consola.



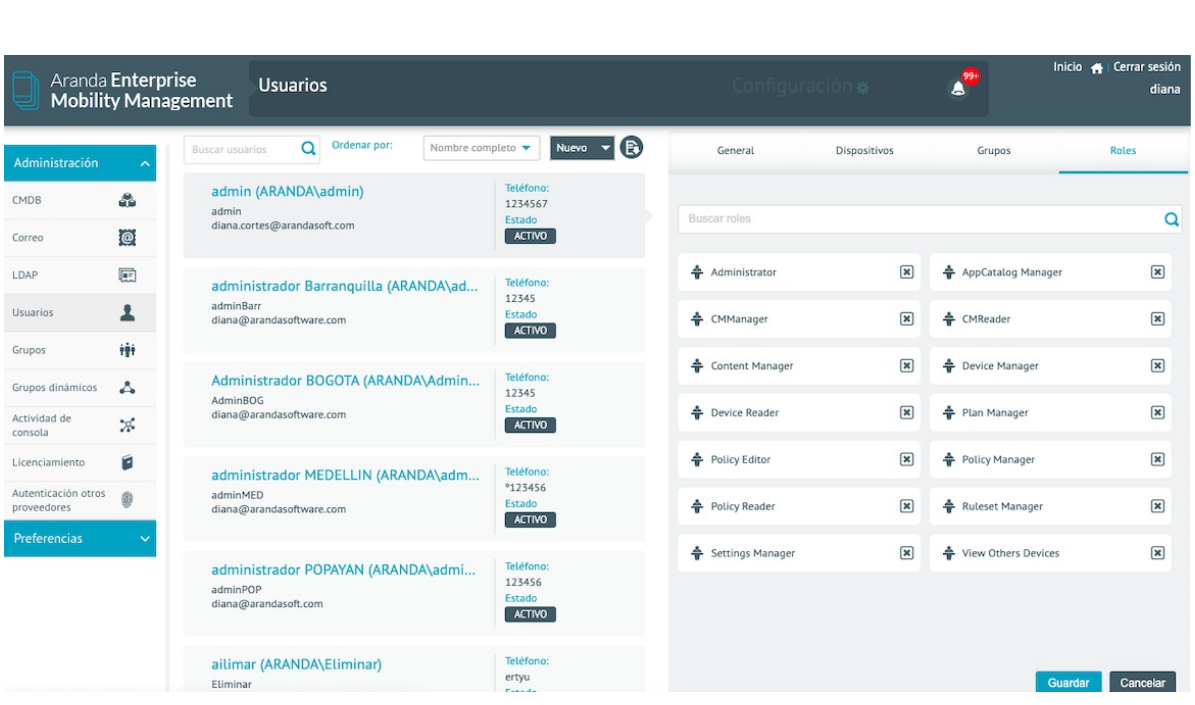
Luego ingrese a la sección **General** desde el menú lzquierdo y posteriormente a **usuarios**.



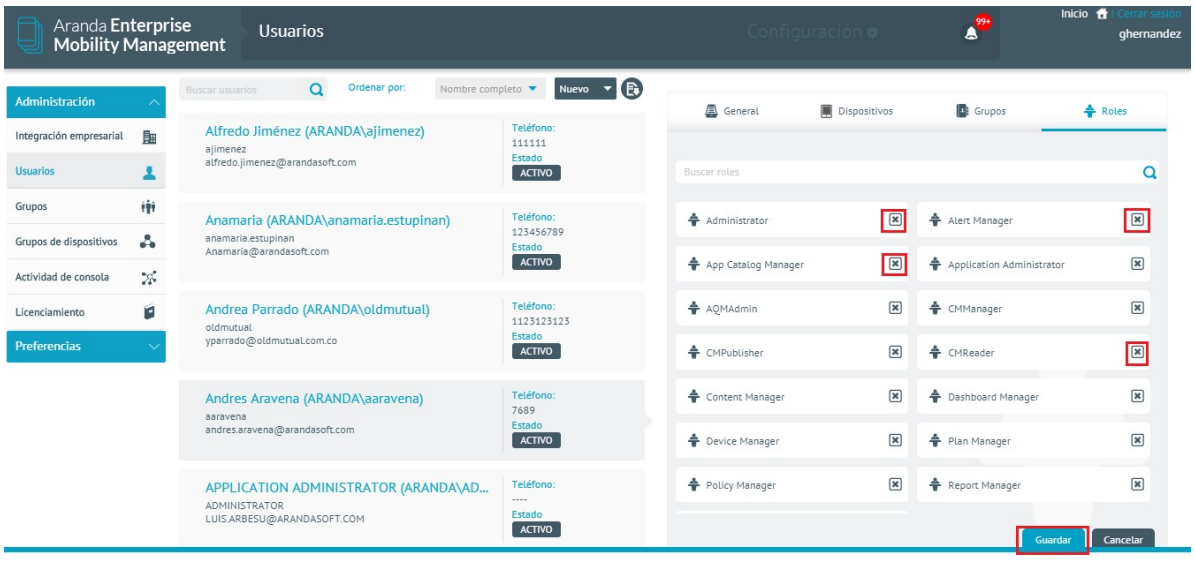
Seleccione el usuario dando clic en el listado de usuarios, si es necesario se puede buscar u ordenar el listado de usuarios para facilitar la ubicación del usuario al que se le quiere asignar los roles, luego de clic en la pestaña **roles** del panel derecho.



En la caja de búsqueda se puede ingresar el texto de búsqueda para obtener el rol que se va a asignar al usuario, repita este procedimiento por cada rol y luego de clic en el botón **Guardar**.



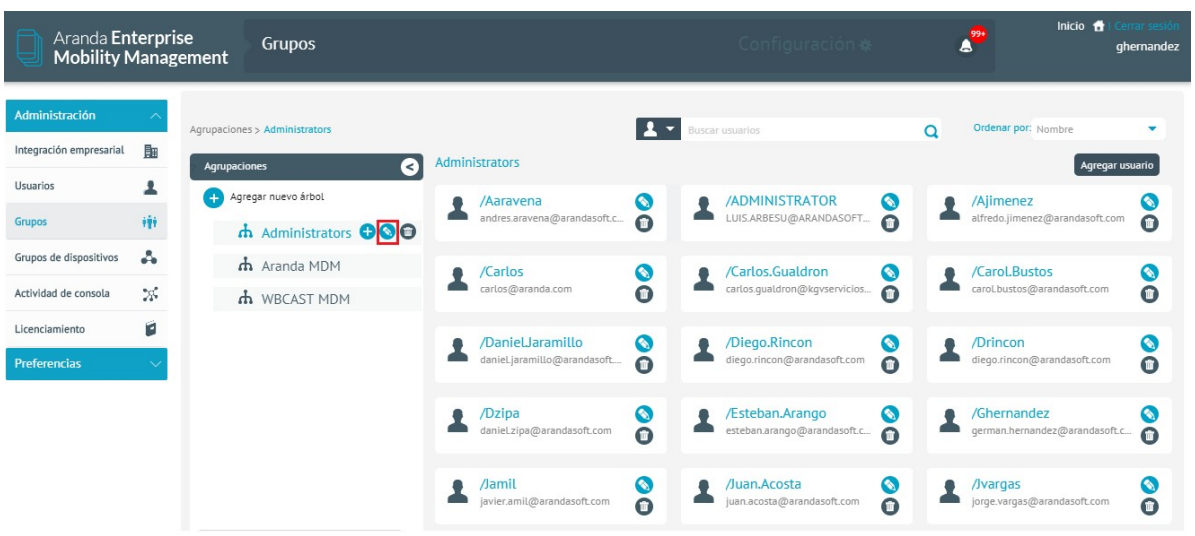
Para quitar un rol a un usuario, este se puede eliminar dando clic en el icono derecho de cada rol asociado al usuario y luego dando clic en el botón **Guardar** del panel derecho.



Asignación de roles a un grupo de usuarios

La asignación de roles a un grupo de usuarios se realiza desde la sección de grupos de usuarios de la interfaz de configuración. Los usuarios que pertenecen a un grupo de usuarios heredan sus roles (incluso se visualizan para el usuario en la pestaña **roles** de forma aditiva con los roles que se han asociado directamente al usuario) sin embargo los roles de un grupo no son heredados por los sub-grupos contenidos en él.

Seleccione el grupo al cual se le van a agregar los roles y de clic en **Editar.**

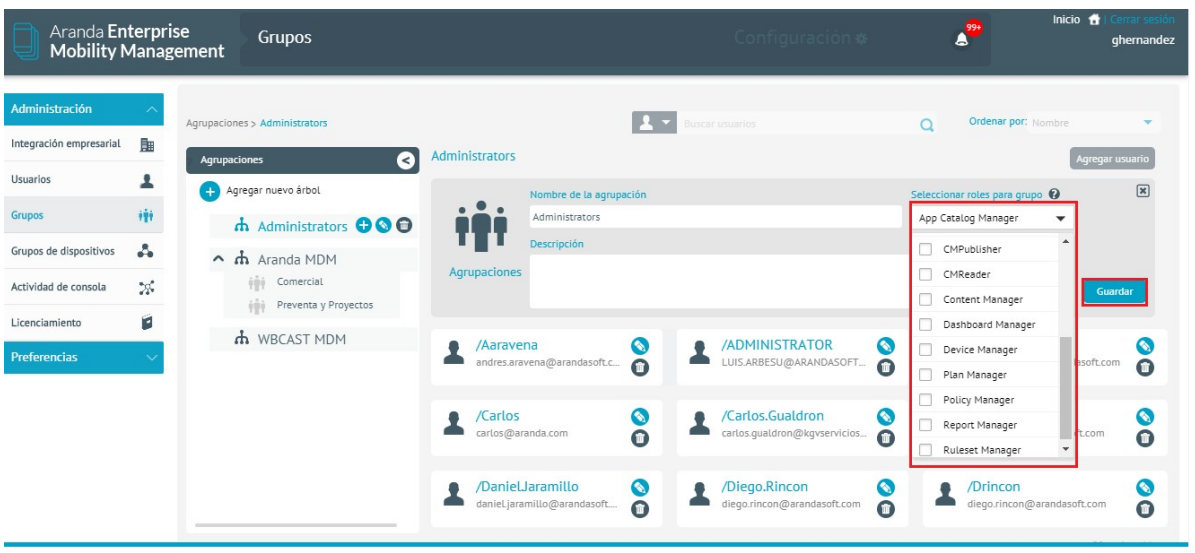


Seleccione los roles que se van a agregar y de clic en **Guardar.**

Para retirarle un rol a un grupo debe dar clic en **Editar.**

Quite el Check de selección de la casilla del rol que desea retirar y luego de clic en **Guardar.**

⚐ **Nota:** La acción de asignación de roles a un grupo solo es posible en grupos creados en la consola AEMM. Los grupos importados en la sincronización con directorio activo no podrán gestionar roles. El administrador debe tener en cuenta que al crear un grupo por defecto, el check del rol View other divices, es para visualizar la todos los datos.



Configuración de View Others Devices

Descripción: El administrador de la consola podrá configurar la visualización de los dispositivos que el usuario puede gestionar desde AEMM. Podrá configurar restricciones para desactivar la visualización completa de todos los dispositivos, segmentar la visualización de acuerdo a la necesidad, así como otorgar el permiso total de visualización de los dispositivos vinculados. A continuación se describe el paso a paso:

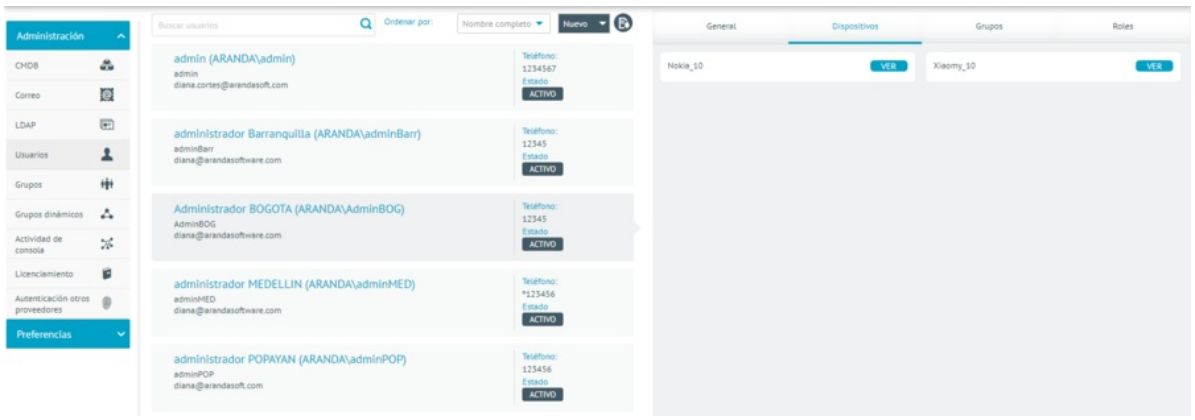
- **Configuración a usuarios por grupos**:

Si el administrador requiere que el usuario de consola visualice todos los dispositivos, debe tener en cuenta:

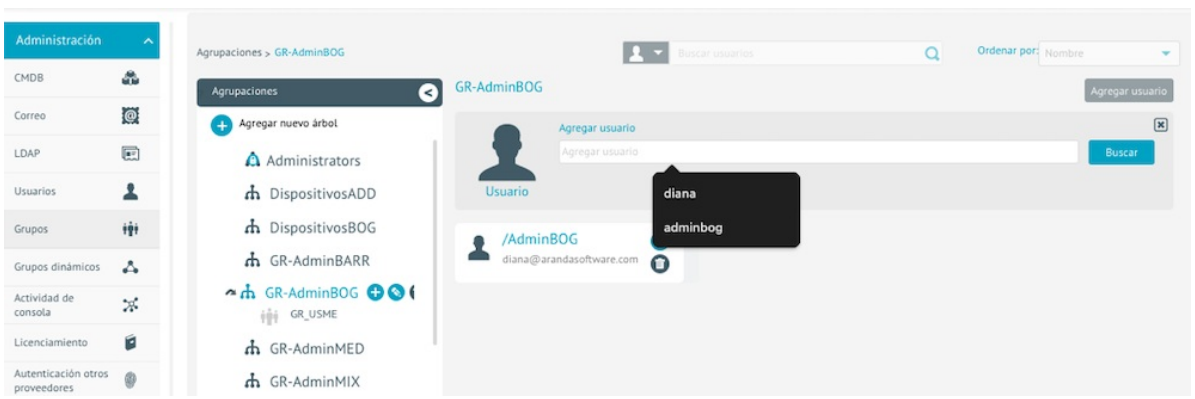
1. Al crear un grupo, desactive el rol "View Other Devices"
2. Asocie al grupo los usuarios y/o dispositivos a los que tendrá acceso de administrar; así el usuario solo podrá realizar acciones de gestión sobre los dispositivos configurados:

- **Asociación por usuario**: Al asociar un usuario al grupo, automáticamente, los dispositivos vinculados o asociados al usuario, hacen parte del grupo.

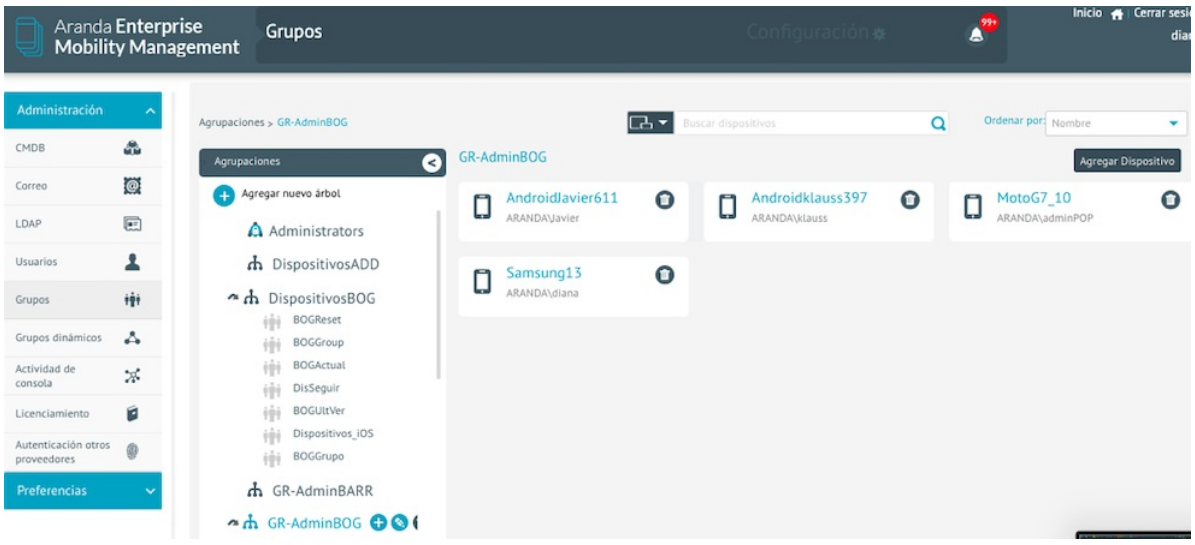
1. En el menú usuarios, al seleccionar un usuario, en la sección Dispositivos podrá visualizar los dispositivos vinculados al usuario y/o que están bajo su responsabilidad.

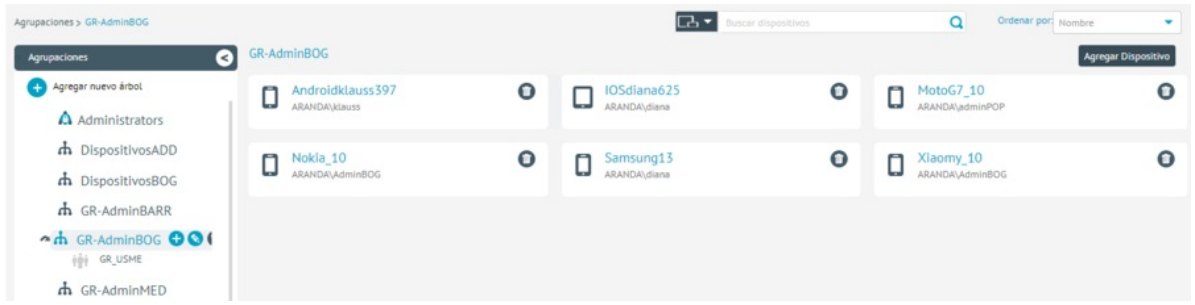


1. Asociar el usuario a un grupo para restringir la visualización de la data:

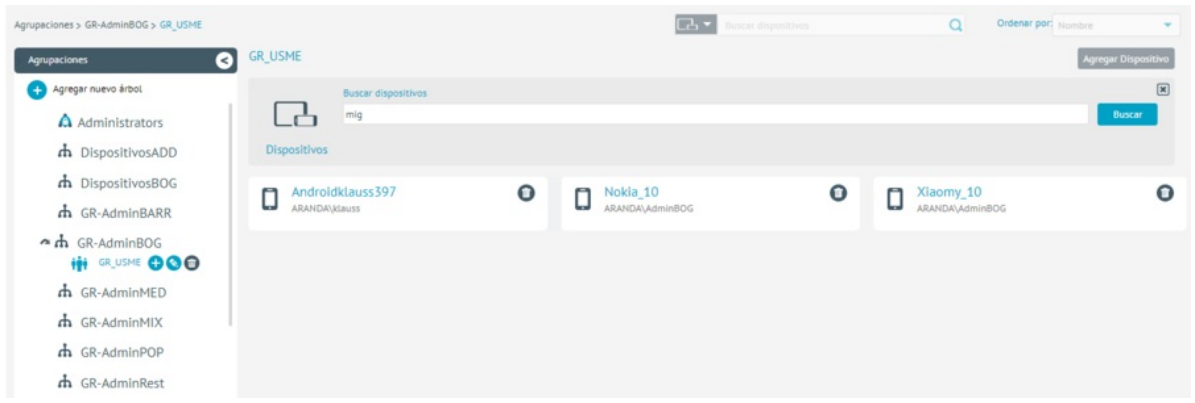


Por defecto se asocia al grupo, los dispositivos que están bajo la responsabilidad del usuario es decir:





3- Asociación por dispositivo: Se asocia directamente el dispositivo al grupo.



- Configuración a usuarios sin restricción:

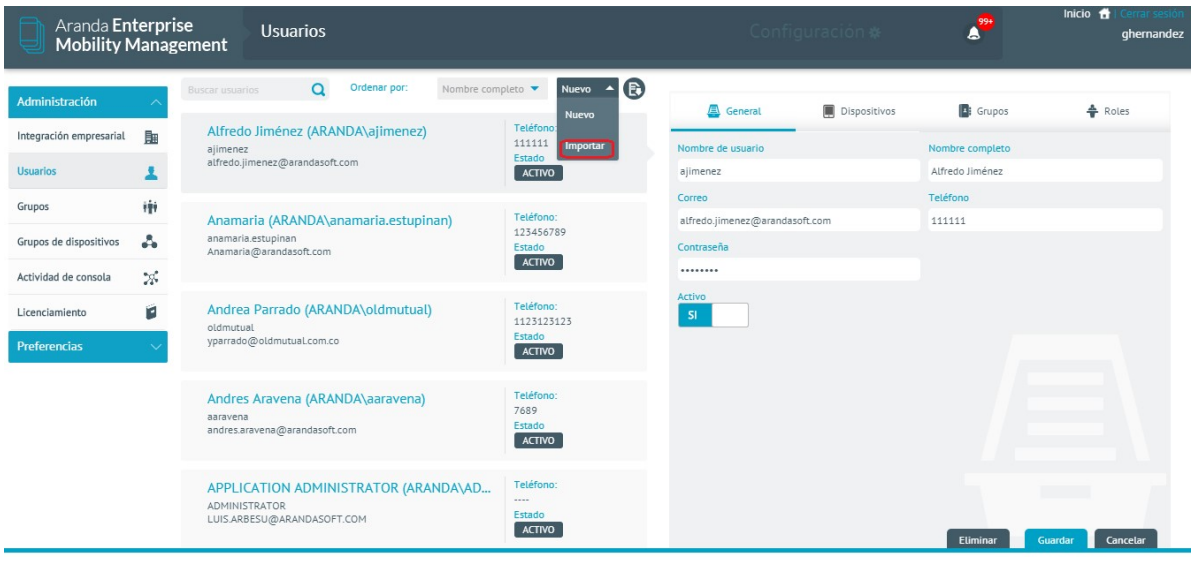
Si el administador requiere que el usuario de consola visualice todos los dispositivos, se debe tener presente:

1. Al crear un grupo, el sistema automáticamente activa el rol "View Others Devices"
2. Al crear un usuario y asociar rol de administrador, asocia todos los roles para visualizar y realizar acciones.

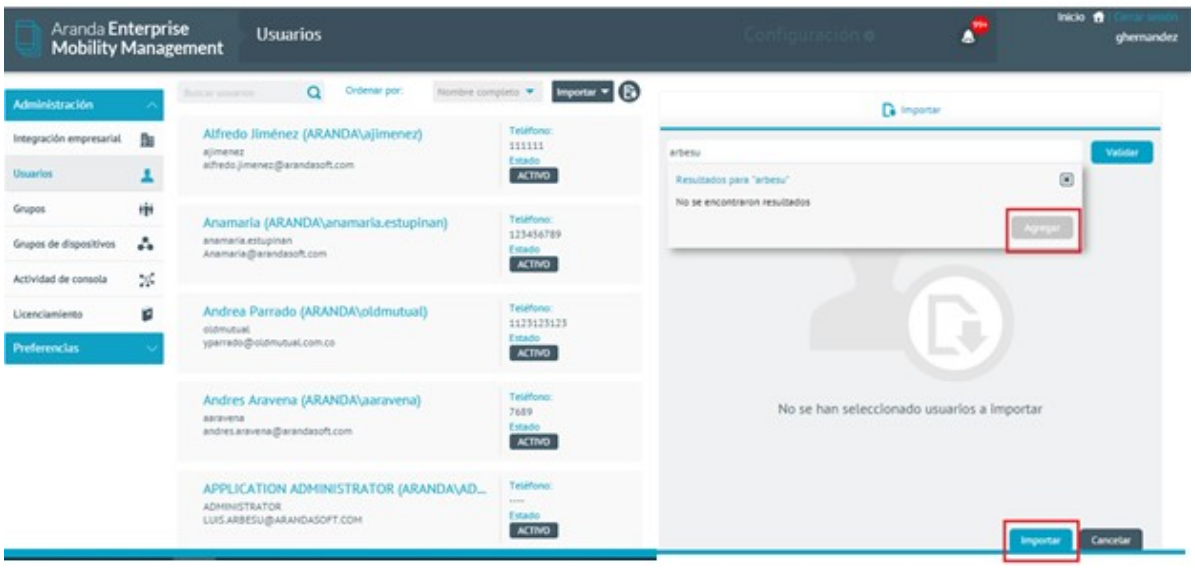
Roles [Item permisos]

Importación de usuarios

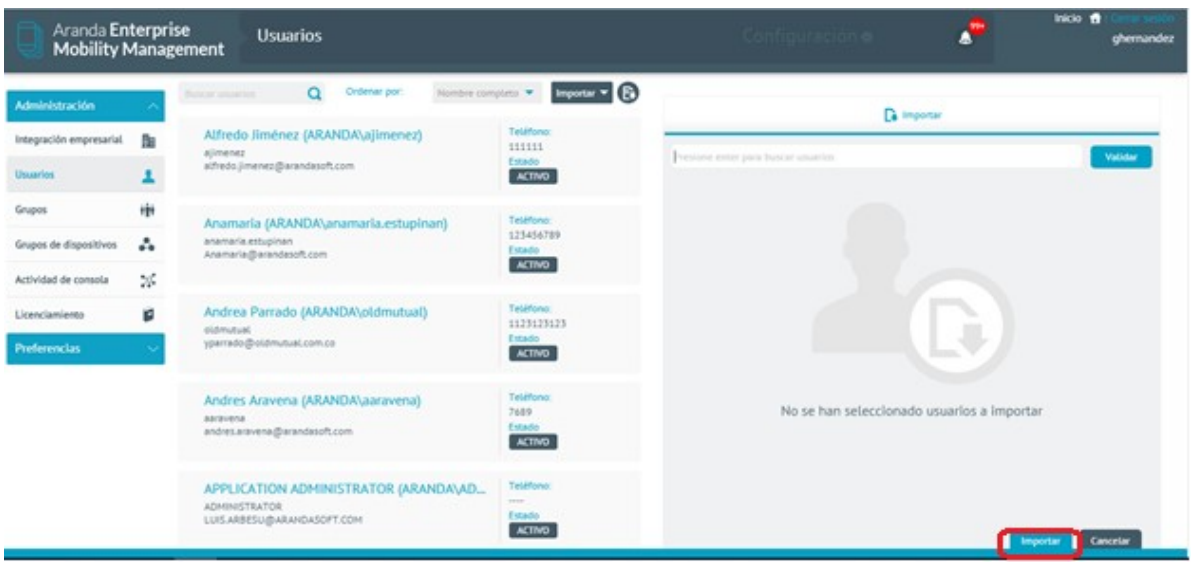
Ingrese a **Usuarios** y seleccione **Importar**



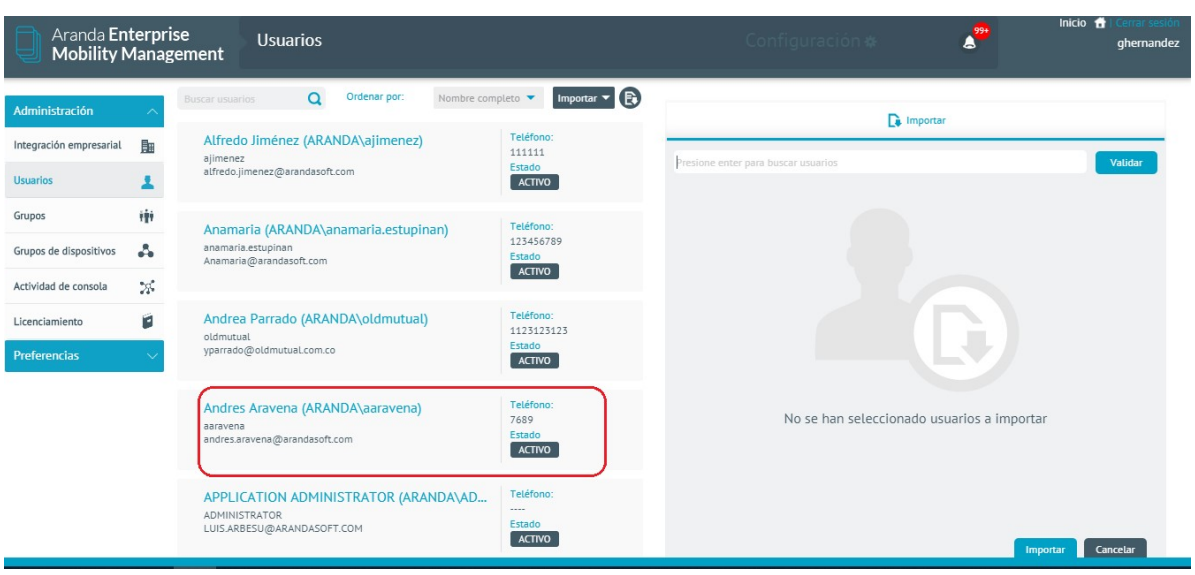
Ingrese y seleccione el nombre de usuario (los usuarios que ya se encuentran importados están acompañados de un recuadro en la imagen).



De clic en la opción **Importar**.



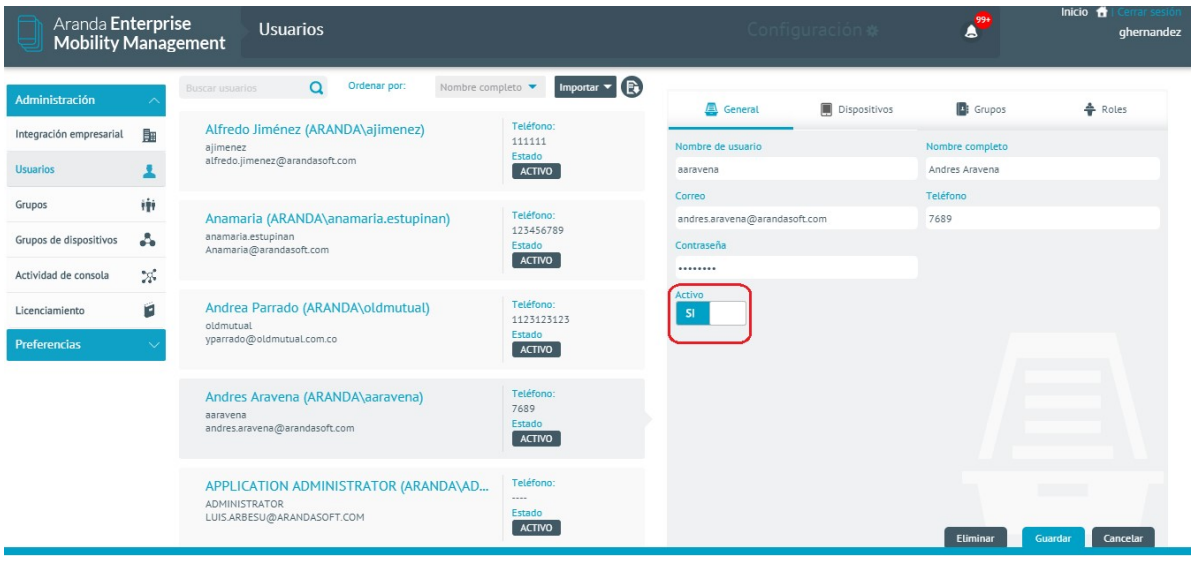
El usuario se importa exitosamente.



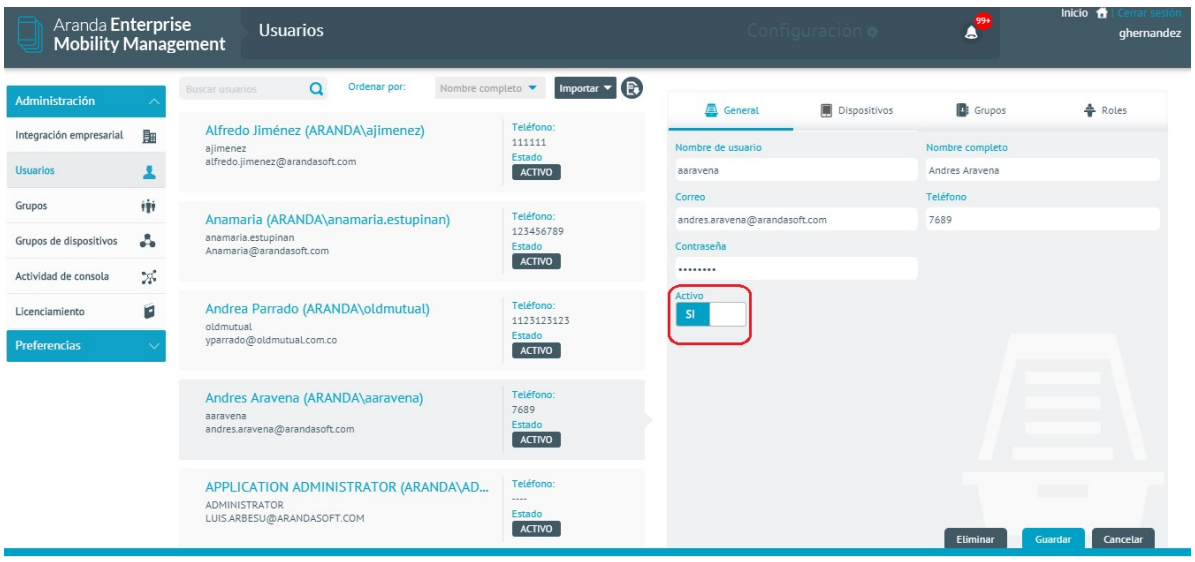
Estado de usuarios

Un usuario o grupo puede tener dos estados (Activo e inactivo), si el usuario o grupo se encuentra inactivo no tiene interacción con ningún proceso en AEMM.

Usuario inactivo: Si el usuario pertenece al Directorio Activo no es posible realizar cambios en el estado.



Si el usuario se obtiene como usuario local, podrá cambiar su estado.

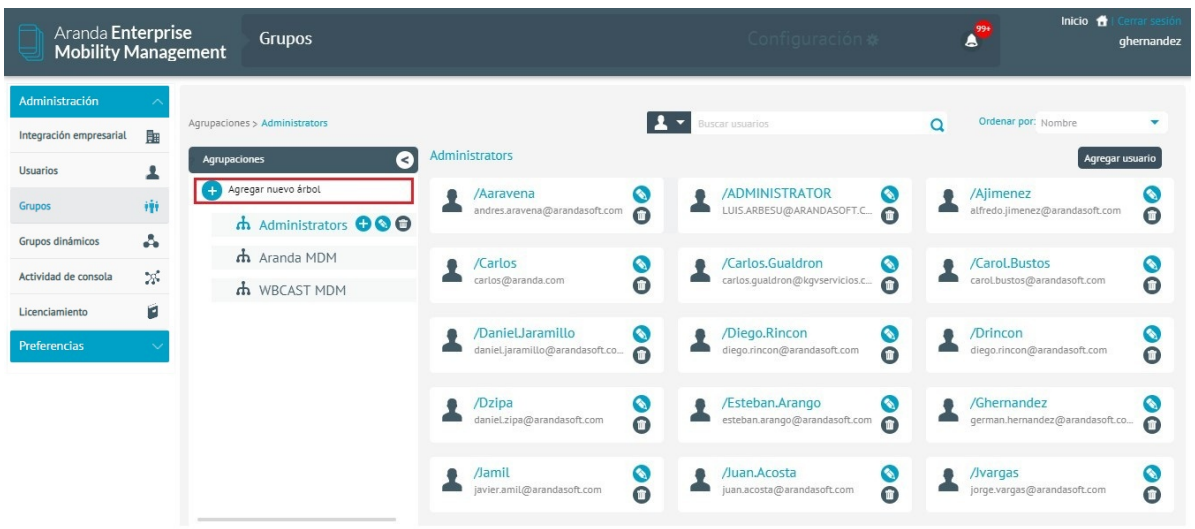


Grupos

Creación de Grupos

Los grupos de consola se crean como grupos locales y se hacen necesarios cuando estos no se obtienen del Directorio Activo, a este tipo de grupos se les es permitido realizar modificaciones a su información, así como también crear sub-grupos (Nodos) dentro de ellos, ya sean un grupo principal (Árbol) o Nodos. Dentro de estos grupos se pueden asociar usuarios y/o dispositivos.

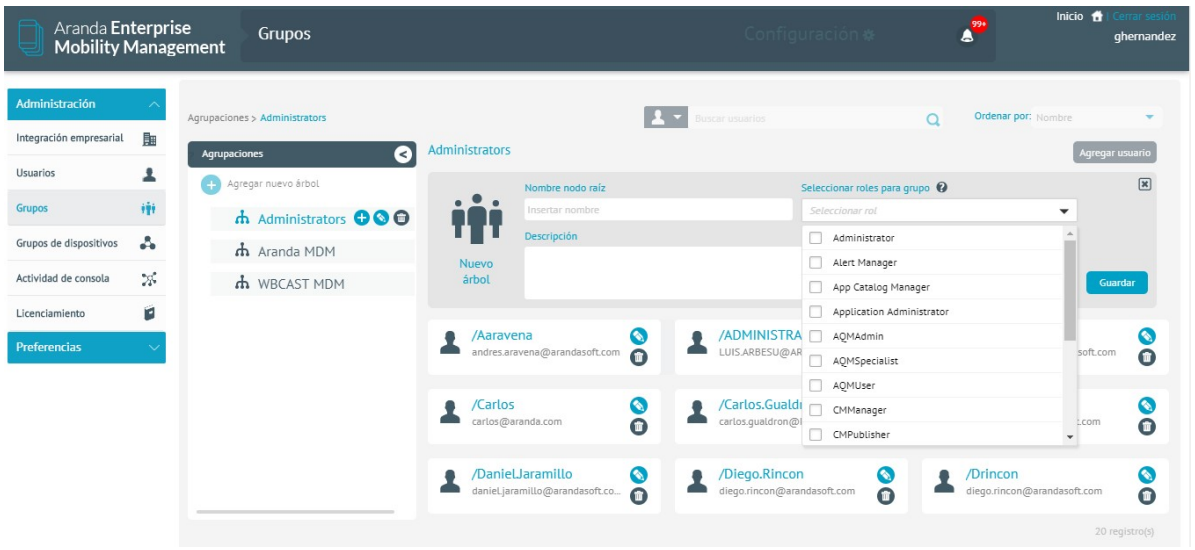
Para crear un grupo, ingrese a la consola de inicio de AEMM, en la sección de **Administración** del menú principal, seleccione la opción **Grupos**. En la vista de información, en la sección de Agrupaciones haga clic en la opción **Agregar nuevo árbol.**



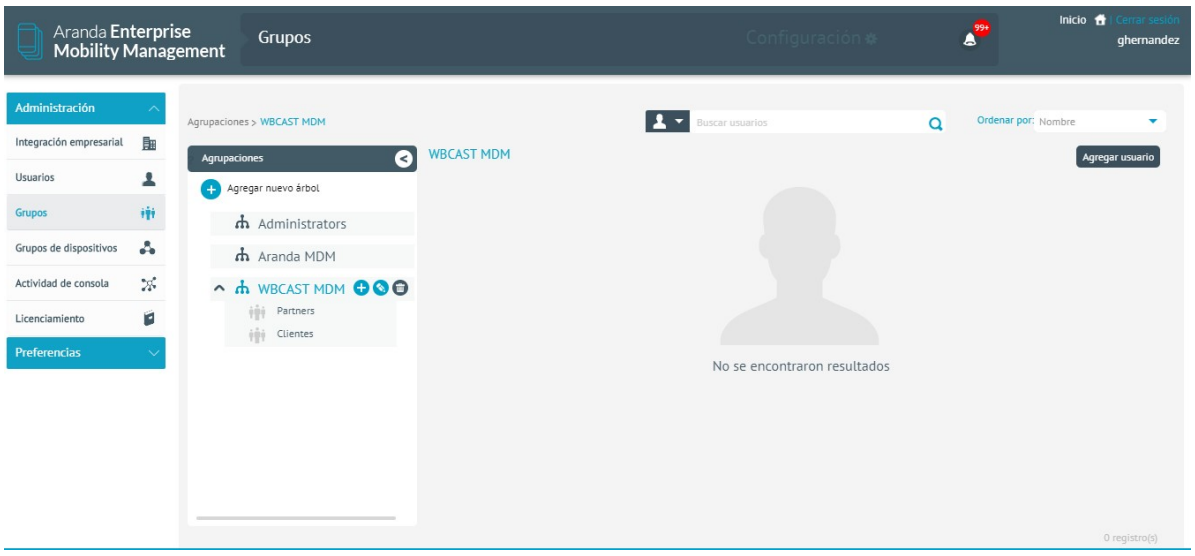
Ingrese la información requerida, si desea puede asociarles roles a los grupos o si no, lo puede hacer posteriormente.

Para tener más detalles de los roles Ver *Descripción de los distintos tipos de Roles*.

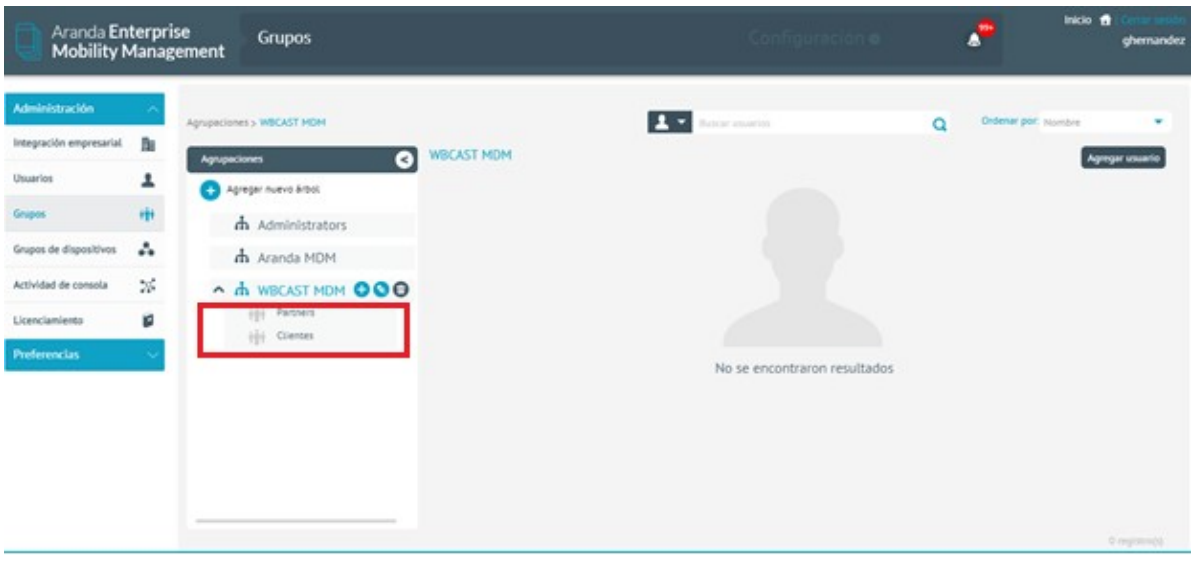
- Device Manager.
- Device Reader.
- Policy Managers.
- Policy Editor.
- Policy Reader.
- Ruleset Manager.
- AppCatalog Manager.
- Content Manager.
- Plan Manager.
- Settings Manager.
- Administrator.
- View Others Devices.



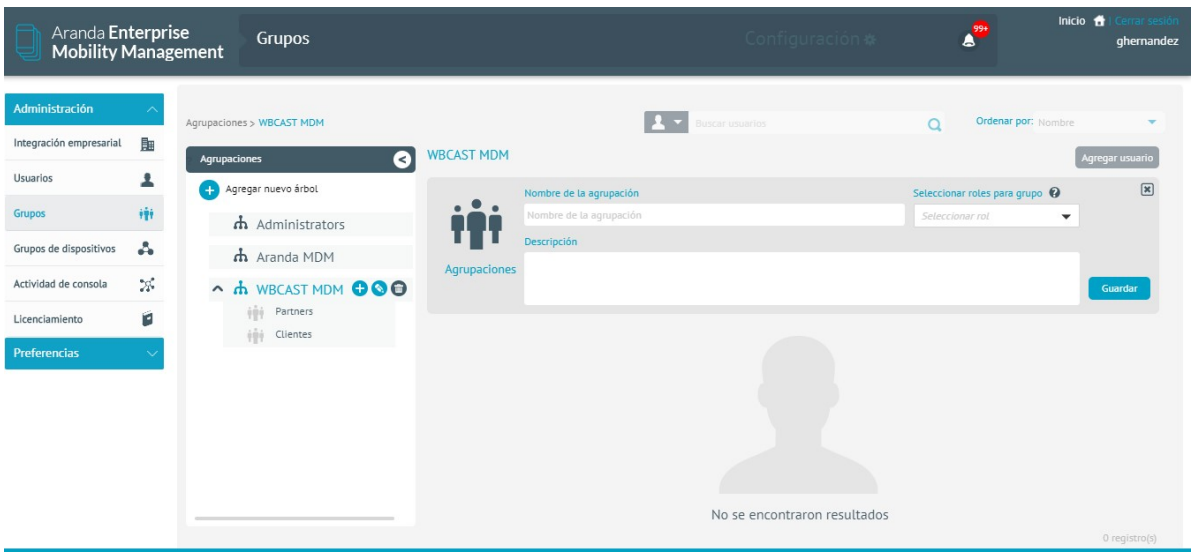
Seleccione **Guardar**.



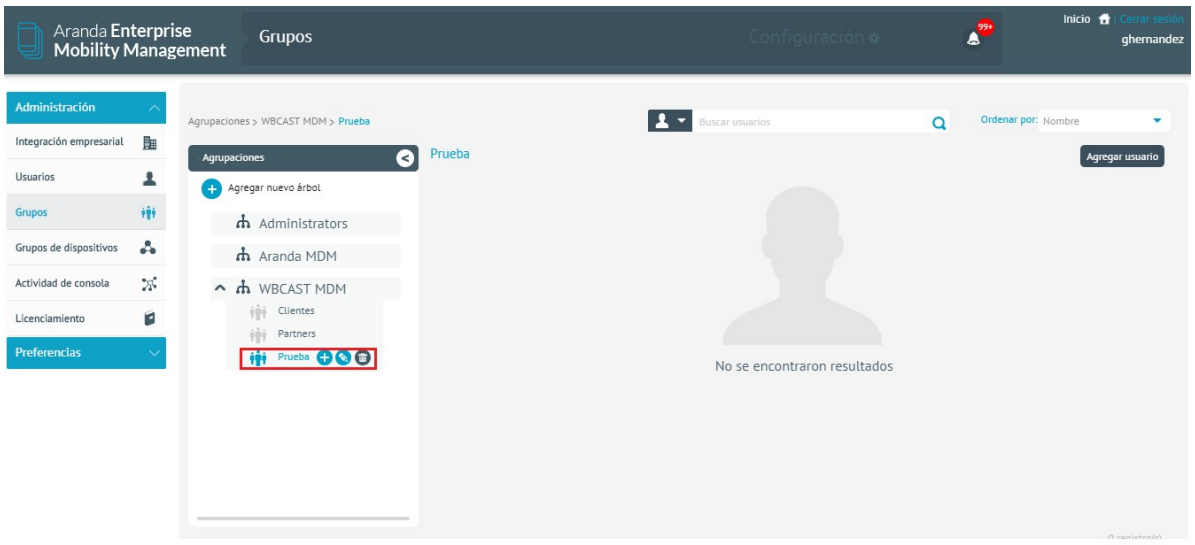
Para la creación de un sub-grupo (Nodo) debe ubicarse en el grupo que lo va a contener y dar clic en **Agregar agrupación.**



Ingrese la información requerida.

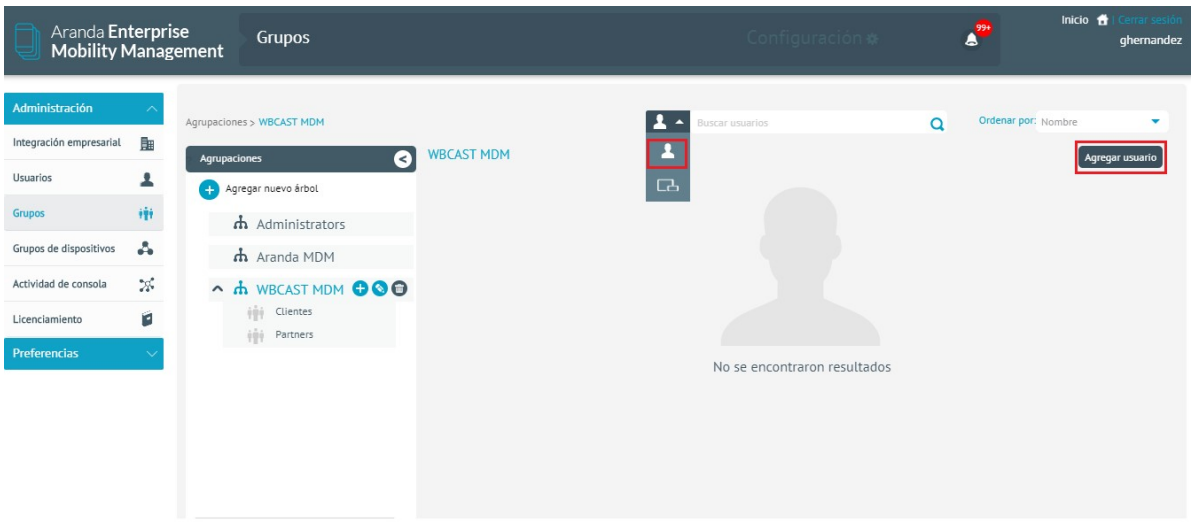


Ahora de clic en **guardar**.

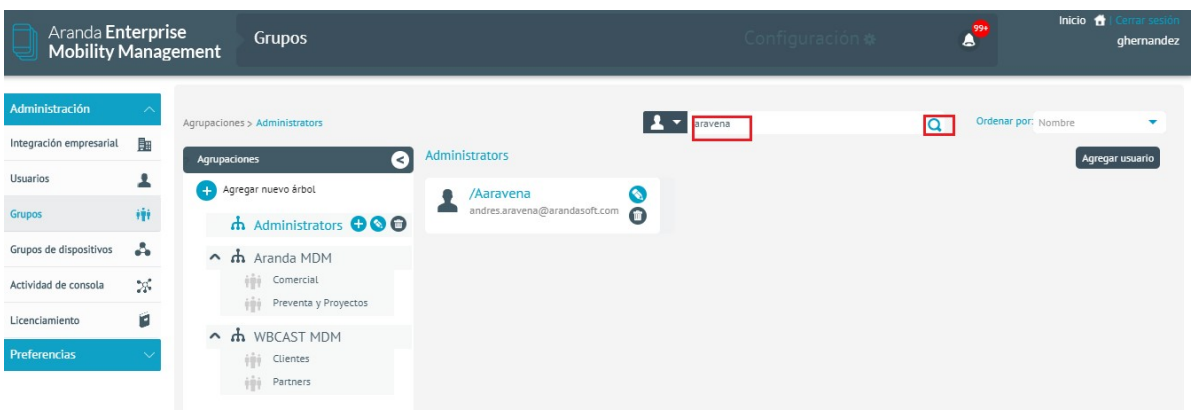


Agregar usuarios a un grupo

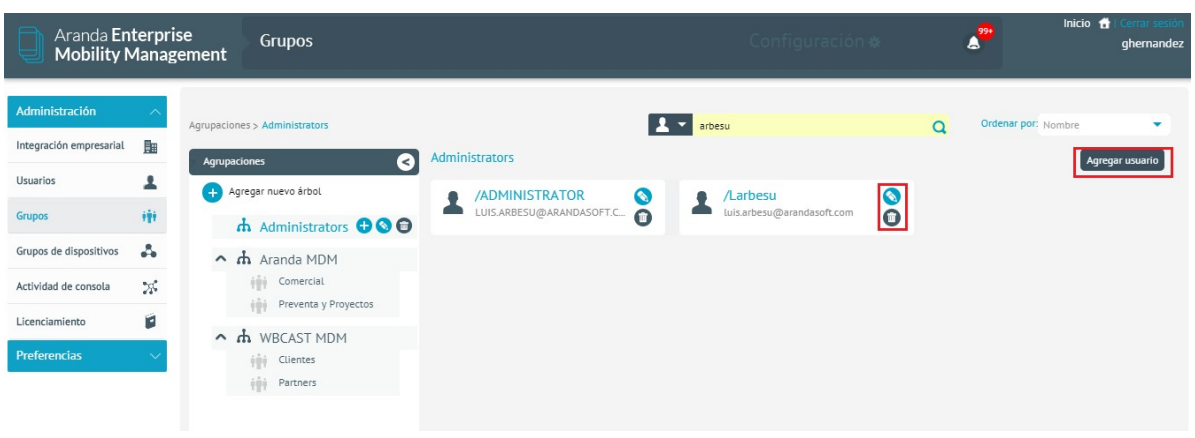
Si desea asociar un usuario a un grupo de clic en **Usuarios** en el selector y luego de clic en **Agregar usuario**.



Ingrese los criterios de búsqueda y haga clic en **Buscar**.



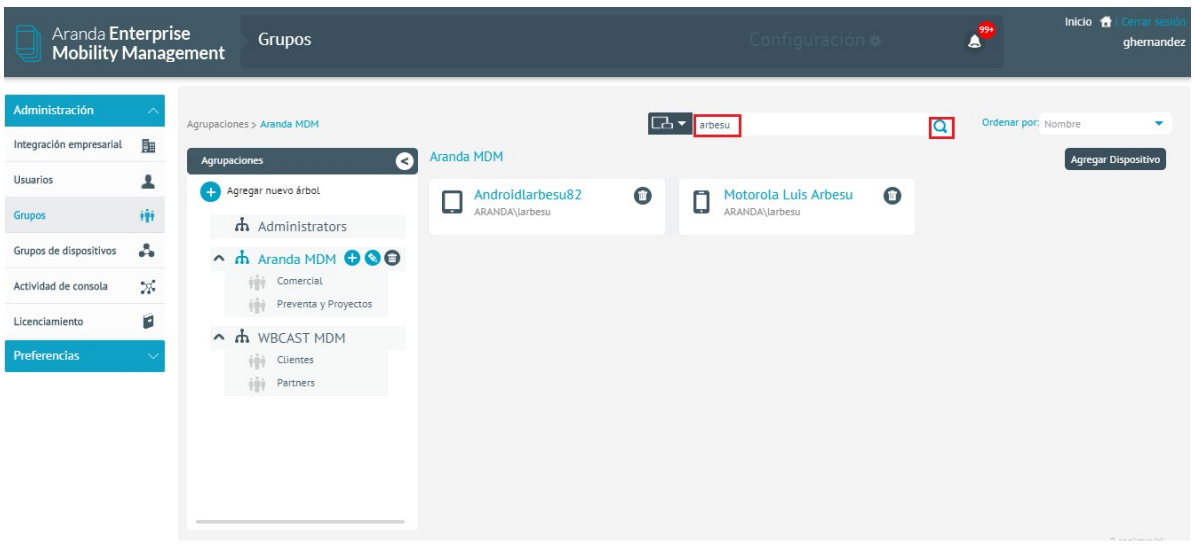
Seleccione los usuarios que desea agregar y luego de clic en **Agregar**.



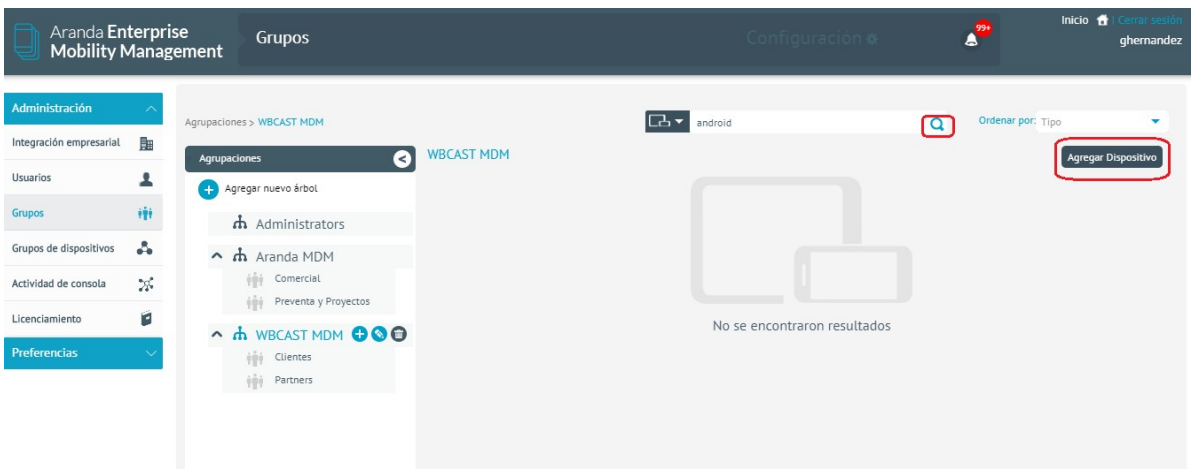
Agregar dispositivos a un grupo

Para asociar un dispositivo a un grupo debe escoger Dispositivos en el selector y luego dar clic en **Agregar dispositivo**.

Ingrese los criterios de búsqueda y de clic en **Buscar**.



Seleccione los dispositivos que desea agregar y de clic en **Agregar**.

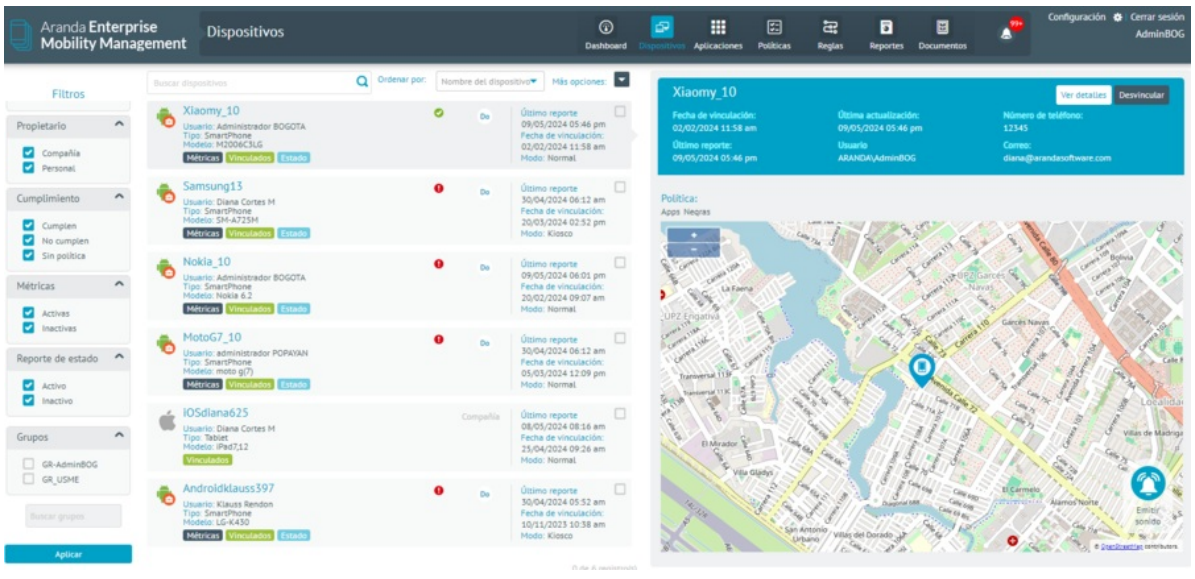


Permisos de Visualización segmentados por grupos

De acuerdo al control de acceso configurado (como un elemento de seguridad) que otorga quién tiene permiso para acceder a determinados dispostivos, segmentando así los datos según su necesidad. A continuación se da ejemplo del permiso de visualización en el del módulo “Dispositivos”, sección “listado de dispositivos”, donde se puede visualizar con y sin restricción en la información:

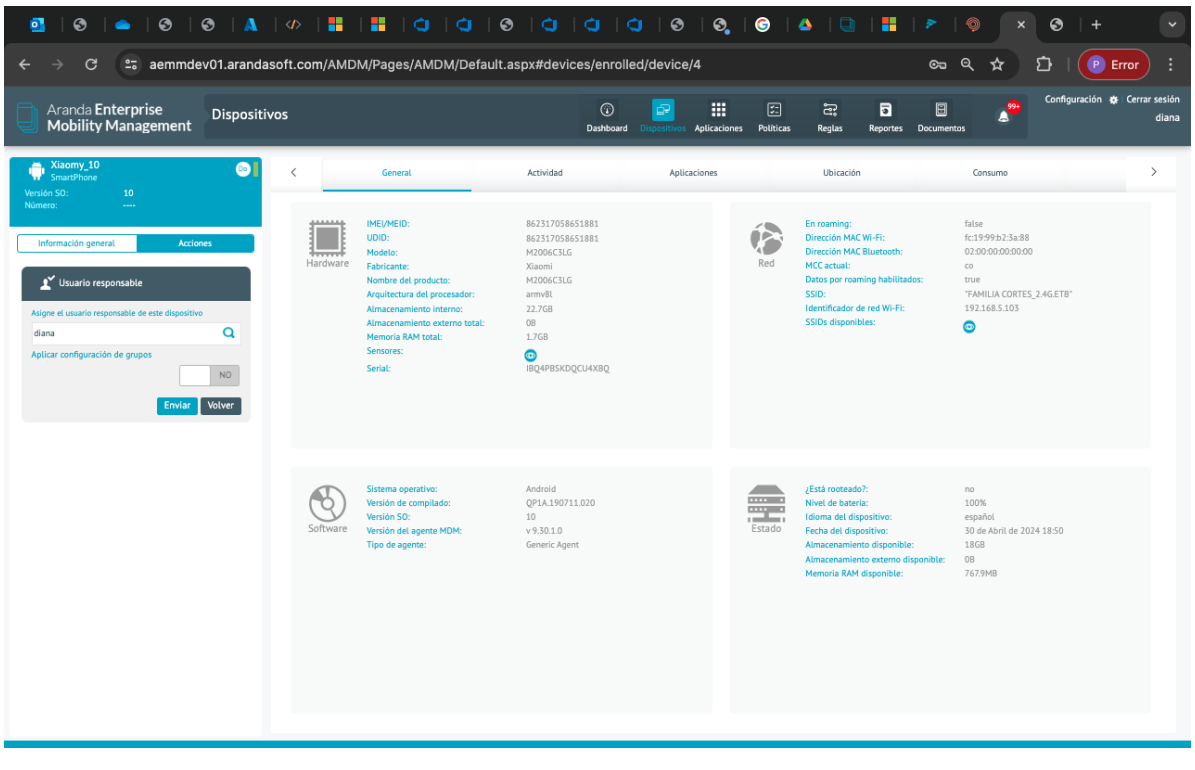
Visualización del módulo devices con restricción

El Administrador de consola otorga al usuario AdminBog (administrador Bogotá), visualización de todos los módulos, permitiendo visualizar los dispositivos y grupos que configuró; en este caso solo los de Bogotá (Ver *Configuración de View Other Devices*. Así, el usuario AdminBog solo podrá administrar y gestionar los dispositivos en los que tiene permiso:



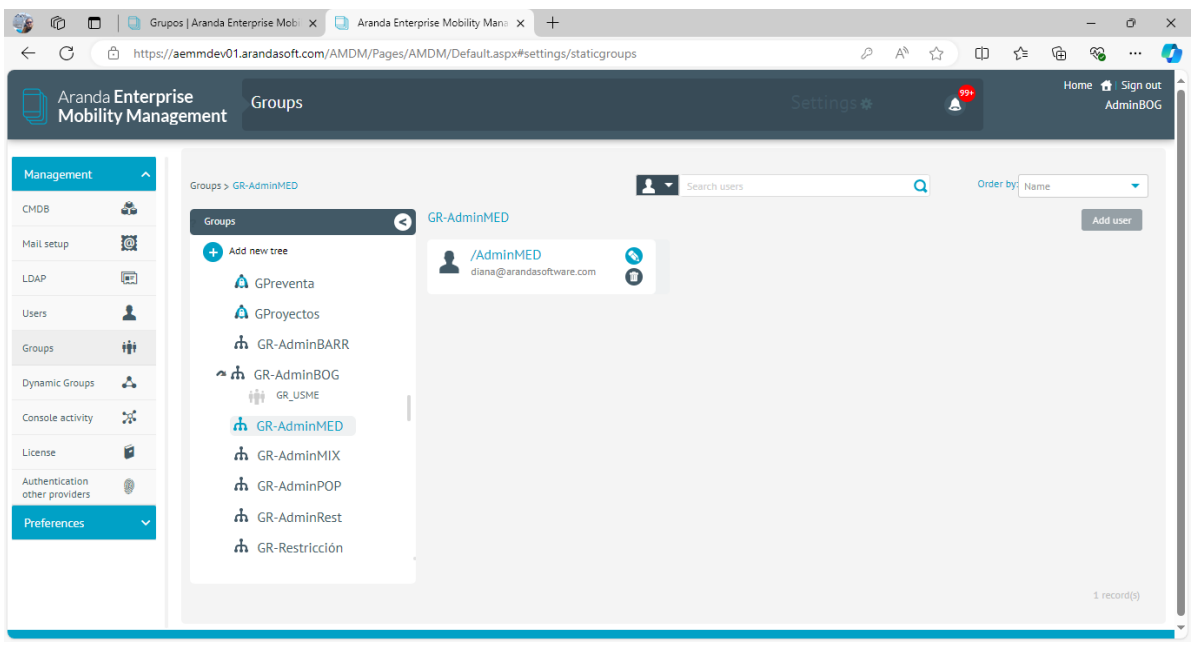
En la imagen anterior se observa que en el listado de dispositivos el usuario AdminBog, visualiza los dispositivos y grupo a los cuales tiene acceso.

- Como cambiar de usuario a un dispositivo: (Ver *Usuarios responsables*)



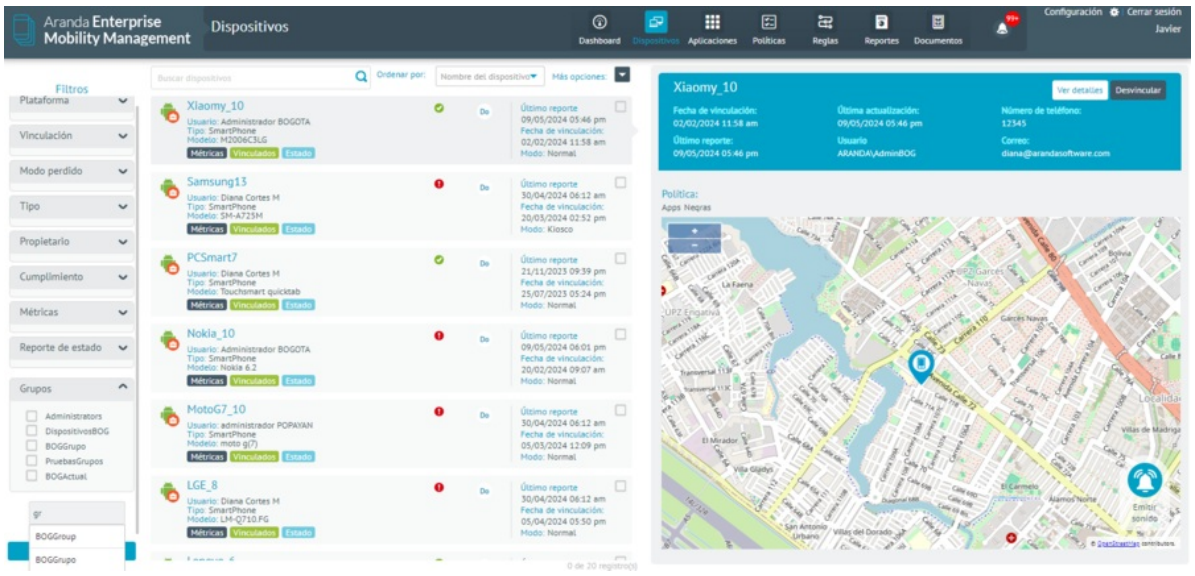
Ver detalle:

Por otro lado, el usuario AdminBog podrá ver todos los grupos creados en la consola y solo podrá gestionar los grupos de los que tiene permiso. Si no tiene el permiso, no podrá ver las opciones agregar, editar y eliminar.



Visualización del módulo devices sin restricción

El Administrador de consola otorga al usuario diana, visualización de todos los módulos y toda la data (información de los dispositivos), es decir puede ver todos los dispositivos vinculados en consola-



⚐ Nota:

Si un usuario se encuentra asociado en múltiples grupos y el grupo tiene activo el rol **View Other Devices**, se dará prioridad a este rol y el usuario podrá navegar sin ningún tipo de restricción. No se recomienda implementar configuraciones hibridas.

La segmentación de datos tiene la excepción en el módulo DashBoard, ya que muestra la información global de la consola.

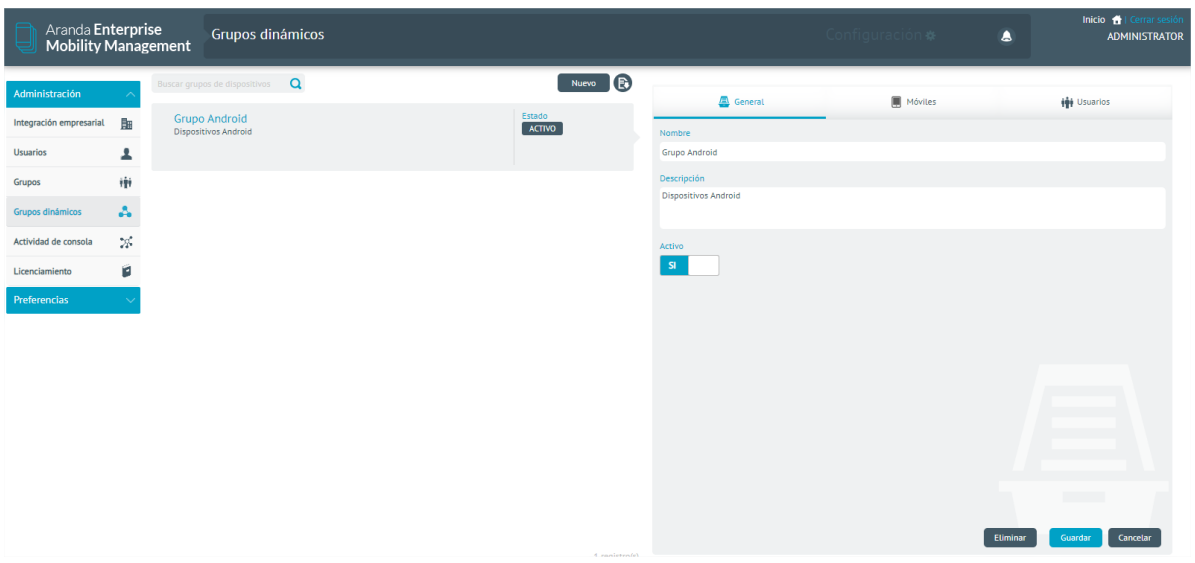
Grupos Dinámicos

En muchos casos se requiere enviar un comando a muchos móviles que comparten una o varias condiciones específicas. Estas condiciones pueden ser variables o fijas por dispositivo. En estos casos los grupos dinámicos proveen un mecanismo para agrupar por una o varias condiciones.

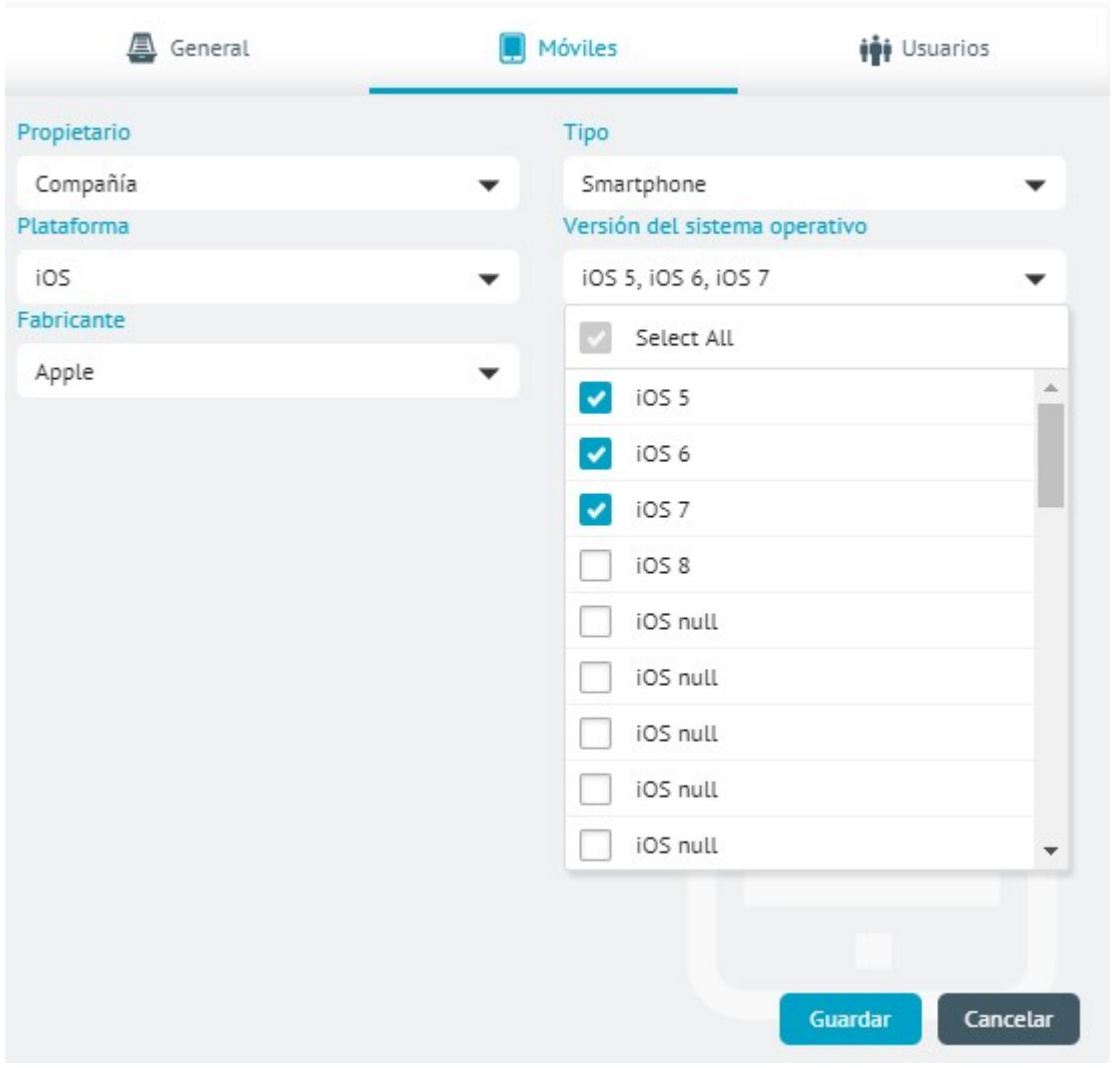
Los grupos dinámicos como su nombre lo indica son totalmente dinámicos con respecto a los dispositivos que agrupan, es decir que los móviles pueden dejar de pertenecer al grupo si cambian una condición importante, por ejemplo, si a un móvil que sea de la compañía se le cambia el tipo de propiedad, automáticamente deja de pertenecer a los grupos que solo incluyan móviles de la compañía. Los grupos dinámicos pueden ser usados al desplegar políticas o conjuntos de reglas.

Para crear un grupo dinámico, ingrese a la consola de inicio de AEMM, en la sección de **Administración** del menú principal, seleccione la opción **Grupos dinámicos**. En la vista de información podrá visualizar un listado con los registros de grupos creados.

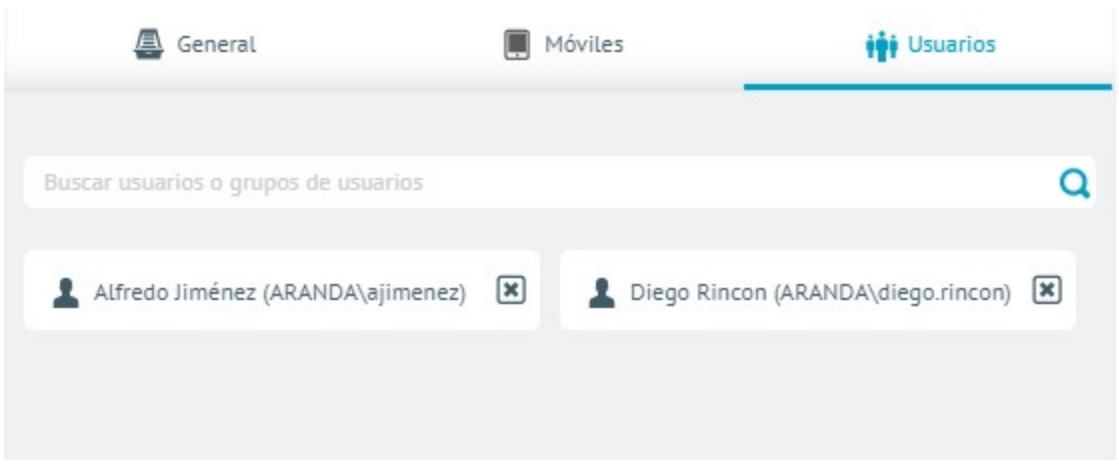
En la vista de información haga clic en el botón **Nuevo**. En la vista detalle podrá configurar la información básica del grupo.

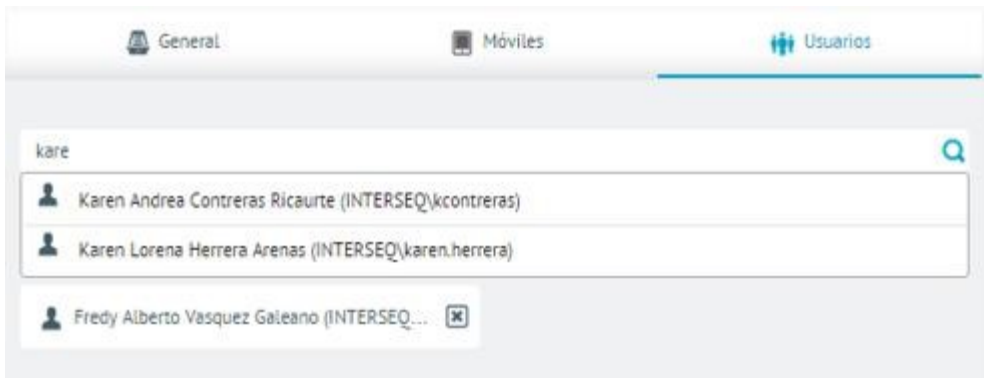


En vista detalle de Grupos, en la pestaña **Móviles** ingrese las condiciones de pertenencia al grupo relacionadas con el móvil. Aquí se puede filtrar por tipo de propiedad (Compañía o Usuario), Plataforma (iOS o Android), Fabricante, Tipo (Smartphone o Tablet) y versión del sistema operativo. Todas las condiciones que se especifiquen deben ser cumplidas para que el móvil pertenezca al grupo.



En la vista detalle de grupos, en la pestaña **usuarios** podrá indicar otra alternativa para que los móviles pertenezcan al grupo, y esta tiene que ver con la persona que porta el dispositivo. Se pueden escoger diferentes usuarios o grupos de usuarios para conformar la condición. Si algún dispositivo es portado por algunos de los usuarios o grupos incluidos, entonces el dispositivo pertenece al grupo.





Actividad de consola

En la sección **Configuración** del menú encabezado, en la consola de AEMM, podrá consultar la actividad registrada en la misma, esta opción le permite revisar y auditar las trazas que dejan las diferentes operaciones que se ejecutan en la consola. Para cada acción registrada se muestra la siguiente información.

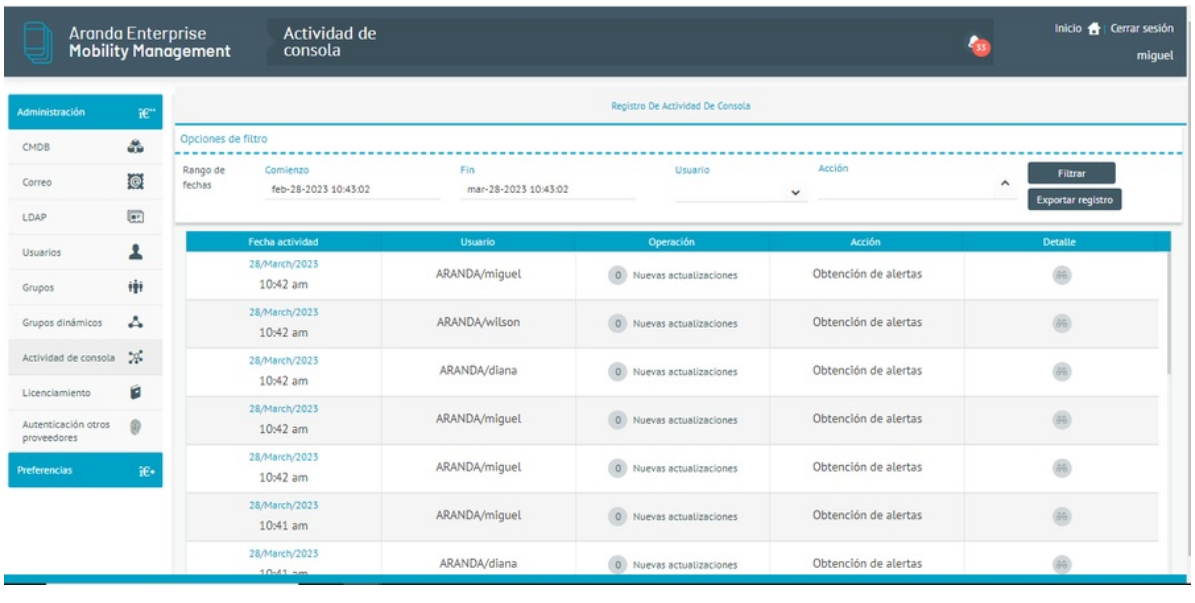
Esta sección presenta las siguientes opciones/funcionalidades:

- *Filtro por rango de fechas:* Permite filtrar los eventos comprendidos entre una fecha inicial y una fecha final.
- *Filtro por usuario:* Permite filtrar los eventos registrados asociados a un usuario específico.
- *Filtro por acción:* Permite filtrar los eventos registrados relacionados con cierta acción u operación sobre la consola
- *Exportar registro:* Permite exportar hasta 1000 registros a un archivo Excel o Csv.

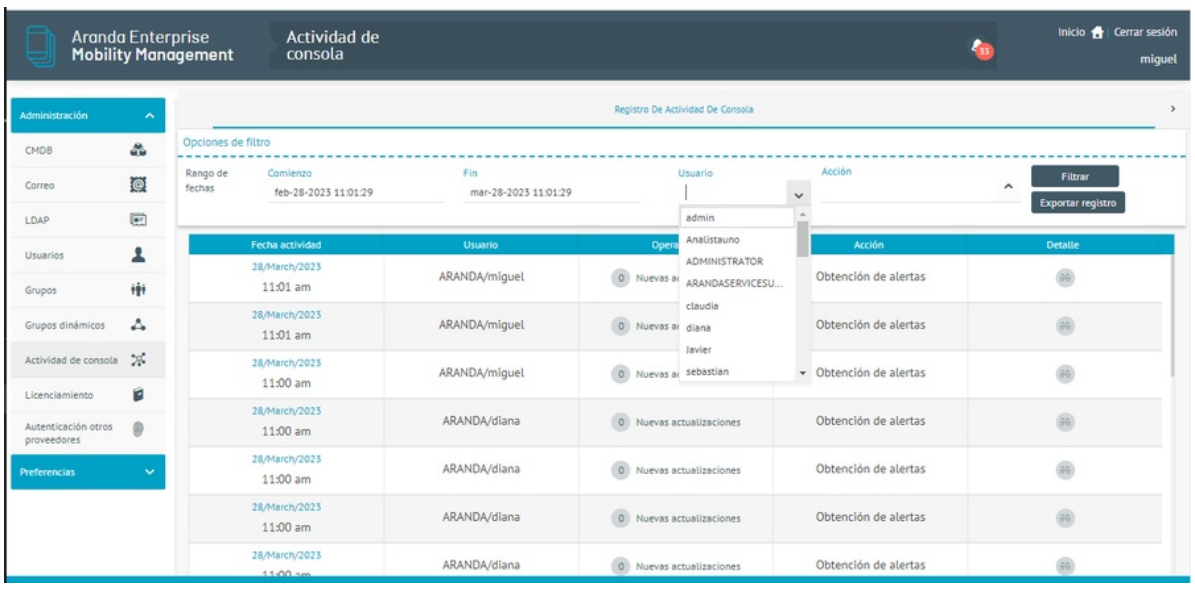
Acciones para consultas

A continuación se especificarán las acciones que se pueden realizar para las consultas:

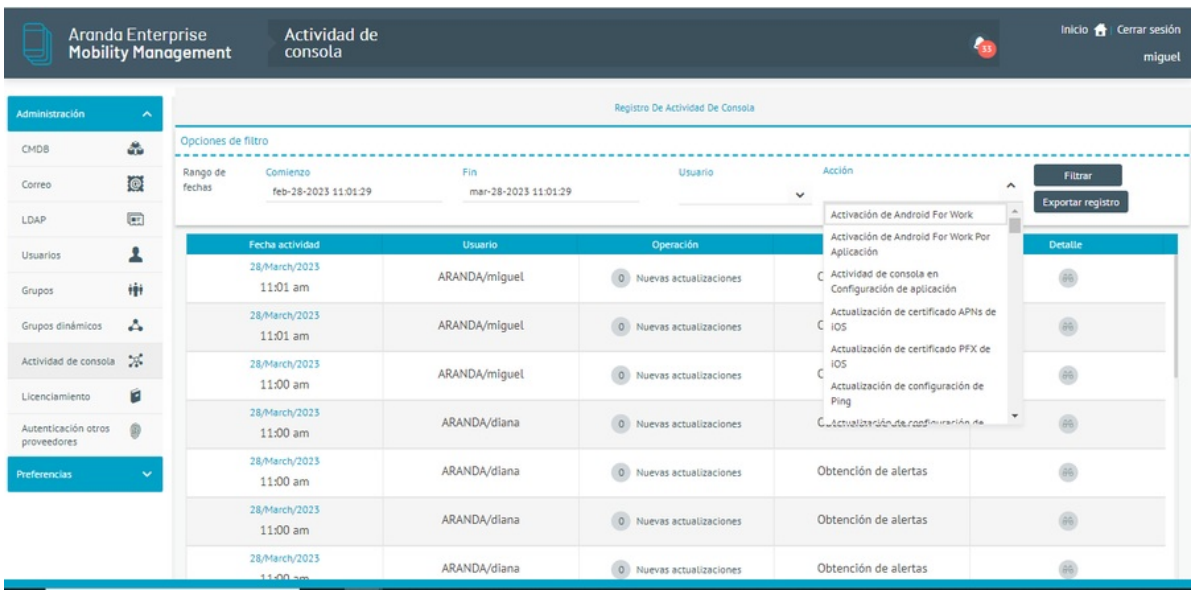
- Podrá especificar un rango de fechas específico.



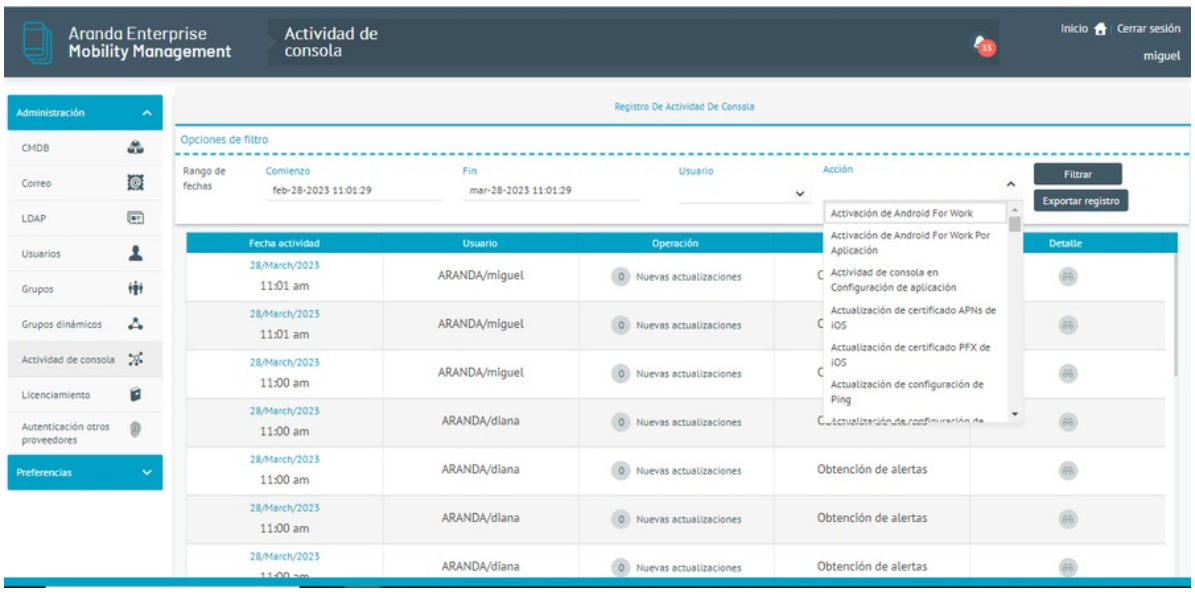
- Usuario que ejecuta una operación.



- O acción en particular.



- Finalmente podrá exportar el registro de actividades en los formatos de csv o excel.



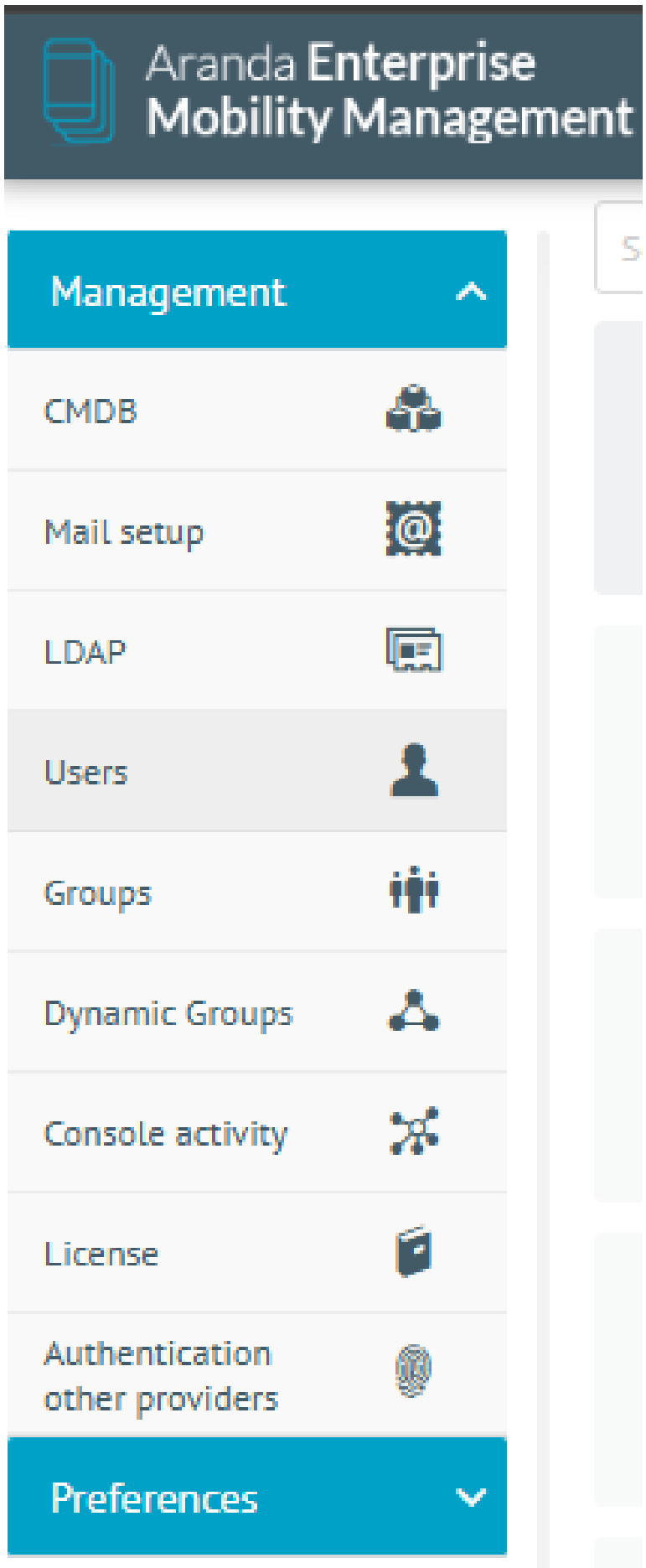
Licenciamiento

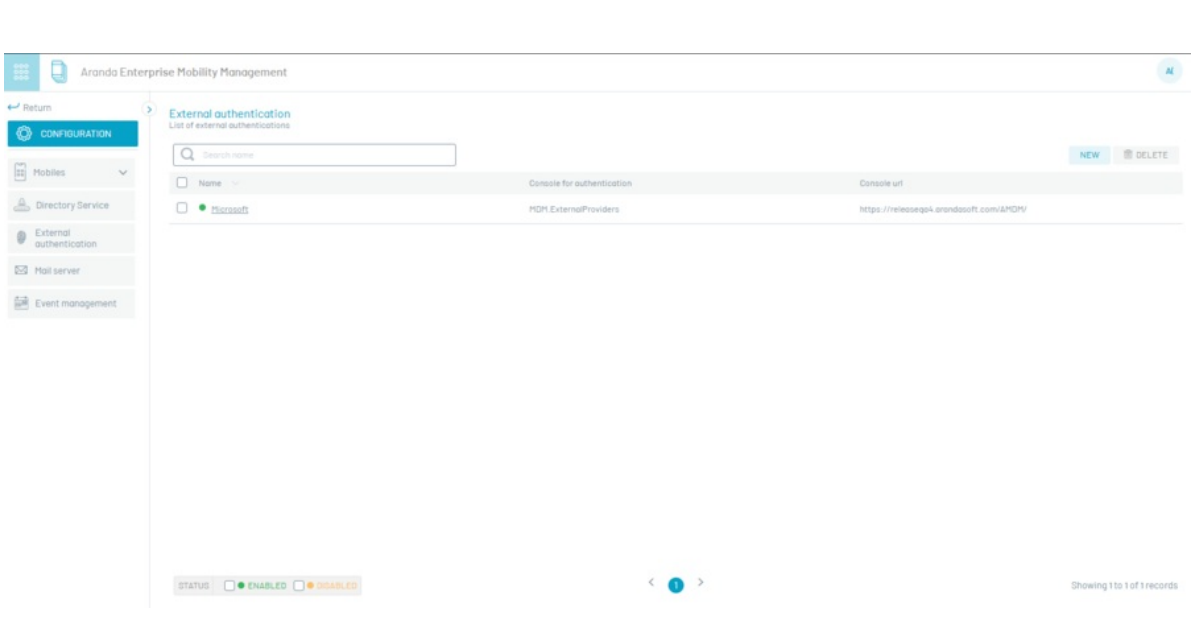
En este módulo ya introducido en la sección Instalación->Configuración de Licenciamiento, se listan y se pueden gestionar las licencias actualmente cargadas en el sistema.

Es importante aclarar que se pueden cargar cuantas licencias se deseen, el sistema sumará el número de dispositivos de todas las licencias vigentes.

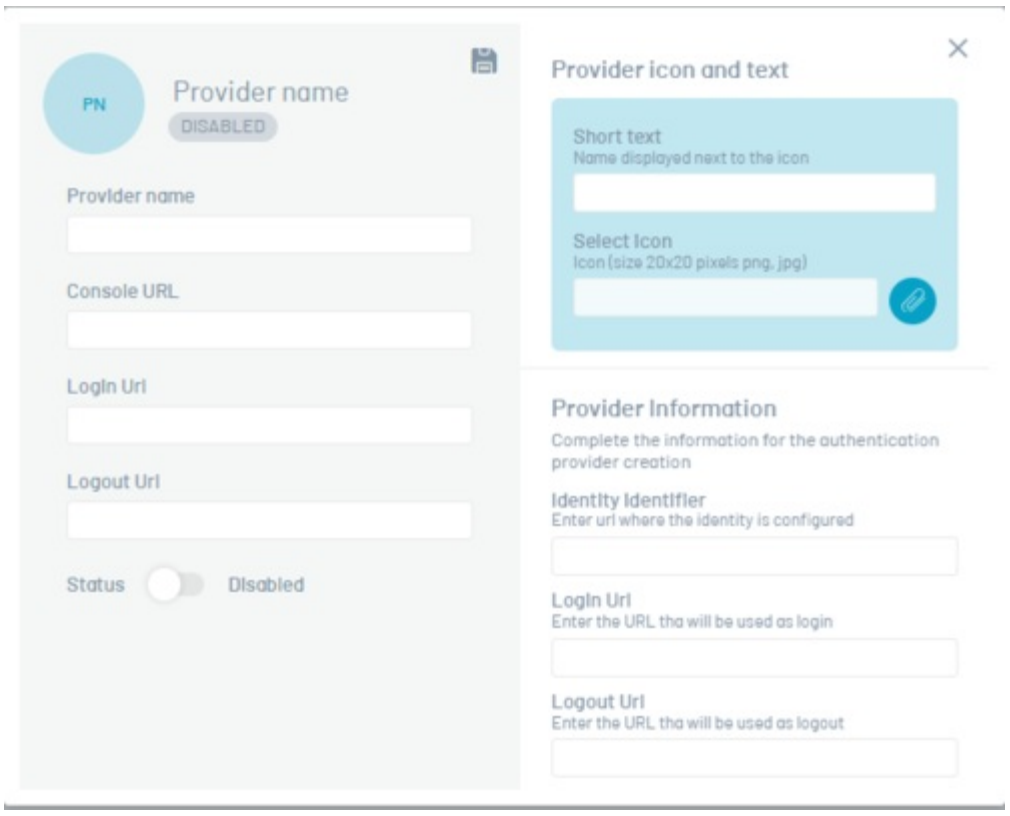
Autenticación con otros Proveedores

Configuración





Para iniciar la configuración haga clic en el botón **NUEVO** y diligencie la siguiente información:



Campo	Descripción
Nombre del Proveedor:	Nombre de la conexión con la cual se identificará en el listado de proveedores configurados y en el botón ubicado en el login de la herramienta para su respectivo ingreso.
URL de la consola:	Debe ingresar la URL de la consola de AEMM hasta el AMDM (https://[dominio de servidor]/AMDM) Ejm: https://mydominio.com/AMDM
URL de inicio de sesión:	Esta información de url de inicio se genera automáticamente al ingresar la URL de la consola
URL de cierre de sesión:	Esta información de url de inicio se genera automáticamente al ingresar la URL de la consola

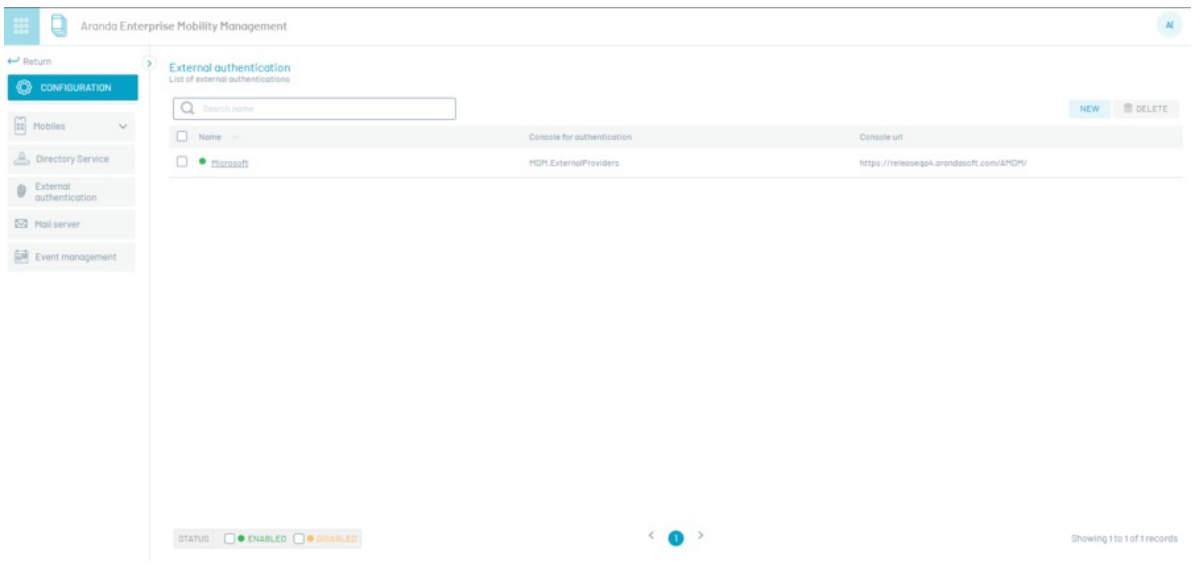
Ícono y texto del Proveedor

Campo	Descripción
Texto corto:	Nombre que aparece junto al ícono.
Seleccionar icono:	Imagen que identificará el proveedor configurado en la pantalla de login. Debe de tener un tamaño máxximo de 20x20 píxeles y formato png o jpg

Información del Proveedor

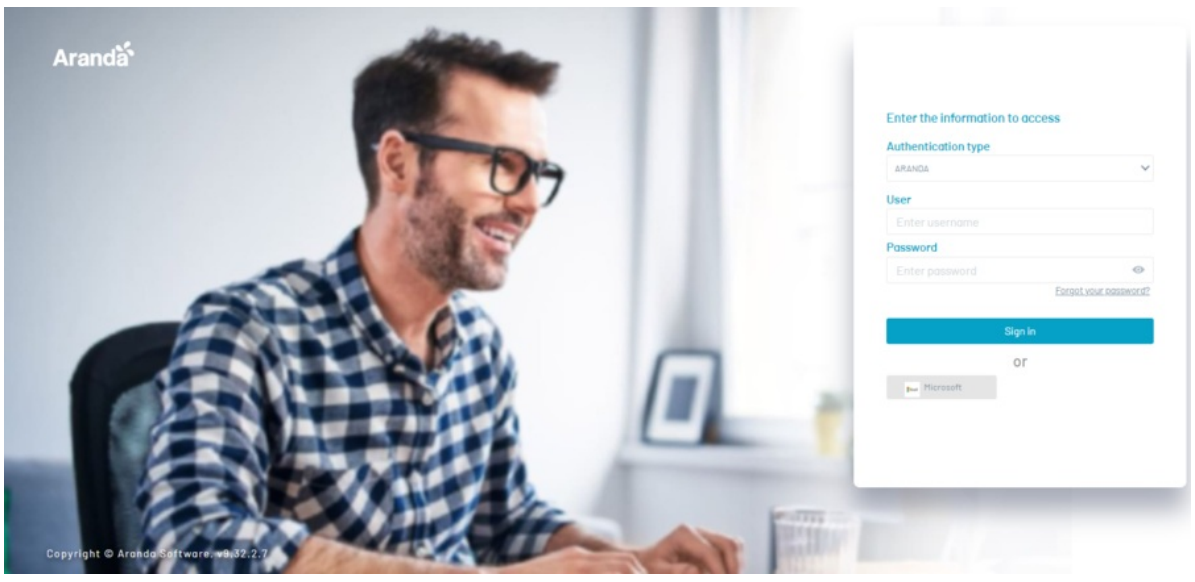
Campo	Descripción
Identificador de Identidad:	Url de identificación de la conexión configurada del sitio
URL de inicio de sesión:	Url de inicio de sesión configurada por el proveedor.
URL de cierre de sesión:	Url de fin de sesión configurada por el proveedor

Después de realizar su configuración, haga clic en **Guardar**, esta configuración se visualizará en el listado de proveedores.

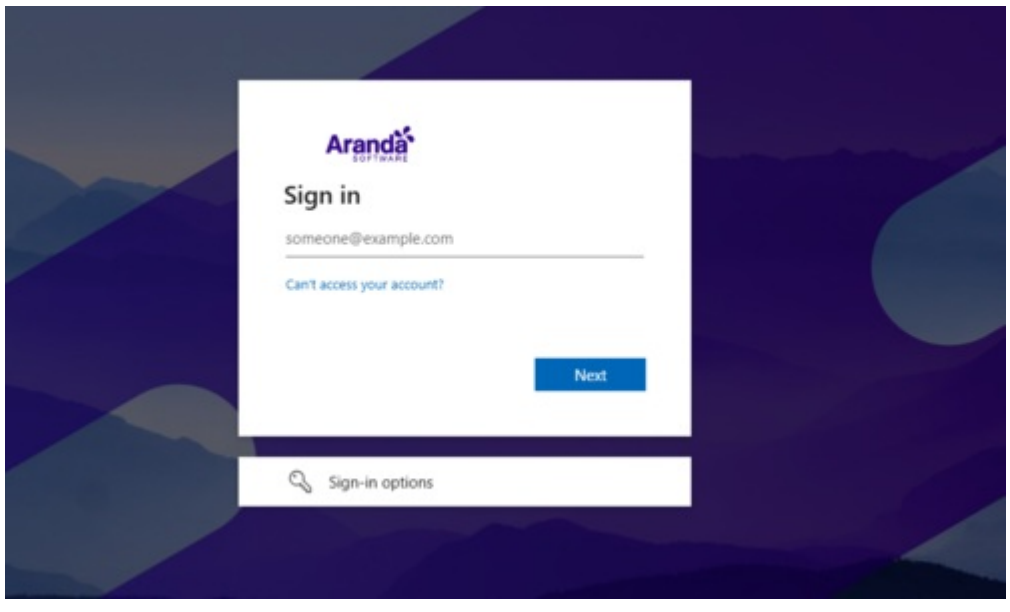


Ingreso por parte del usuario

El usuario se encuentra en el login de la consola AEMM, donde podrá visualizar la información de los proveedores de autenticación, para su ingreso debe hacer clic en el botón del proveedor que requiera



El sitio envía al usuario a la herramienta central de inicio de sesión, el usuario ingresa sus credenciales, estos datos ingresados son validados y notifica a la aplicación que el usuario esta validado.



Una vez autenticado en el proveedor externo se hace una redirección normal a la consola, presentando la pantalla inicial.

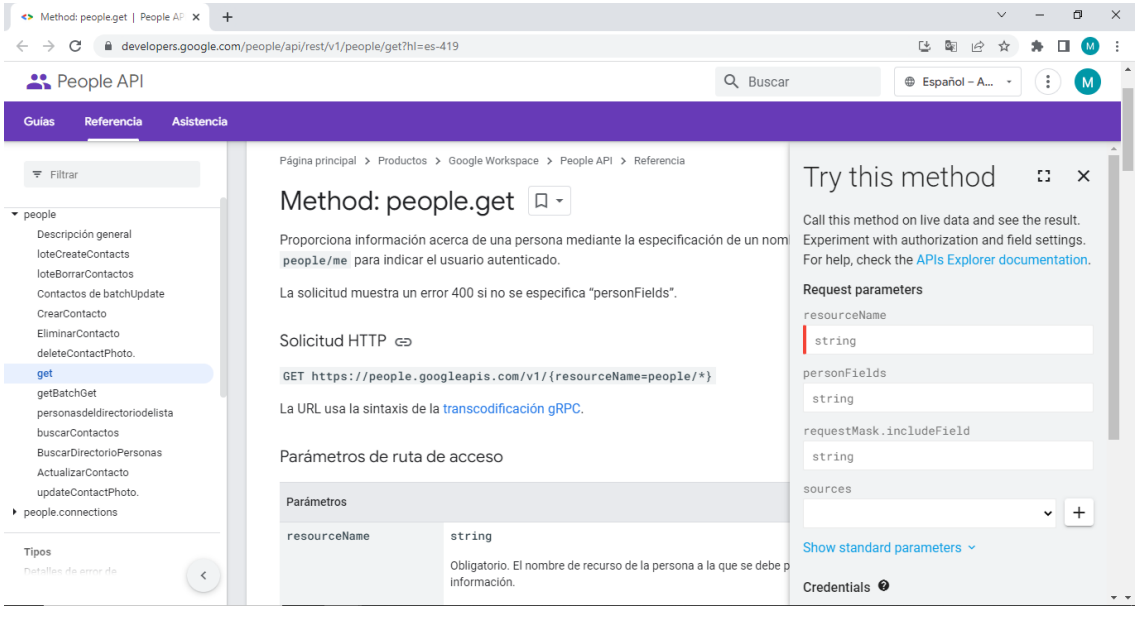
ID cuenta google (Android Factory Reset)

Su ID es un número exclusivo que se utiliza para identificar su cuenta de Google.

Procedimiento para recuperar el ID de la cuenta de Google

> ⚠ **Advertencia:** Un ID de Google no es lo mismo que el nombre de usuario o el correo electrónico de la cuenta..

1. Ingrese en su navegador web predilecto al siguiente sitio web https://developers.google.com/people/api/rest/v1/people/get?hl=es-419



2. Agregue los siguientes valores

Parámetro solicitado	Valor
resourceName	people/me
personFields	metadata,emailAddresses
requestMask.includeField	[dejar vacío]

1. Presione el botón **EXECUTE**. Inicie sesión con su correo de Google y acepte los permisos que solicita el API. Éste retornará el JSON.


```
{
"resourceName": "people/XXXXXXXXXXXXXXXXXXXX",
"etag": "%EgUBCS43PhoEAQIFBw==",
"metadata": {
   "sources": [
    {
      "type": "PROFILE",
```

```
        "id": "XXXXXXXXXXXXXXXXXXXX",
        "etag": "#mUFoiy/UMSw=",
        "profileMetadata": {
        "objectType": "PERSON",
        "userTypes": [
          "GOOGLE_USER"
        ]
        },
        "updateTime": "2022-10-14T14:38:34.223762Z"
      }
      ],
      "objectType": "PERSON"
    },
    "emailAddresses": [
      {
        "metadata": {
        "primary": true,
        "verified": true,
        "source": {
        "type": "ACCOUNT",
        "id": "XXXXXXXXXXXXXXXXXXXX"
        },
        "sourcePrimary": true
      },
      "value": "XXXXXXX@arandasoft.com"
      }
    ]
    }
```


1. Busque en el JSON la propiedad ID que está embebida en metadata.sources.id.
2. Finalmente utilice el ID con el comando de Protección Reset Android.

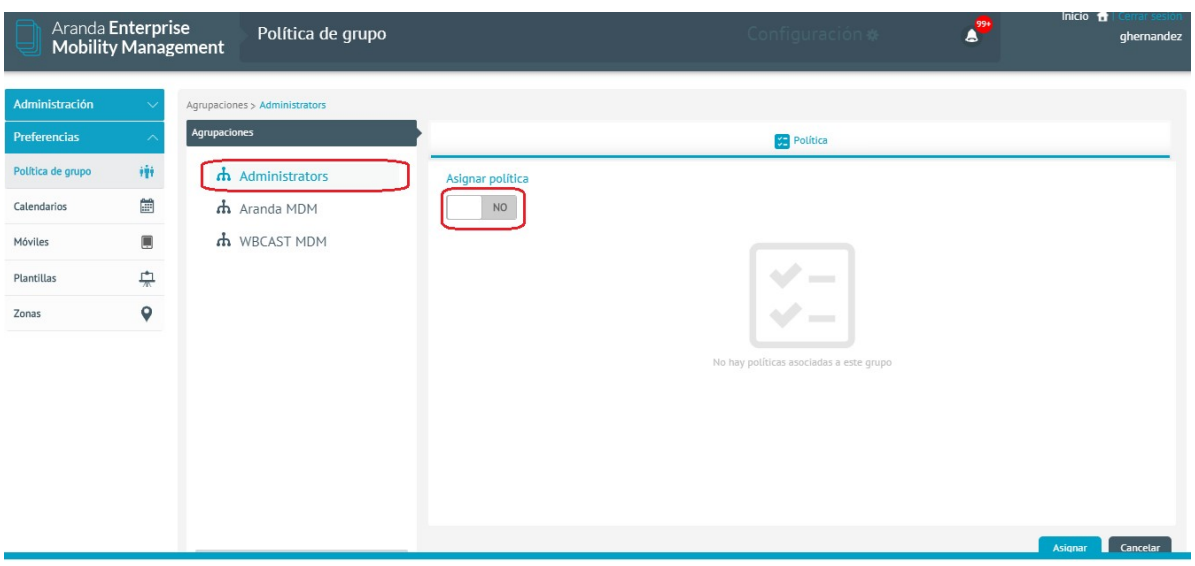
Preferencias

Política de Grupo

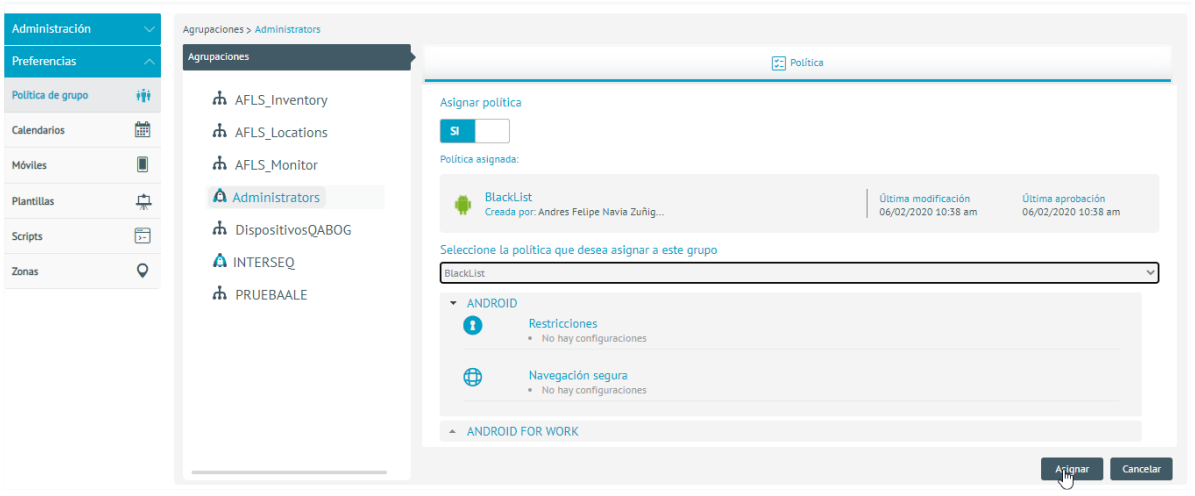
Esta opción le permite asignar la política a asignar a un dispositivo perteneciente al grupo en cuestión.

Esta asignación se realizará en el contexto de acción de regla de cambio de política, en la que se puede escoger la política de grupo, en tanto que, la política asignada en el presente módulo será la que se le asigne al dispositivo cuanto la acción de regla se ejecute.

Para configurar la política de grupo acceda al módulo:



Luego escoja el grupo y a continuación la política, luego dé clic en Asignar.

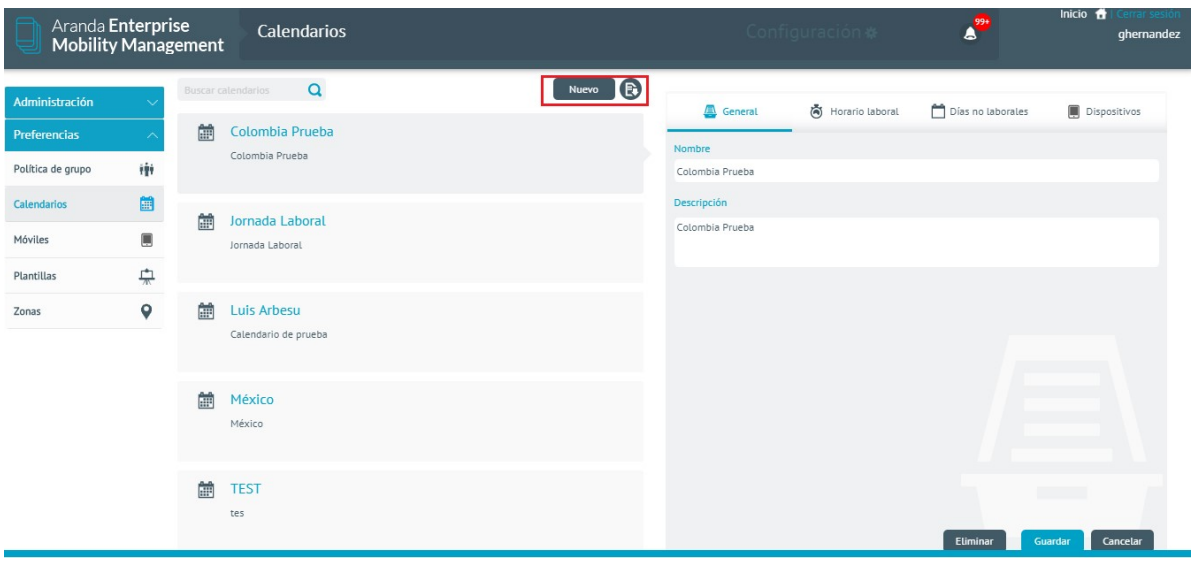


Es preciso aclarar que la política que se escoja solo será enviada a los dispositivos que su plataforma coincida con la de la política.

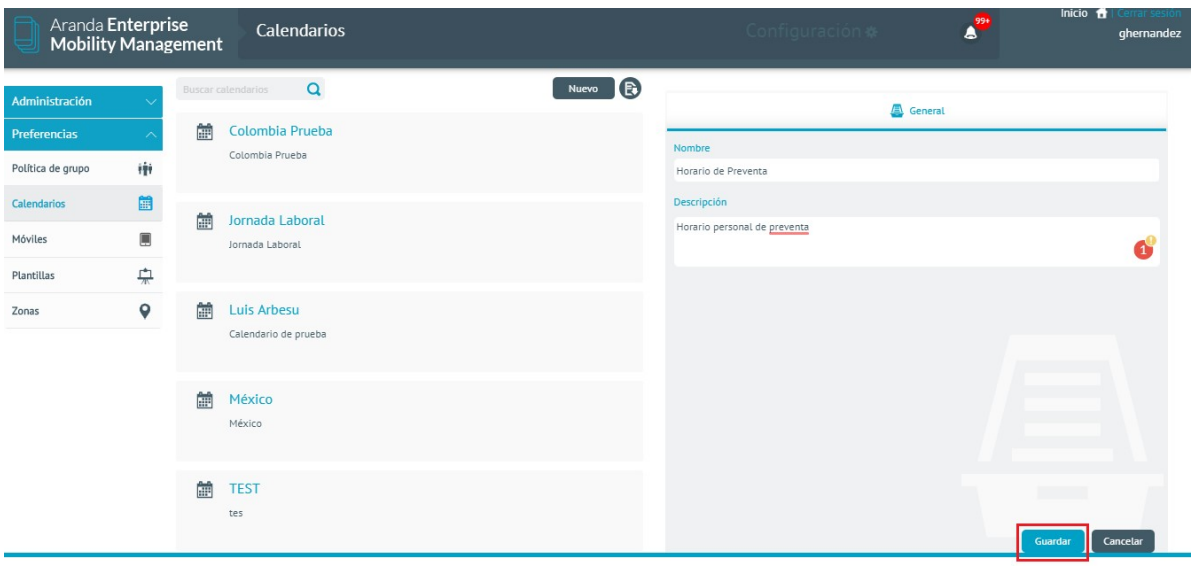
Configuración de Calendarios

Los Calendarios se deben configurar para hacer uso de las reglas de Timefencing (Franjas horarias). A continuación:

Ingresar a calendarios dentro del menú EMM y de clic en **Nuevo**.

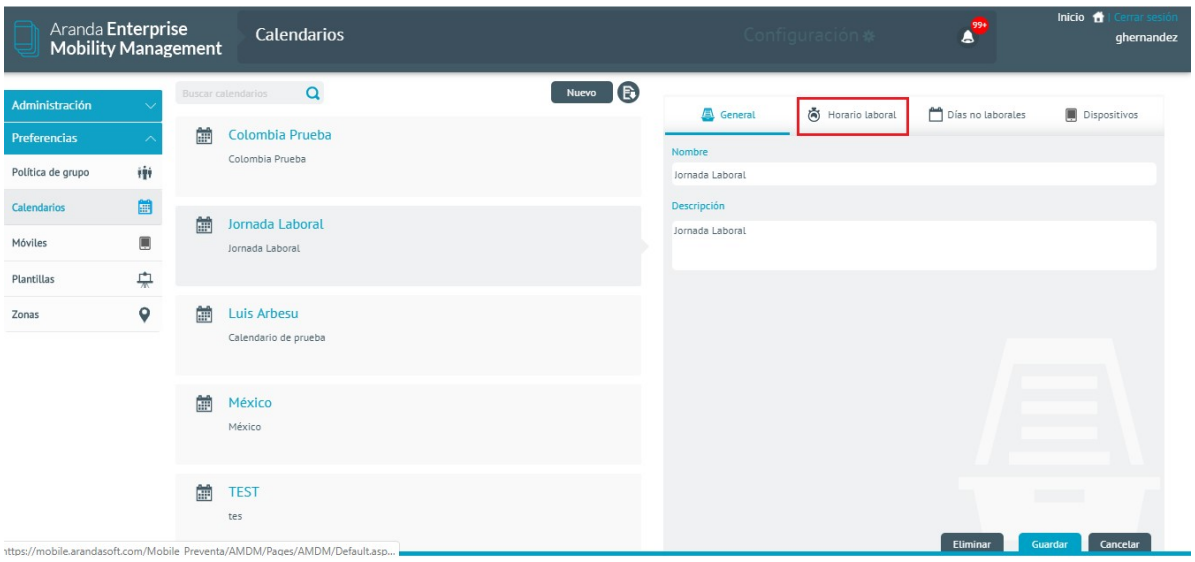


Ingrese los datos solicitados y de clic en **Guardar**

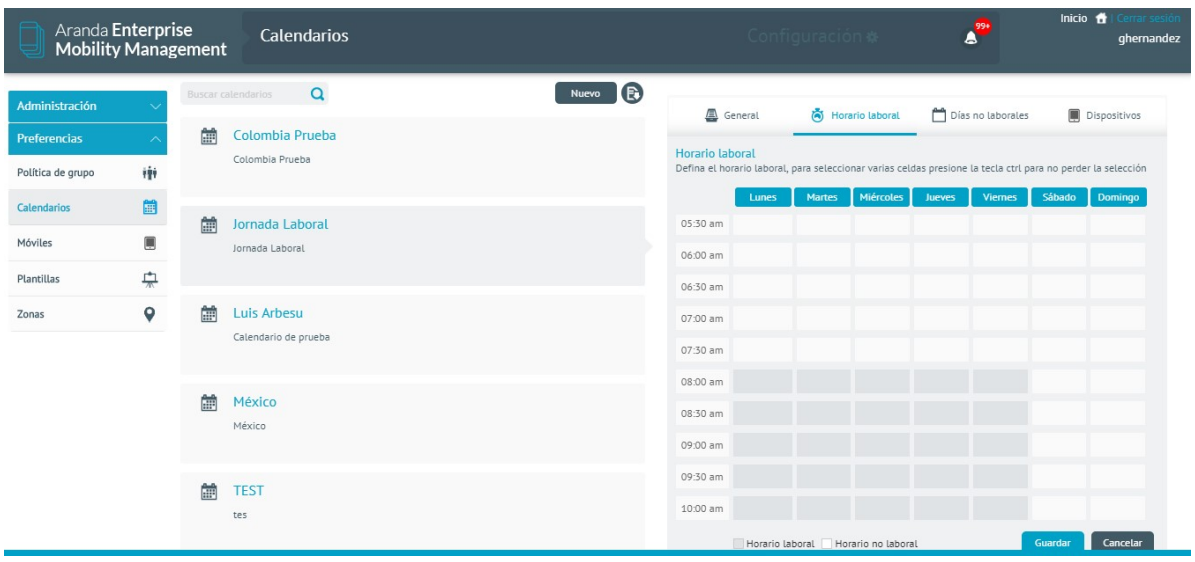


Horario laboral

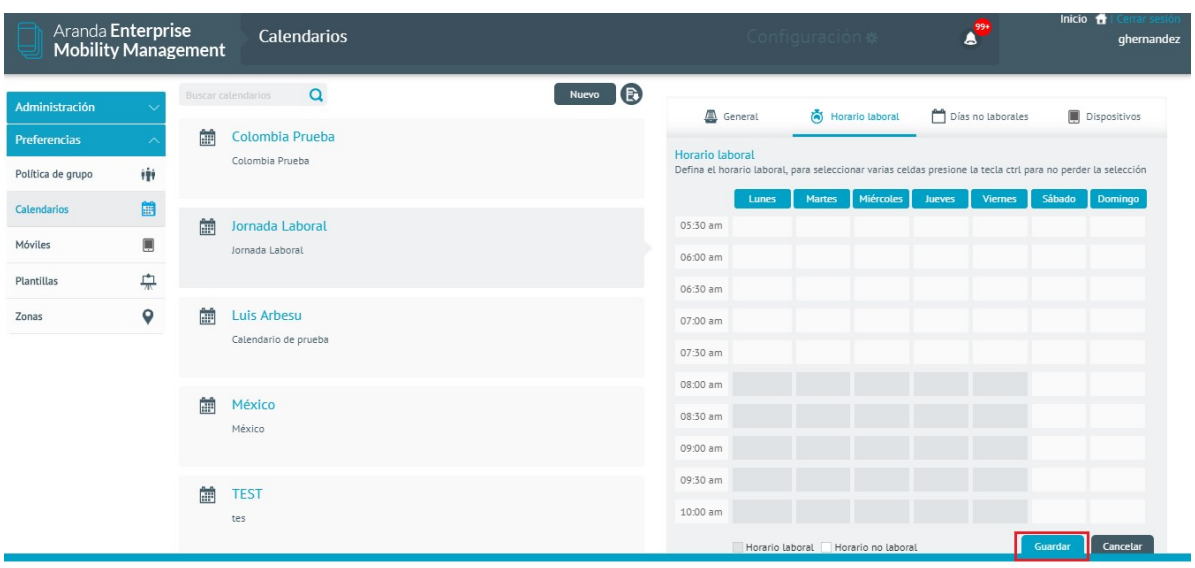
Para configurar las horas laborales de clic en la opción **Horario laboral.**



Seleccione las horas laborales de la semana, mediante clic sostenido.

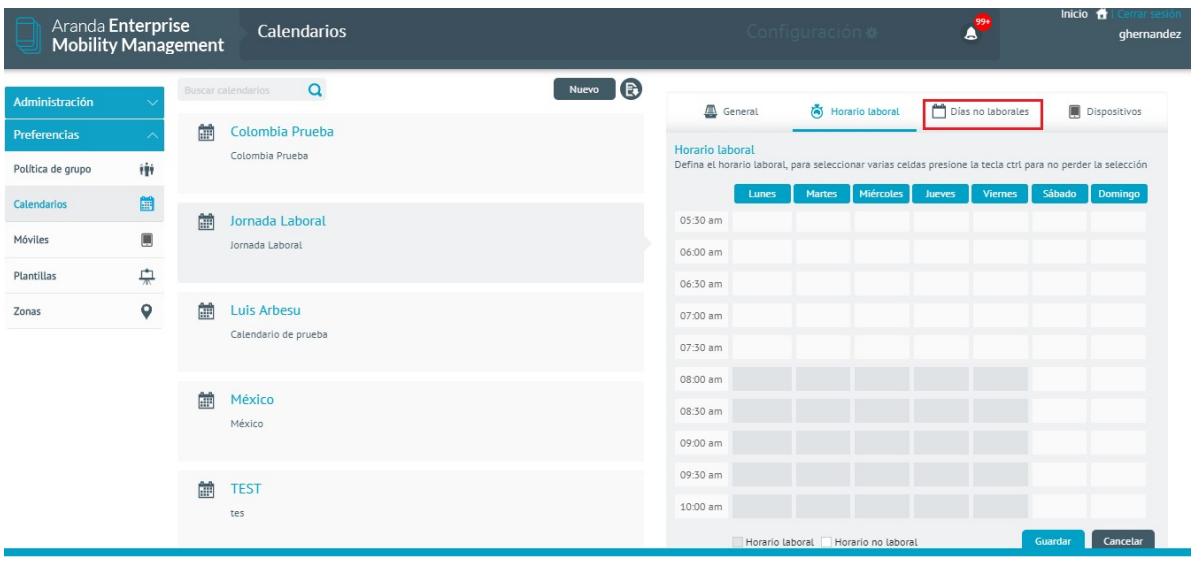


Luego de clic en la opción **Guardar**.

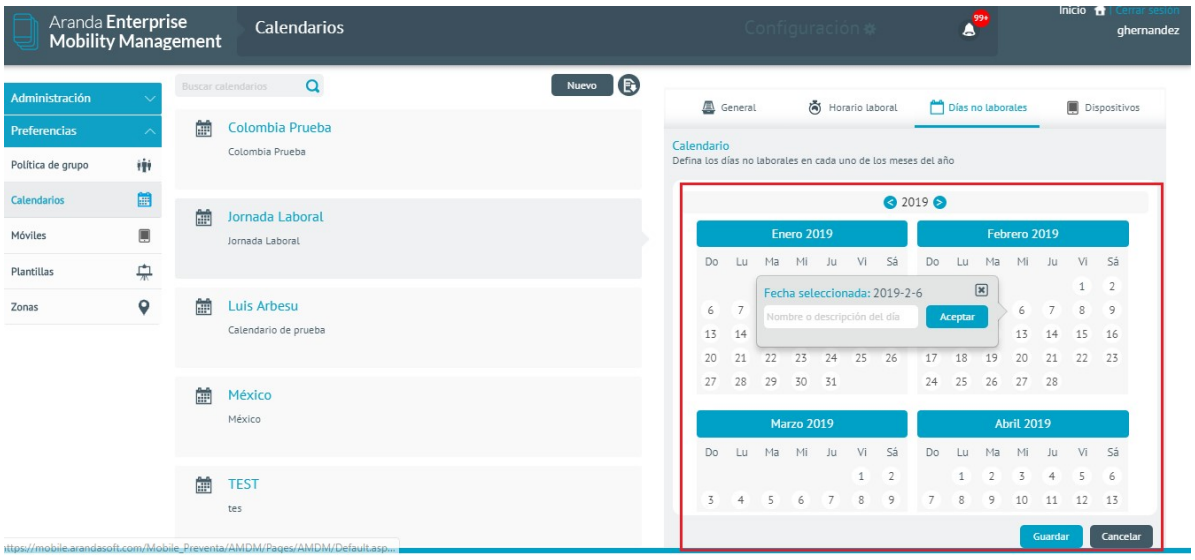


Días no laborales

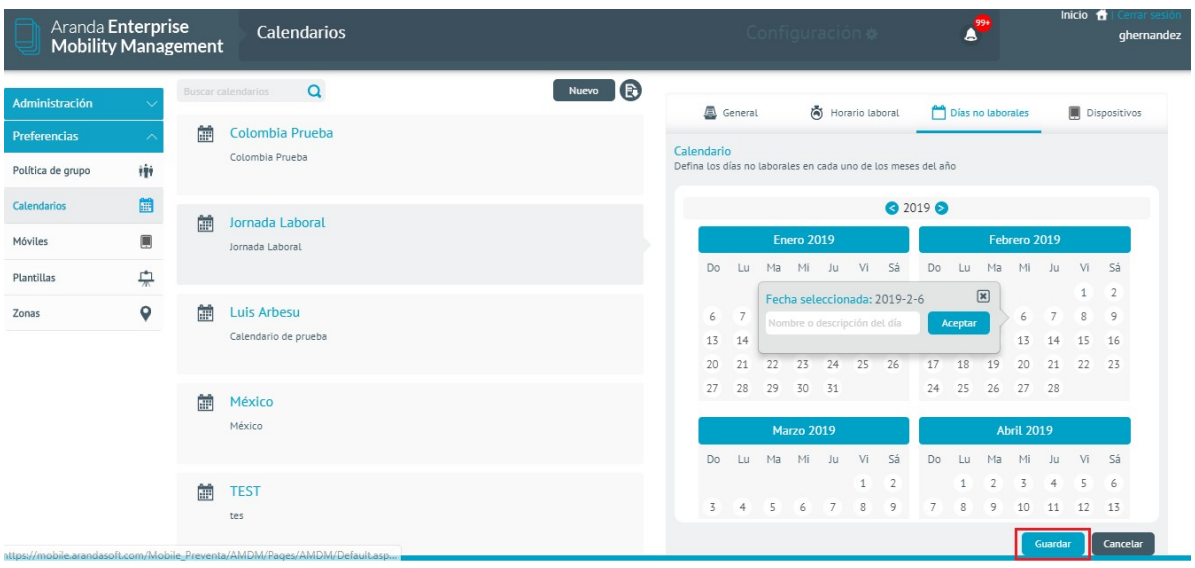
Para configurar los días en los que no se labora de todo el año, de clic en la opción **Días no laborales**.



De clic sobre el día que desea marcar como no laboral e ingrese el dato solicitado

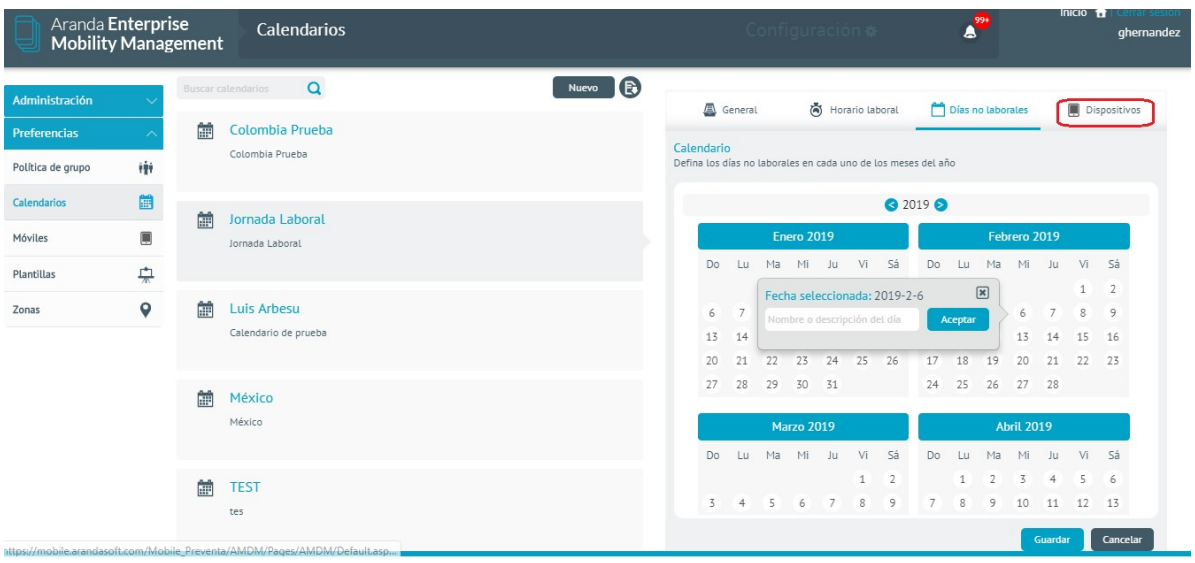


Luego de clic en la opción **Guardar**.

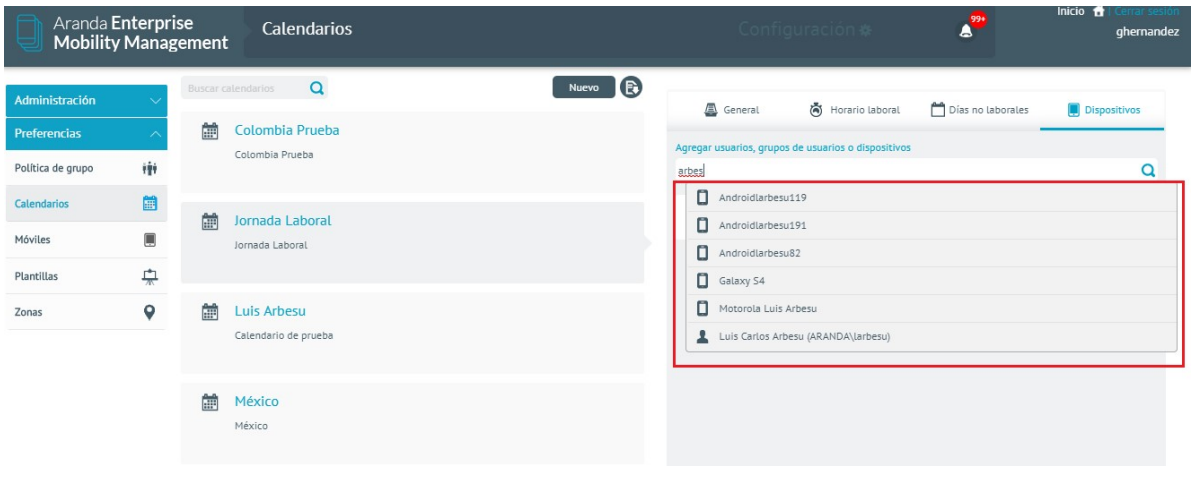


Dispositivos

Para asociar un calendario, dé clic en la opción **Dispositivos**



Para realizar la búsqueda de usuarios y/o dispositivos, seleccione el que desea agregar, y luego de clic en **Guardar**.



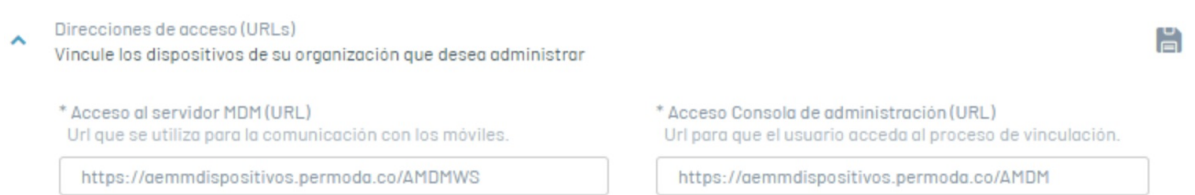
Móviles

Vinculación

En esta sección de configuran las opciones para realizar la vinculación de los dispositivos ante el servidor AEMM. Se pueden diligenciar las siguientes propiedades:

Propiedad de comunicación:Direcciones de acceso

Campos	Descripción
Url de acceso al servidor MDM:	Url que se utilizará para establecer comunicación entre los dispositivos y el servidor AEMM, los dispositivos deben de poder alcanzar esta url para poderse vincular al servidor.
Url de la consola de administración:	Url de la consola desde donde se hace la administración de los dispositivos y se usa para realizar invitaciones de vinculación vía correo electrónico.



Propiedad configuración en los dispositivos: Configuración de Políticas por Sistema Operativo

Campos	Descripción
Política por defecto iOS:	Política que será aplicada a los dispositivos de la plataforma iOS cuando éstos se vinculen.
Política por defecto Android:	Política que será aplicada a los dispositivos de la plataforma Android cuando éstos se vinculen.
Política por defecto Windows:	Política que será aplicada a los dispositivos de la plataforma Windows cuando éstos se vinculen.
Conjunto de reglas por defecto:	Conjunto de reglas que será aplicado a todo dispositivo que se vincule.
Casilla de verificación "Solicitar la instalación del agente en dispositivos iOS":	Casilla que al marcarla realiza la acción de envío de comando de instalación automáticamente cuando un dispositivo iOS ha realizado la vinculación tipo web.

Propiedad configuración de notificaciones: Notificación Push

En esta sección se puede configurar la notificación push que se debe enviar a los dispositivos para forzar periódicamente el contacto con el servidor, y así mantener actualizado la lista de dispositivos gestionados.

Para configurar el ping diligencie las siguientes opciones:

Campos	Descripción
Periodo::	Duración de un ciclo de ping hacia todos los dispositivos. Tras finalizar este intervalo todos los dispositivos han recibido al menos una notificación push.
Intervalos:	Cantidad de grupos de dispositivos en los que se dividirá el conjunto total de dispositivos vinculados. Esto para no encolar todas las notificaciones push al tiempo, sino basadas en esta cantidad de grupos.
Acciones:	Comandos que se encolaran antes de enviar la notificación push a cada dispositivo, se pueden escoger comandos de: Inventario, Localización y bloqueo de pantalla.

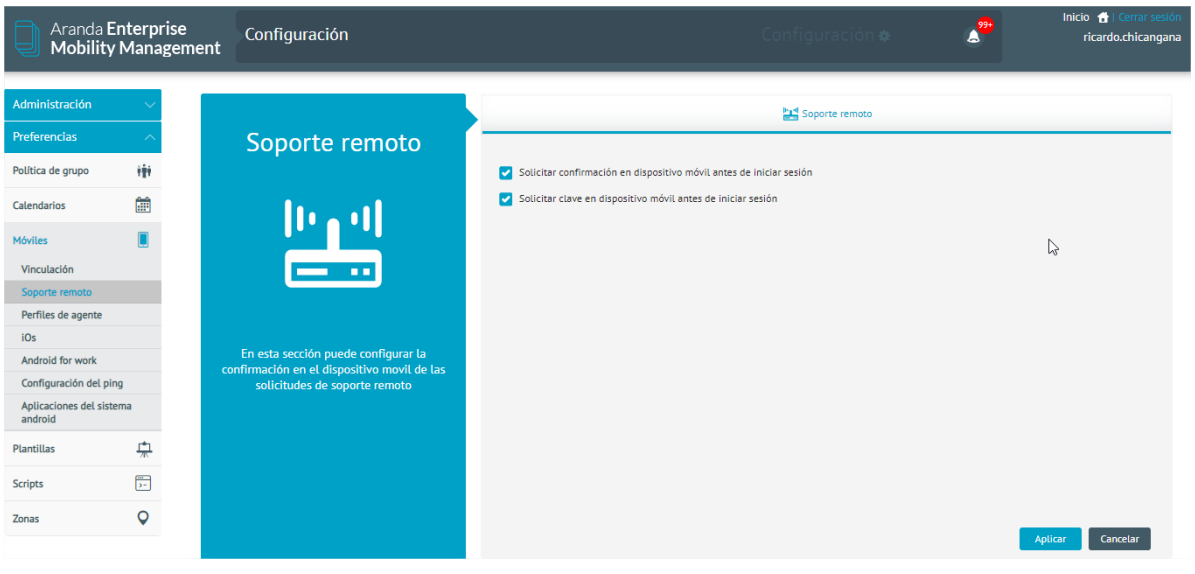
Una vez realizada las anteriores configuraciones haga clic en “Guardar”, para persistir y activar el mecanismo de ping.

Soporte Remoto

En esta sección de pueden configurar las opciones para sesiones de control remoto hacia dispositivos:

Campos	Descripción
Solicitar confirmación en dispositivo móvil antes de iniciar sesión:	Al estar marcada esta casilla la sesión solicitará confirmación por parte del usuario del dispositivo para iniciarse.
Solicitar clave en dispositivo móvil antes de iniciar sesión:	Al estar marcada esta casilla, en dispositivo al iniciar sesión se generará un código numérico de 6 dígitos que se tendrá que digitar correctamente en consola para iniciar efectivamente la sesión.

Marque o desmarque las casillas de acuerdo a lo requerido y luego haga clic en “Aplicar”.

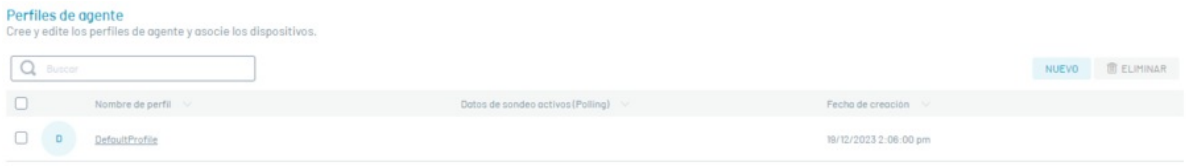


Perfiles de Agente

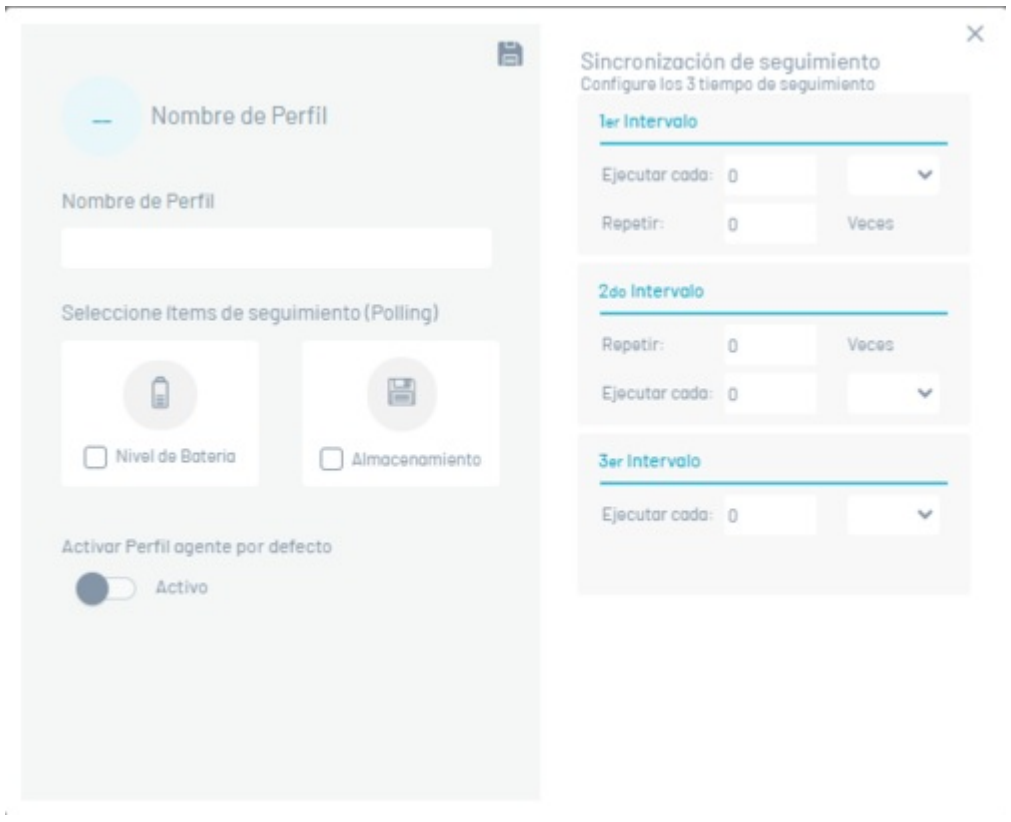
Esta sección se presenta la configuración disponible para la funcionalidad de “polling”, desde los dispositivos, que consiste en que cada cierto periodo de tiempo el dispositivo por sí mismo, sin necesidad de una notificación push, contacte al servidor de AEMM, en busca de comandos pendientes. Adicionalmente este contacto son servidor se puede aprovechar para entregar cierta información configurable de estado del dispositivo.

Creación de un perfil de agente

Para crear un perfil de agente de clic en **Nuevo**



Complete la siguiente información y haga clic en el ícono **Guardar**.

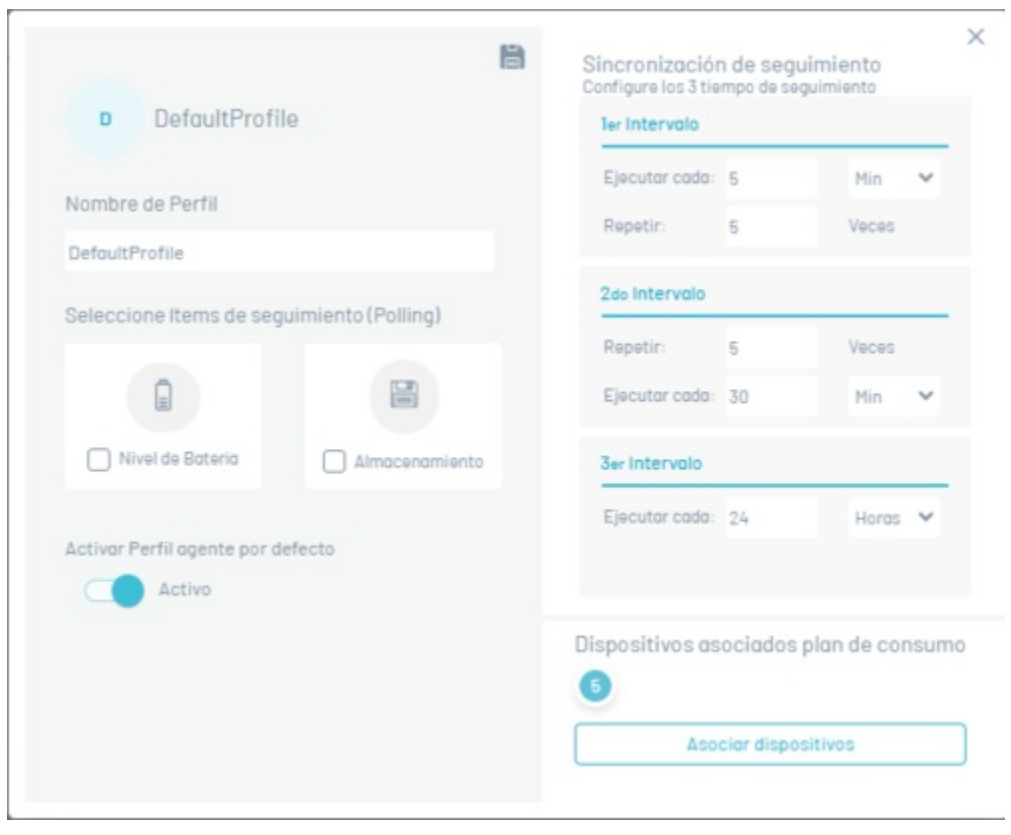


Los campos presentados corresponden a las tres etapas consecutivas del polling desde los dispositivos:

Campos	Descripción
Primer intervalo:	Primera etapa, donde se puede configurar el intervalo de tiempo y la cantidad de veces a ejecutar.
Segundo intervalo:	Primera etapa, donde se puede también configurar el intervalo de tiempo y la cantidad de veces a ejecutar.
Tercer intervalo:	Tercera etapa, en la que sólo se puede configurar el intervalo de tiempo, ya que este es el intervalo que quedará permanentemente una vez se hayan superado las dos primeras etapas.

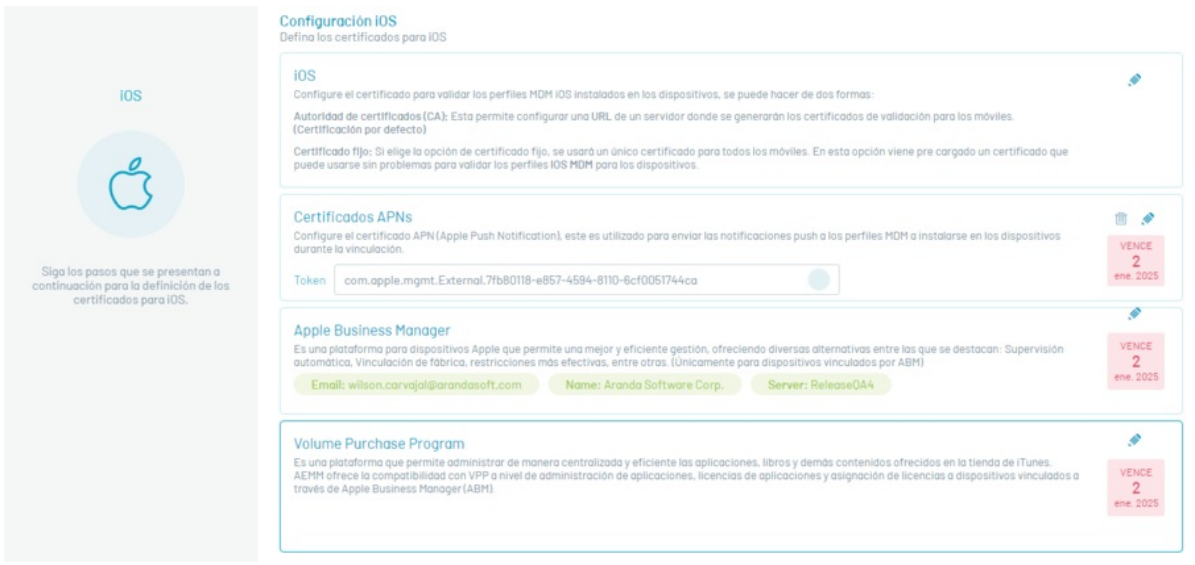
Asociación de dispositivos a un perfil de agente

Haga clic sobre una de las reglas previamente creadas y en la opción que se habilita, haga clic en el botón Asociar dispositivos, donde podrá asociar o eliminar dispositivos a la regla.



iOS

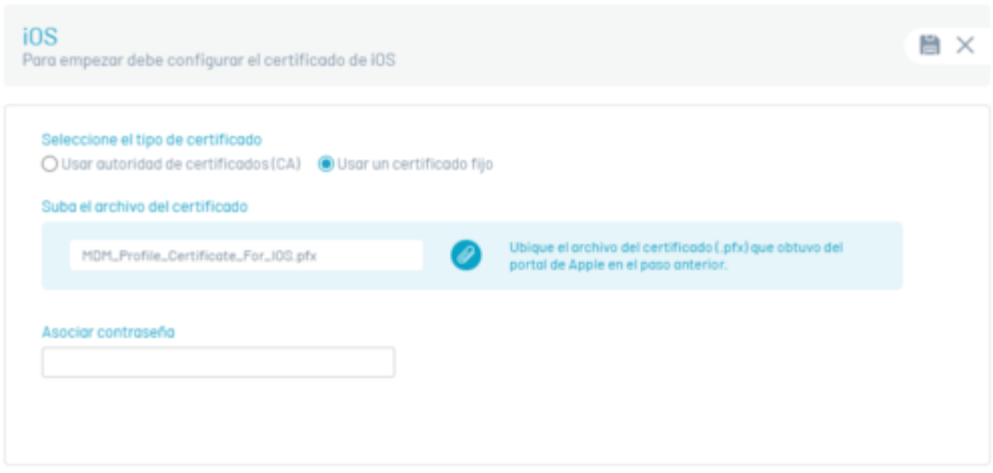
En esta sección se pueden configurar las opciones correspondientes para la gestión de dispositivos de la plataforma iOS



Sección "iOS"

En esta sección podrá configurar el certificado con el que se validarán los perfiles MDM iOS instalados en los dispositivos. Para realizar la configuración, haga clic en la opción de Edición (ícono de lápiz) para visualizar la ventana donde podrá configurar el certificado de dos formas:

Campos	Descripción
Usando autoridad de certificados (CA):	Esta opción permite configurar una url de un servidor donde se generarán los certificados de validación para los móviles.
Certificado fijo:	Si elige la opción de certificado fijo, se usará un único certificado para todos los móviles. En esta opción viene precargado un certificado que puede usarse sin problemas para validar los perfiles iOS MDM para los dispositivos.

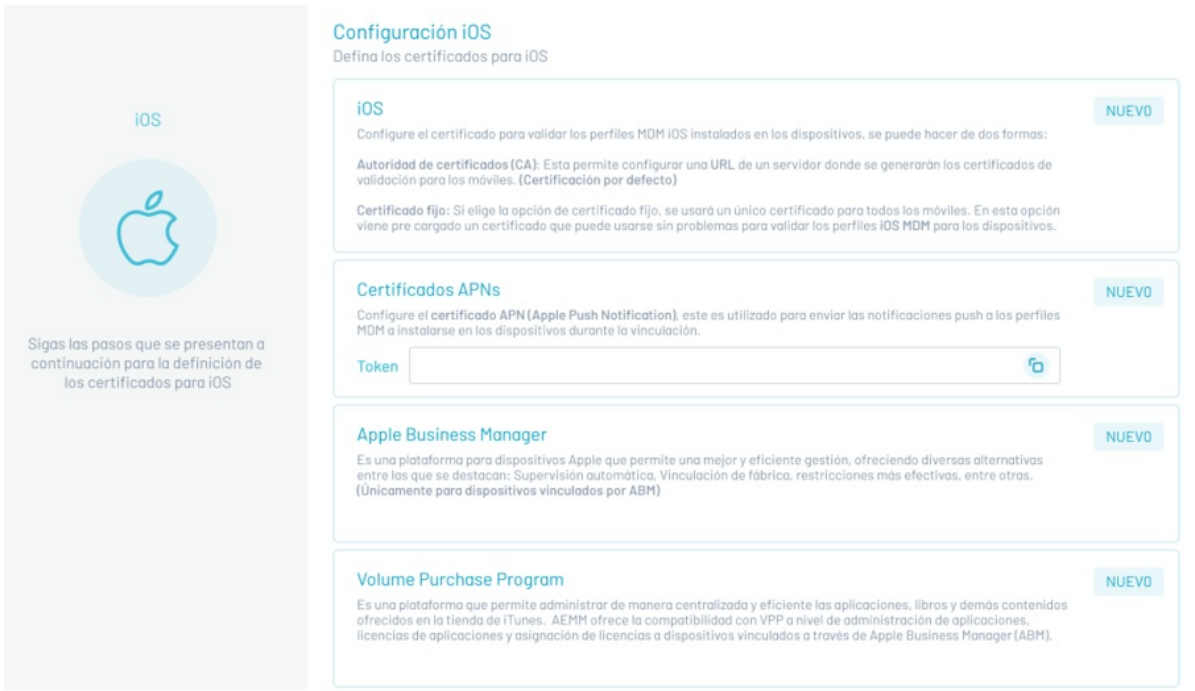


Sección Certificado APNs

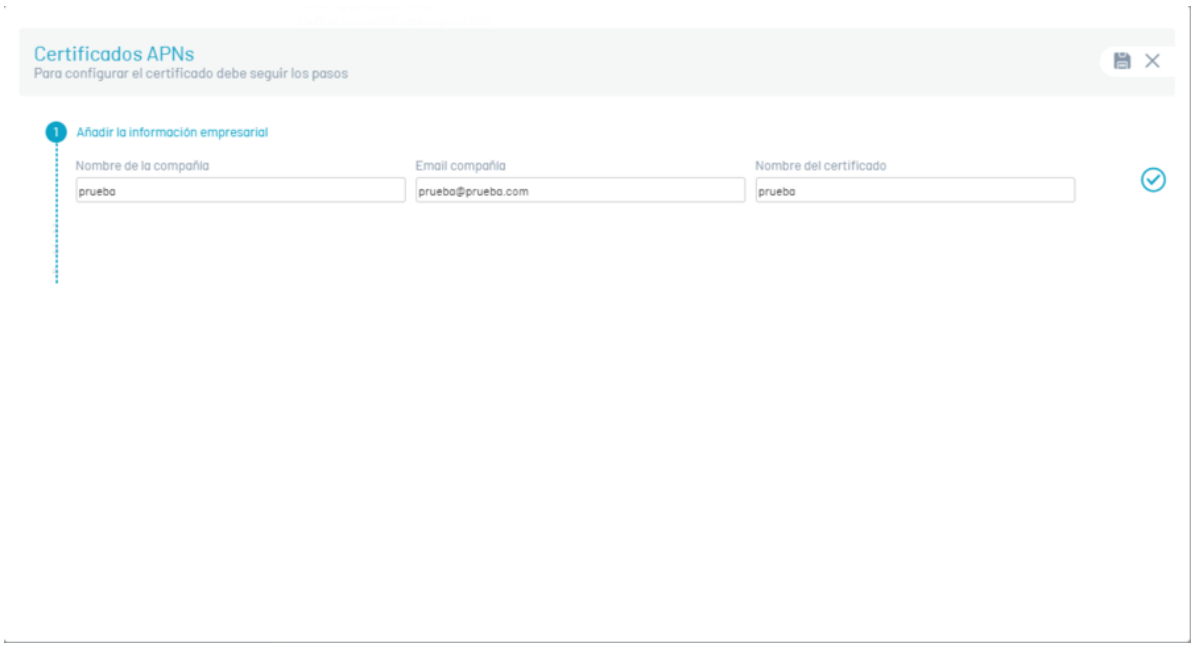
En esta sección podrá configurar el certificado APN (Apple Push Notification), utilizado para enviar las notificaciones push a los perfiles MDM a instalarse en los dispositivos durante la vinculación. Para realizar la configuración siga los siguientes pasos:

Creación de un Certificado APN Nuevo

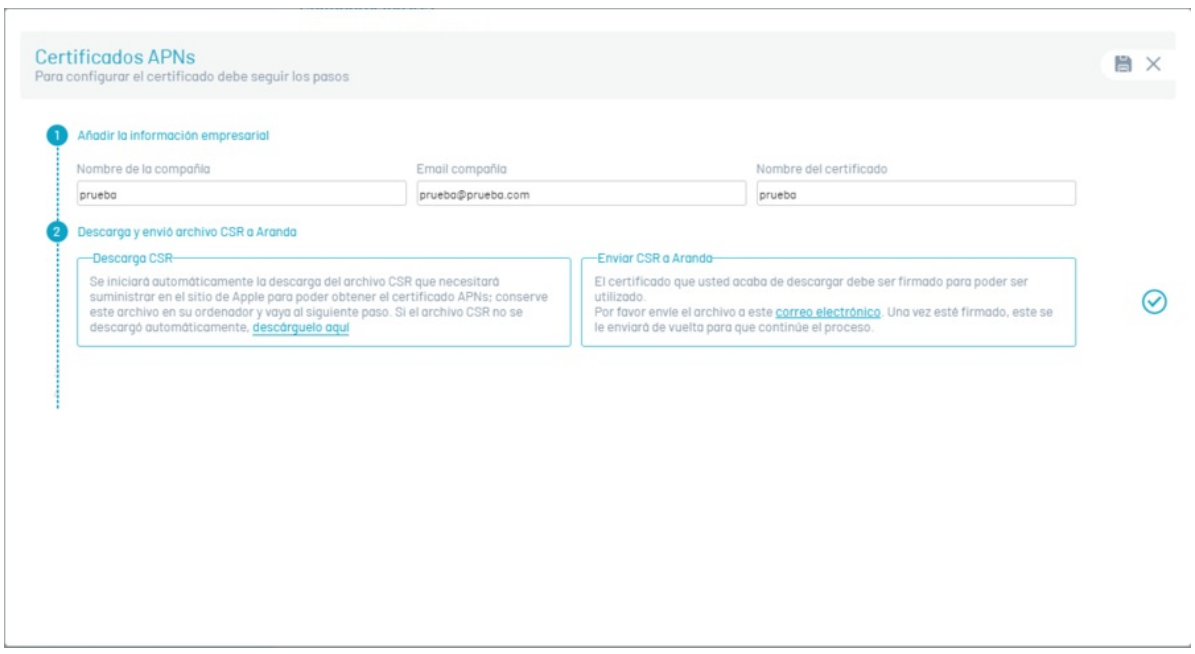
Ingrese a **certificado APNs** y de clic en **Nuevo**



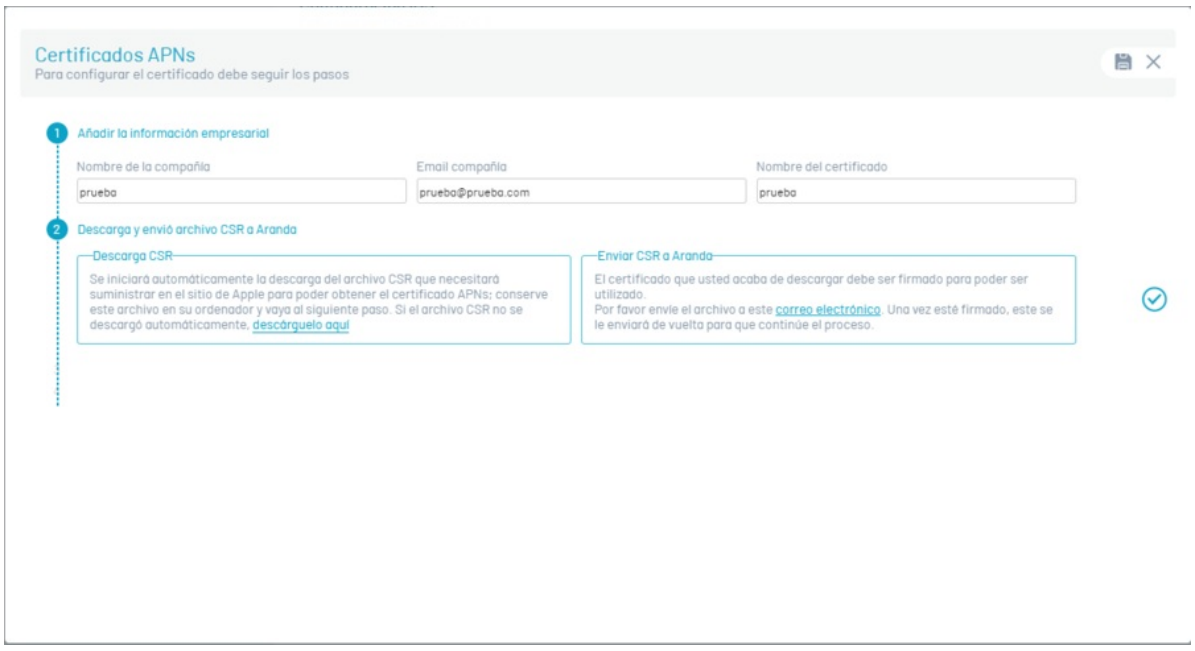
Ingrese el nombre y correo de la compañía, adicional el nombre del certificado y después de clic en Continuar (ícono de check).



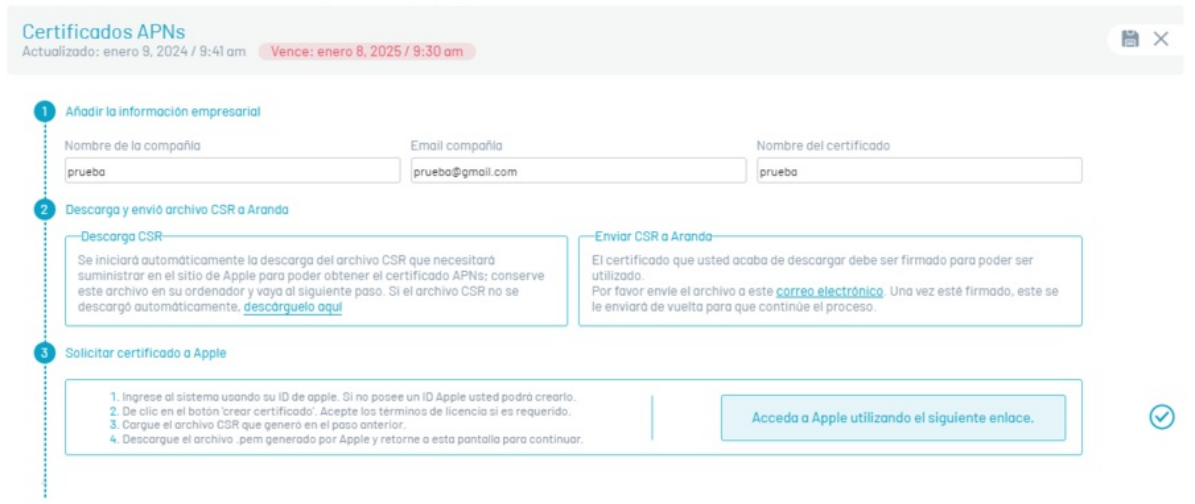
A continuación se descarga automáticamente el archivo CSR que deberá guardar. Este archivo CSR cambia cada vez que se realice este proceso; se recomienda completar el proceso de configuración de APN con el mismo archivo CSR.



Envíe el archivo CSR a su representante en Aranda a través de correo electrónico y haga clic en el ícono de check correspondiente al paso 2.

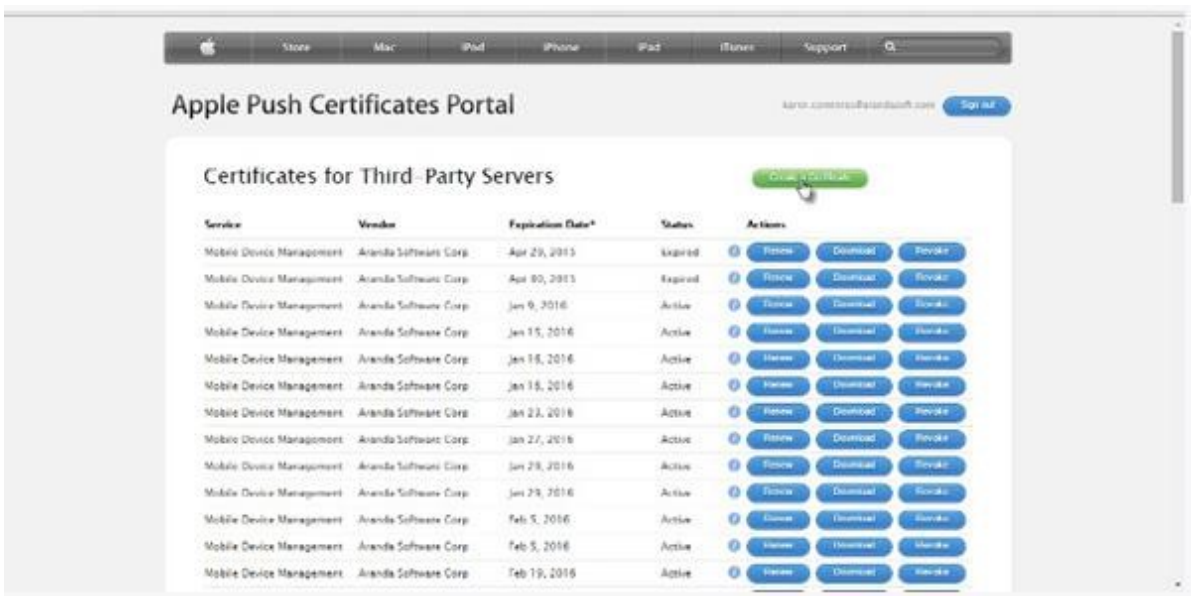


Ingrese a la página de Apple para generar el certificado APNs



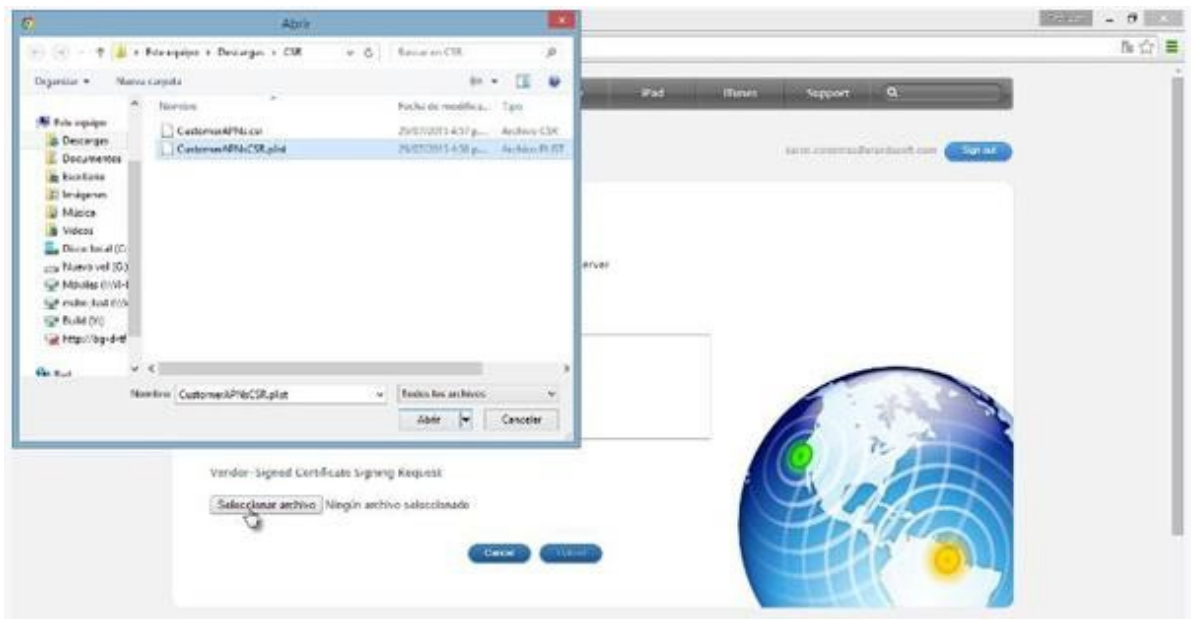
Digite su Apple ID y contraseña

Haga clic en la opción **Crear certificado**



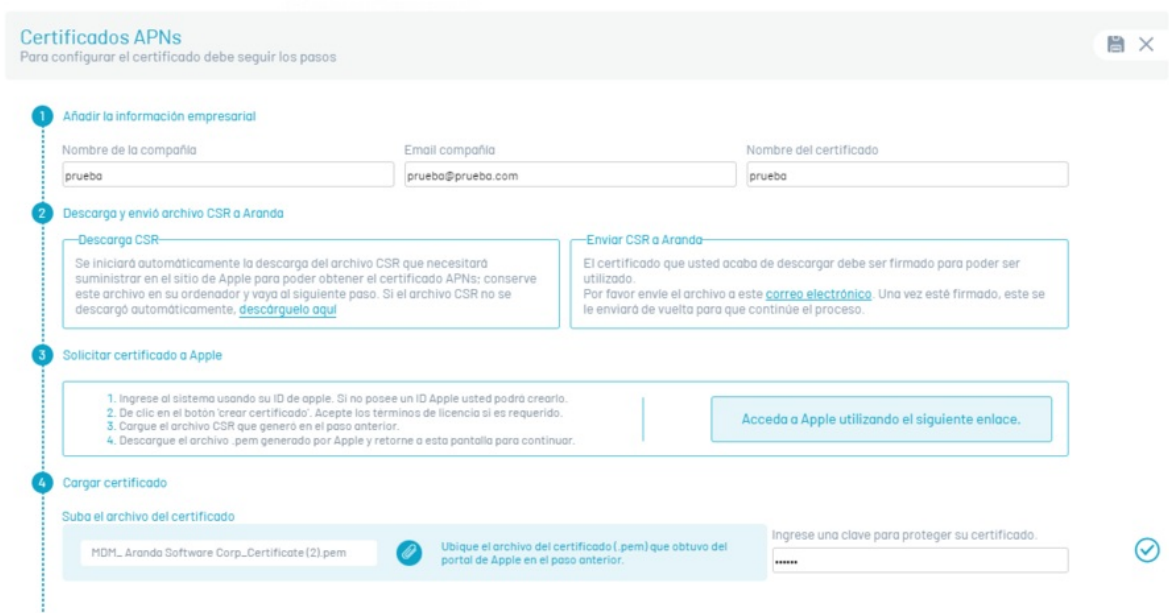
Acepte términos y condiciones.

Seleccione el archivo “PLIST”, que recibió por correo electrónico del representante en Aranda.

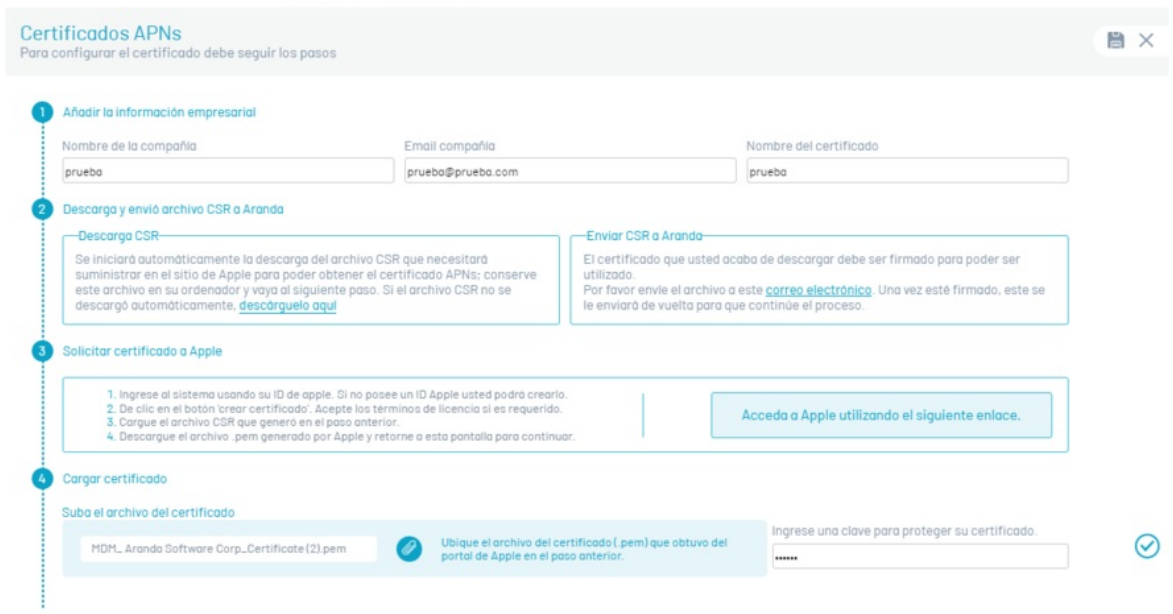


Escriba una breve descripción del certificado que se está creando, con el objetivo de identificarlo en el futuro. Descargue y guarde el archivo PEM que se genera.

Continúe dentro de la consola y después haga clic en el ícono de check correspondiente al paso 1 y adjunte el archivo “PEM” que fue generado en el paso anterior.



En la sección **Cargar Certificado** haga clic en el ícono de check correspondiente al paso 4.



El certificado debe quedar cargado exitosamente.

El certificado creado y cargado en el servidor AEMM tendrá validez de un año, contado a partir su generación en la plataforma de APN Push Notificacion de Apple.

Este certificado se asocia a las subsiguientes vinculaciones de dispositivos de la plataforma iOS en tanto que no puede reemplazarse con un certificado nuevo, acto tal que tendría como consecuencia el aislamiento de los dispositivos del servidor AEMM y su derivada imposibilidad de recibir y procesar comandos.

Este certificado creado tiene que ser renovado antes de su vencimiento y para tal cuando se crea se pone una alerta de sistema que realiza un recordatorio un mes antes del vencimiento del certificado.

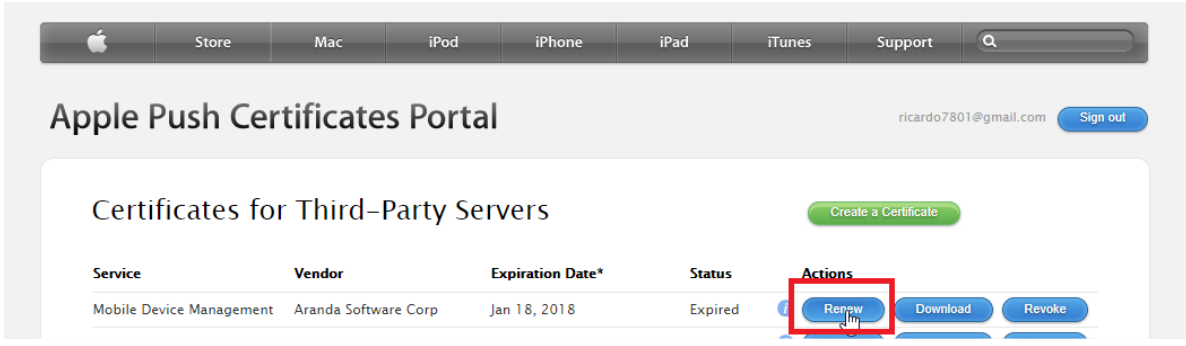
Si no se hace el procedimiento de renovación a tiempo, ocasionará un efecto semejante al de cambiar el certificado por otro nuevo, que es el aislamiento total e irreversible de los dispositivos ya vinculados y que usen el presente certificado APN.

En el siguiente numeral se detalla el proceso de renovación del certificado APN.

Renovación de un certificado APN previamente creado

Ejecute 5 primeros pasos del proceso anterior (Creación de un Certificado APN Nuevo) y continuación realice lo siguiente:

Una vez en la plataforma de APN de Apple ubique el registro del certificado en cuestión y haga clic en "Renew" (Renovar).Para la identificación del registro en cuestión puede usar la descripción corta ingresada al momento de su creación, esto en el caso de que posea más de un registro en su cuenta de APN.

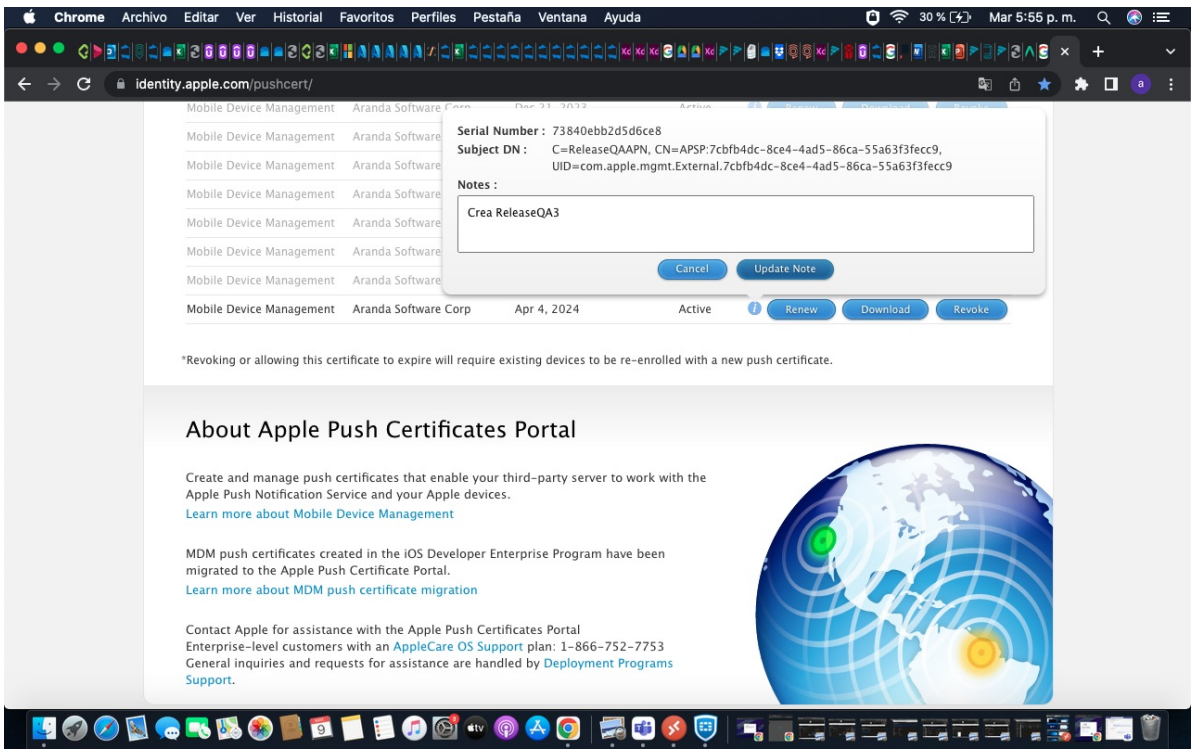


A continuación, ejecute los pasos h, i, j, k, l, m del numeral anterior, para completar el proceso.

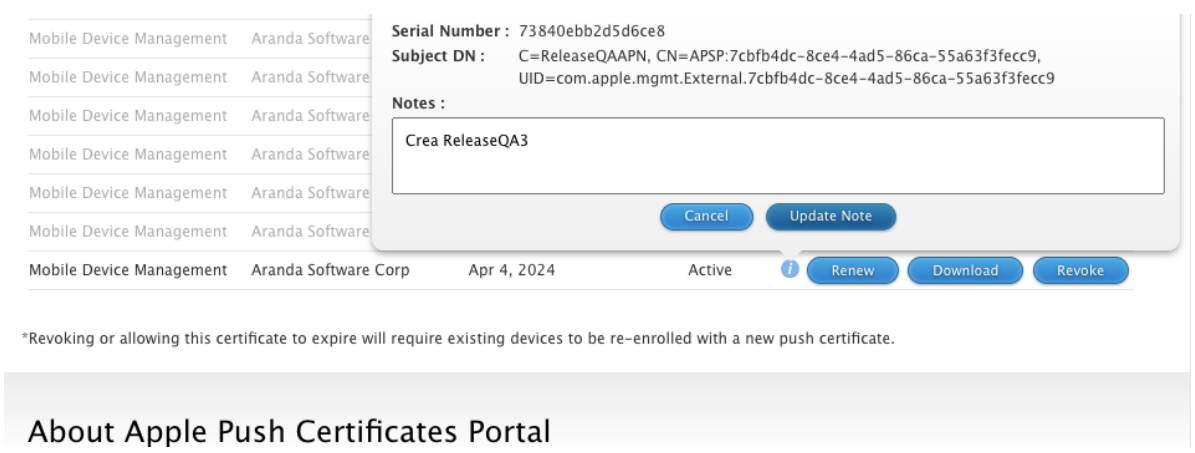
El certificado renovado tendrá el mismo periodo de validez de 1 año y deberá también ser renovado antes que expire, para no alcanzar las consecuencias ya descritas.

Validación del certificado APN

En el proceso de renovación (actualización) del APN, el APN configurado debe coincidir con el nuevo archivo APN que se va actualizar y podrá consultarlo desde la consola de Apple donde creó y renovó el certificado (https://identity.apple.com/pushcert/). En la autenticación ingrese el mismo correo con el que se creó el certificado.



Al seleccionar el registro, en el ícono de información, le mostrará los siguientes datos: serial number y subject DN; este último item en la etiqueta UID: (com.apple.mgmtExternal.XXXX, como se muestra en la imagen)

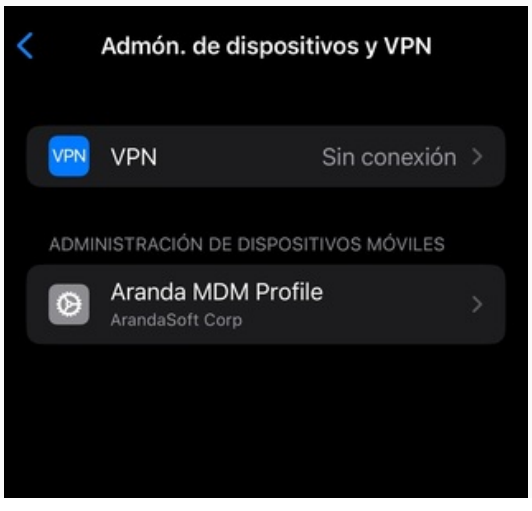


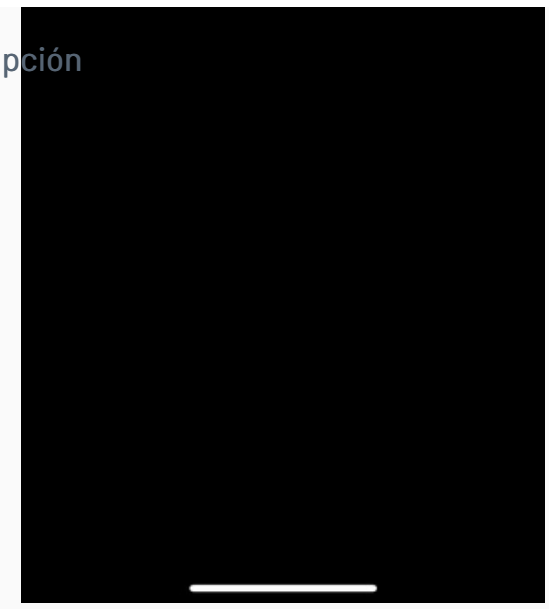
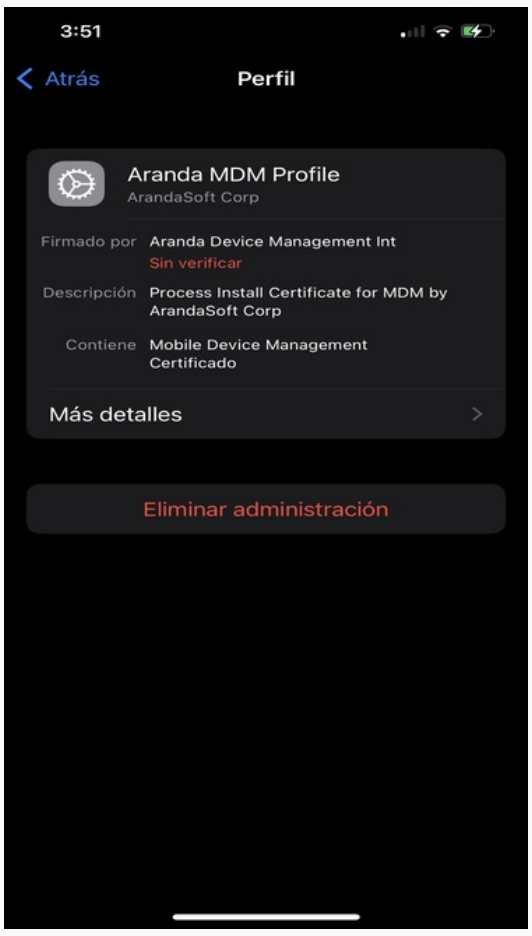
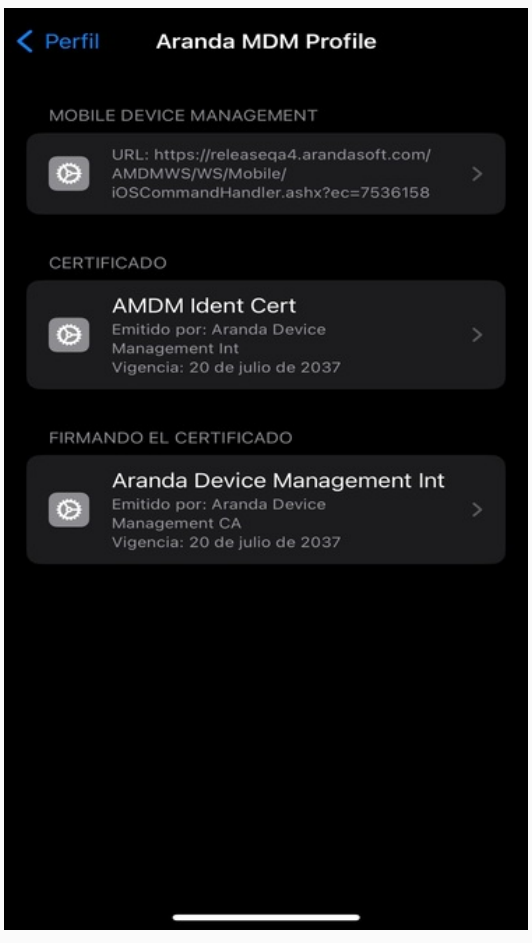
Está información debe coincidir con la del perfil que se encuentra en los dispositivos vinculados, como se describe a continuación:

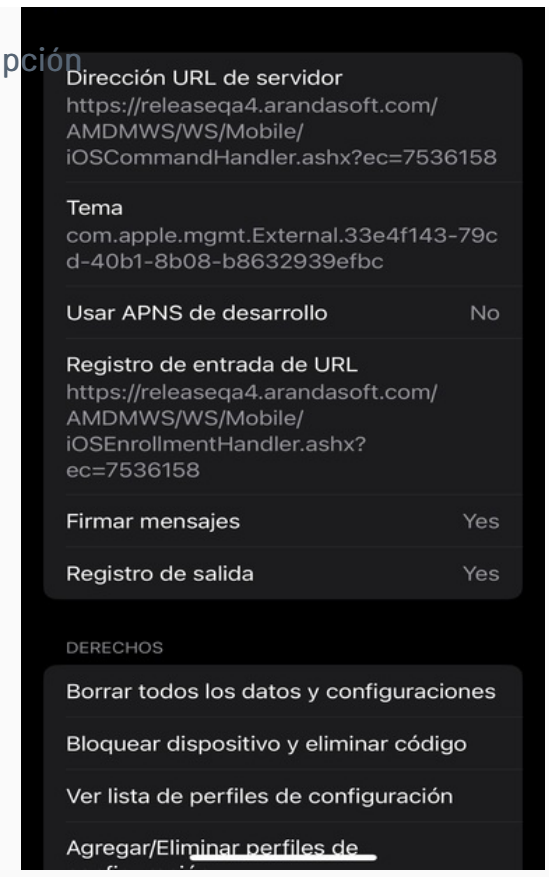
1- Seleccione un dispositivo vinculado antes de realizar la actualización del APN.

2- En el dispositivo ir a la opción configuraciones ->Admón de dispositivos y VPN->Aranda MDM Profile-> Mas detalles-> Mobile device management-> Tema1

Visualización del tema del APN en los dispositivos iOS

Campo	Descripción
	

Settings	Descripción
Settings	
Settings	
Settings	
	

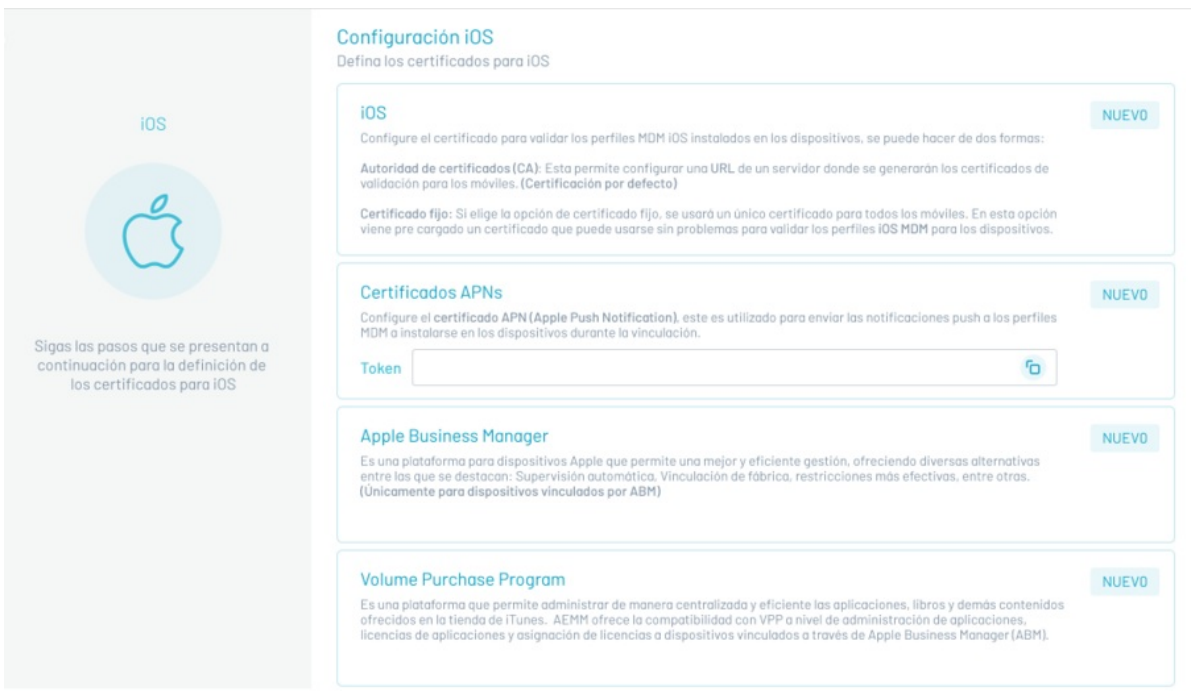
Campo	Descripción
Settings	

Sección Apple Business Manager (ABM)

Apple Business Manager es una plataforma para dispositivos Apple que permite una mejor y eficiente gestión, ofreciendo diversas alternativas entre las que se destacan: Supervisión automática, Vinculación de fábrica, más efectivas restricciones, entre otras.

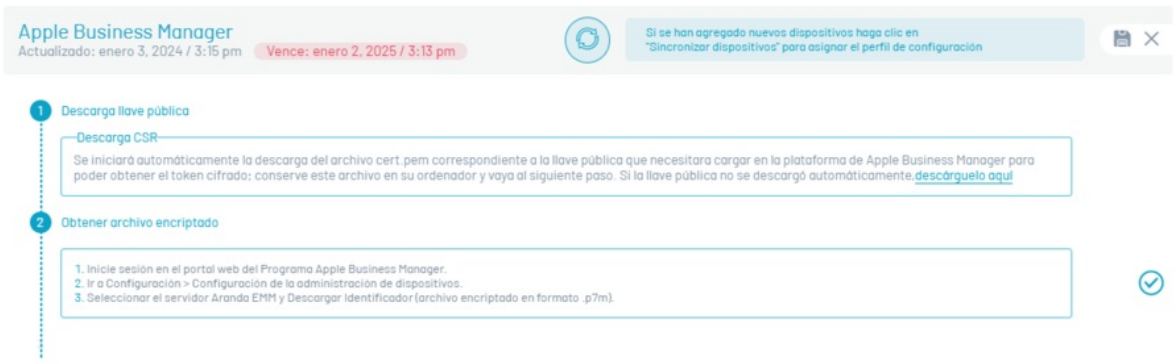
Para activar esta funcionalidad es necesario tener una cuenta vigente en la plataforma de Apple Business Manager (https://business.apple.com/) y realizar los siguientes pasos:

Navegue hasta la sección Apple Business Manager y haga clic en **Nuevo**

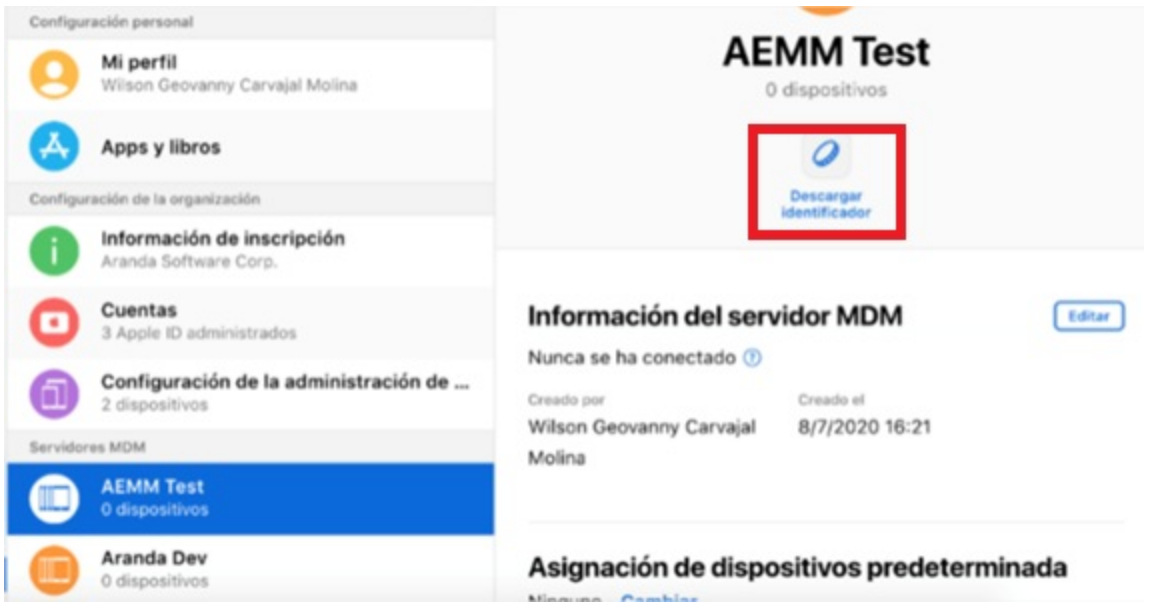


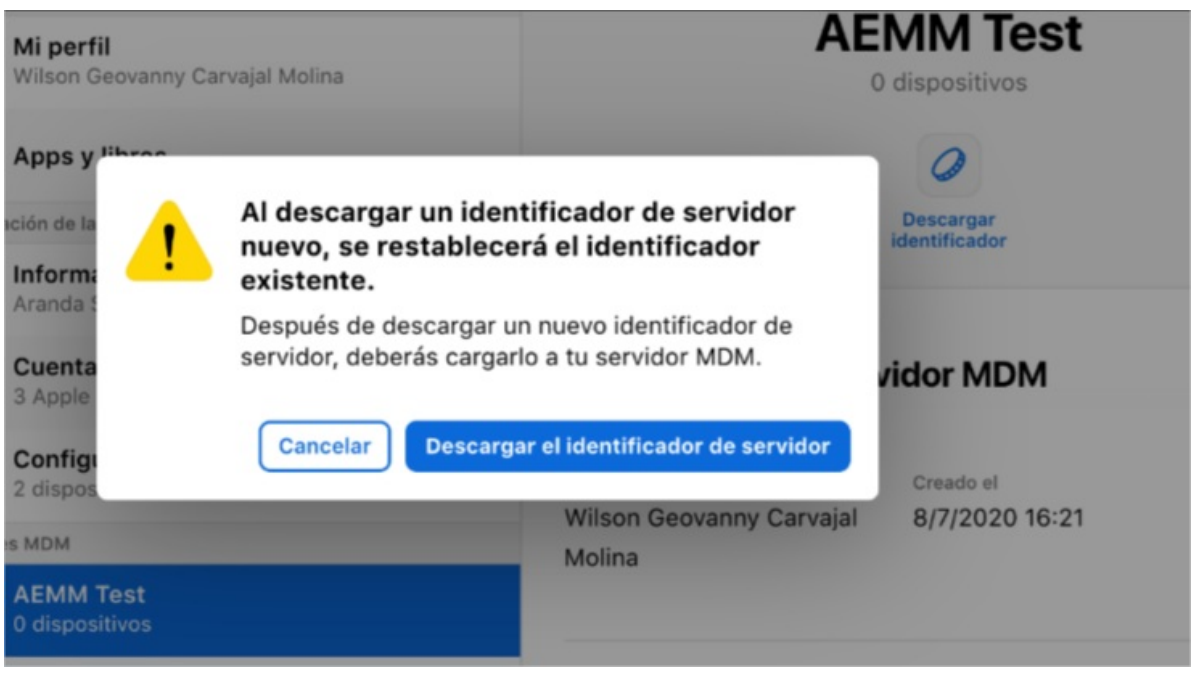
Guarde el archivo cert.pem que identificará la instancia del servidor AEMM de manera única. Guárdelo en un lugar seguro y haga clic en el ícono de check correspondiente al paso 1.

A continuación, se darán las indicaciones correspondientes para vincular la consola AEMM con la llave pública descargada en el paso anterior, en la consola de administración de Apple Business Manager.



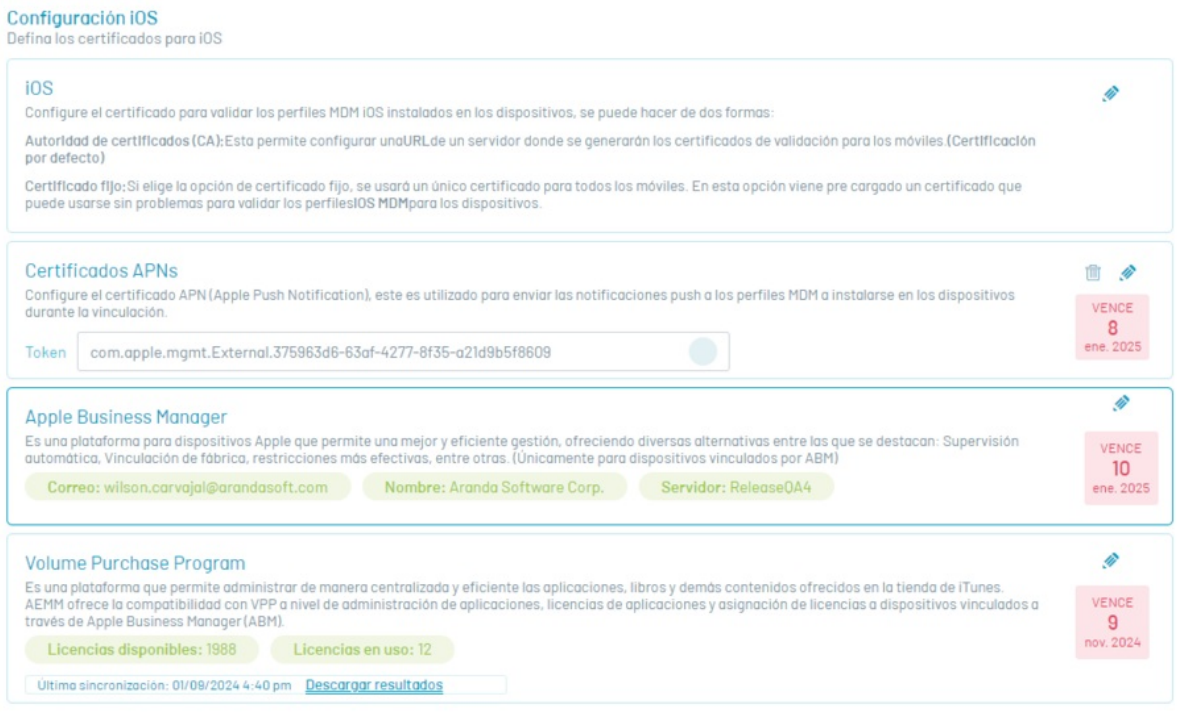
Seleccione Guardar y para finalizar descargue del archivo con extensión **p7m** en la opción **Descargar identificador.**





En la consola de AEMM, haga clic en el ícono check correspondiente al paso 2 y cargue en la consola AEMM el archivo de extensión p7m descargado de la consola de administración de Apple Business Manager. Cargue el archivo de extensión p7m.

Después de seleccionar el archivo, haga clic en el check, correspondiente al paso 3.



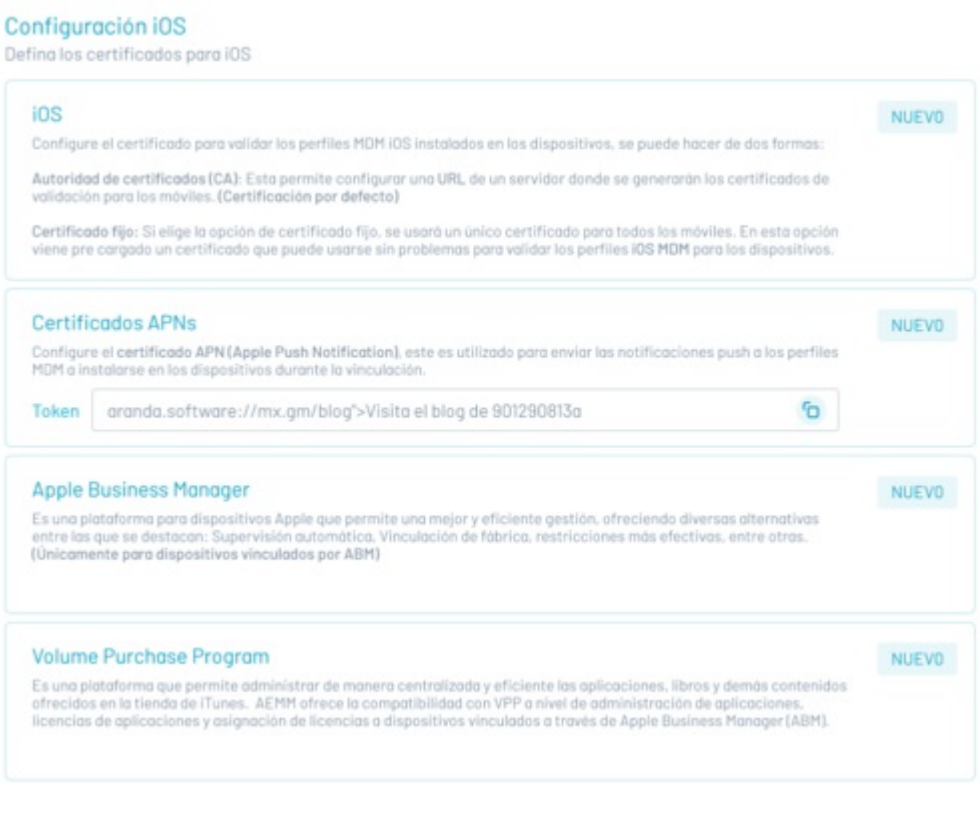
Sección Volume Purchase Program (VPP)

Volume Purchase Program de Apple es una plataforma que permite administrar de manera centralizada y eficiente las aplicaciones, libros y demás contenidos ofrecidos en la tienda de iTunes.

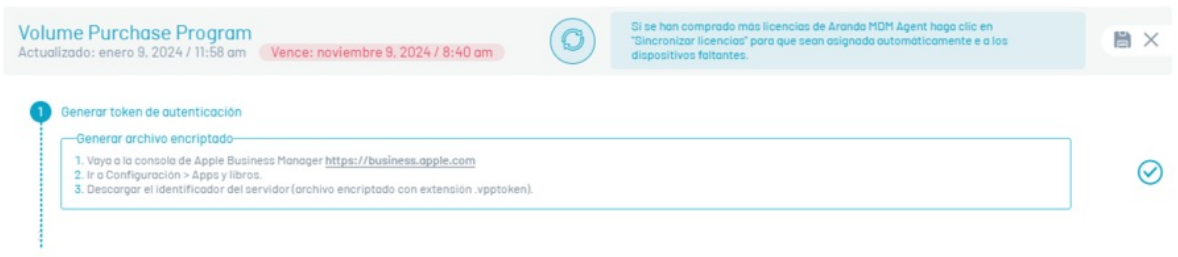
AEMM ofrece la compatibilidad con VPP a nivel de administración de aplicaciones, licencias de aplicaciones y asignación de licencias a dispositivos vinculados a través de Apple Business Manager (ABM).

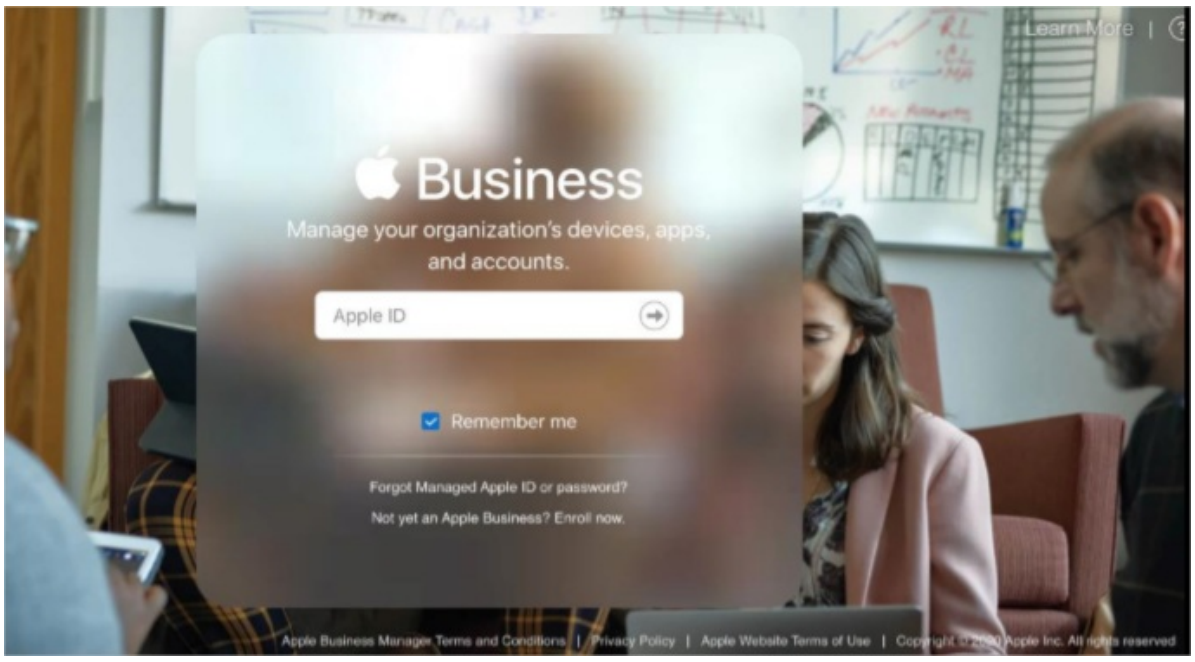
Para vincular el servidor AEMM con VPP realice las siguientes acciones:

En la sección Volume Purchase Program, haga clic en **Nuevo**

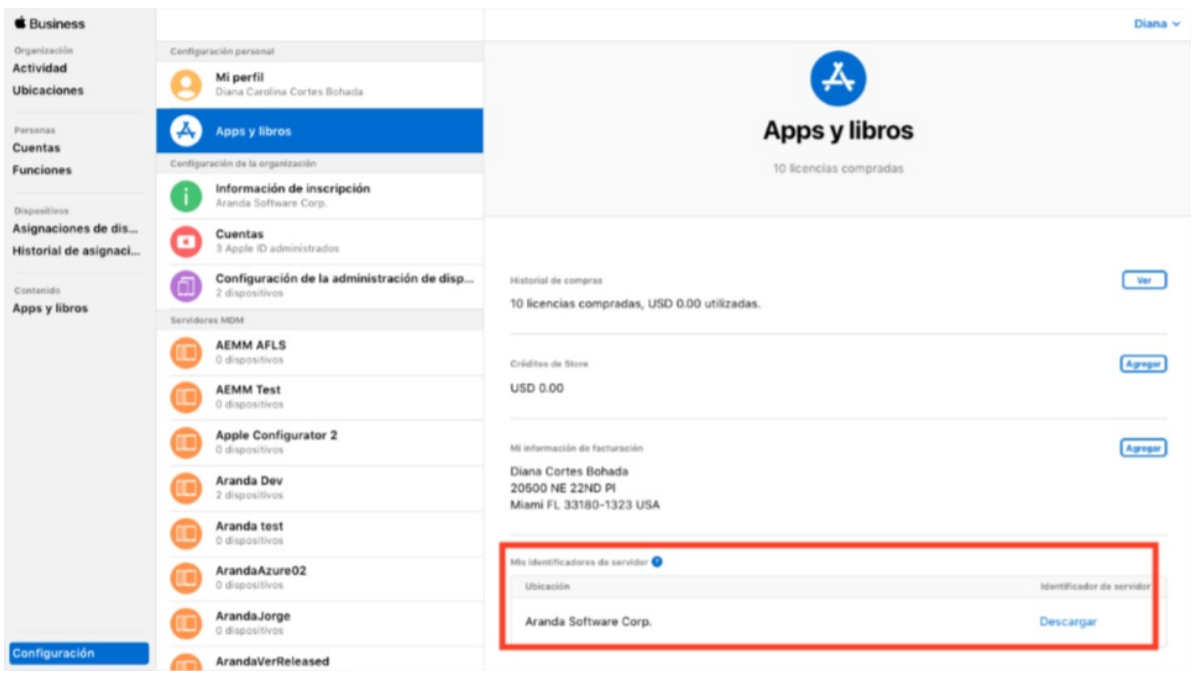


De acuerdo a las instrucciones presentadas, ingrese a la consola de Apple Business Manager, para generar el token de autenticación.



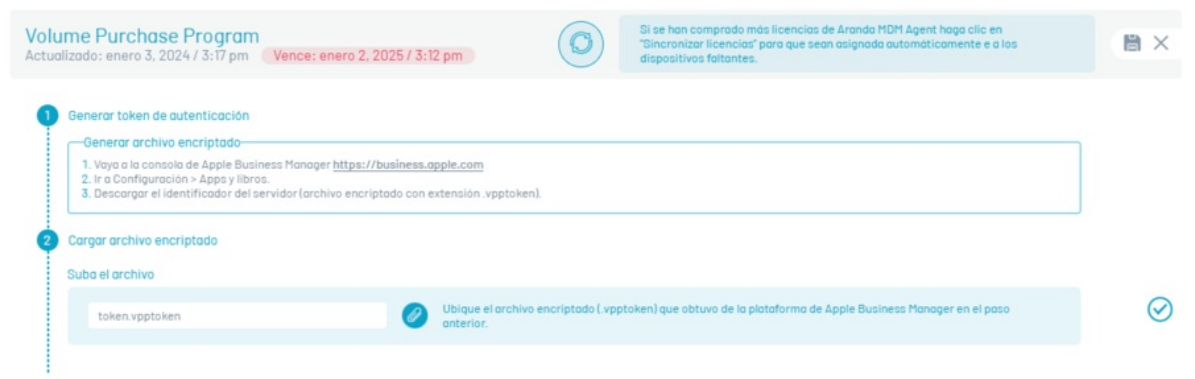


Una vez dentro de la consola de administración de ABM diríjase a la opción **Configuración** > **Apps y Libros**, allí visualizará la identificación de los servidores configurados; haga clic en **Descargar**.

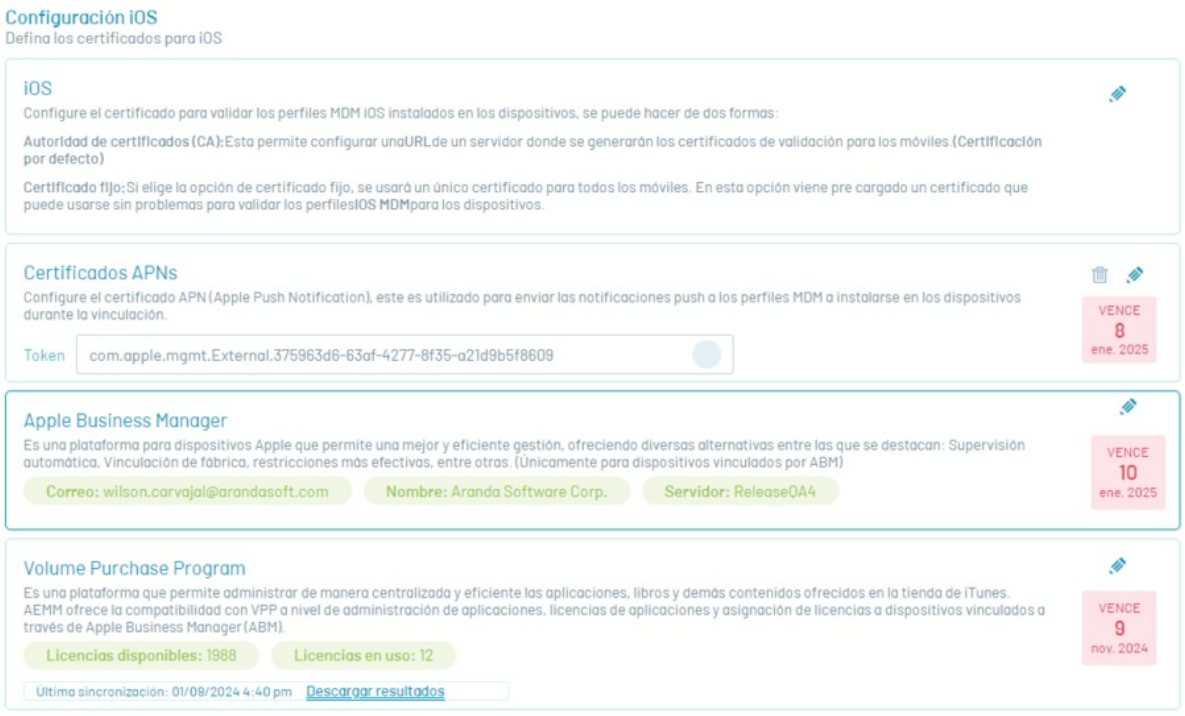


Guarde el archivo descargado en un lugar seguro, ingrese a la consola de AEMM y haga clic en el ícono de check correspondiente al paso 1.

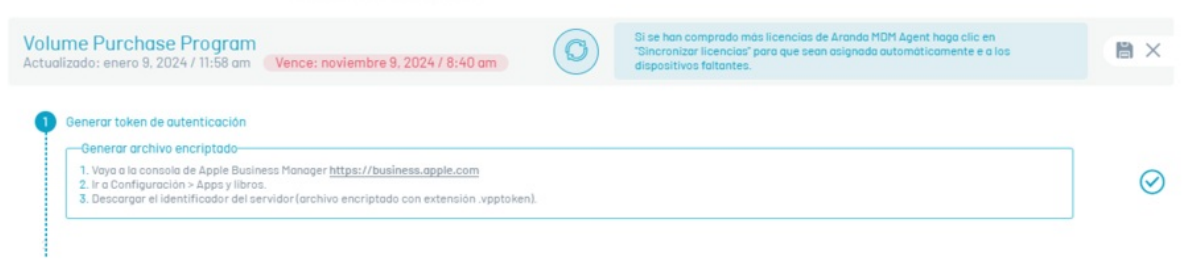
Cargue el archivo descargado de la consola ABM del paso anterior, haga clic en el botón y cargue el archivo.



Haga clic en el ícono de check correspondiente al paso 2 para finalizar el proceso.



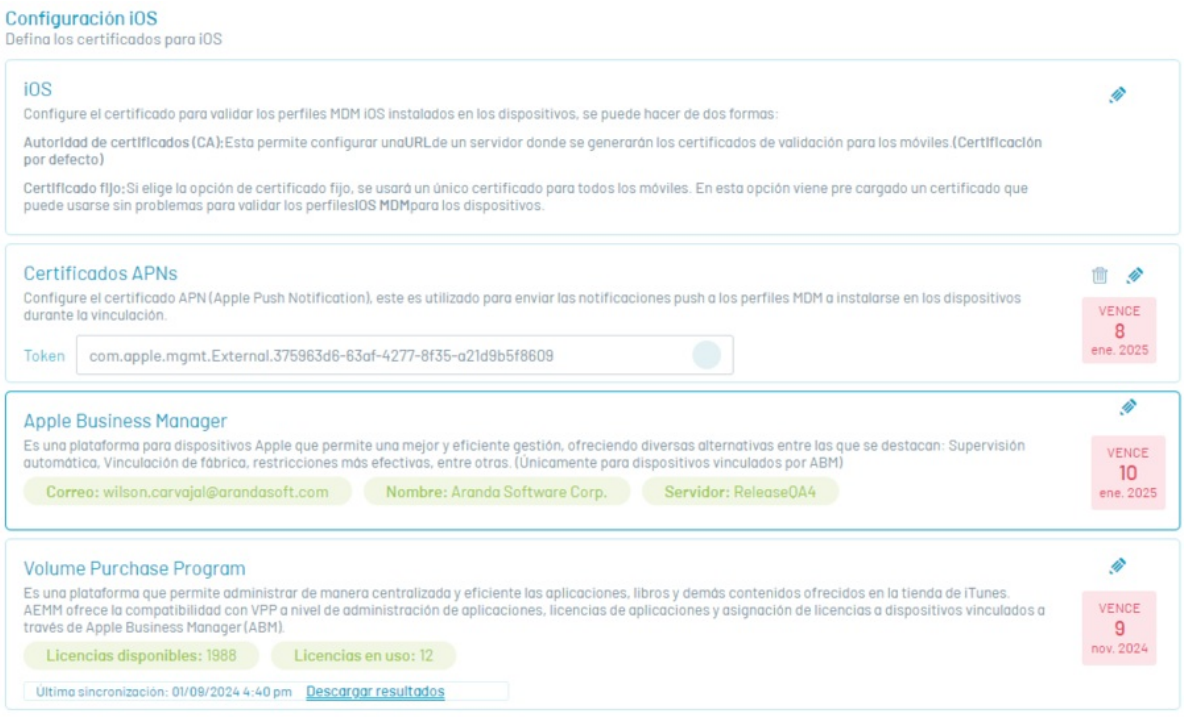
Para realizar el proceso de sincronización de licencias, en la sección **Volume Purchase Program** haga clic en el ícono **Editar** y en la ventana que se habilita, hacer clic en el ícono **Sincronizar licencias**. El sistema realizará una asignación automática de licencias del agente AEMM para iOS en los dispositivos que se encuentran vinculados por ABM.



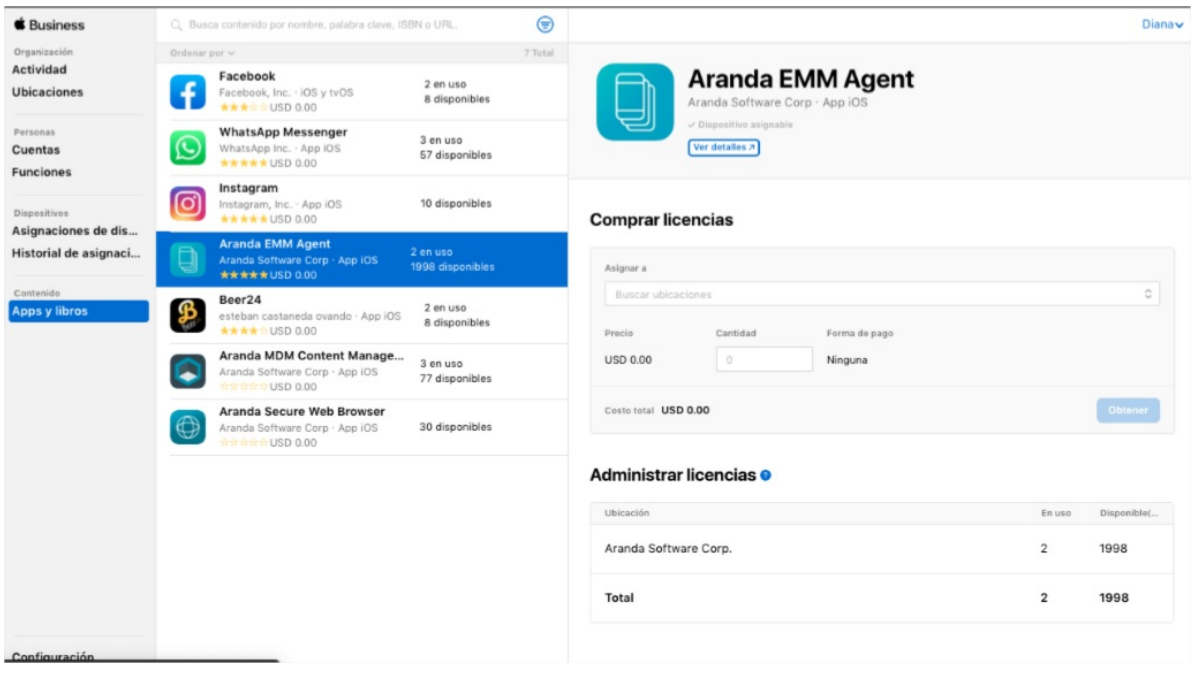
Finalmente, usted observará datos correspondientes a las licencias de Aranda EMM, tales como su estado (disponibles y en uso), la fecha de inscripción del VPP y su vencimiento. Recuerde que las licencias tienen una duración de 1 año.

También aparece una opción para descargar un archivo de resultados, que indica a cuáles dispositivos se les asignó la licencia y a cuáles no.

En consola AEMM:



En consola ABM – VPP



Aspectos a tener presente:

- Antes de realizar la sincronización debe haber licencias disponibles de la aplicación de Aranda EMM en ABM para los dispositivos que se vayan a asignar.
- La aplicación Aranda EMM Agent debe estar importada en el módulo de aplicaciones de la consola de AEMM.

Android for work

En esta sección podrá configurar las opciones necesarias para activar la compatibilidad con el entorno de trabajo empresarial para dispositivos Android, llamado Android for Work (AFW) o Android Enterprise.

Pestaña "Android For Work"

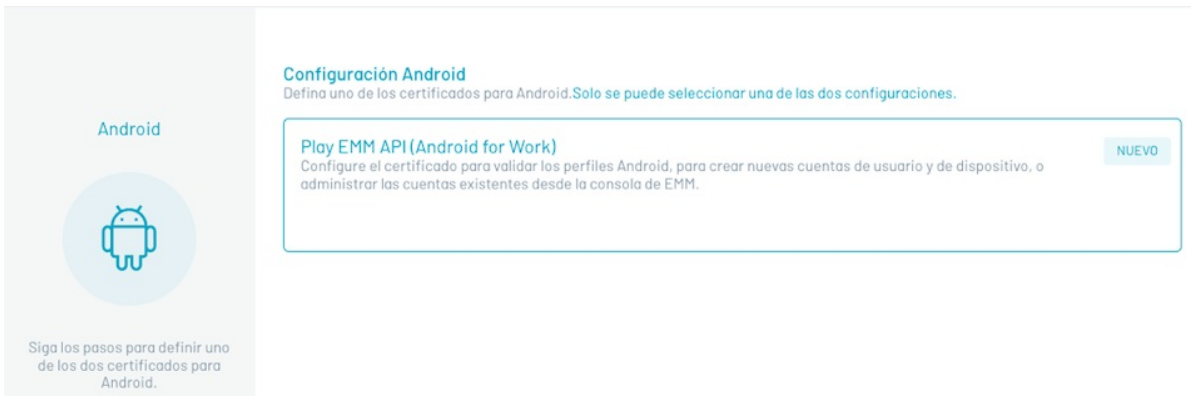
Android For Work o actualmente llamado Android Enterprise es una Infraestructura y Plataforma Integrada para la gestión de dispositivos Android, creada por Google.

AFW ofrece funcionalidades de gestión de dispositivos a nivel de aplicaciones, restricciones y configuraciones que permiten a AEMM tener un mayor control sobre los dispositivos de la plataforma Android.

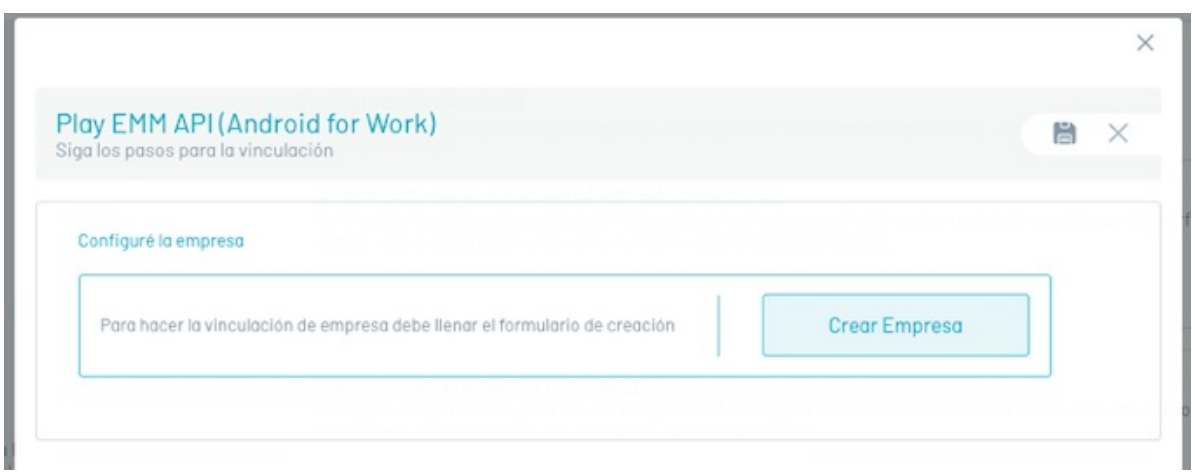
Para el uso de AFW en AEMM se deben de seguir los siguientes pasos:

Ingrese a la consola de Inicio de AEMM, en el menú encabezado seleccione la opción **Configuración**. En la sección *Preferencias del menú principal seleccione la opción **Móviles y Android**.

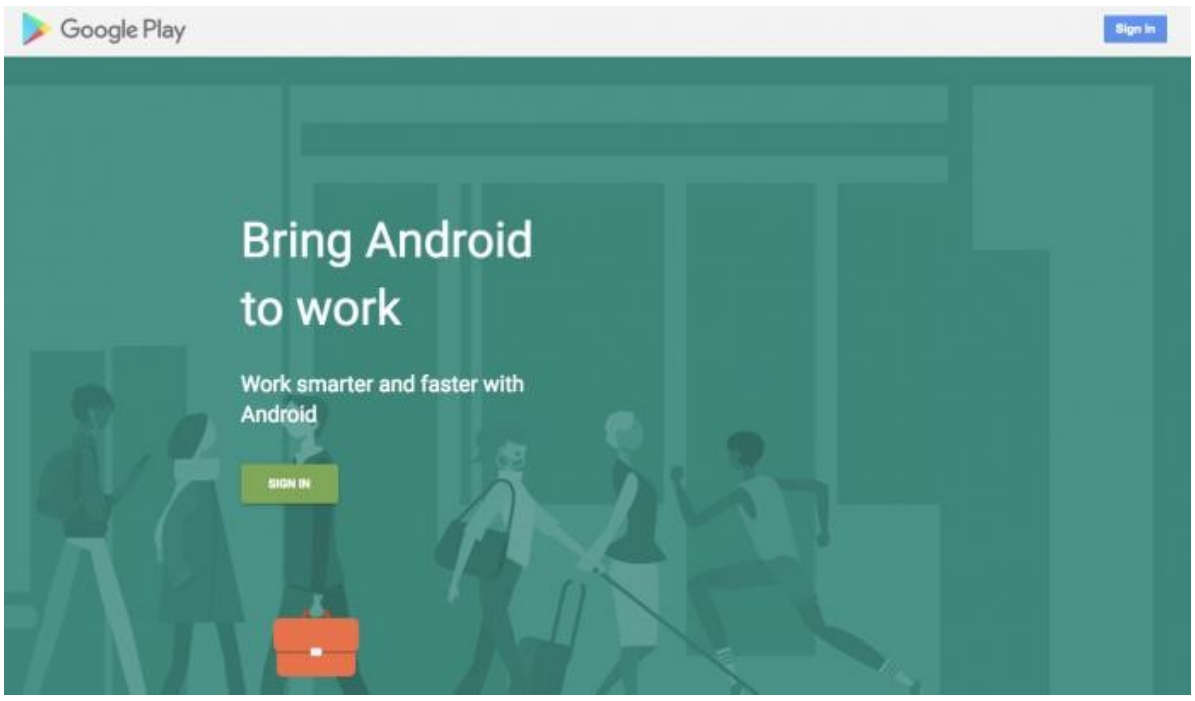
Descripción



Active la configuración Android for Work como se muestra a continuación.

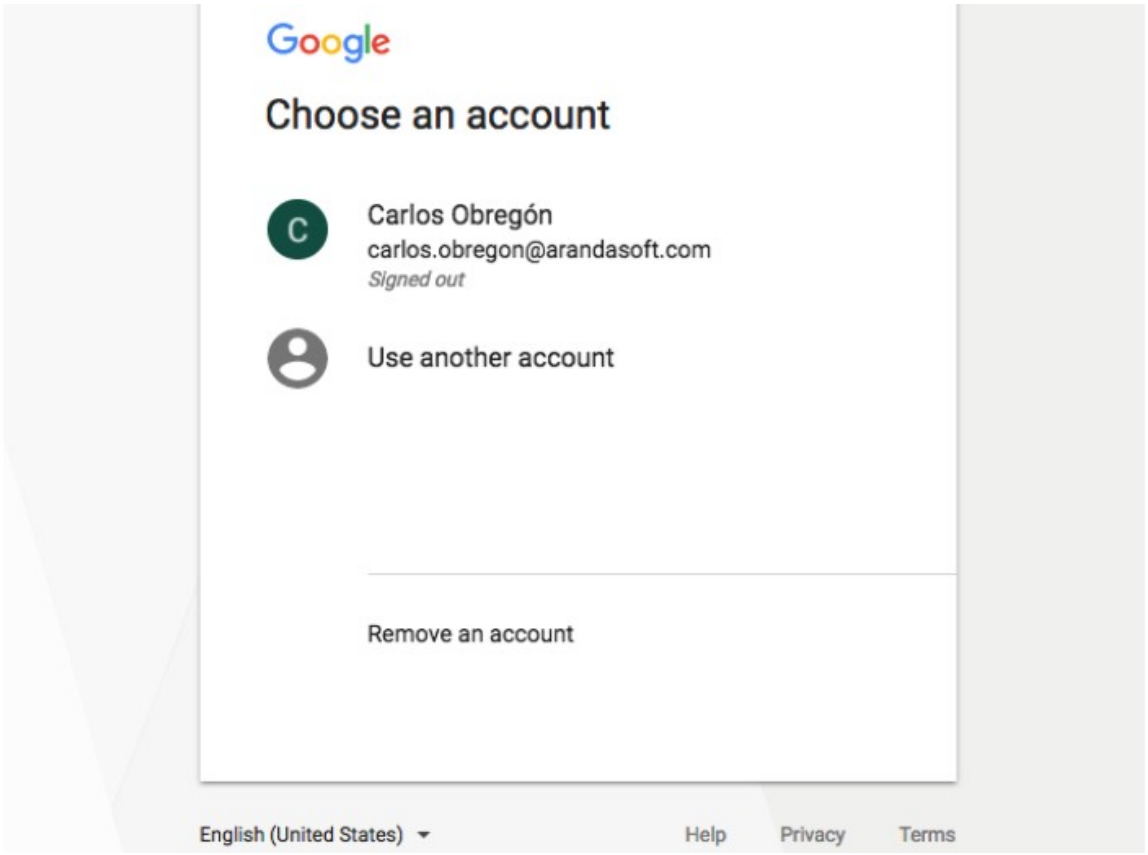


Siga la guía de activación de google.



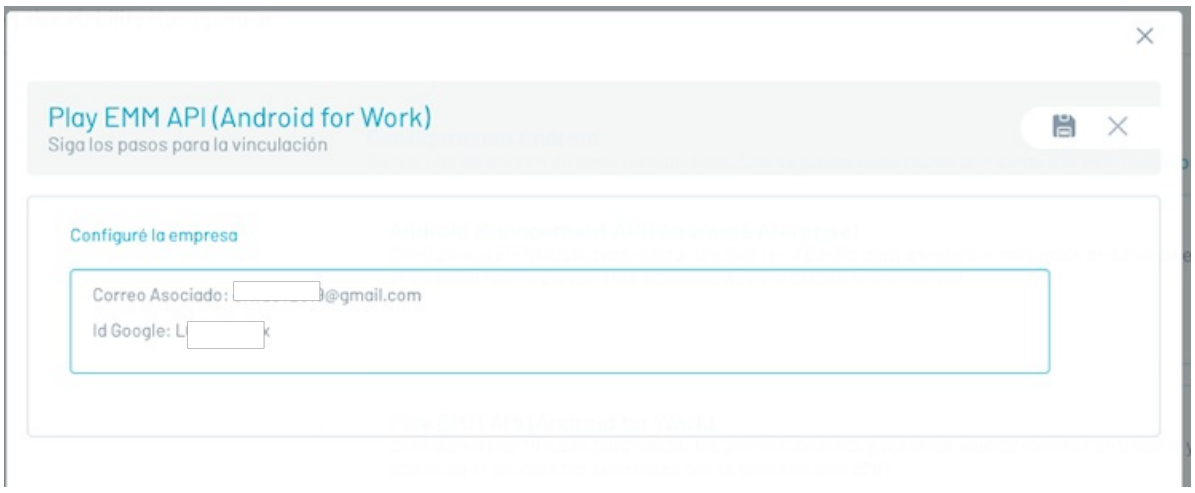
Dentro de esta activación es necesario una cuenta administradora de la organización.

Con esta debe ingresar para registrarse con Android For Work.

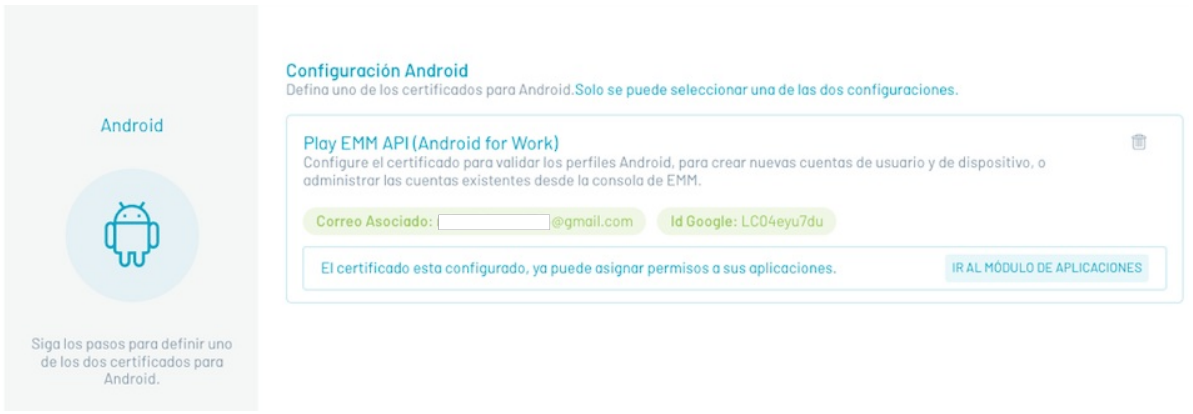


Luego diligencie el formulario de registro solicitado por google y confirme el registro

Si el proceso es exitoso, la consola EMM se debe ver de la siguiente forma:



Haga clic en el ícono guardar, el sistema muestra el correo relacionado y el Id asignado a la consola por google:



Una vez registrada la consola ante Android for Work, se presentan las siguientes opciones:

- Ir al módulo de aplicaciones: Navega a la sección de aplicaciones donde se pueden iniciar operaciones de gestión de aplicaciones ante Android for Work.

Aplicaciones del sistema Android

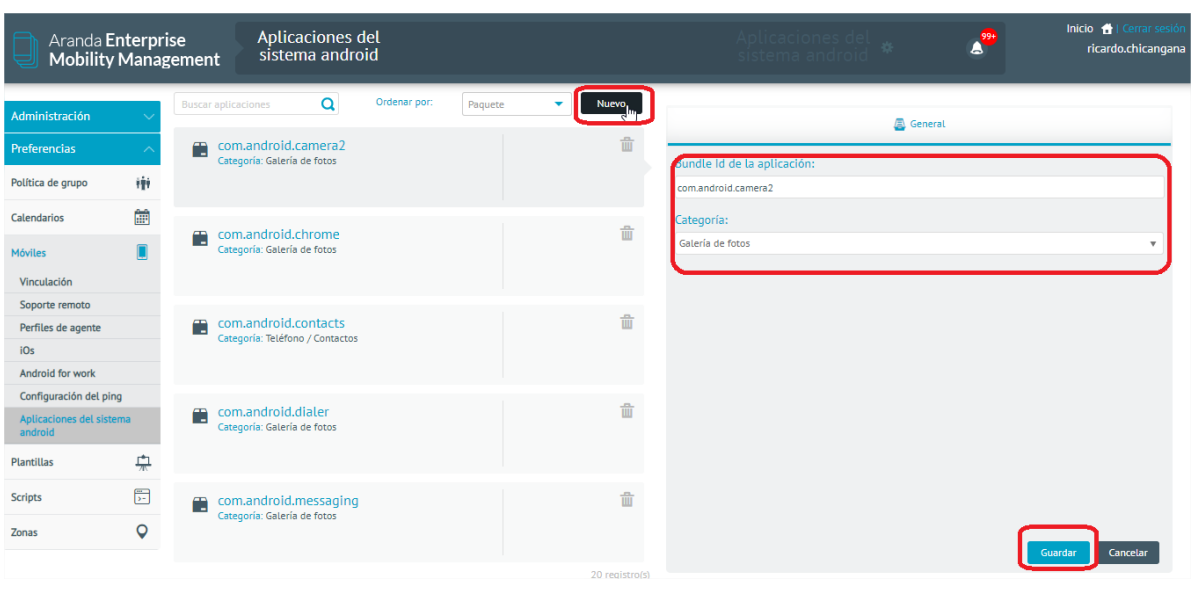
En esta sección de pueden gestionar los nombres de paquetes utilizados para ser visualizados en dispositivos Android en modo de vinculación AFW Device Owner.

Estos paquetes son usados en la sección de aplicaciones del módulo de políticas y en la sección kiosco del mismo módulo.

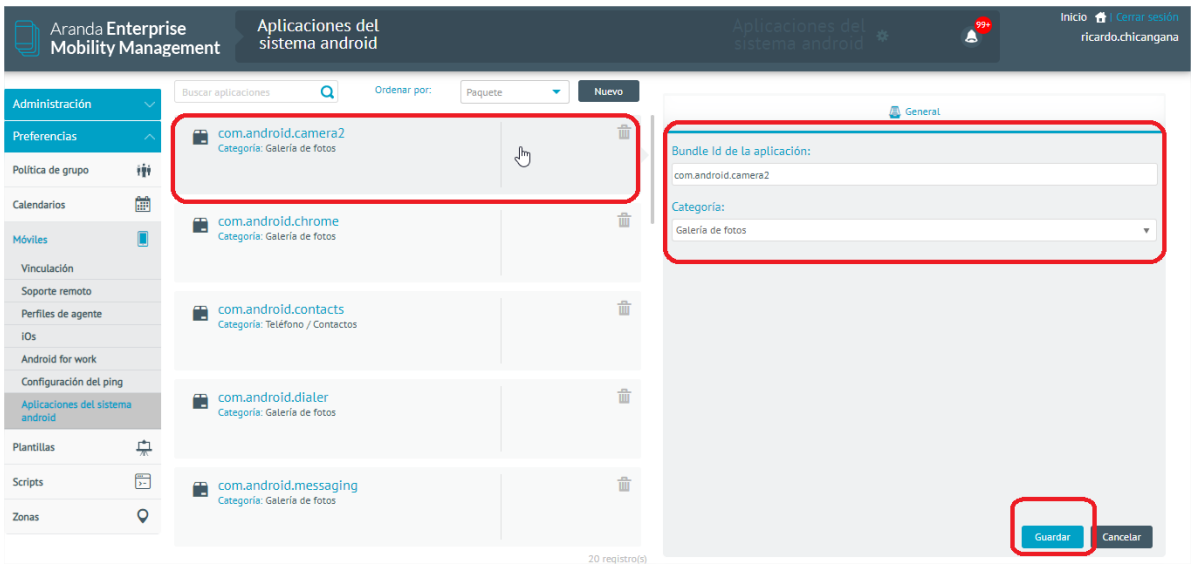
Los paquetes agregados serán enviados a los dispositivos como parte de la política que incluya los ítems ya nombrados.

El dispositivo "destapará" las aplicaciones correspondientes a los nombres de paquetes aquí configurados.

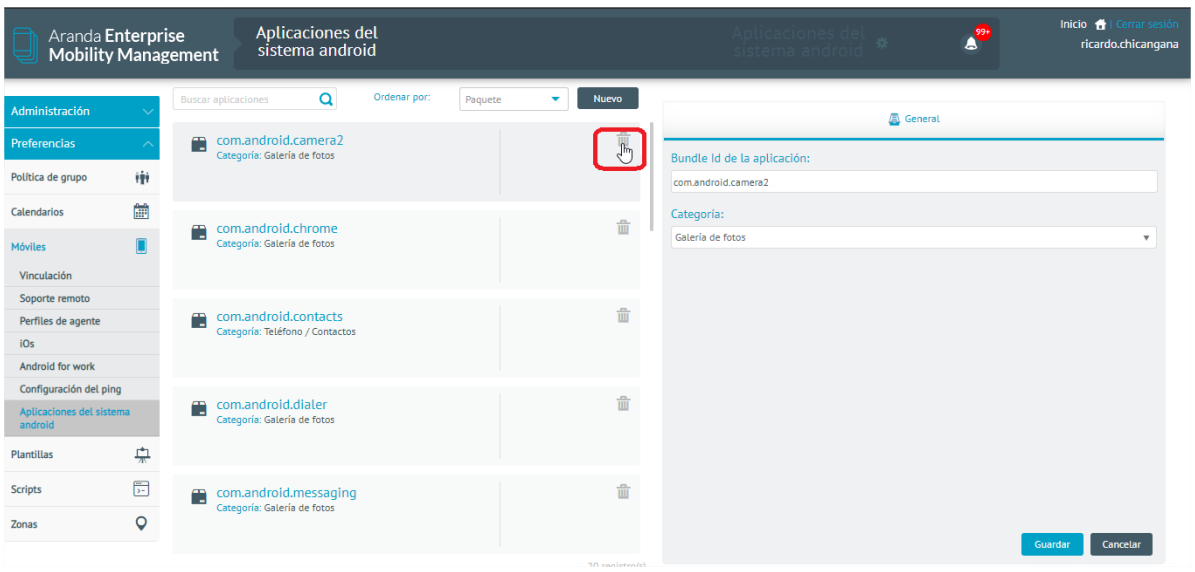
Para configurar un nuevo paquete haga clic en Nuevo y a continuación diligencie los datos de Bundle Id de la aplicación y Categoría, para persistir la información dé clic en Guardar.



Para editar un paquete existente ubíquelo en la lista de paquetes y actualice sus datos, luego haga clic en Guardar.



Para eliminar un paquete haga clic en el ícono de eliminar del registro del paquete en cuestión.



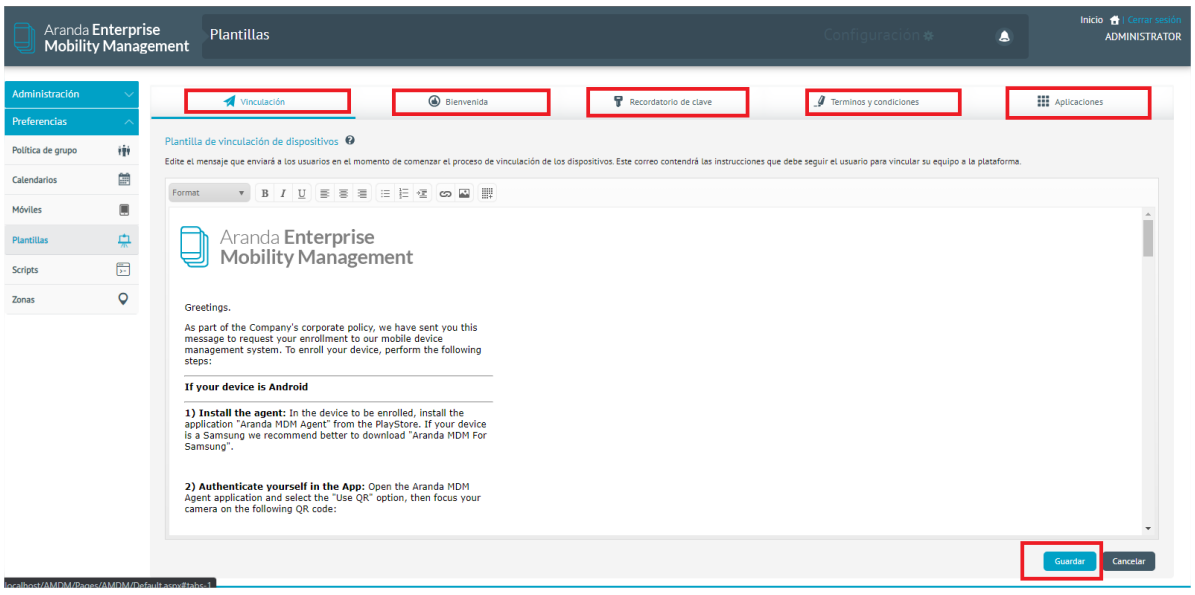
Plantillas

En esta sección podemos configurar el contenido de los correos electrónicos enviados por el servidor AEMM, al realizar ciertas acciones.

Dentro de las plantillas de correo podemos configurar las siguientes opciones:

- **Bienvenida**: Este nos permite configurar un saludo y él envió de confirmación del nombre de usuario y contraseña.
- **Recordatorio de clave**: Este nos envía una respuesta automática de la clave cuando esta es olvidada.
- **Términos y condiciones**: Nos permite configurar en el mensaje el correspondiente párrafo con los términos y condiciones.
- **Aplicaciones**: Nos envía información acerca de alguna aplicación.

Para configurar algunas de las secciones antes mencionadas, de clic en alguna de estas, luego realice los cambios pertinentes y por último haga clic en **Guardar**.

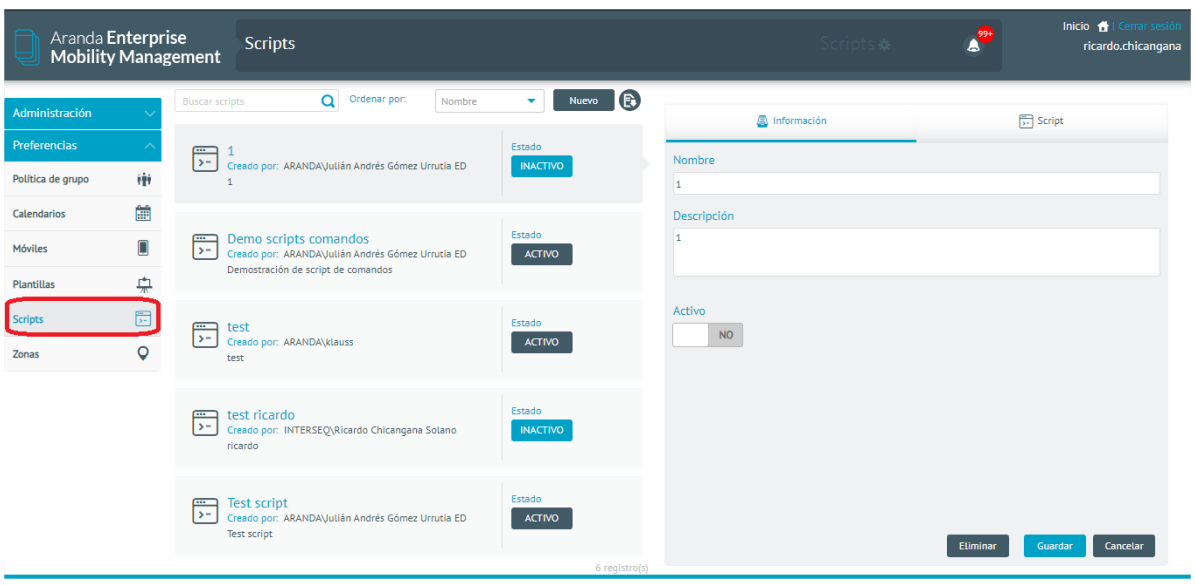


Por defecto AEMM provee plantillas prediseñadas para cada una de las secciones disponibles.

Scripts

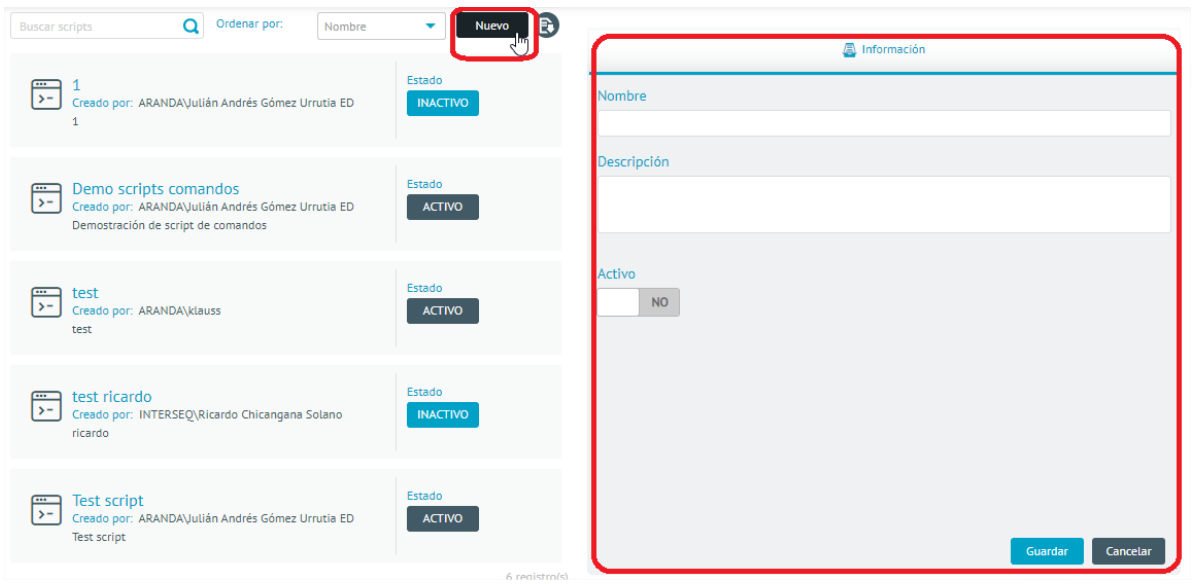
Los scripts son series secuenciales de comandos que son ejecutables sobre uno o varios dispositivos mediante un proyecto de gestión.

Para configurar scripts se debe de ingresar al módulo destinado para tal, en esta pantalla se presentan el listado de scripts creados y las opciones para gestionar dichos scripts:

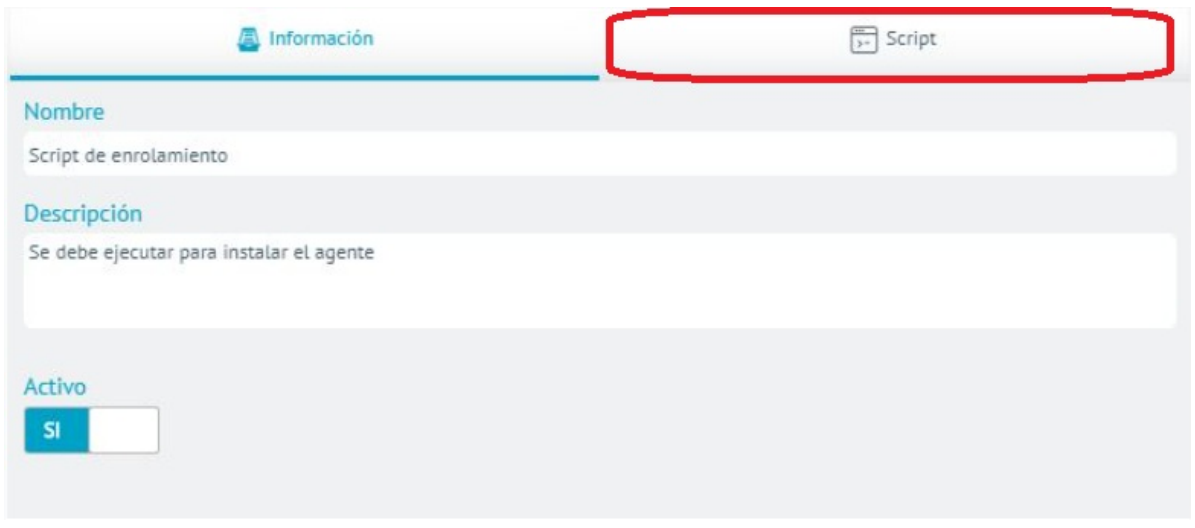


Creación de scripts

Para crear un nuevo script haga clic en “Nuevo”, y a continuación se le solicitarán los datos de Nombre (nombre único del script), Descripción (Descripción corta del script) y Estado (Activo/Inactivo).



Luego de diligenciar los datos solicitados, haga clic en guardar. Luego de esto se habilitará la pestaña “Script”, donde se creará la secuencia de comandos.



Edición del Script

Para la edición del script como tal acceda a la pestaña “Script”, donde se presentará la interfaz de edición de los comandos a incluir.

En esta interfaz se pueden ingresar los comandos a incluir, en la secuencia de ejecución deseada.

Como ayuda para la correcta escritura en cuento a estructura y sintaxis, se pone a disposición el botón “Verificar”, el cual valida la secuencia de órdenes escritas y presenta un mensaje claro y visible ante el evento de encontrarse algún error o por el contrario si la secuencia esta correcta.

Comandos disponibles para scripts

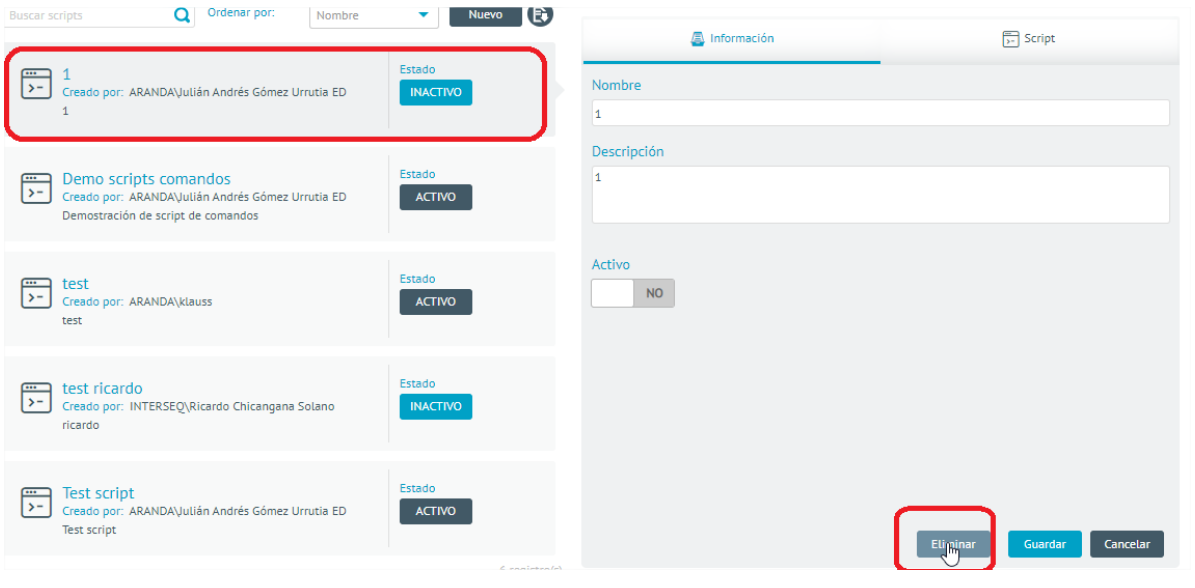
La siguiente tabla describe los comandos disponibles actualmente para incluirse en scripts.

Script	Descripción	Cantidad de Parámetros	Ejemplo
text	Muestra un mensaje en el timeline del dispositivo (No es el mensaje que se envía al dispositivo, este comando no interactúa directamente con el dispositivo)	Los necesarios	text Inicio de prueba de scripts de comandos
copy	Copia un elemento (archivo o carpeta) de una ruta origen a una ruta destino en el dispositivo	2	copy ruta/origen ruta/destino
del	Elimina un elemento (archivo o carpeta) del dispositivo	1	del ruta/elemento
start	Ejecuta una aplicación en el dispositivo	1	start com.facebook.katana
install	Instala una aplicación en el dispositivo	1	install com.facebook.katana
uninstall	Desinstala una aplicación del dispositivo	1	uninstall com.facebook.katana
validateVersion	Verifica la versión de una aplicación específica instalada en un dipositivo	2	valicateVersion com.facebook.katana 1.2
policy	Envia un comando de política	1	policy DefaultPolicy

Eliminación de scripts

Para eliminar un script ubíquelo en el listado y haga clic en “Eliminar”

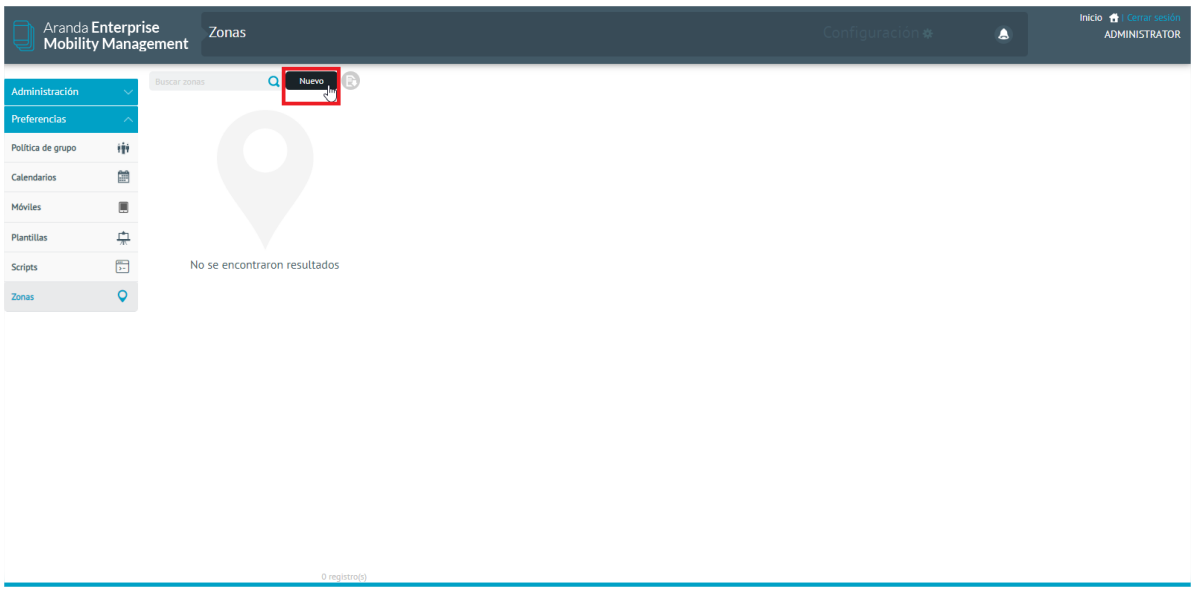
Se debe de tener en cuenta que, para la eliminación de un script de comandos, es necesario que este no se encuentre vinculado con ningún proyecto de gestión.



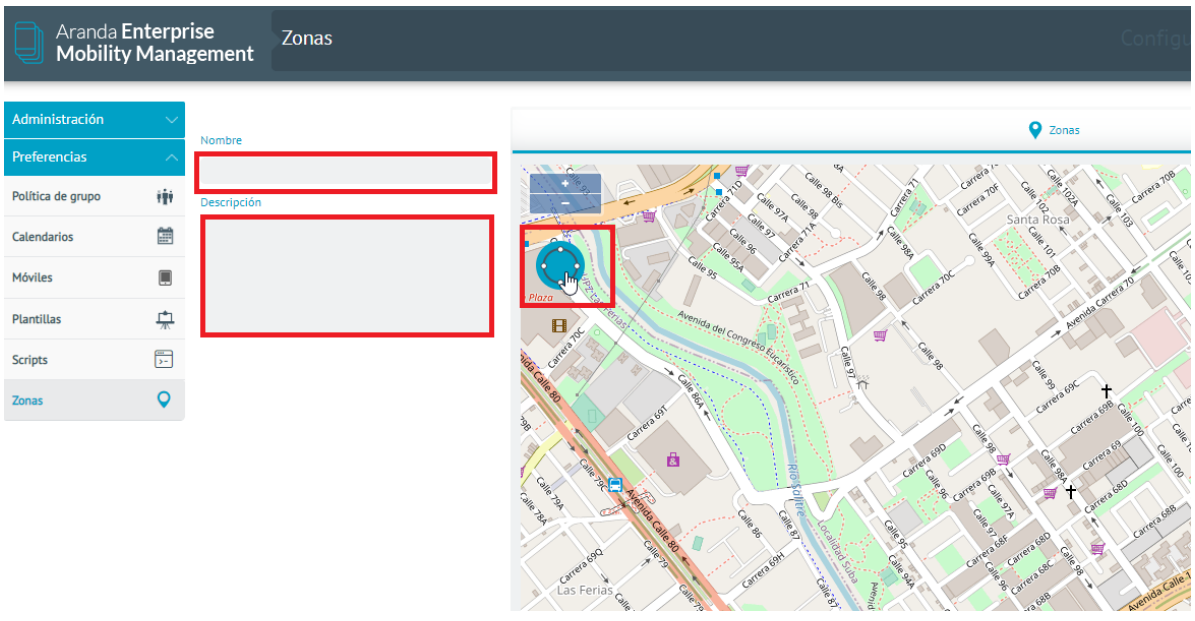
Zonas

La sección de zonas se destina para gestionar las zonas que posteriormente serán utilizadas en la configuración de conjuntos de reglas que tengan ítem de “Geofencing” (Frontera geográfica).

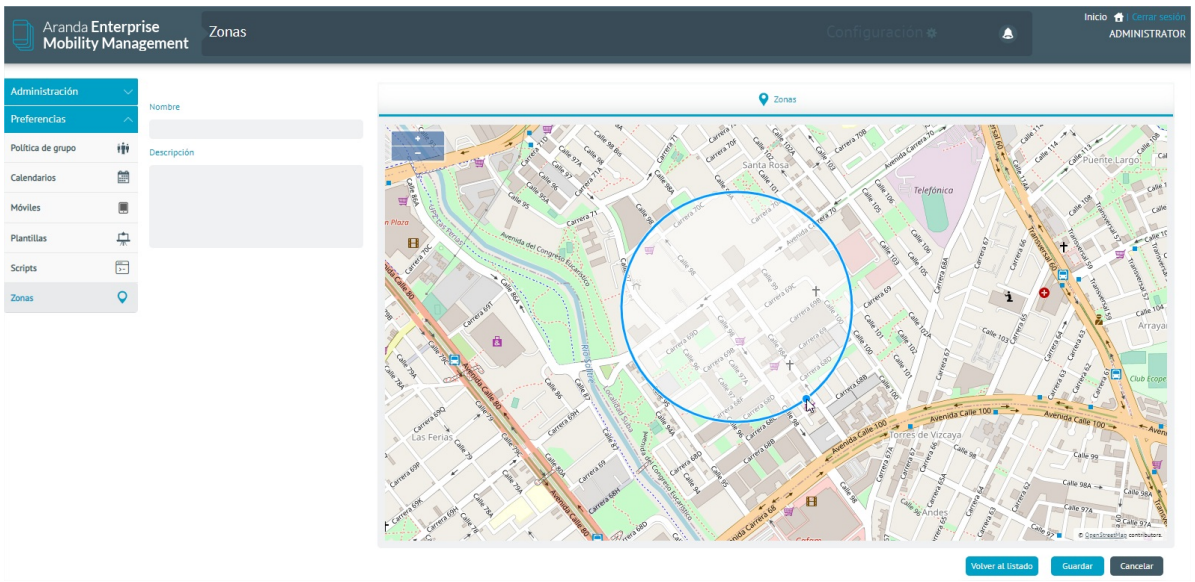
Para configurar una zona geográfica acceda a la sección de zonas y haga clic en **Nuevo**.



Ingrese los datos solicitados y de clic en el círculo azul para delimitar la zona.



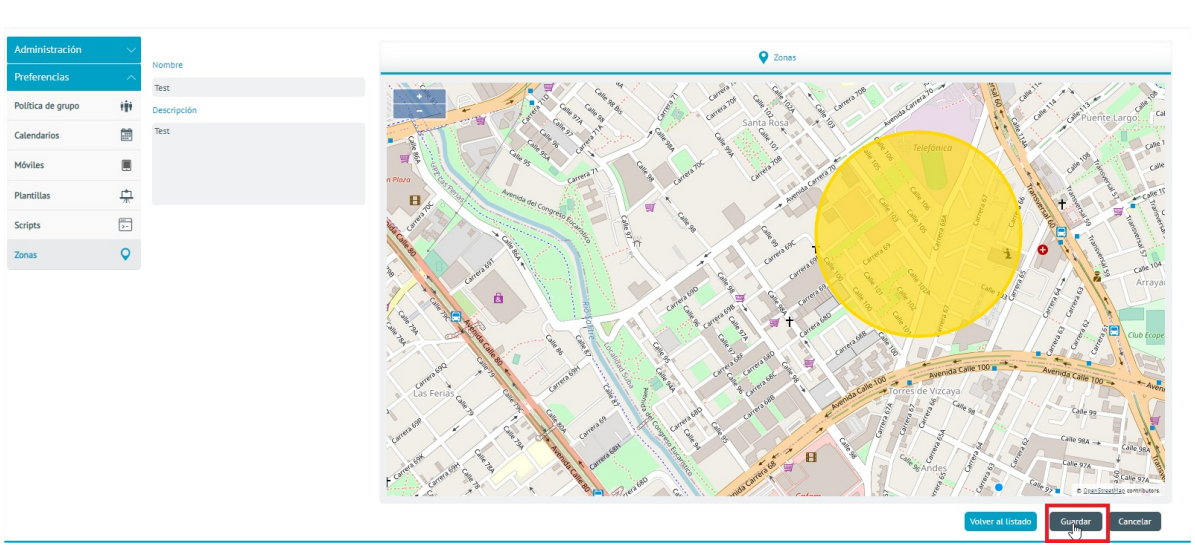
Luego haga un clic y suelte para marcar el centro de la zona, y luego mueva el ratón para ampliar o disminuir la zona, y luego un clic final para terminar de dibujar la zona.



Si desea puede editar la zona ya dibujada, dando clic sostenido en su centro para cambiarla de lugar o dando clic sostenido en su borde para cambiar el tamaño.

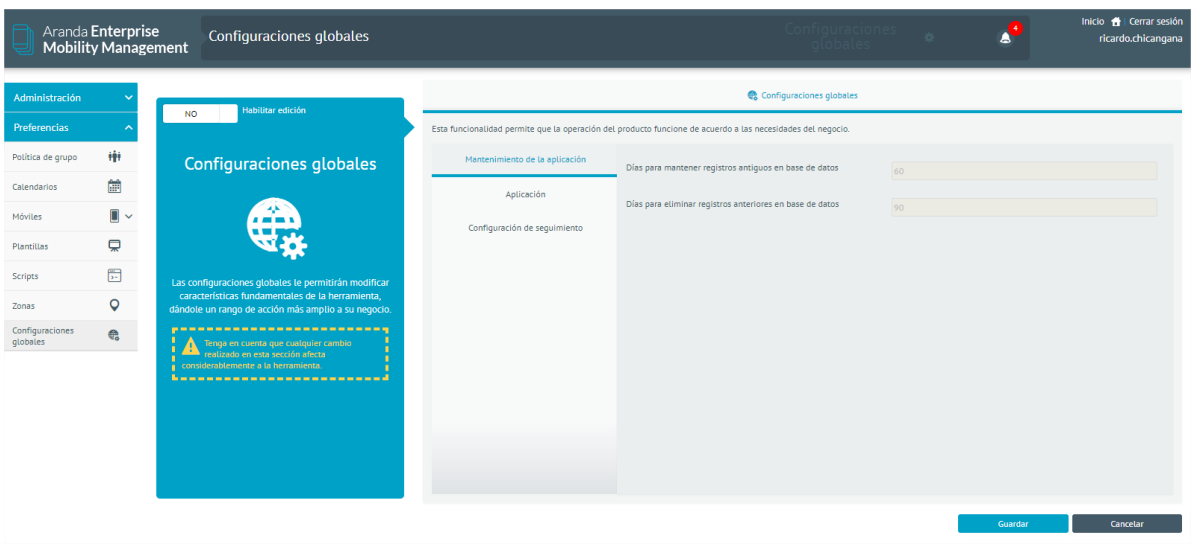
Si da un clic por fuera de la zona ya dibujada el proceso empezara de nuevo.

Por último, haga clic en **Guardar** para persistir la zona.

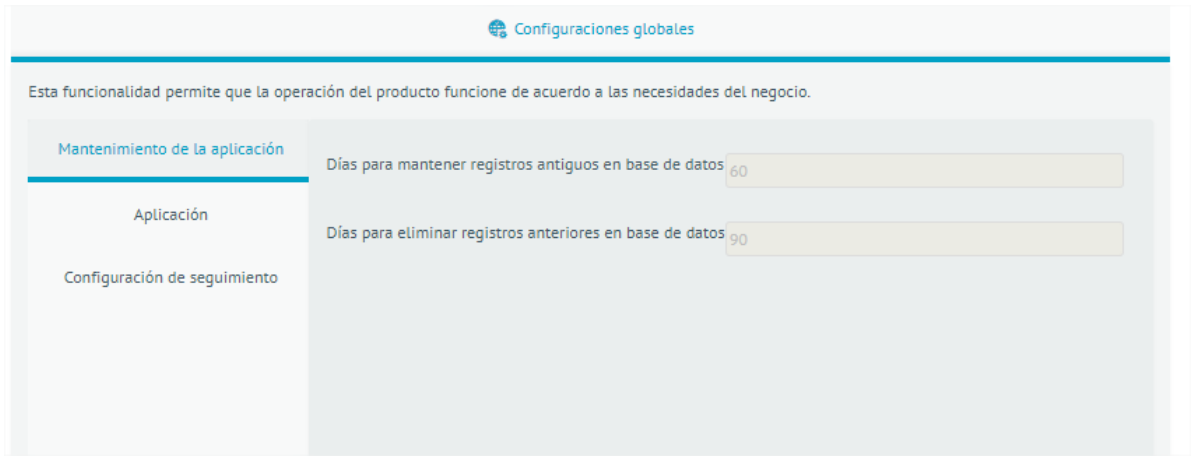


Configuraciones Globales

Esta sección ofrece una interfaz amigable para configurar ciertos ítems de la aplicación, susceptibles a ser configurados por parte del usuario final.



Se presentan tres subgrupos de configuraciones:

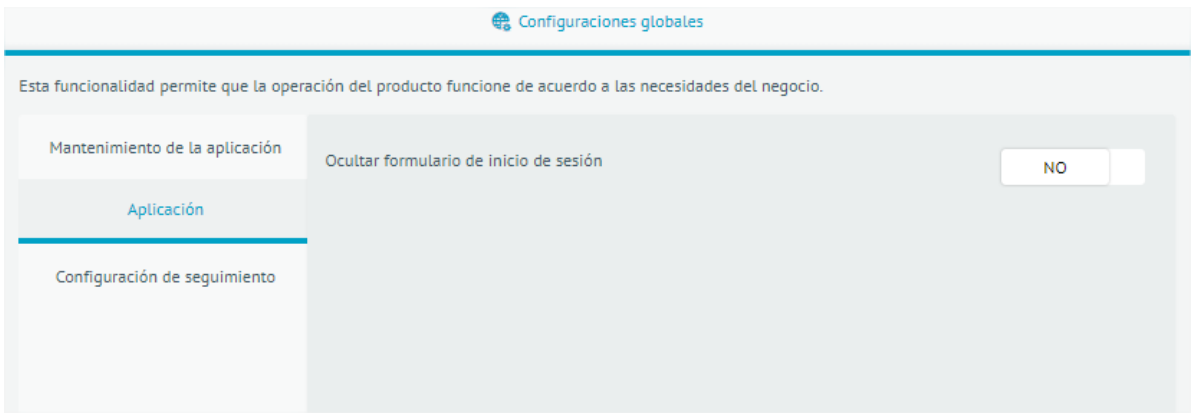


Mantenimiento de la Aplicación

Se presentan las opciones de:

Campos	Descripción
Días para mantener registros antiguos en base de datos:	Cantidad de días que se conservan registros históricos de comandos, localizaciones, registros de consumo y registros de eventos de dispositivo. Luego de transcurridos los días configurados los registros se moverán a tablas históricas en base de datos.
Días para eliminar registros anteriores en base de datos:	Cantidad de días que registros antiguos se conservarán en tablas históricas antes de ser eliminados definitivamente.

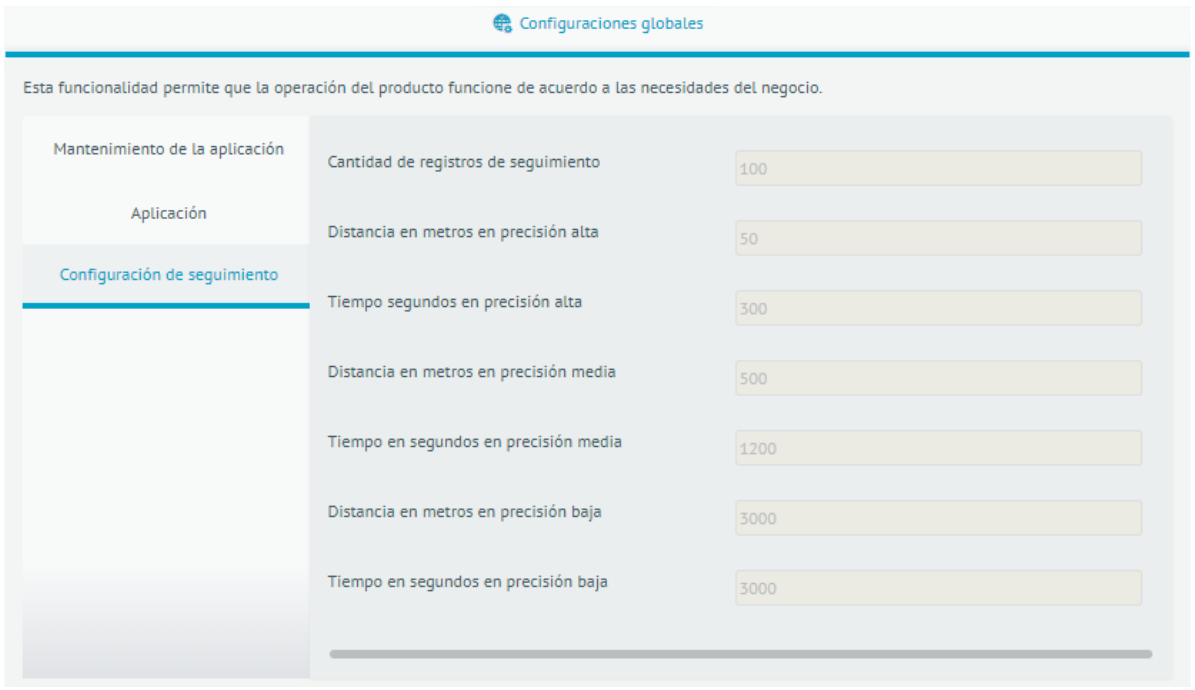
Aplicación



Se presenta la opción de:

Campos	Descripción
Ocultar formulario de inicio de sesión:	Opción que permite ocultar el formulario de inicio de sesión por defecto de la aplicación. Esto se puede usar cuando se hayan configurado proveedores de autenticación externa y no sea ya necesario la autenticación por defecto.

Configuración de seguimiento

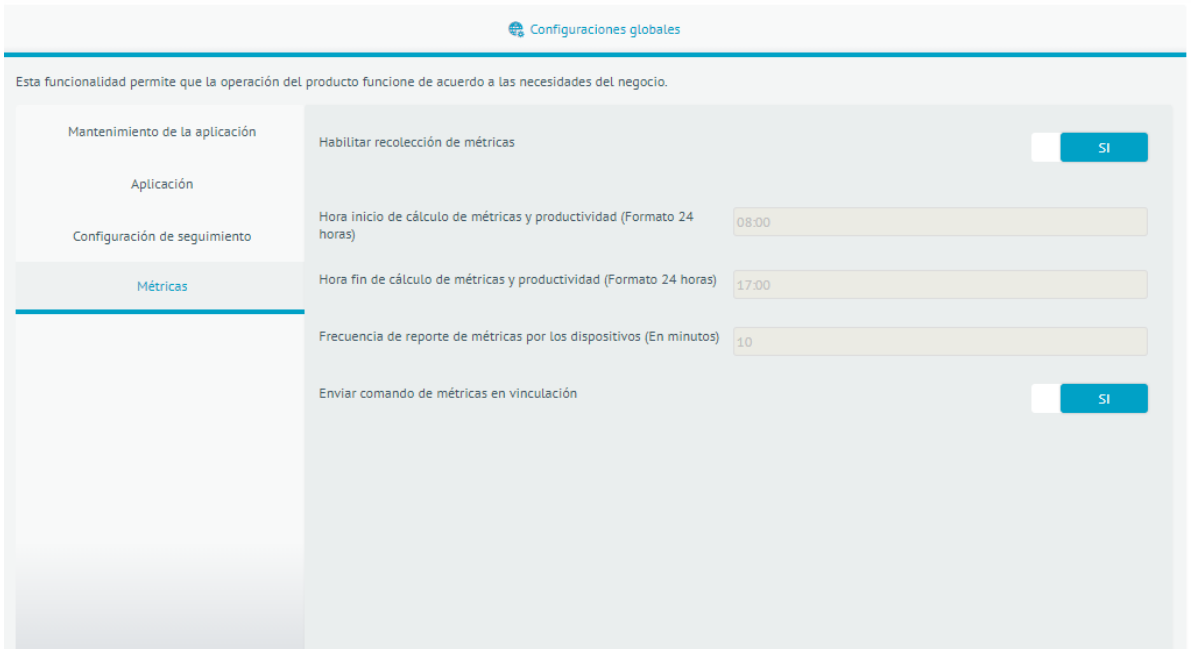


En esta sección se permite la configuración de valores por defecto para los niveles de seguimiento cuando el comando de seguimiento es enviado a un dispositivo.

Se presentan las opciones de:

Campos	Descripción
Cantidad de registros de seguimiento:	Cantidad máxima de registros que un dispositivo puede enviar en una sola invocación al servicio de reporte de localización, expuesto por el servidor.
Distancia en metros precisión alta:	Distancia en metros máxima antes de reportar localización en precisión alta de seguimiento.
Tiempo segundos precisión alta:	Tiempo máximo transcurrido antes de reportar localización en precisión alta de seguimiento.
Distancia en metros precisión media:	Distancia en metros máxima antes de reportar localización en precisión media de seguimiento.
Tiempo segundos precisión media:	Tiempo máximo transcurrido antes de reportar localización en precisión media de seguimiento.
Distancia en metros precisión baja:	Distancia en metros máxima antes de reportar localización en precisión baja de seguimiento.
Tiempo segundos precisión baja:	Tiempo máximo transcurrido antes de reportar localización en precisión baja de seguimiento

Métricas

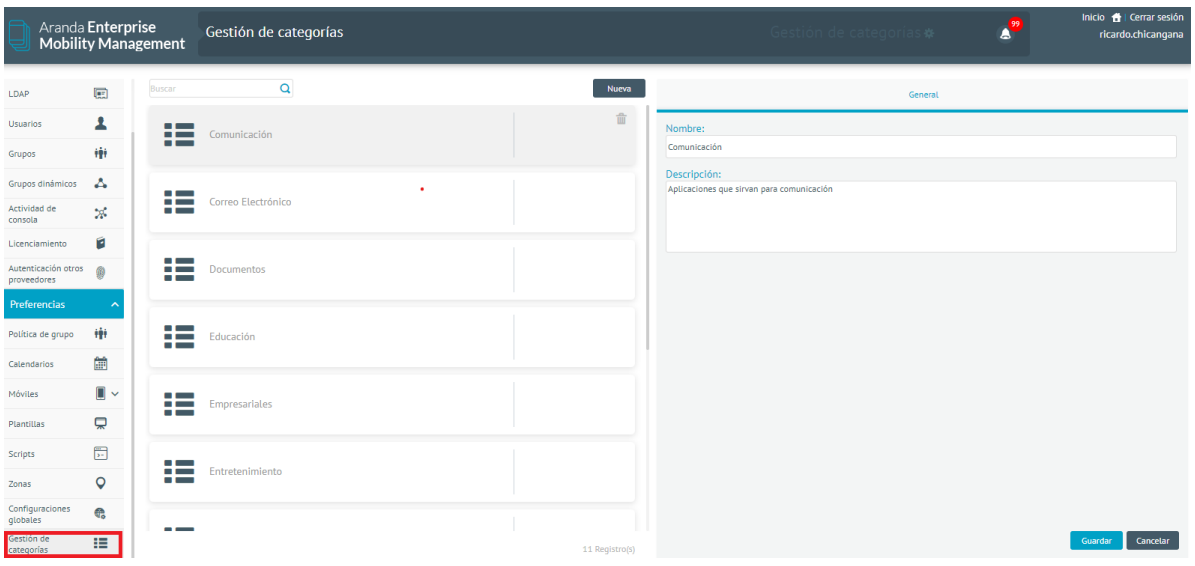


Esta sección presentan configuraciones que controlan la recolección de datos de métricas por parte de los dispositivos hacia el servidor.

Se presentan opciones de:

Campos	Descripción
Habilitar recolección de métricas:	Habilita/Desabilita de manera global si los dispositivos móviles pueden reportar estadísticas de métricas.
Hora inicio de cálculo de métricas y productividad:	Hora inicial en el día en que los dispositivos iniciarán a reportar datos de métricas.
Hora fin de cálculo de métricas y productividad:	Hora final en el día en que los dispositivos dejarán de reportar datos de métricas.
Frecuencia de reporte de métricas por los dispositivos:	Intervalo de tiempo con el que los dispositivos enviarán un reporte de actualización de métricas hacia servidor.
Enviar comando de métricas en vinculación:	Determina si al momento de vincular un dispositivo se activará por defecto el envío de métricas del dispostivo en cuestión.

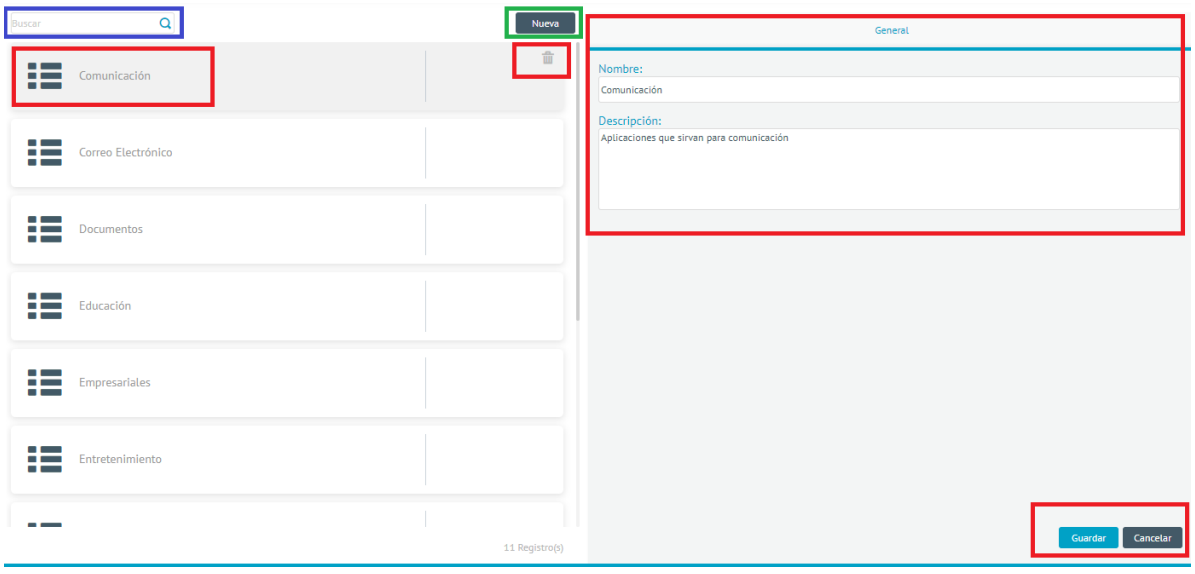
Gestión de Categorías de Aplicaciones



En esta sección se puede llevar a cabo la gestión de las categorías de aplicaciones, que luego se podrán utilizar para clasificar las aplicaciones en una o varias de dichas categorías.

Esto tiene un efecto directo en el modo en que se presenta el Dashboard de Métricas, dado que las categorías aqui configuaradas se toman como referencia para clasificar y filtrar la información posteriormente.

Listado Principal



Se presentan las categorias actualmente creadas, con opción de eliminación. Para detallar una categoria haga clic sobre el nombre de ésta y la información se mostrará en la parte derecha.

Para **eliminar** una categoría, haga clic en la categoría y luego clic en el ícono de basurero para proceder a eliminarla. Sólo se podrá eliminar una categoría si ninguna aplicación la esta refiriendo.

Para **editar** una categoría, haga clic en el nombre de la categoría y luego edite los campos de ésta en la parte izquierda, a continuación haga clic en Guardar para persistir los cambios o haga clic en Cancelar para descartar los cambios.

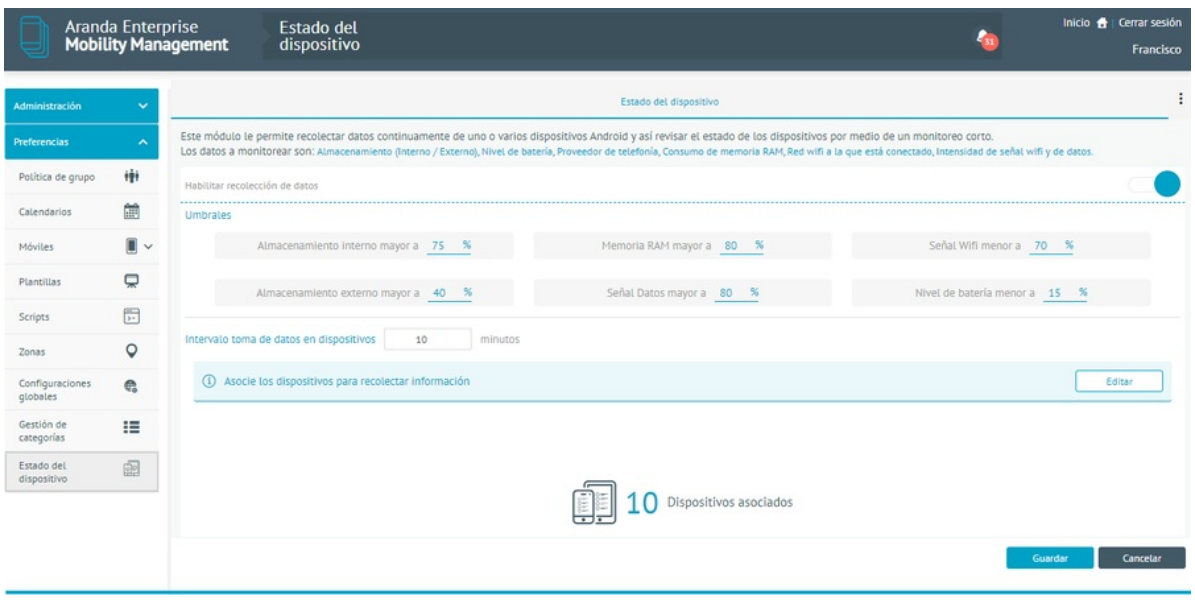
Para **crear** una nueva categoría haga clic en el botón Nueva, luego diligencie los campos en la parte izquierda y luego clic en Guardar. La nueva categoria será desplegada automáticamente en el listado.

Para **buscar** una categoría en el listado ingrese el parámetro de búsqueda en el cajon de texto para búsquedo y luego haga clic en la lupa o presione Entrar. El listado se filtrará de acuerdo al parámetro de búsqueda ingresado.

Estado del Dispositivo

Este módulo de permite configurar la recolección de datos para determinar el estado de undispositivo.

1. Para definir el estado de los dispositivos ingrese a la consola de configuración de Aranda ENTERPRISE MOBILE MANAGEMENT AEMM, en la sección de **Preferencias** del menú principal, seleccione la opción **Estado del Dispositivo**. En la Vista Detalle podrá configurar los umbrales y editar los dispositivos asociados.



Umbrales

Los umbrales son topes mínimos o máximos con los que se determina si un dispositivo está en riesgo o no en algún dato de los anterior reportados.

2. En la Vista detalle del estado del dispositivo en la consola de configuración AEMM, seleccione la pestaña **Estado del dispositivo**, donde podrá determinar los umbrales de acuerdo al tipo da dato.Los datos que es posible recolectar son los siguientes:

- Almacenamiento Interno usado
- Almacenamiento Externo usado
- Nivel de batería
- Memoria RAM usada
- Intensidad de señal wifi y de datos
- Intensidad de señal de datos en la red celular

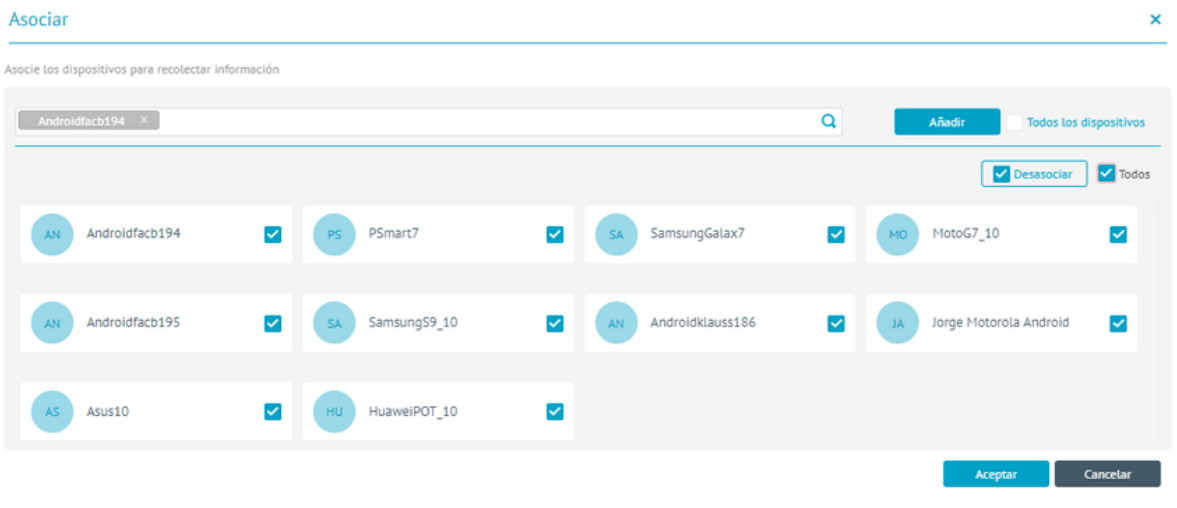
3. Establezca el umbral (porcentaje) para el tipo de dato.

> ⚐ **Nota:** Se reportará un dispositivo en riesgo en la categoria específica si se cumple alguna de las siguientes condiciones:
> - Almacenamiento Interno usado mayor al dato configurado (porcentaje)
> - Nivel de batería menor al dato configurado (porcentaje)
> - Memoria RAM usada mayor al dato configurado (porcentaje)
> - Intensidad de señal wifi y de datos menor al dato configurado (porcentaje)
> - Intensidad de señal de datos en la red celular menor al dato configurado (porcentaje).

Asociación de Dispositivos

El módulo permite la edición de los dispositivos que actualmente reportan datos de estado

4. Para editar la asociación de dispositivos, en la Vista detalle del estado del dispositivo en la consola de configuración AEMM, seleccione la pestaña **Estado del dispositivo**, haga clic en el botón **Editar** y en la ventana **Asociar** podrá ejecutar las siguientes acciones:



- Para asociar nuevos dispositivos al reporte de estado, en la búsqueda por dispositivo, ingrese el nombre del elemento a asociar y haga clic en "Añadir" para agregarlo.
- Para desasociar uno o varios dispositivos, seleccione el registro(s) correspondiente(s) y haga clic en la opción "Desasociar"

5. Si habilita la opción Todos, podrá desasociar los registros seleccionados.

6. Para aplicar los cambios hechos haga clic en "Aceptar"; para descartarlos haga clic en "Cancelar" o clic en el ícono de cierre.

7. Al terminan de configurar el estado del dispositivo, Haga clic en **Guardar** en la Vista detalle de la consola de configuración AEMM, ara confirmar los cambios realizados.

Vinculación de Dispositivos

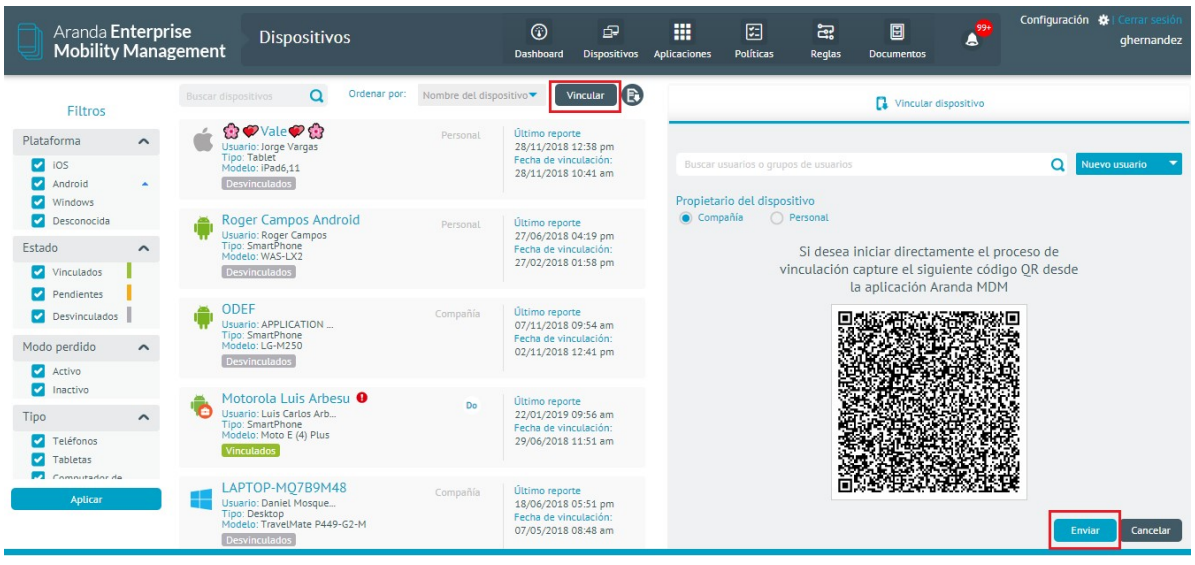
Vinculación desde consola

Si la compatibilidad con Android for Work fue habilitada haciendo el respectivo proceso descrito en la sección

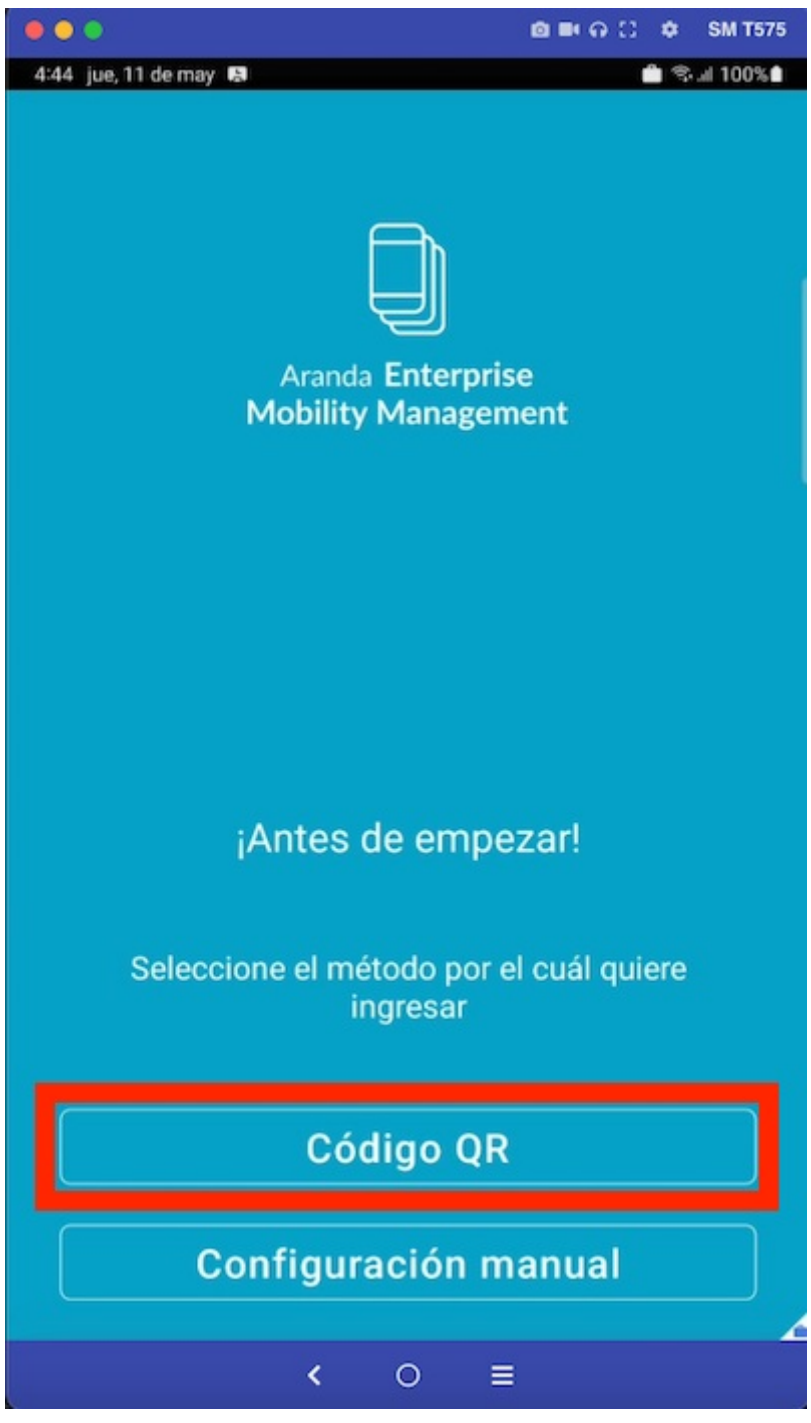
Preferencias->Móviles, estará ya disponible la vinculación de los dispositivos Android compatibles con Android for Work.

Vinculación desde consola Web

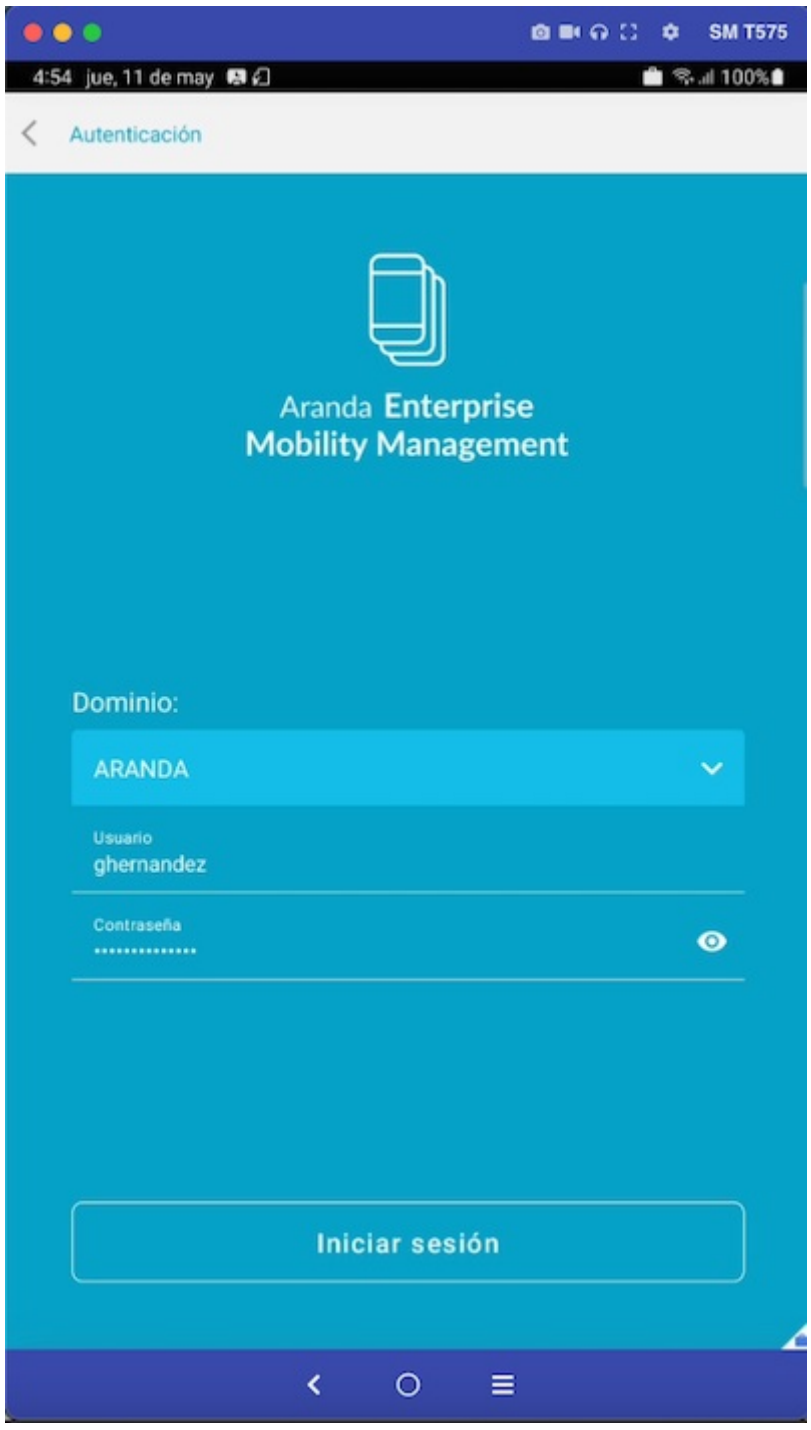
Se debe seleccionar el botón **Vincular**, luego aparecerá en la parte derecha un código QR que contiene la información del servidor y dominio para continuar el proceso.



Para capturar el código QR se abre la aplicación móvil, y se selecciona la opción **Ingresar código QR**

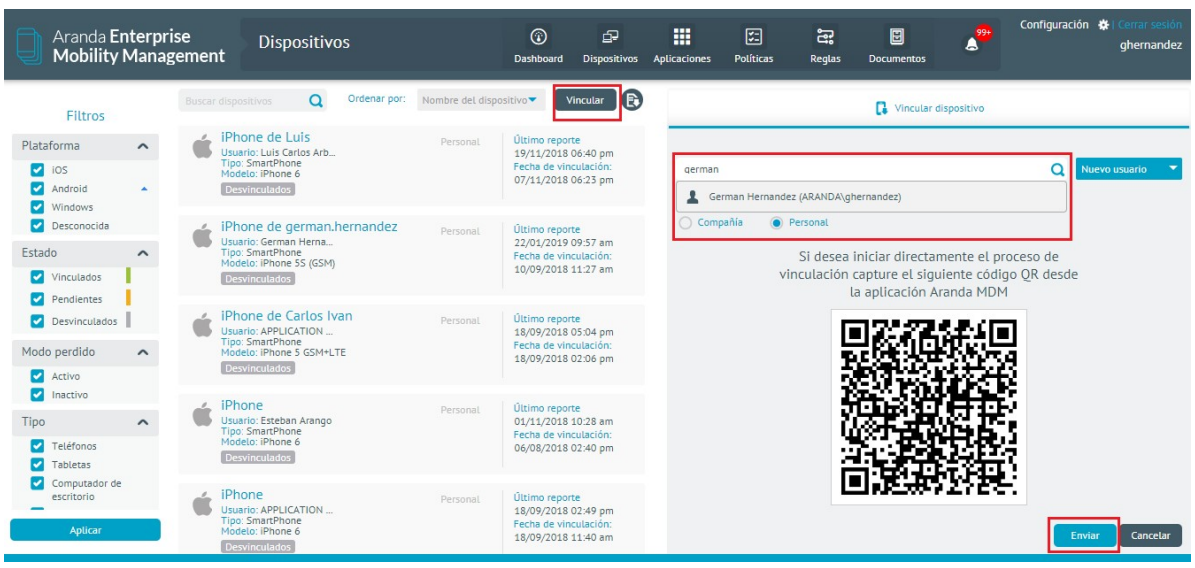


La aplicación usa la cámara del dispositivo para realizar la captura del código, este se detecta de forma automática, después de que la aplicación captura la información del código, realiza la validación del servidor y el dominio y deja al usuario en la vista para ingresar las credenciales correspondientes (usuario y contraseña).



Vinculación desde el correo de invitación

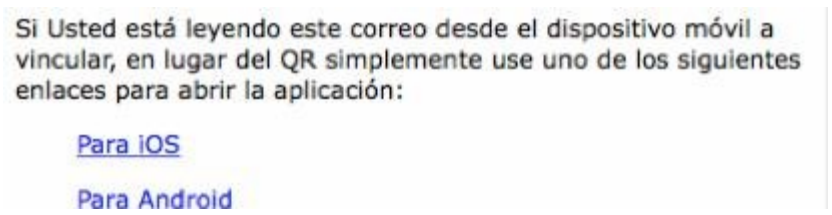
Para enviar un correo de invitación, ingrese a la consola web y seleccione la opción **Vincular**, en la parte derecha de la pantalla ingrese el usuario o grupo de usuarios a los cuales desea enviar el correo, cuando tenga la lista de usuarios seleccione el botón **Enviar** ubicado en la parte inferior.



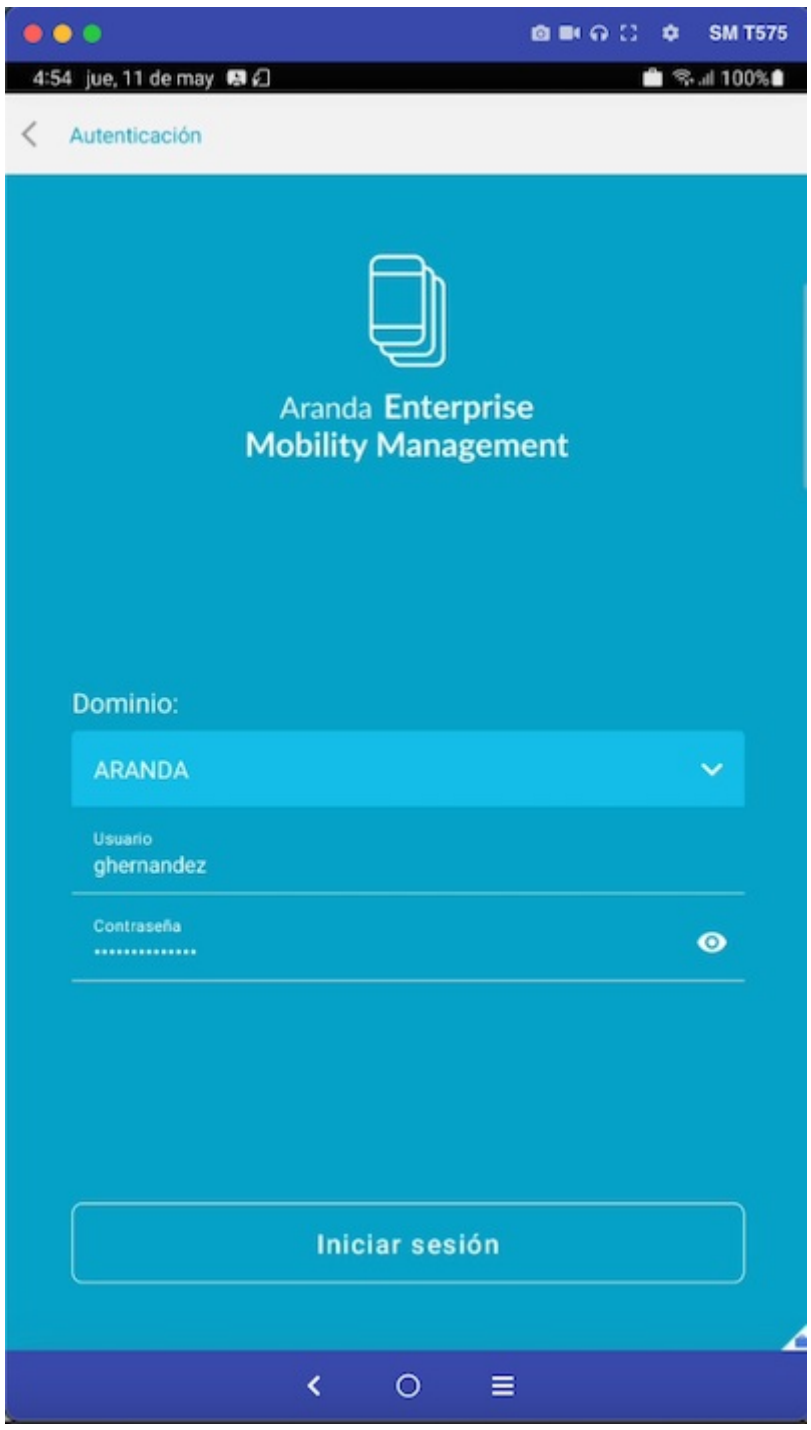
El (Los) usuario(s) recibirá(n) un correo con unas instrucciones a seguir para vincular el dispositivo, desde el correo se puede realizar la vinculación del dispositivo de tres formas diferentes.

Vinculación usando link

En el correo hay un mensaje como el presentado en la imagen:



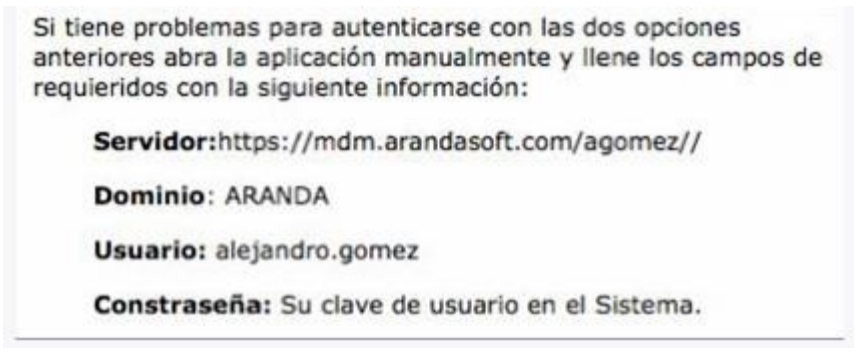
Los dos links contienen la información necesaria para que el sistema realice el proceso de validación de servidores de forma automática y deje al usuario en la vista de autenticación.



El proceso continuo de la misma forma sin importar la opción seleccionada, y se explica en la sección **Continuación del proceso**.

Vinculación ingresando la información de forma manual

En la parte inferior del correo se indica al usuario la información de servidor, dominio y usuario.


Si tiene problemas para autenticarse con las dos opciones anteriores abra la aplicación manualmente y llene los campos de requieridos con la siguiente información:

Servidor:https://mdm.arandasoft.com/agomez//

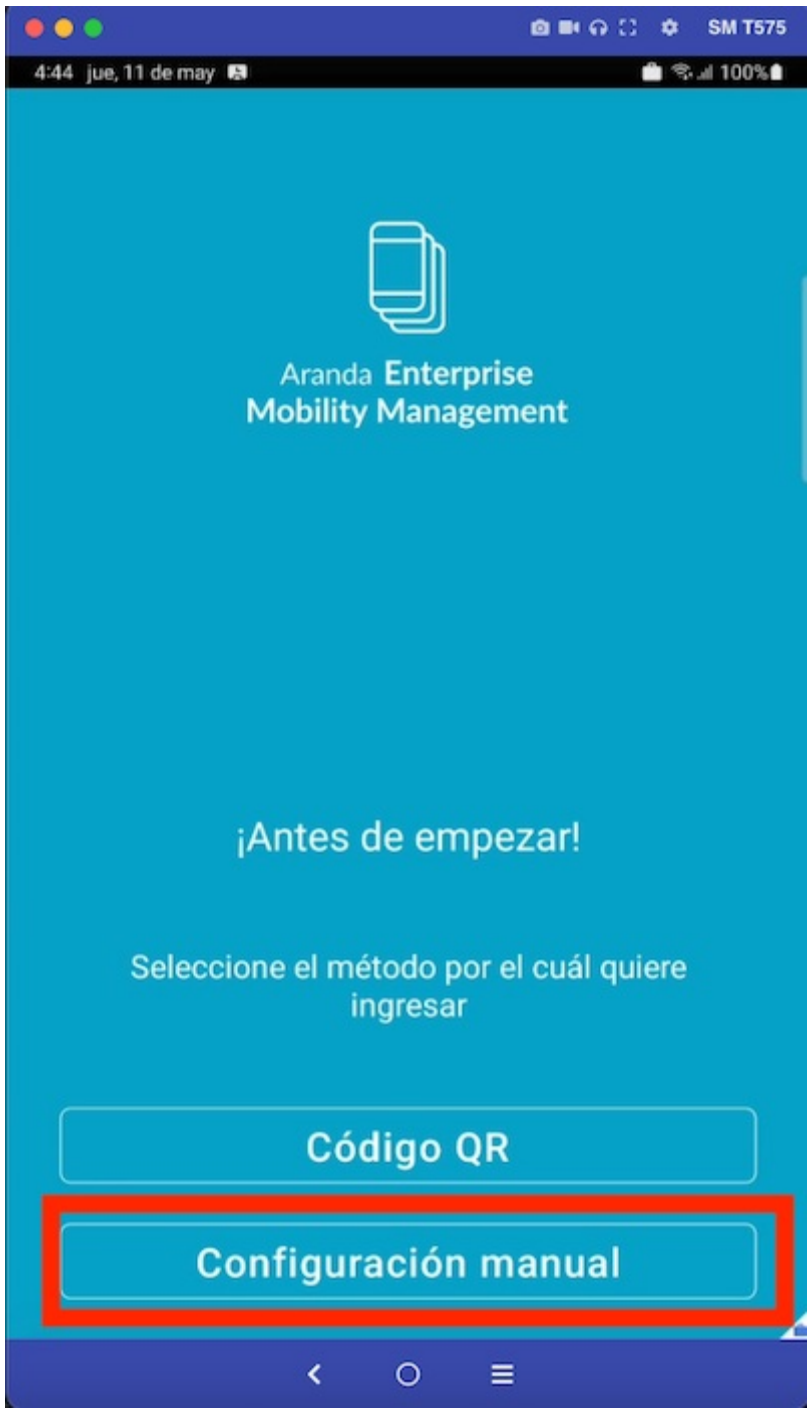
Dominio: ARANDA

Usuario: alejandro.gomez

Constraseña: Su clave de usuario en el Sistema.

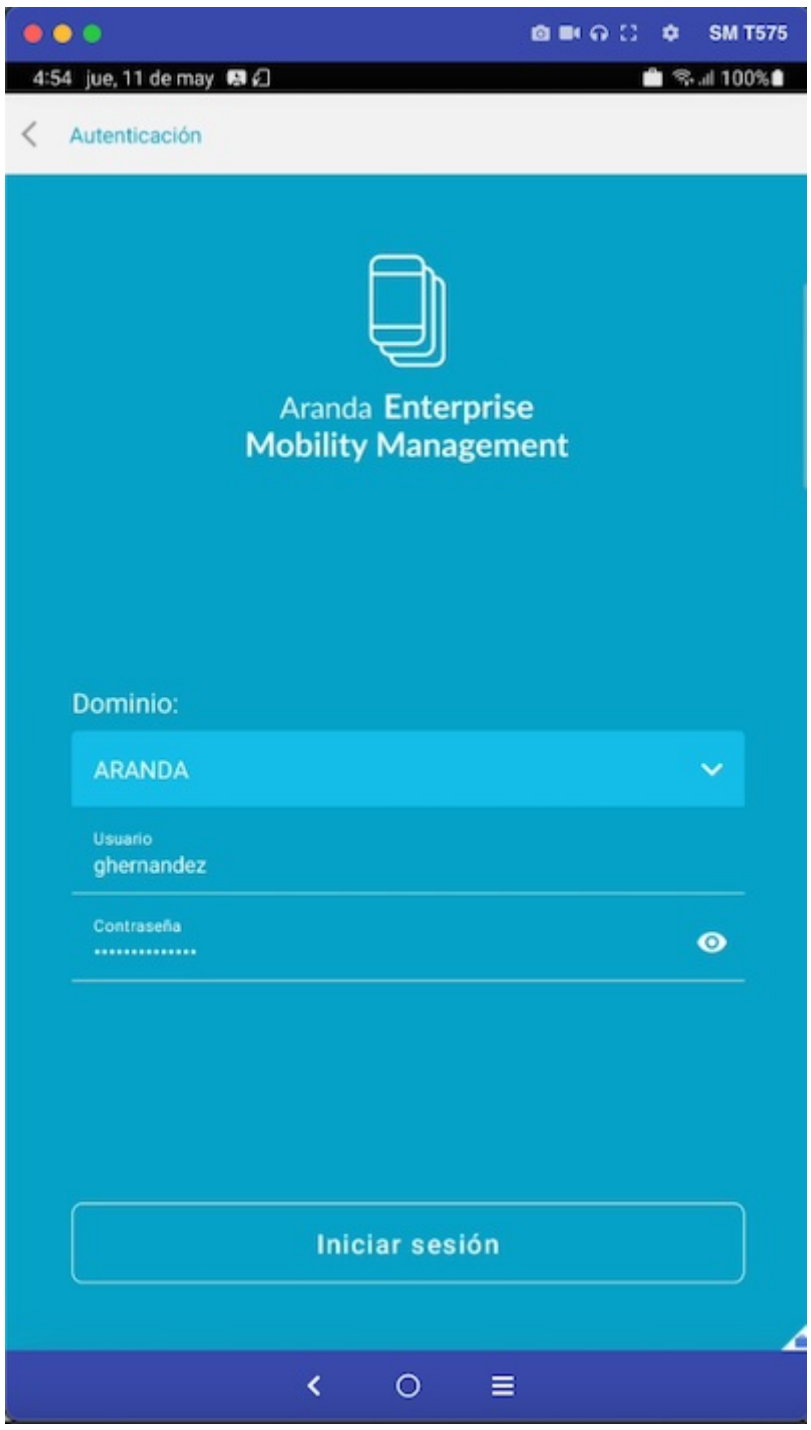
Esta información puede ser ingresada manualmente desde la aplicación ingresando a la opción

Ingresar URL de servidor.



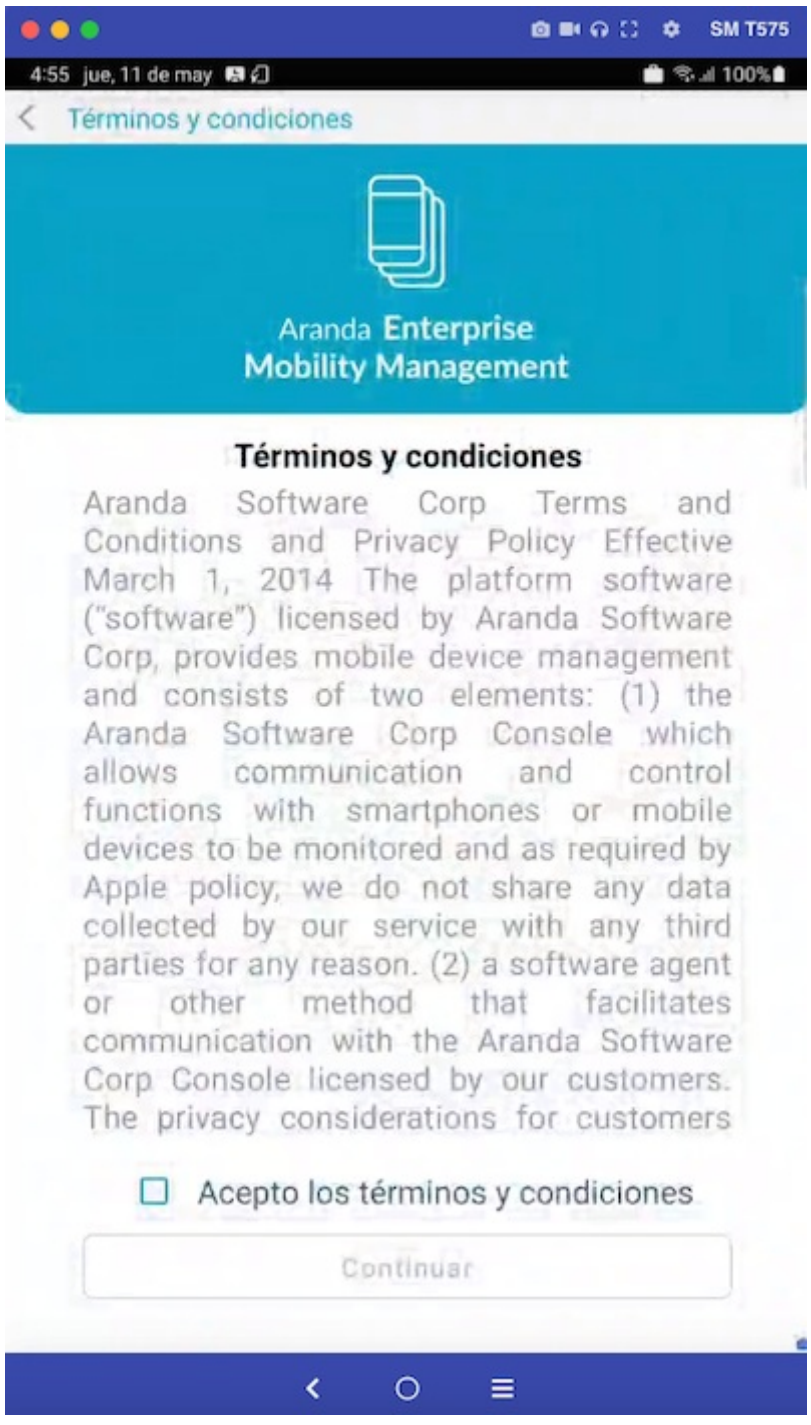
La aplicación presenta la vista para ingresar la dirección del servidor EMM.

Cuando el servidor validó que la dirección ingresada es correcta la aplicación deja al usuario en la vista de autenticación para que ingrese las credenciales de usuario y contraseña.



El proceso continúa de la misma forma sin importar la opción seleccionada, este se explica a continuación.

Después de ingresar las credenciales de autenticación y que el sistema valide que estas son correctas, se presenta la vista de términos y condiciones.



Cuando el usuario selecciona la opción **Acepto los términos y condiciones** y presiona el botón **Continuar**, el sistema ctualiza esta información y permite que el usuario avance al siguiente paso del proceso que varía dependiendo del sistema operativo.

Windows

En AEMM es posible realizar vinculación de dispositivos con sistema operativo Windows 10 Pro y Windows 10 Mobile.

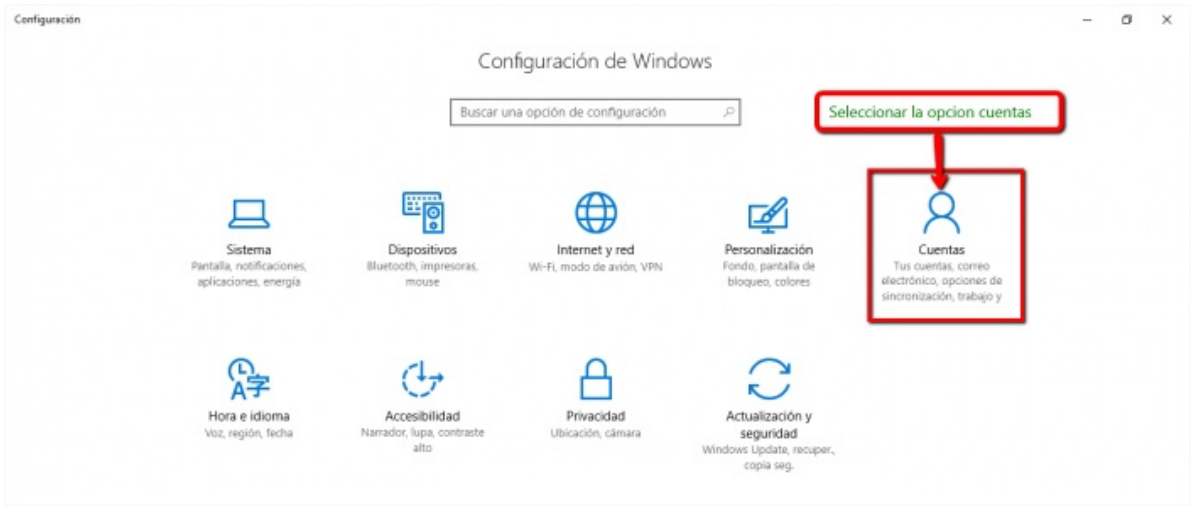
Estos dispositivos ya cuentan con un mecanismo propio de gestión MDM ofrecido por Microsoft Windows y sobre el cual AEMM trabaja.

Vinculación Windows 10 Pro

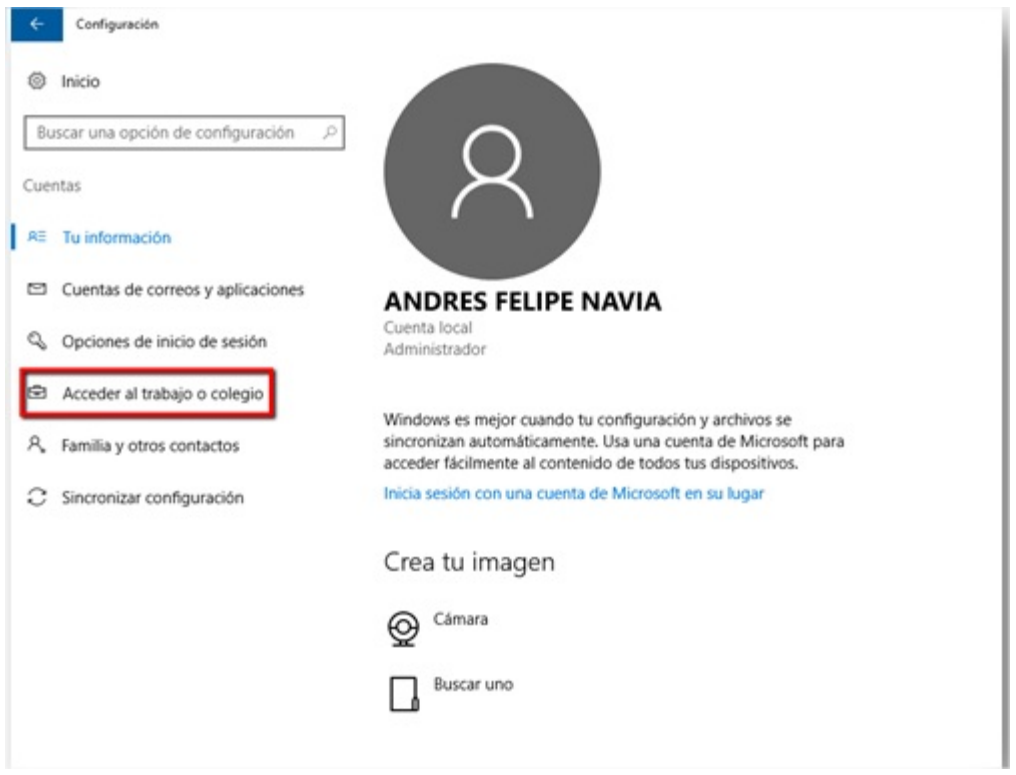
Vinculación al MDM Nativo de Microsoft Windows

La vinculación nativa de Windows se realiza usando herramientas propias del sistema operativo. Una vez terminada el dispositivo es dado de alta en el Servidor ya se puede iniciar la gestión del mismo.

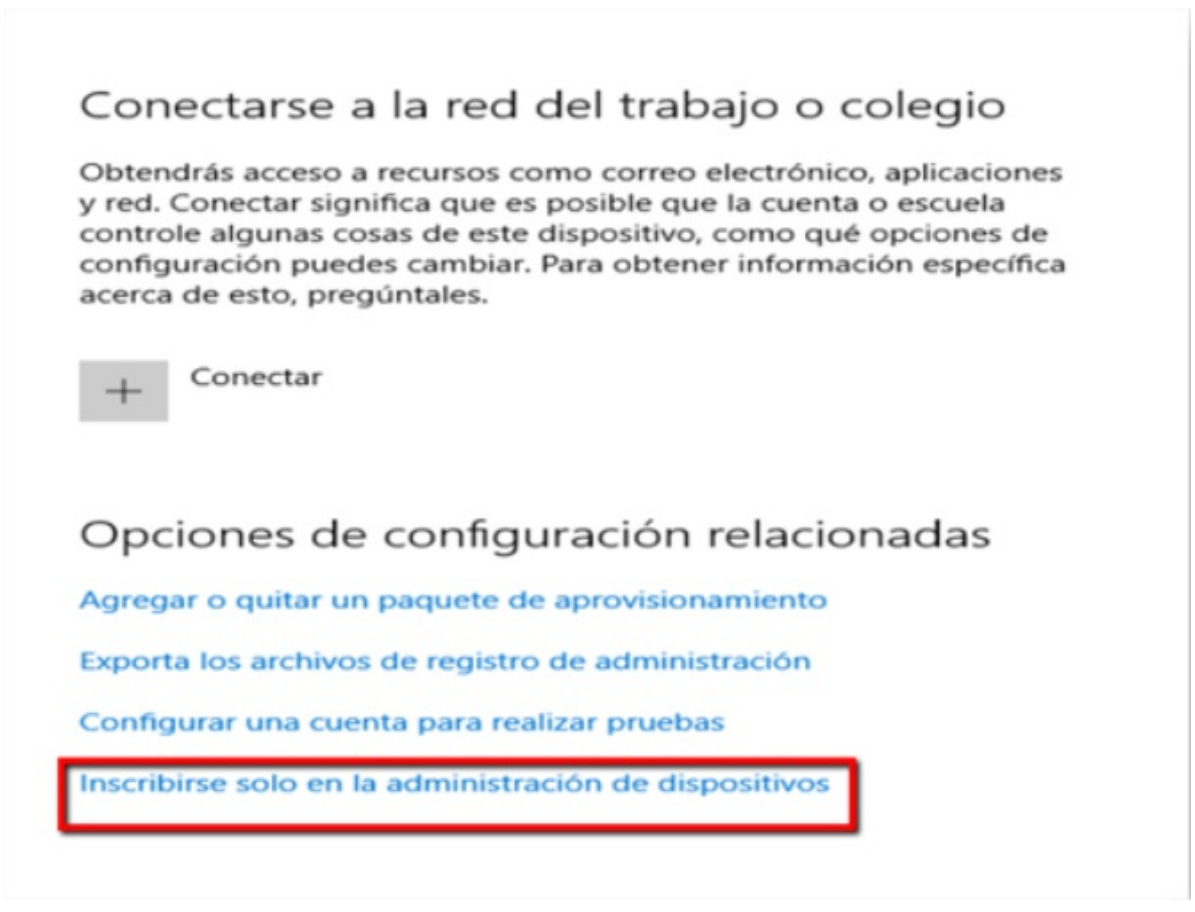
Ingresar al módulo de Configuración de Windows y seleccionar la opción Cuentas



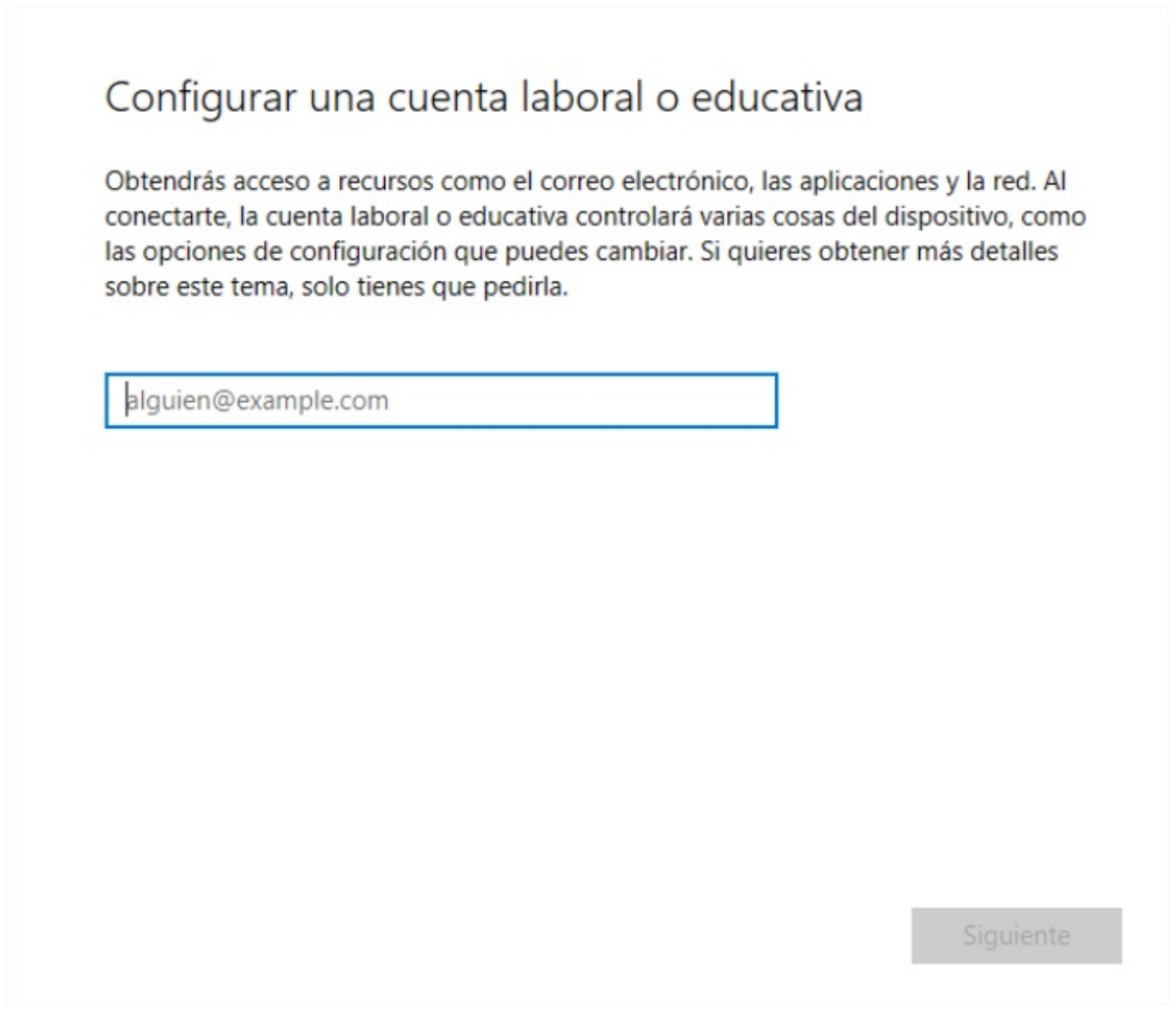
Después de seleccionar la opción cuentas, se debe seleccionar la opción “acceder al trabajo o colegio “



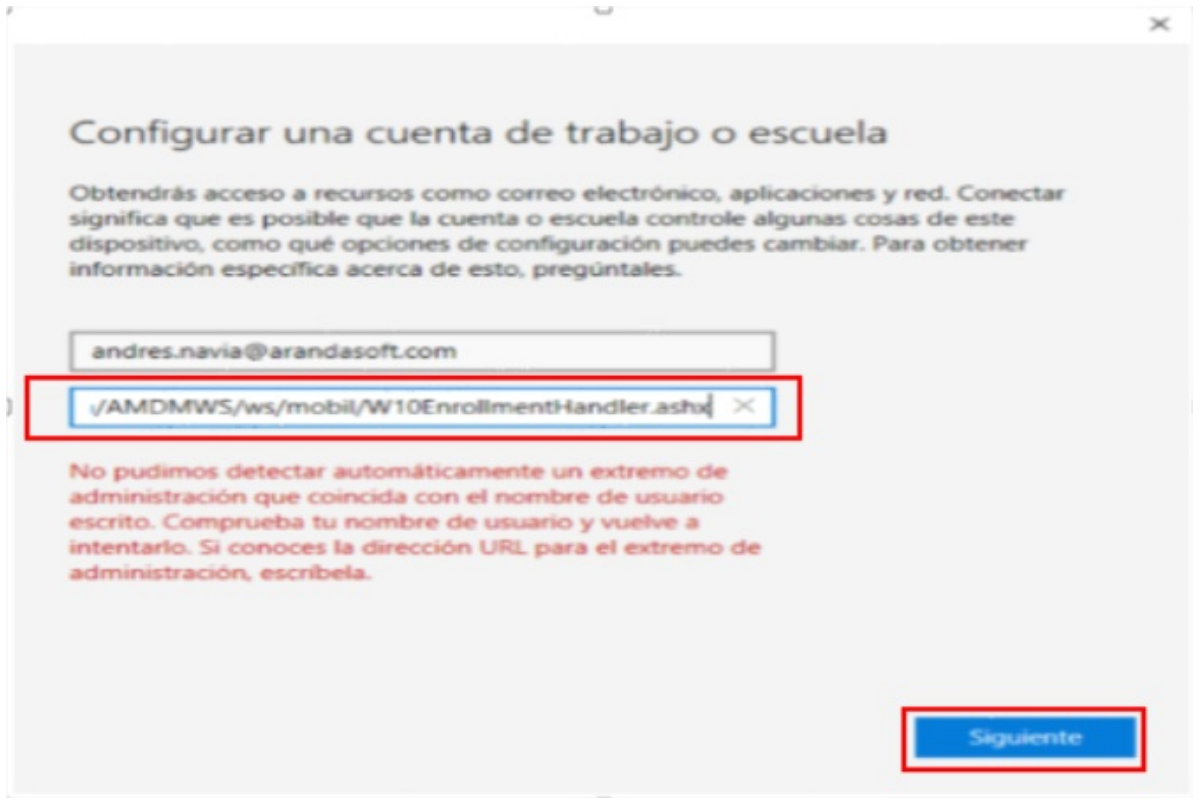
En la siguiente pantalla se debe seleccionar la opción: “Inscribirse solo en la administración de dispositivos”



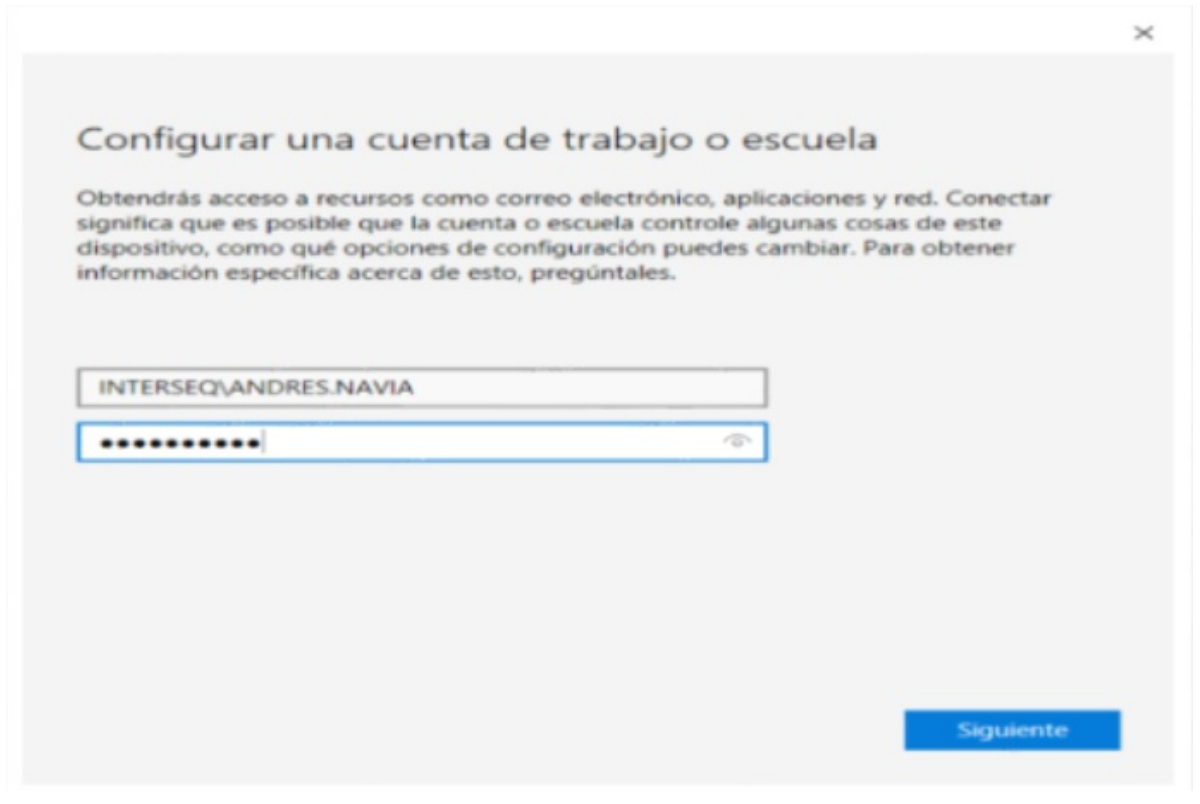
En la siguiente pantalla digitar el usuario de la cuenta con la cual se va a vincular el dispositivo.



En la siguiente pantalla se debe registrar la url de vinculación Windows, la cual consiste en la url completa del servidor MDM más la ruta interna "ws/mobile/W10EnrollmentHandler.ashx":

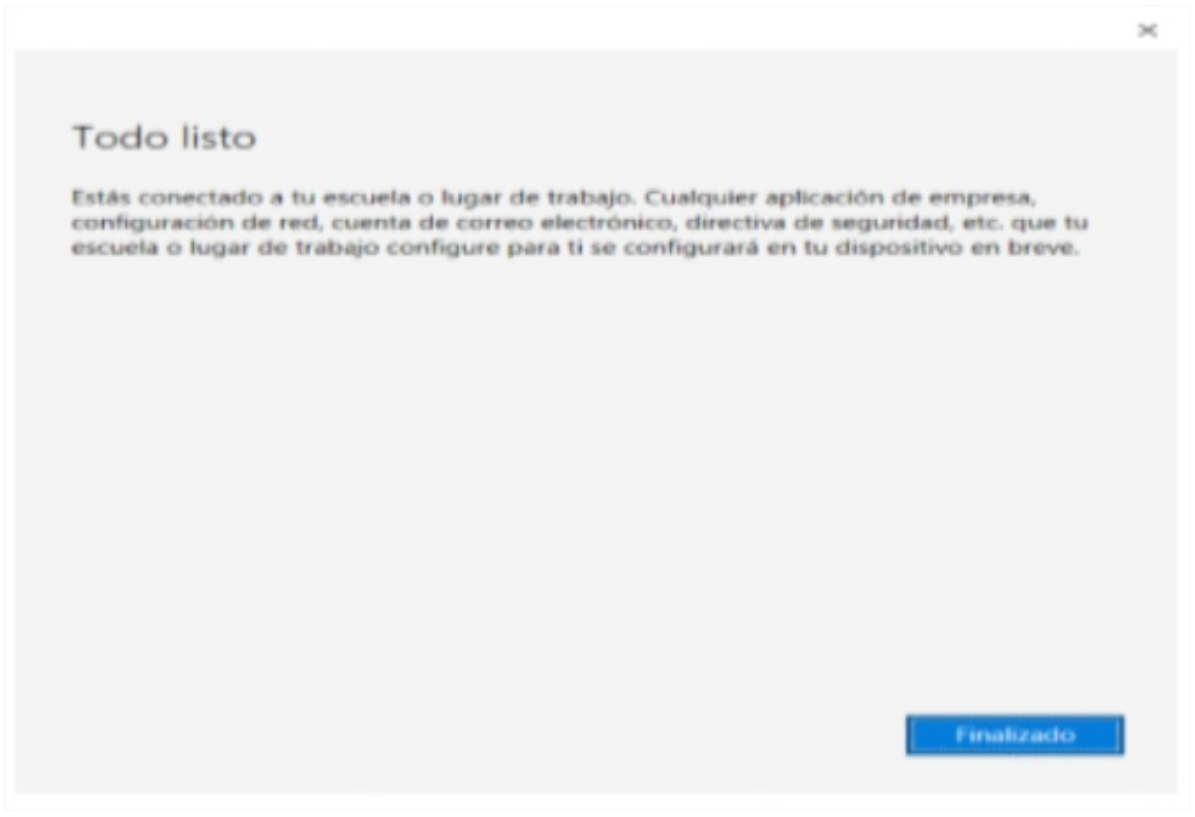


Si los datos solicitados se registraron correctamente al dar clic sobre el botón siguiente, se desplegará la siguiente pantalla, donde es necesario registrar el usuario y la contraseña de la cuenta correspondiente al directorio activo.

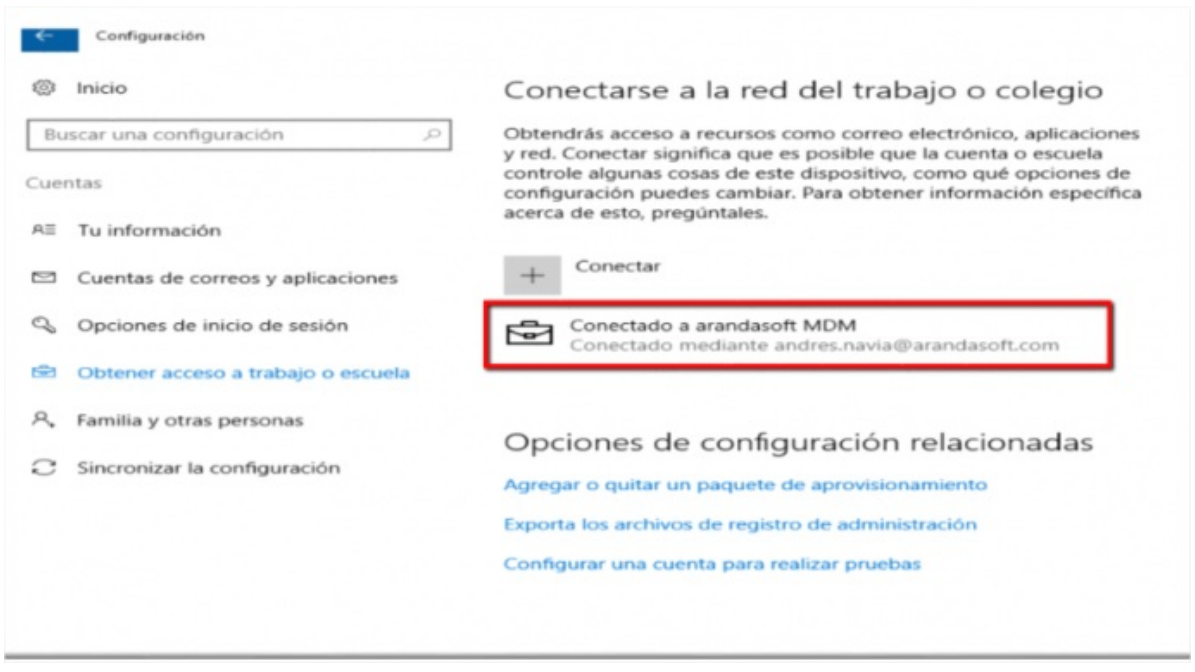


Al dar clic sobre el botón siguiente, el sistema registrara el dispositivo en cuestión.

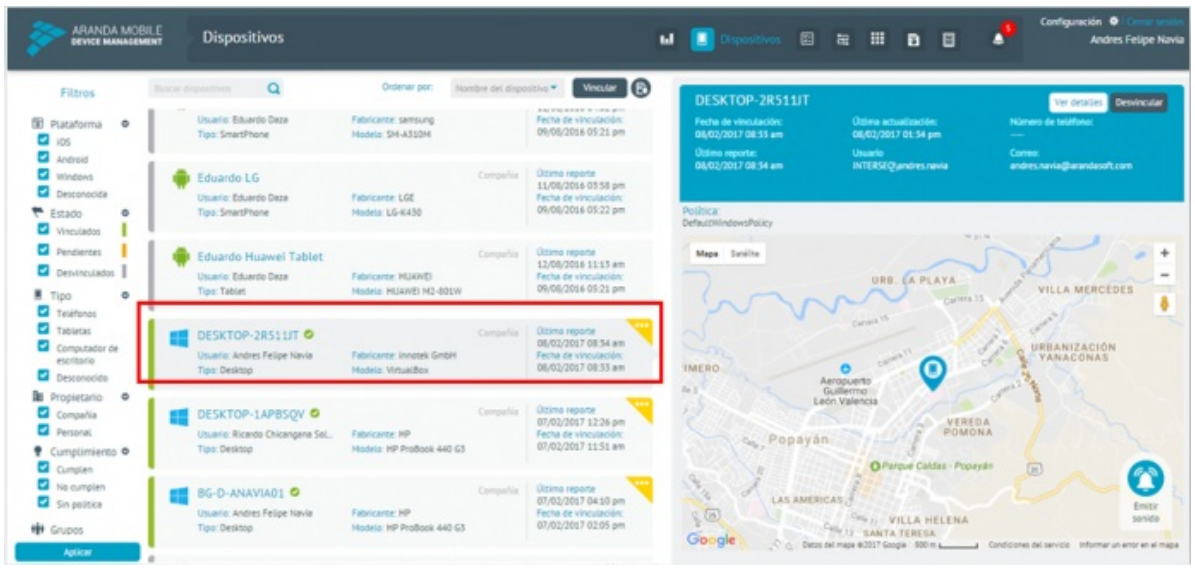
Y finalmente se despliega la pantalla de confirmación indicando que el proceso terminó satisfactoriamente.



Automáticamente el sistema lleva al usuario al módulo de configuración de Windows, donde se debe visualizar el dispositivo conectado la consola de Aranda AEMM.



Para verificar lo anteriormente mencionado, ingresar en la consola de AMDM a la sección de Dispositivos donde se podrá visualizar el nombre del dispositivo vinculado:

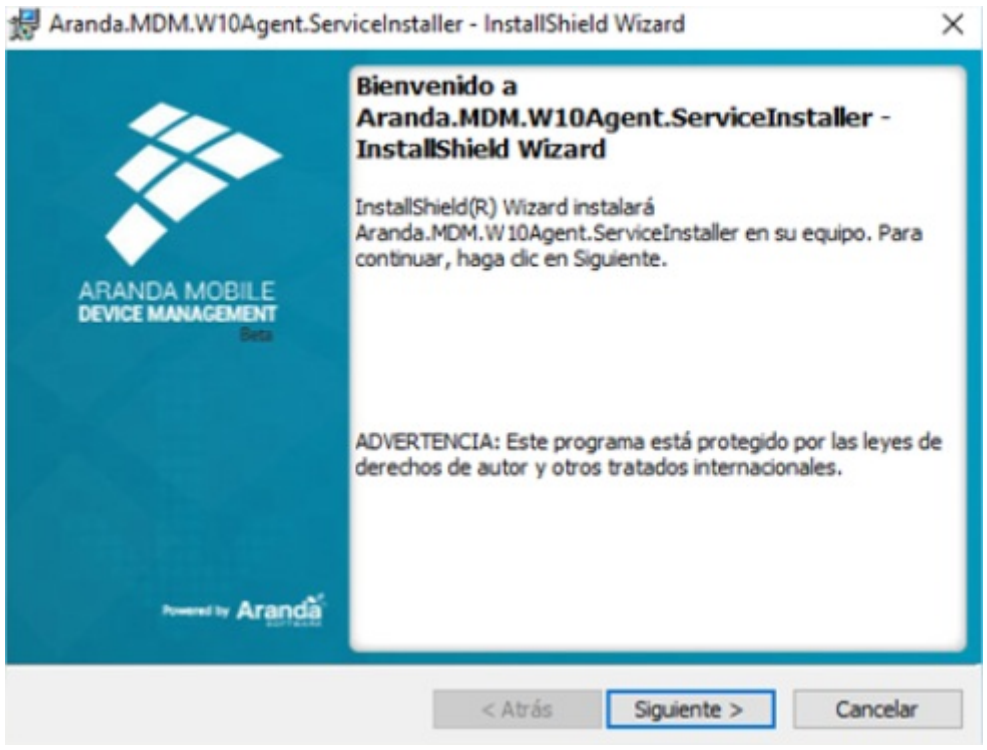


Vinculación del Agente Aranda AEMM para Windows

Una vez terminada la vinculación nativa se debe realizar la instalación del agente para alcanzar mayor capacidad de gestión sobre el dispositivo. Para ello se requiere la última versión del siguiente instalador:

Aranda.MDM.W10Agent.Service.Installer.exe

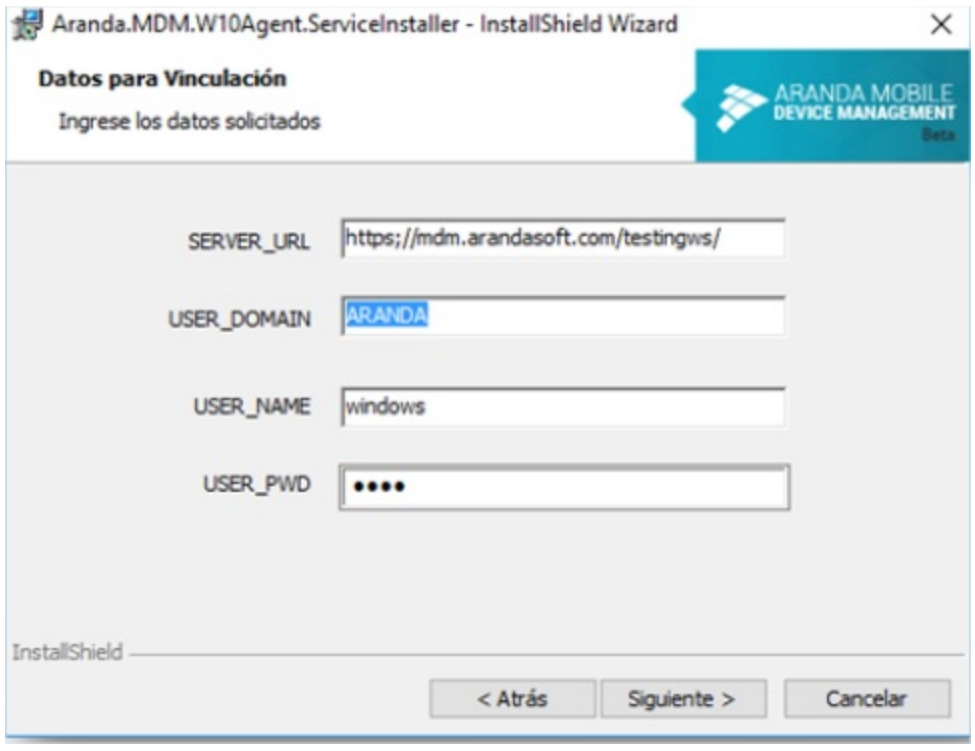
Ejecute el instalador y haga clic en siguiente:



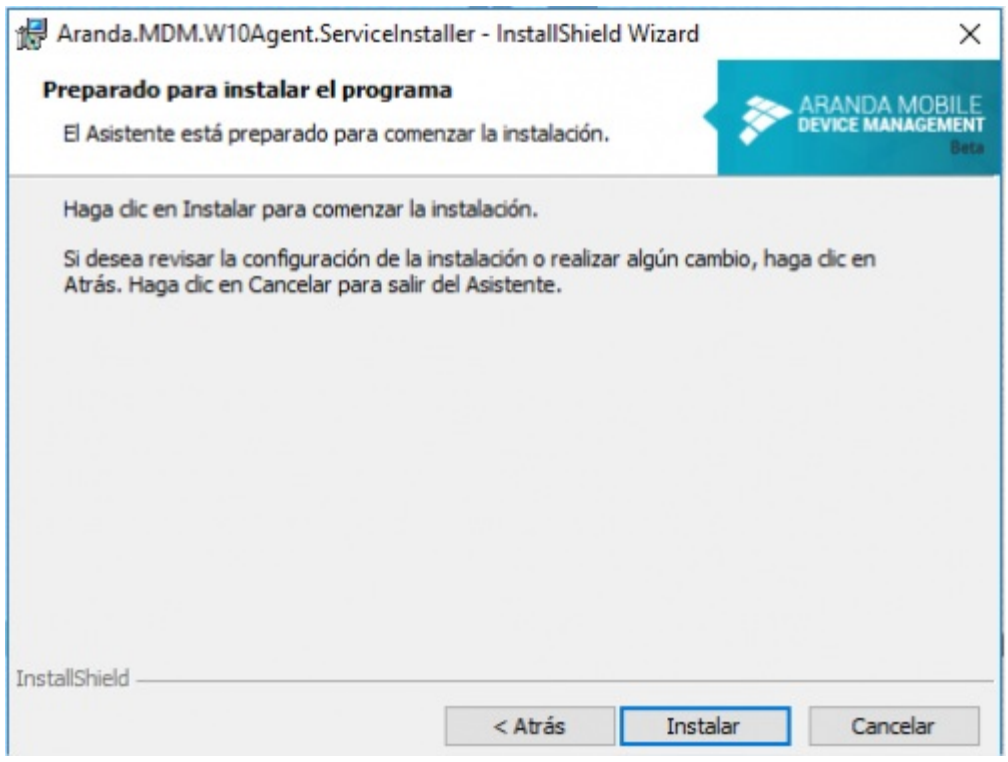
Confirmar la instalación registrando correctamente los datos que a continuación se describen:

Datos	Descripción
SERVER_URL:	Corresponde a la dirección url del servidor donde se están desplegando los servicios web de la consola, sin incluir rutas internas.
USER_DOMAIN:	Corresponde al tipo de autenticación del usuario en el dominio, ya sea ARANDA (usuarios locales) o el nombre del directorio activo
USER_NAME:	Nombre del usuario existente en el dominio respectivo.
USER_PWD:	Contraseña del usuario

⚐ **Nota:** actualmente no se está realizando la validación en cuanto a la calidad de los datos ingresados, por lo tanto, es vital que este proceso se haga cuidadosamente, para no requerir una corrección manual o la reinstalación del servicio



Al dar clic sobre el botón Siguiente, se realizará la instalación y debemos esperar que el proceso termine.

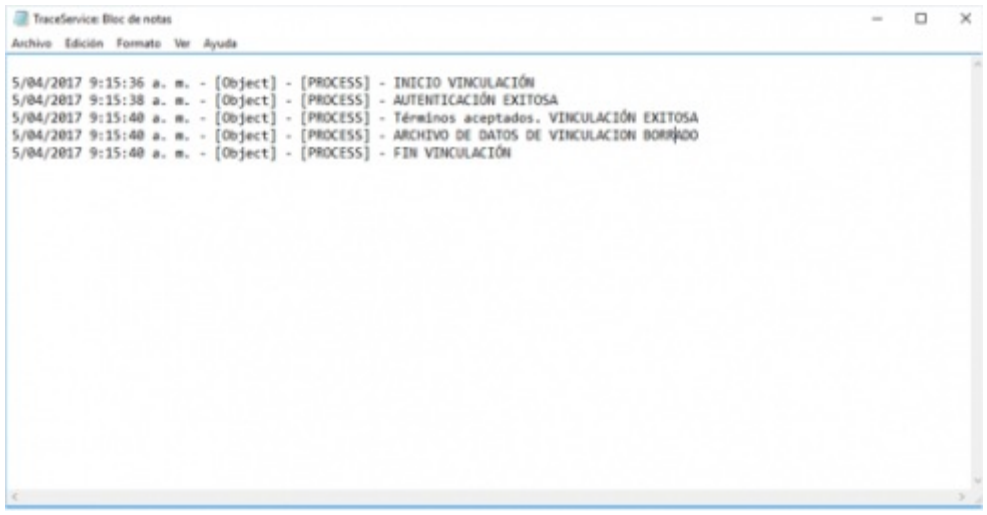


Una vez terminada la copia de archivos, librerías y paquetes necesarios damos clic en finalizar.

Después de instalado el agente, para corroborar que la instalación fue satisfactoria, debemos buscar el archivo TraceService.log en la siguiente ruta:

C:\Program Files (x86)\Aranda\MDM Agent\Logs

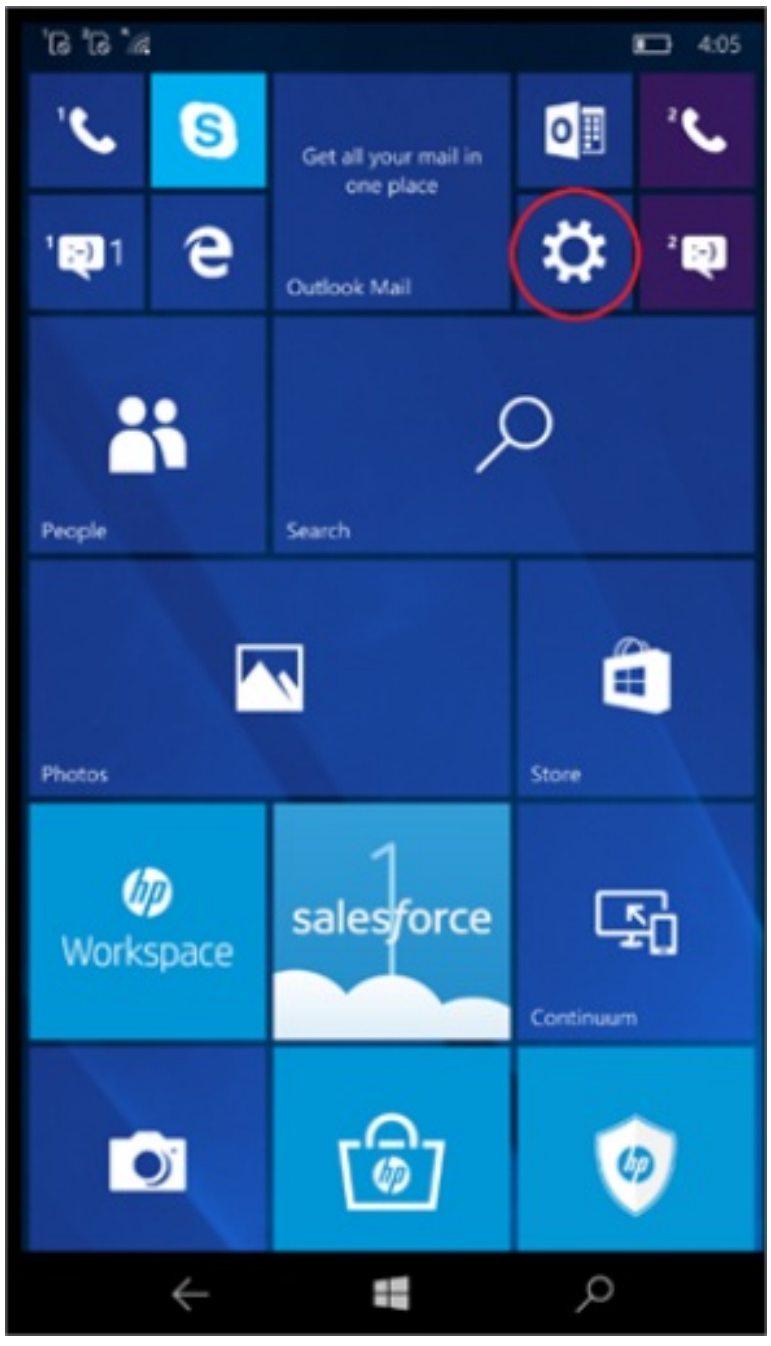
Al abrir dicho archivo se debe visualizar el siguiente contenido, con lo cual es posible validar que el proceso fue exitoso



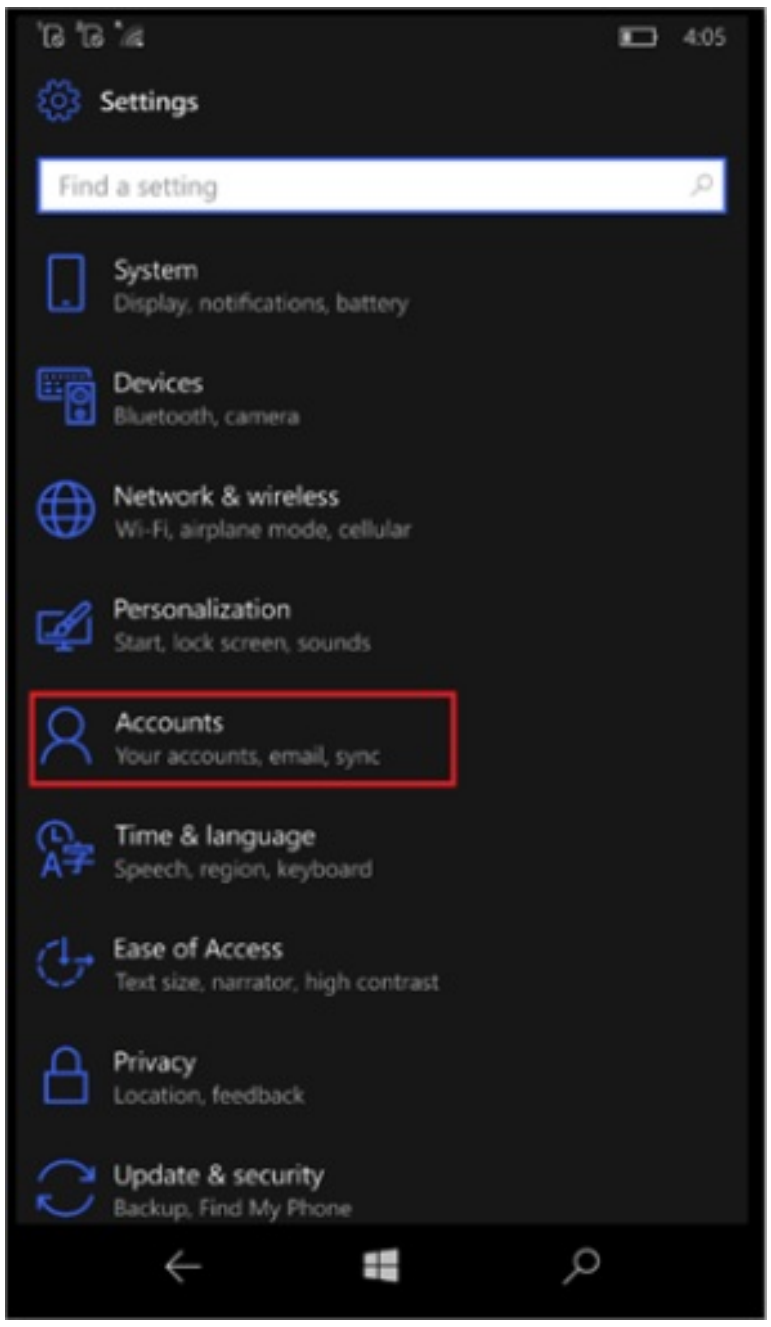
Vinculación Windows 10 Mobile

En Windows 10 Mobile solo está disponible la vinculación nativa, la cual se realiza usando herramientas propias del sistema operativo; para ello siga los siguientes pasos:

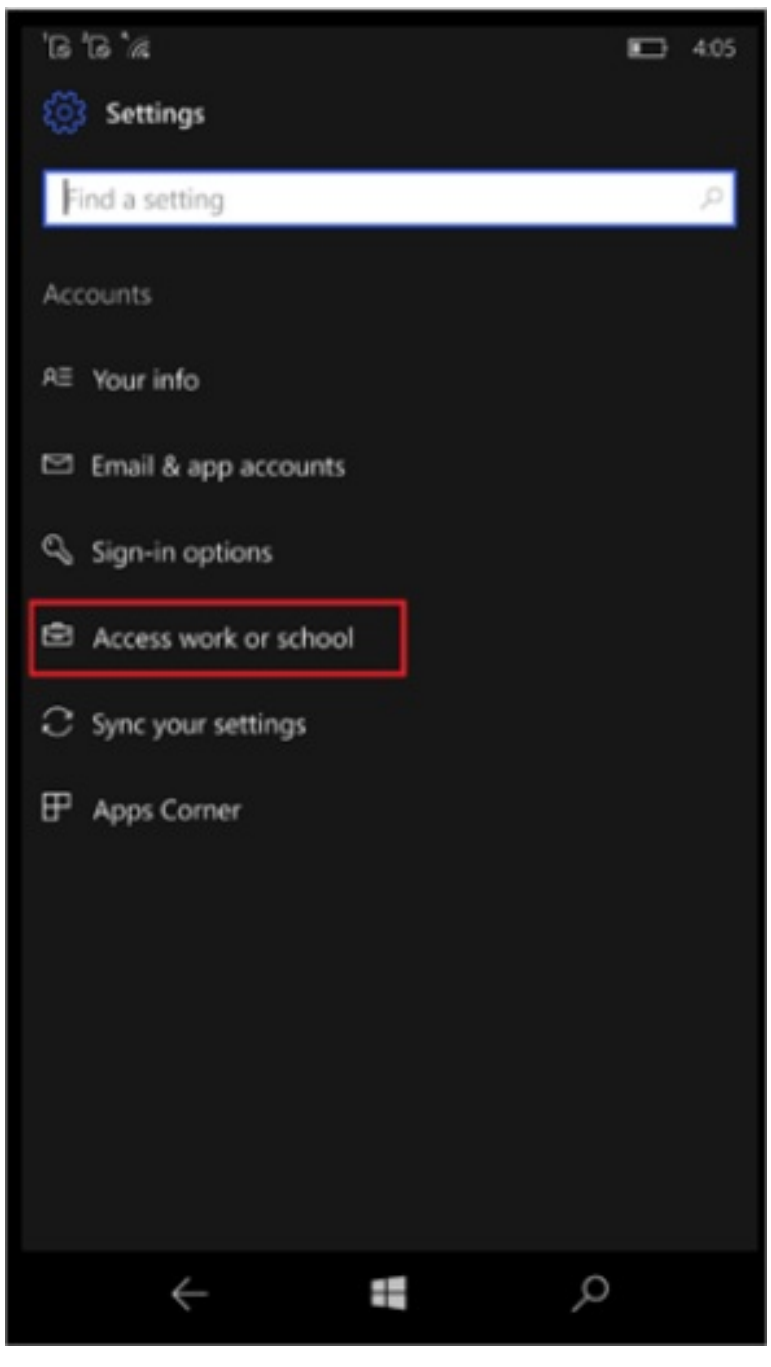
Buscar e Ingresar a la configuración del dispositivo



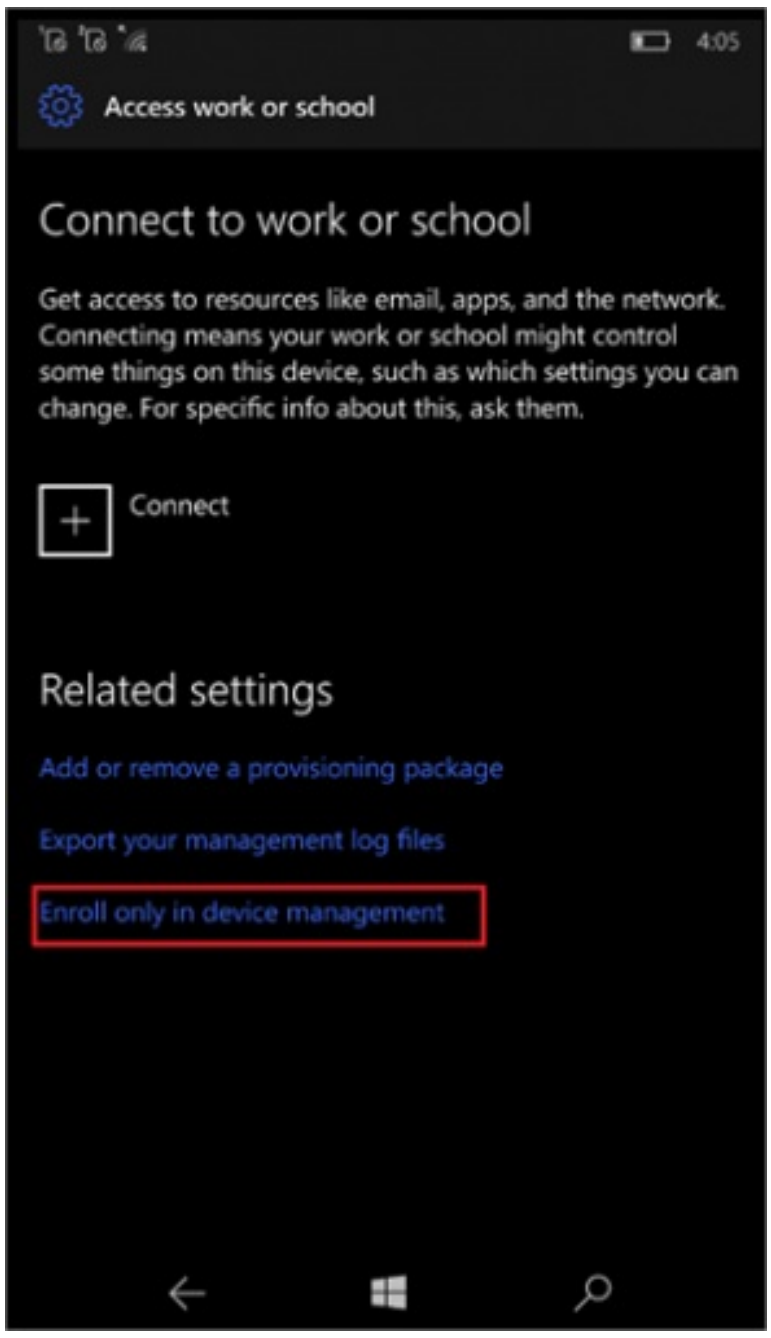
Acto seguido buscar e ingresar a la opción Accounts (cuentas)



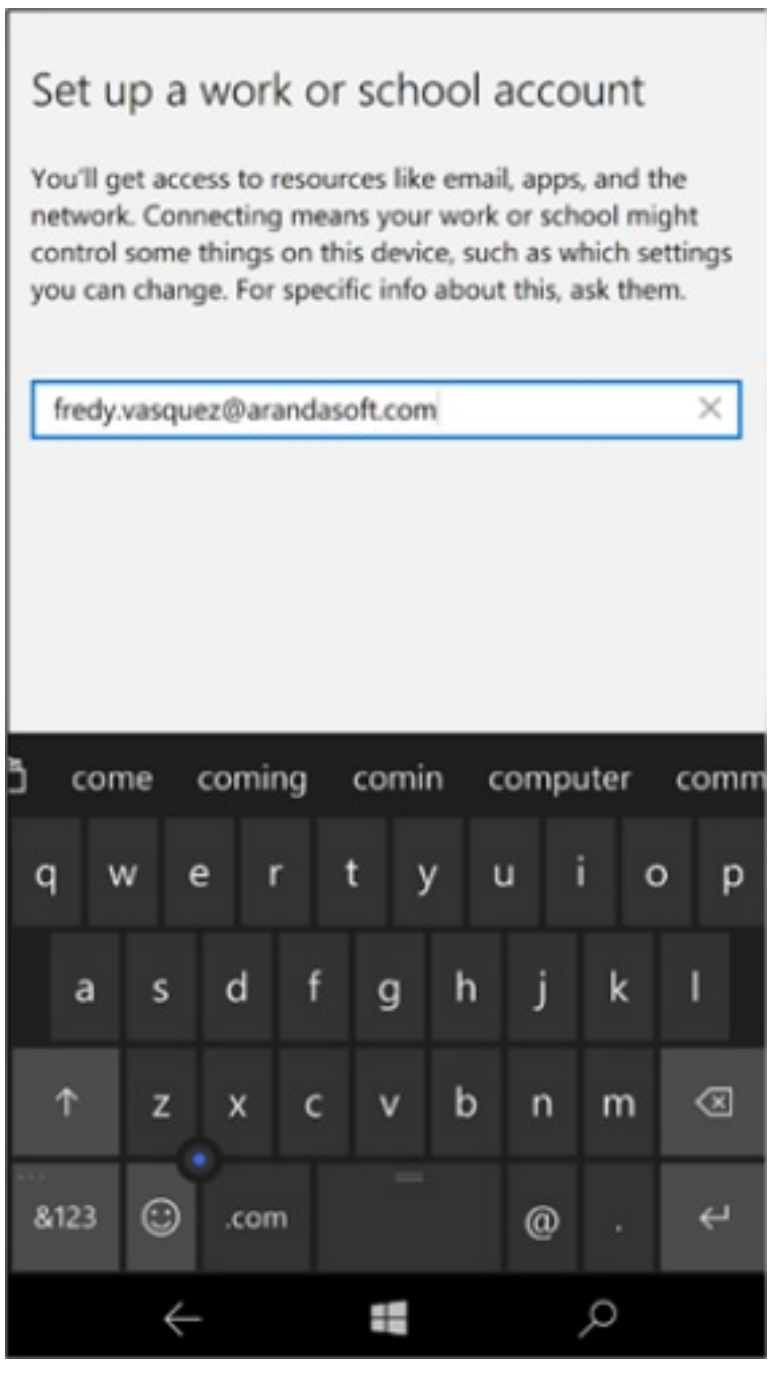
Después de seleccionar la opción cuentas, es necesario buscar e ingresar a la opción "Acceder al Trabajo o Colegio " (Access work or school).



Posteriormente se debe seleccionar la opción Inscribirse solo en la administración de dispositivos:

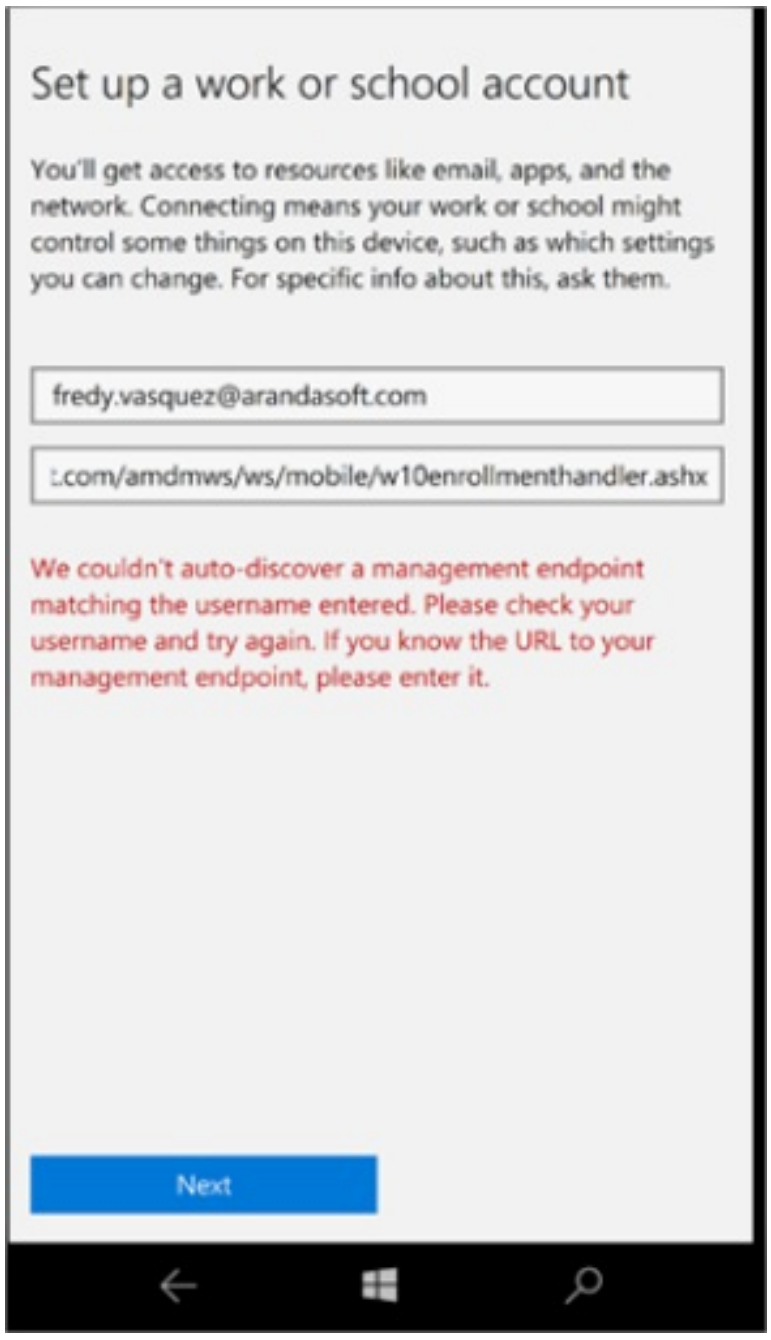


Una vez hayamos igresado al administrador de dispositivos, el paso a seguir es digitar correctamente la cuenta de correo.



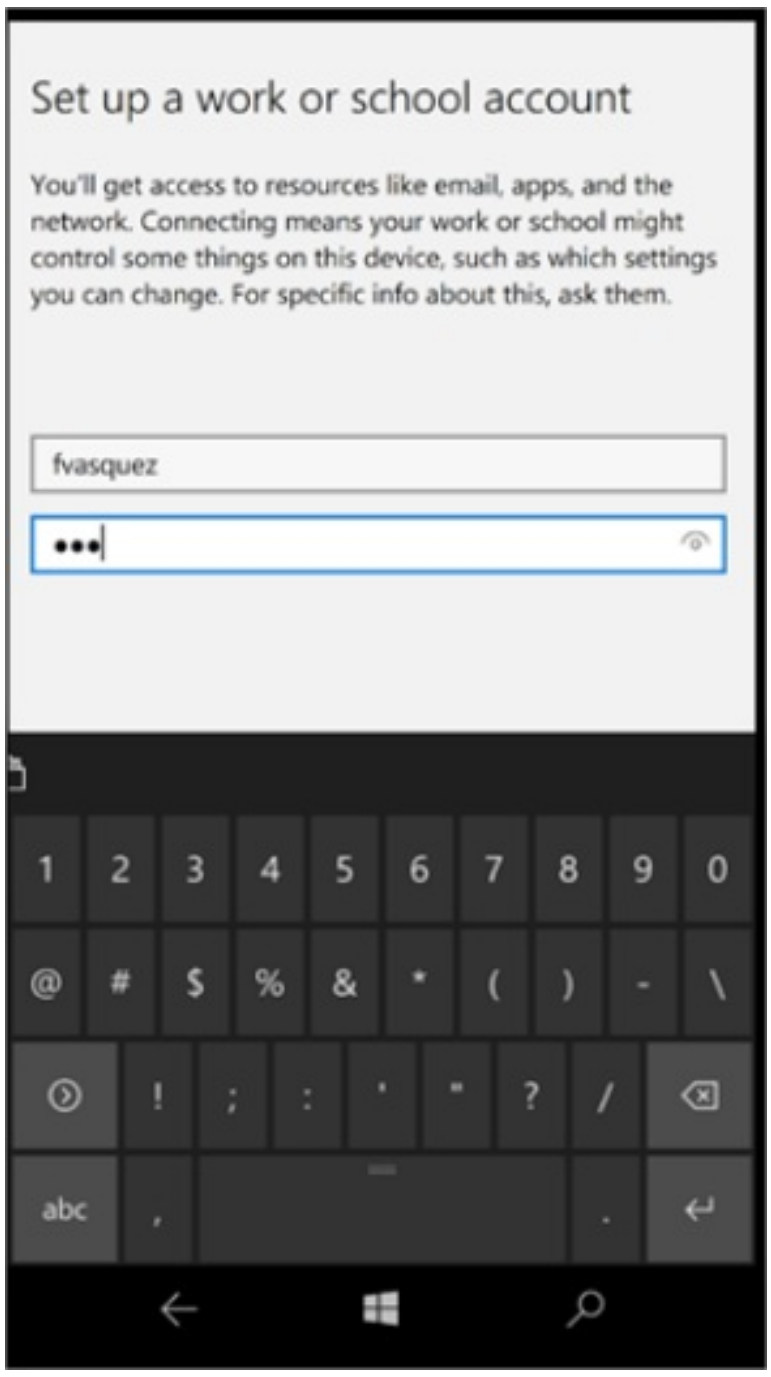
Aparece una pantalla donde informa que no encuentra el endpoint de auto descubrimiento, por lo que se debe ingresar la URL del servidor, el site que contiene los servicios y la ruta al handler de enrolamiento. https:

//{serverl}/{servicios}/WS/Mobile/W10EnrollmentHandler.ashx

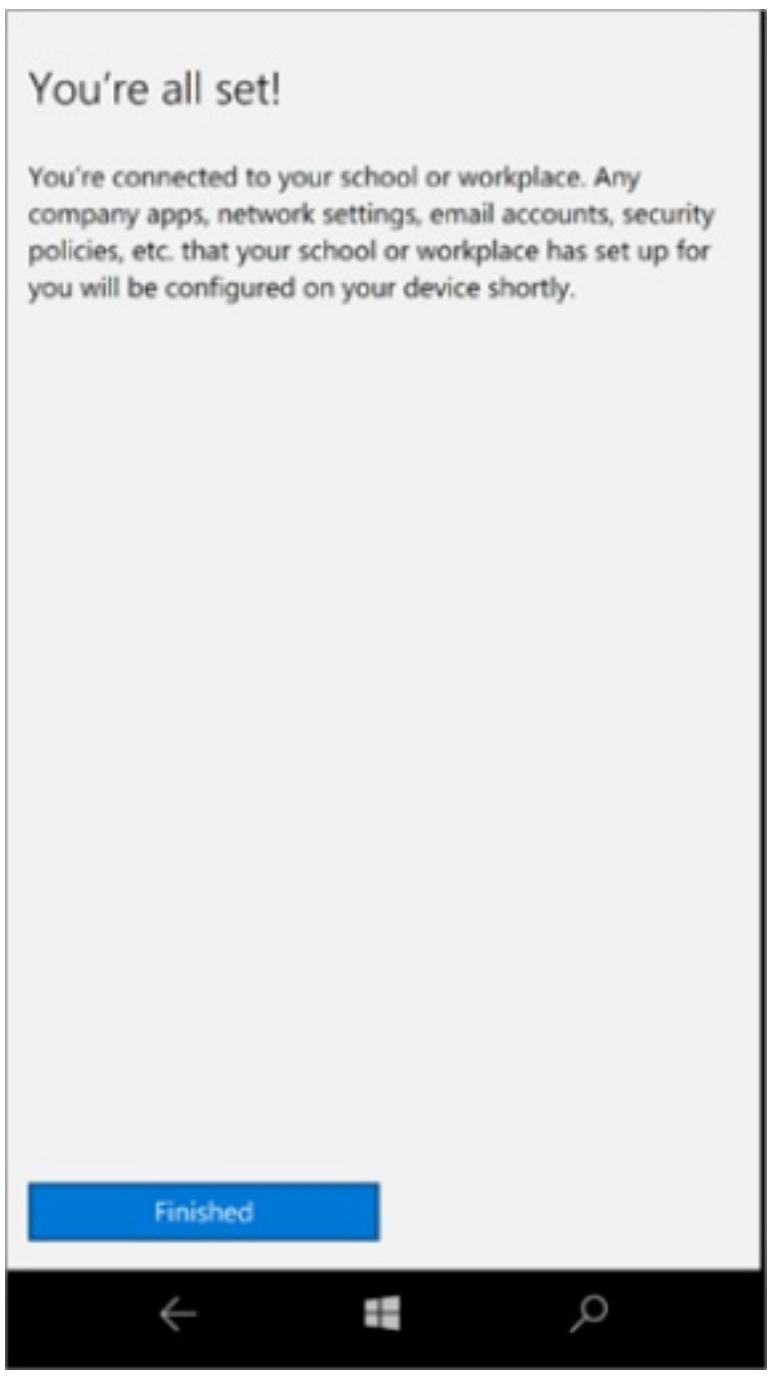


Si la ruta se escribió correctamente, el siguiente paso es Ingresar un usuario de Aranda o del dominio y el password.

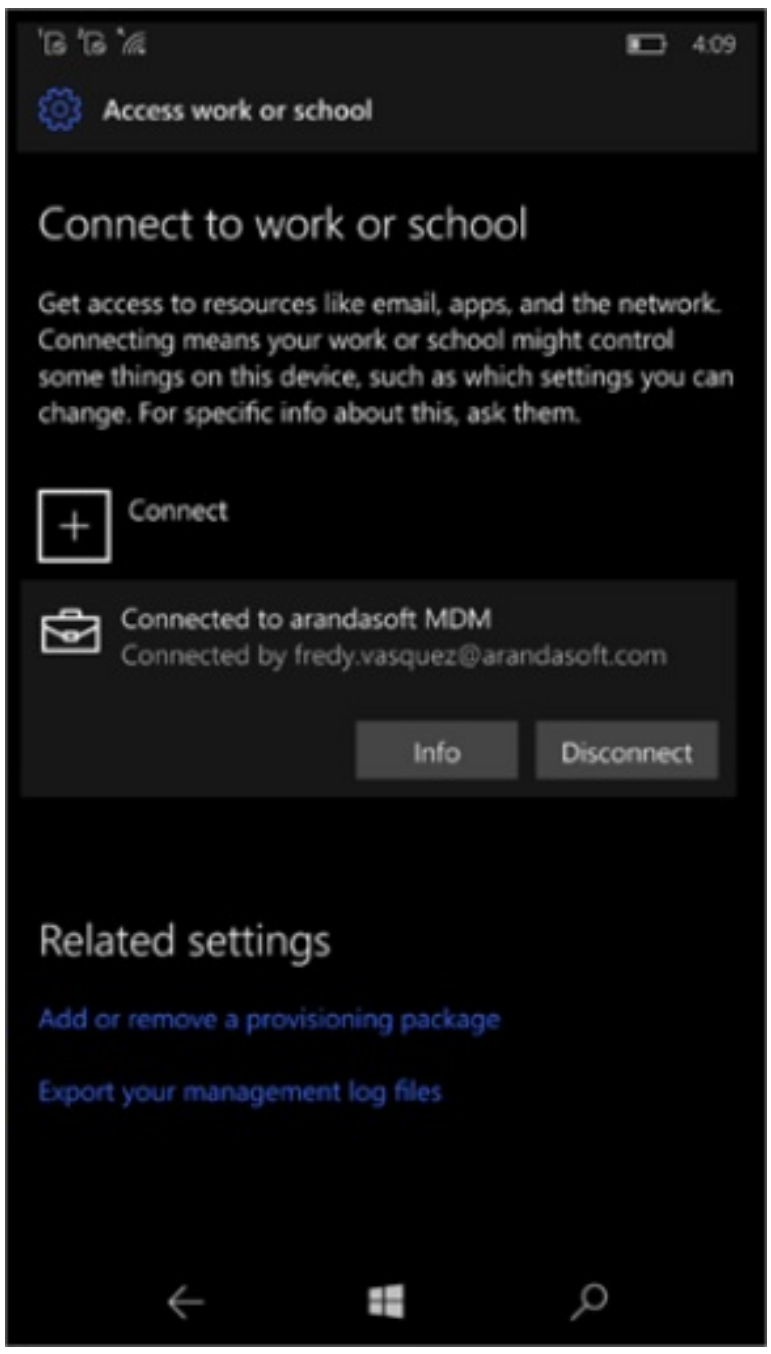
Al hacer tap en “Siguiente”, se envían los datos al servidor y se realiza el proceso de vinculación.



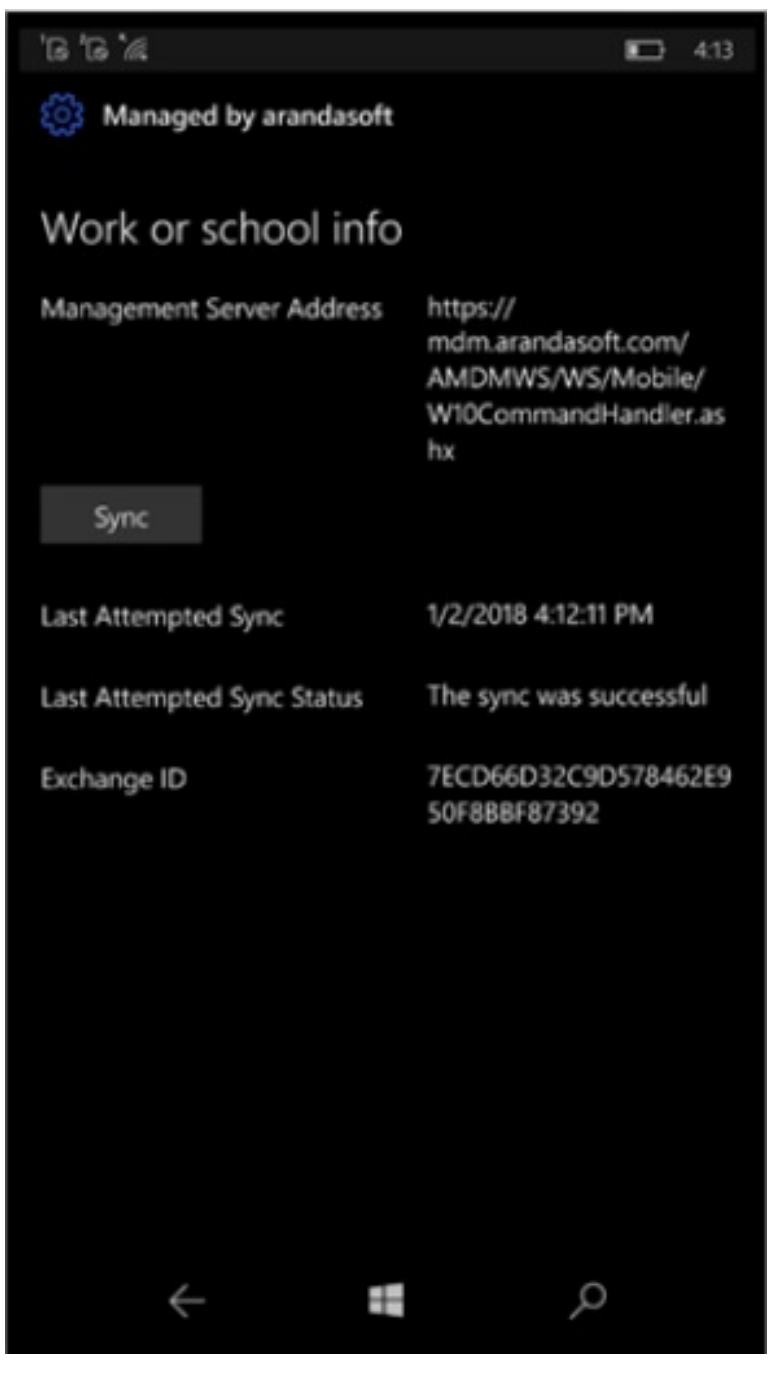
La siguiente pantalla en el dispositivo móvil indicará que se finalizó correctamente el proceso de vinculación



Para validar que la vinculación se realizó con éxito, se debe mostrarse la información de la conexión al servidor de Aranda AEMM.



Se puede hacer tap en los detalles de la conexión y ver más información del proceso y llevar a cabo el proceso de sincronización con el servidor.



Tipos de Vinculación Android

Vinculación Device Owner (DO)

Para la plataforma Android se tienen disponibles en la tienda de Google Play las siguientes aplicaciones de Agente de Aranda, que permiten la vinculación de dispositivos hacia el servidor AEMM.

Aplicaciones de Agente	Descripción
ArandaEMM:	Agente genérico para Android, que permite la vinculación de cualquier dispositivo Android
ArandaEMM for Samsung:	Agente diseñado para gestionar dispositivos Samsung usando la gestión avanzada que ofrece Knox.
ArandaEMM for LG:	Agente diseñado para gestionar dispositivos LG, usando la gestión ofrecida por LG Gate.
ArandaEMM for Cyrus:	Agente diseñado para gestionar dispositivos Cyrus, incluye la firma de fabricante de Cyrus.
ArandaEMM for Panasonic:	Agente diseñado para gestionar dispositivos Panasonic, incluye la firma de fabricante de Panasonic.

Los agentes descritos en la anterior sección (Vinculación->android) son compatibles con vinculación Android for Work (AFW).

Vinculación AFW Device Owner

El modo de vinculación AFW Device Owner ofrece una gestión completa del dispositivo por parte del servidor AEMM. Este tipo de vinculación es recomendada cuando los dispositivos son propiedad de la empresa.

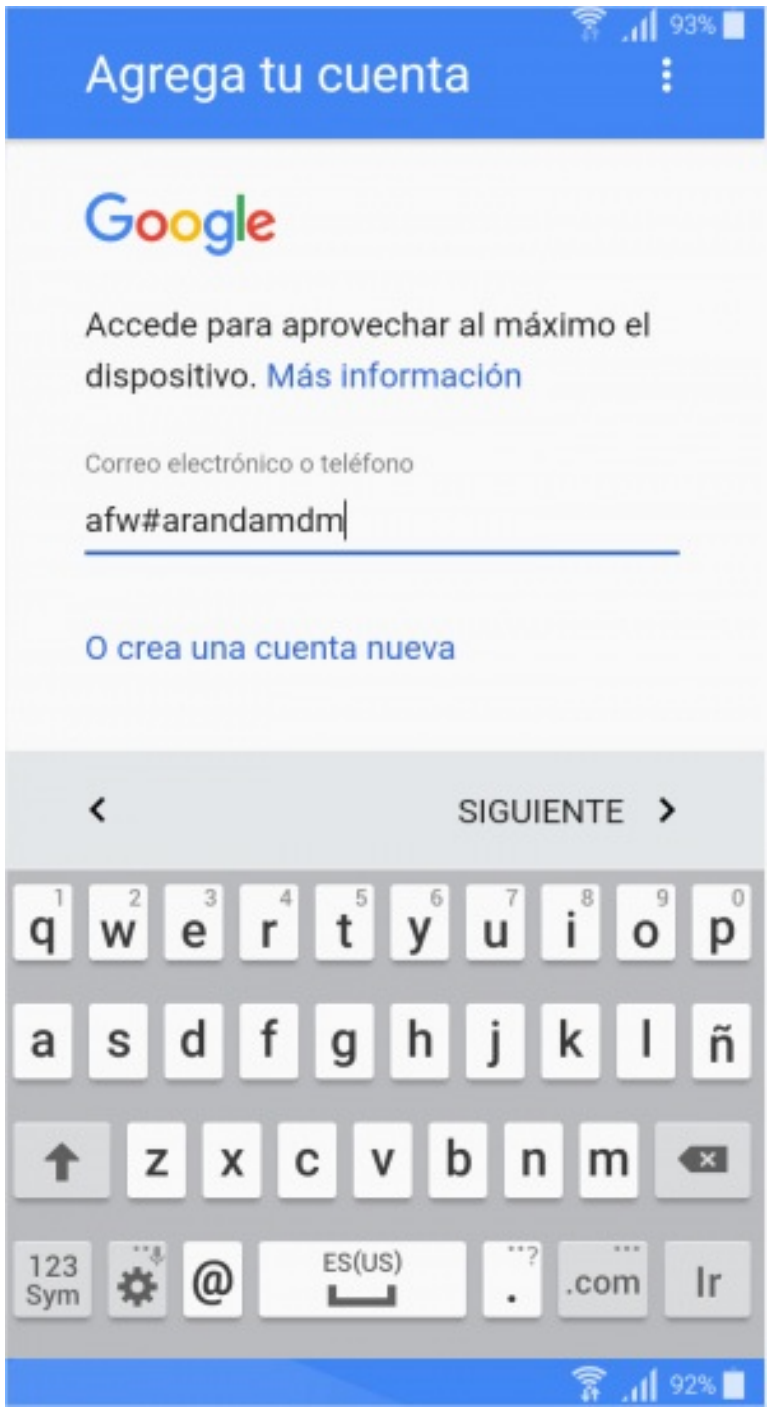
Para acceder al modo device owner es necesario disponer de dispositivos nuevos y/o realizarles un reseteo de fábrica.

Para este proceso es necesario conocer el identificador DPC (DPC id), que identifica el agente que administrará el dispositivo. La siguiente tabla describe cada uno de los agentes con su DPC id correspondiente:

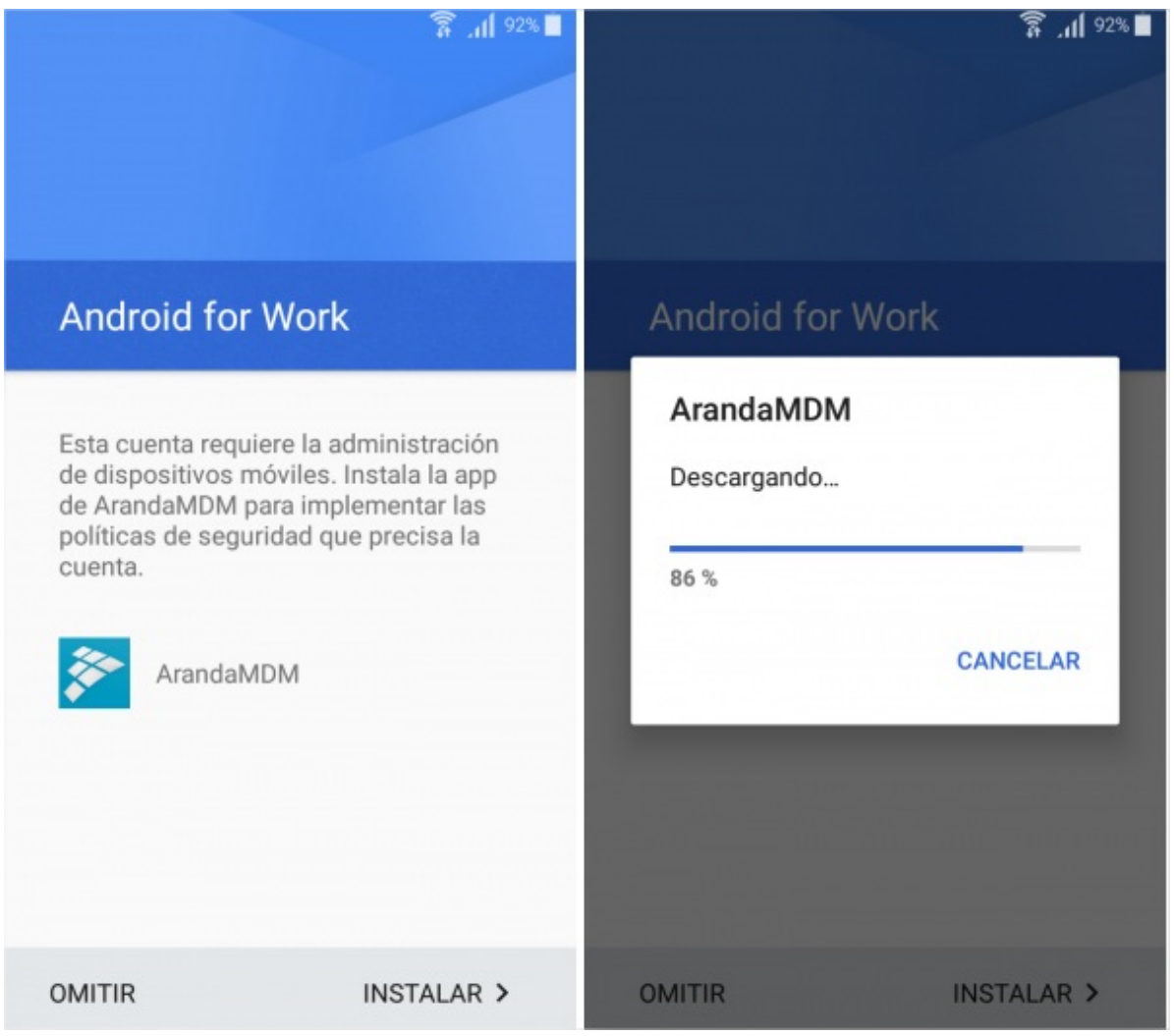
Agente	Identificador DPC
ArandaEMM	afw#arandamdm
AradaEMM for Samsung	afw#arandamdmknox
ArandaEMM for LG	afw#arandamdmlge
ArandaEMM for Cyrus	afw#arandamdmcyrusnew

Para iniciar la vinculación es indispensable conectar el dispositivo a Internet, bien sea por datos móviles o agregando una red wifi.

El dispositivo debe estar nuevo o restaurado de fábrica, una vez se solicite una cuenta de google para iniciar la configuración inicial del dispositivo, se debe de ingresar uno de los identificadores DPC descritos en la anterior tabla, esto dependiendo del fabricante del dispositivo.



Luego de ingresar el DPC id el sistema operativo iniciará la descarga del agente correspondiente.



Luego de preparado el dispositivo para AFW Device Owner continúa el proceso de vinculación normal descrito en la seccion Vinculacion -> Vinculación desde consola.

Vinculación Profile Owner (PO)

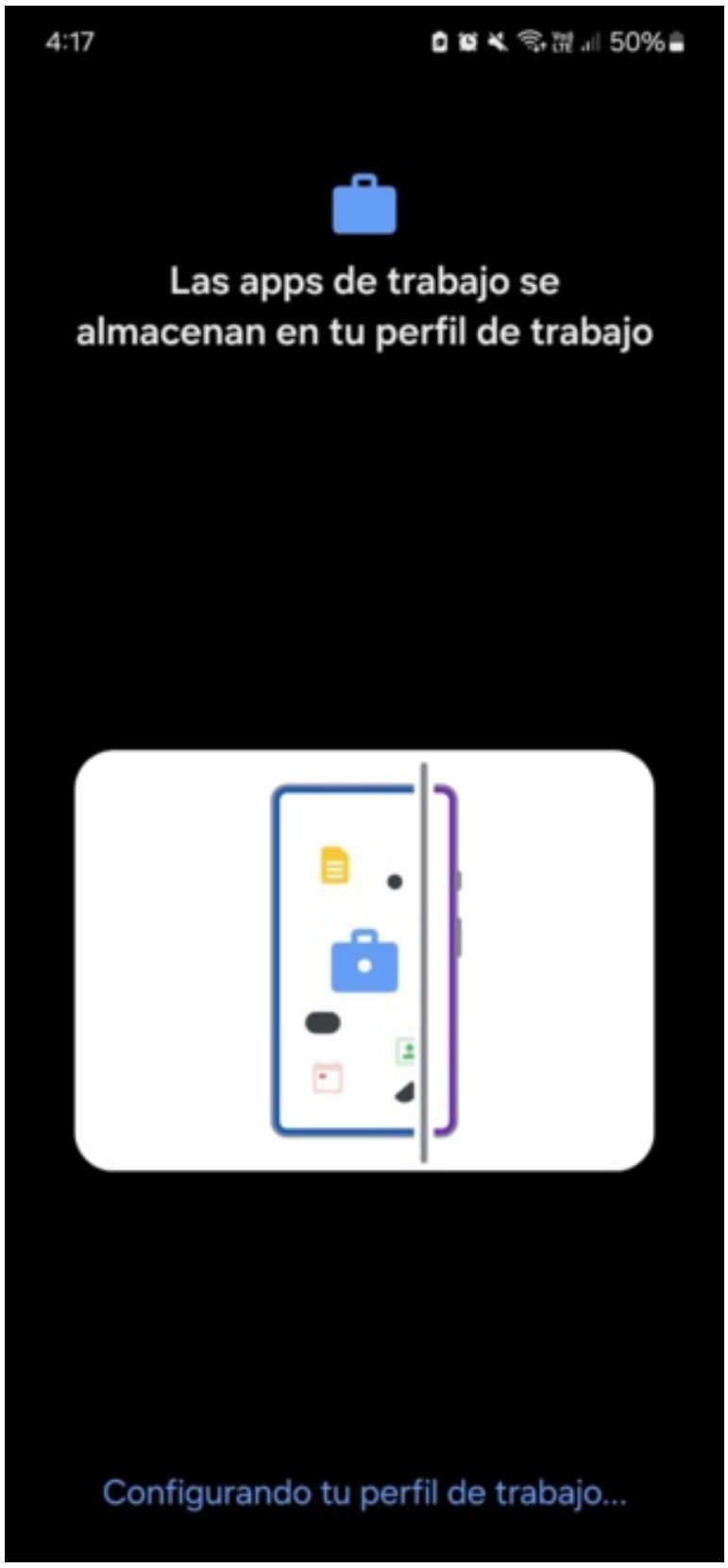
Para la plataforma Android se tienen disponibles en la tienda de Google Play las siguientes aplicaciones de Agente de Aranda, que permiten la vinculación de dispositivos hacia el servidor AEMM.

Aplicaciones de Agente	Descripción
ArandaEMM:	Agente genérico para Android, que permite la vinculación de cualquier dispositivo Android
ArandaEMM for Samsung:	Agente diseñado para gestionar dispositivos Samsung usando la gestión avanzada que ofrece Knox.
ArandaEMM for LG:	Agente diseñado para gestionar dispositivos LG, usando la gestión ofrecida por LG Gate.
ArandaEMM for Cyrus:	Agente diseñado para gestionar dispositivos Cyrus, incluye la firma de fabricante de Cyrus.
ArandaEMM for Panasonic:	Agente diseñado para gestionar dispositivos Panasonic, incluye la firma de fabricante de Panasonic.

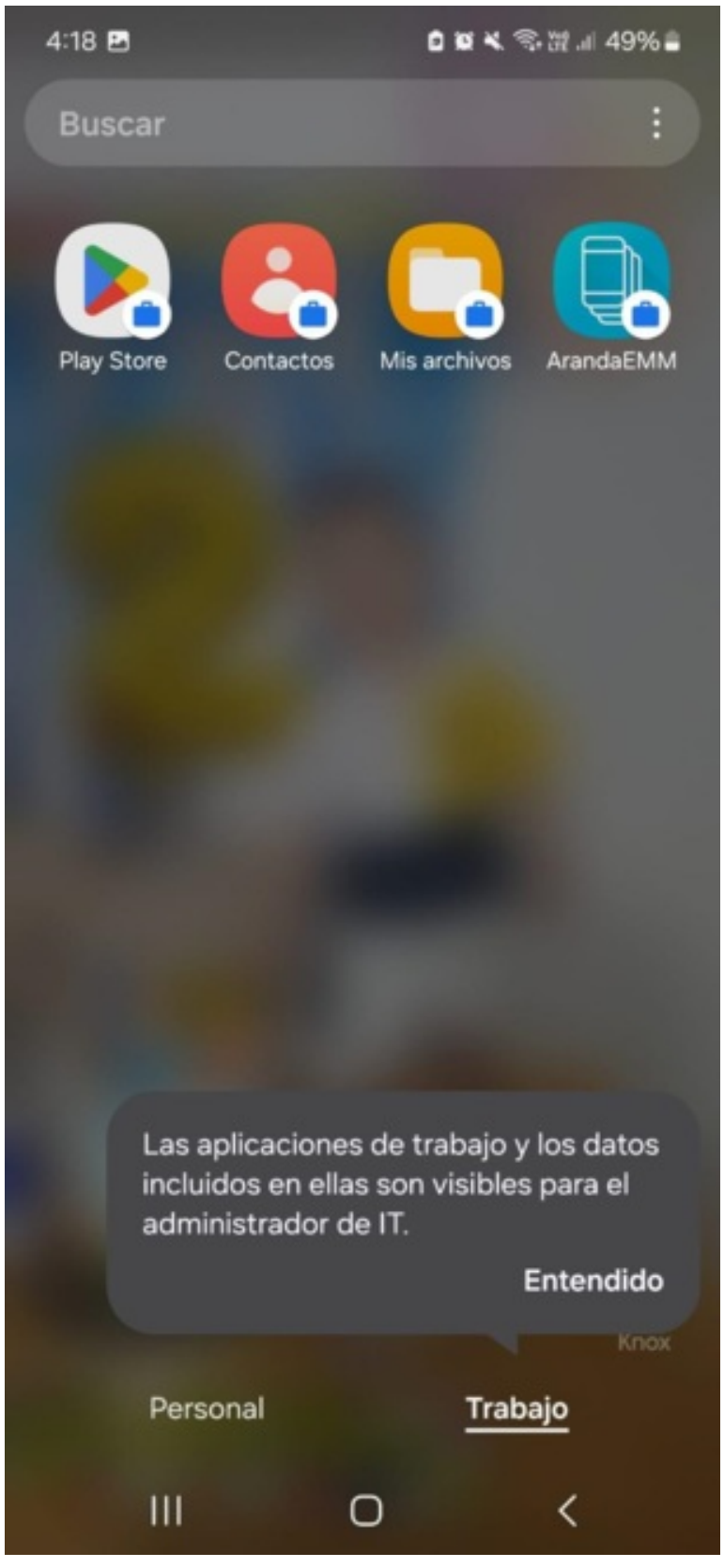
Vinculación AFW Profile Owner

El modo AFW Profile Owner ofrece una vinculación donde el servidor AEMM tendrá control de una sección separada del dispositivo, llamada Perfil de Trabajo. Este tipo de vinculación se recomienda cuando el dispositivo es propiedad del usuario y no puede administrarse en su totalidad. Este modo de vinculación es muy similar a la descrita en las sección anterior (Vinculación-> Vinculación en consola) La diferencia radica en las pantallas que se presentan al usuario donde se indica que se está activando en el dispositivo el perfil de trabajo.

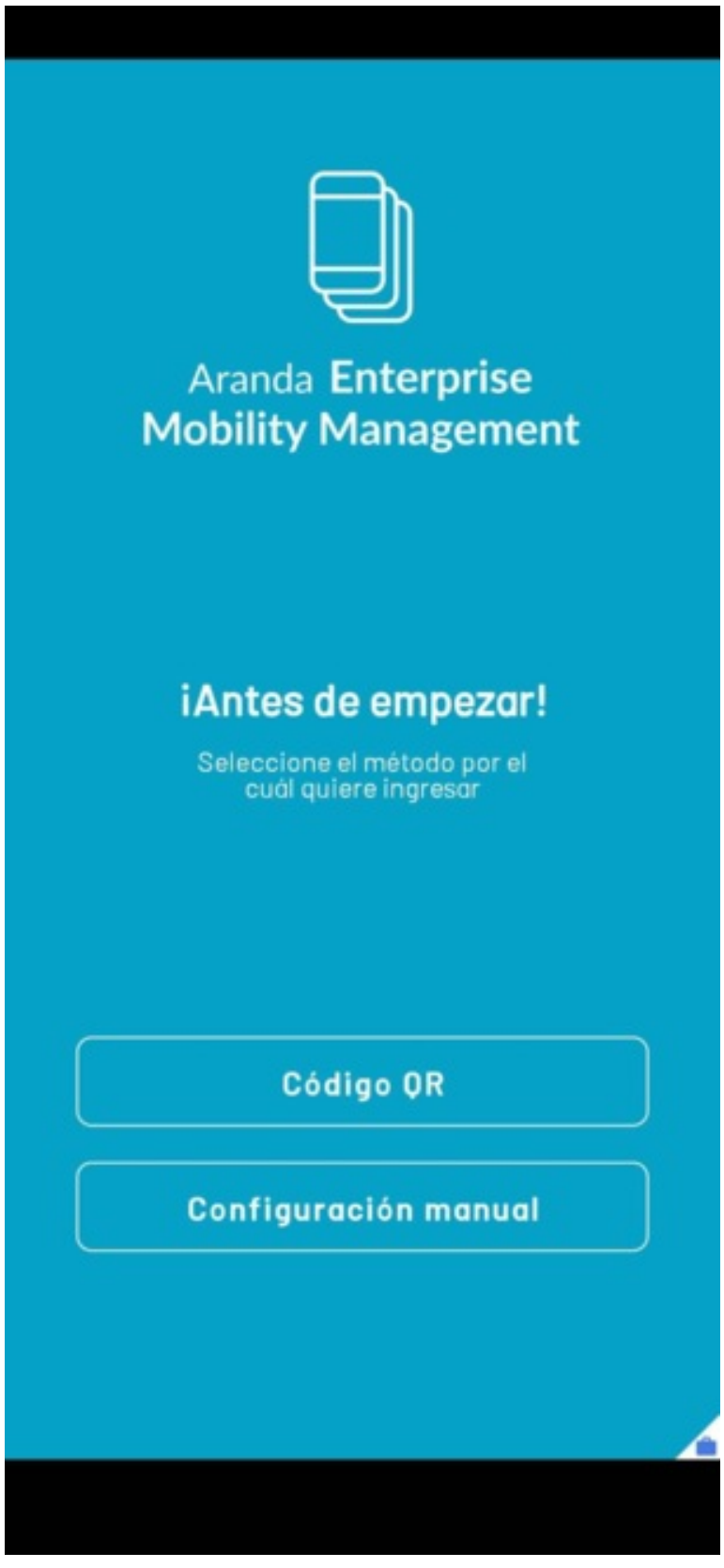

4:11
51%
Aranda Enterprise
Mobility Management
Es necesario instalar el siguiente perfil
Personal
Corporativo
Instalar



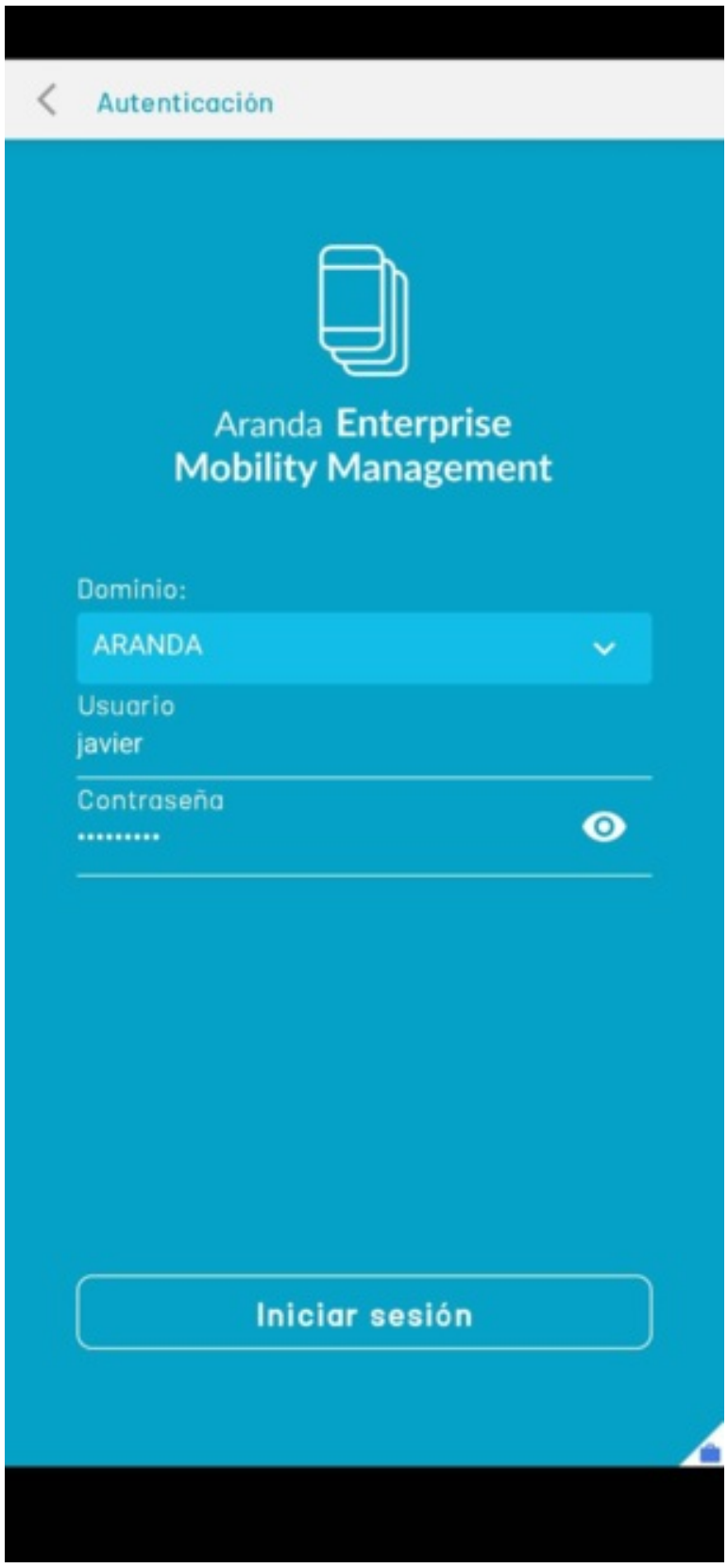
Una vez terminado el proceso de creación del perfil de trabajo, se creará una sección separada en el menú de aplicaciones del dispositivo identificada como trabajo y donde las aplicaciones ahí presentes tendrán una distinción en la esquina inferior derecha que indica que son parte del perfil de trabajo.



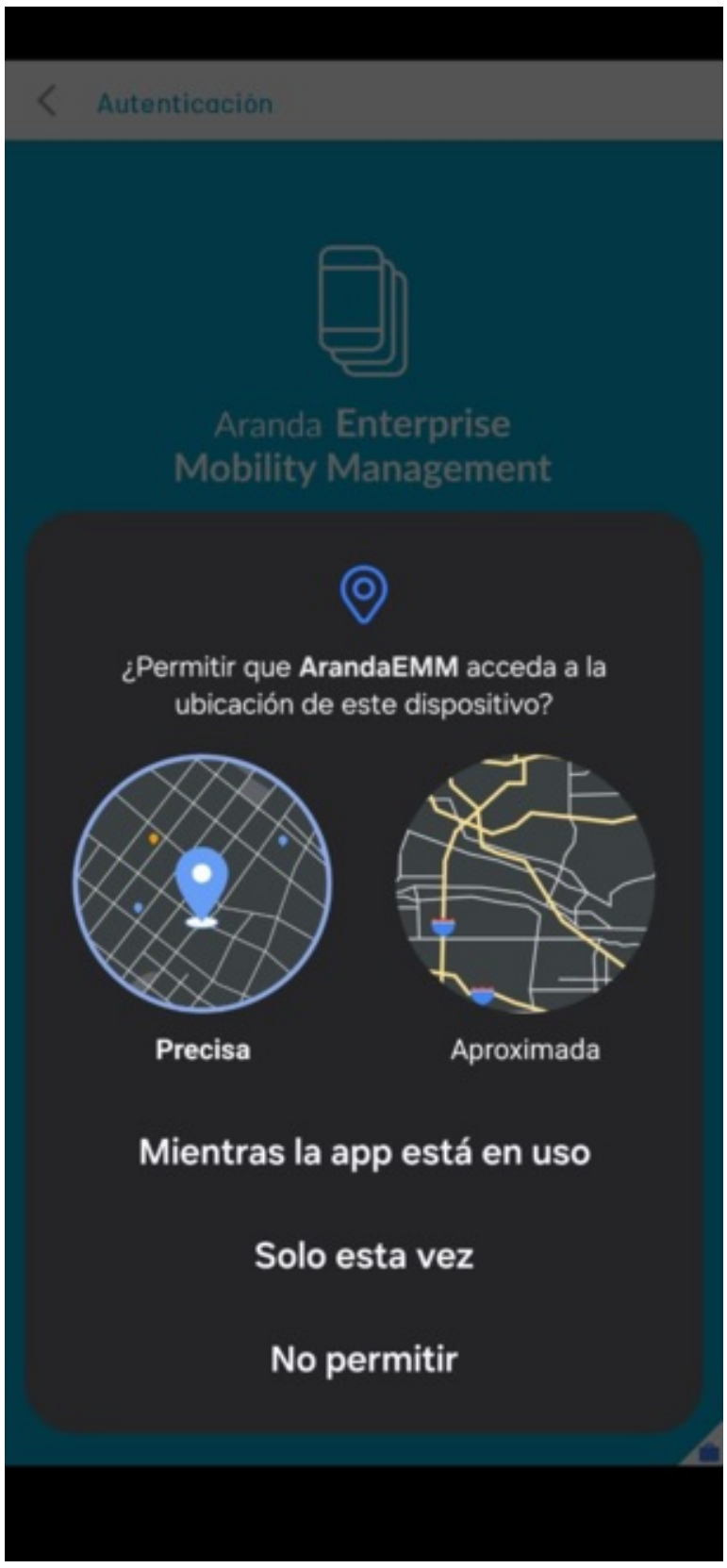
Al ingresar a la aplicación ArandaEMM, se solicitará el método de vinculación a la consola de AEMM

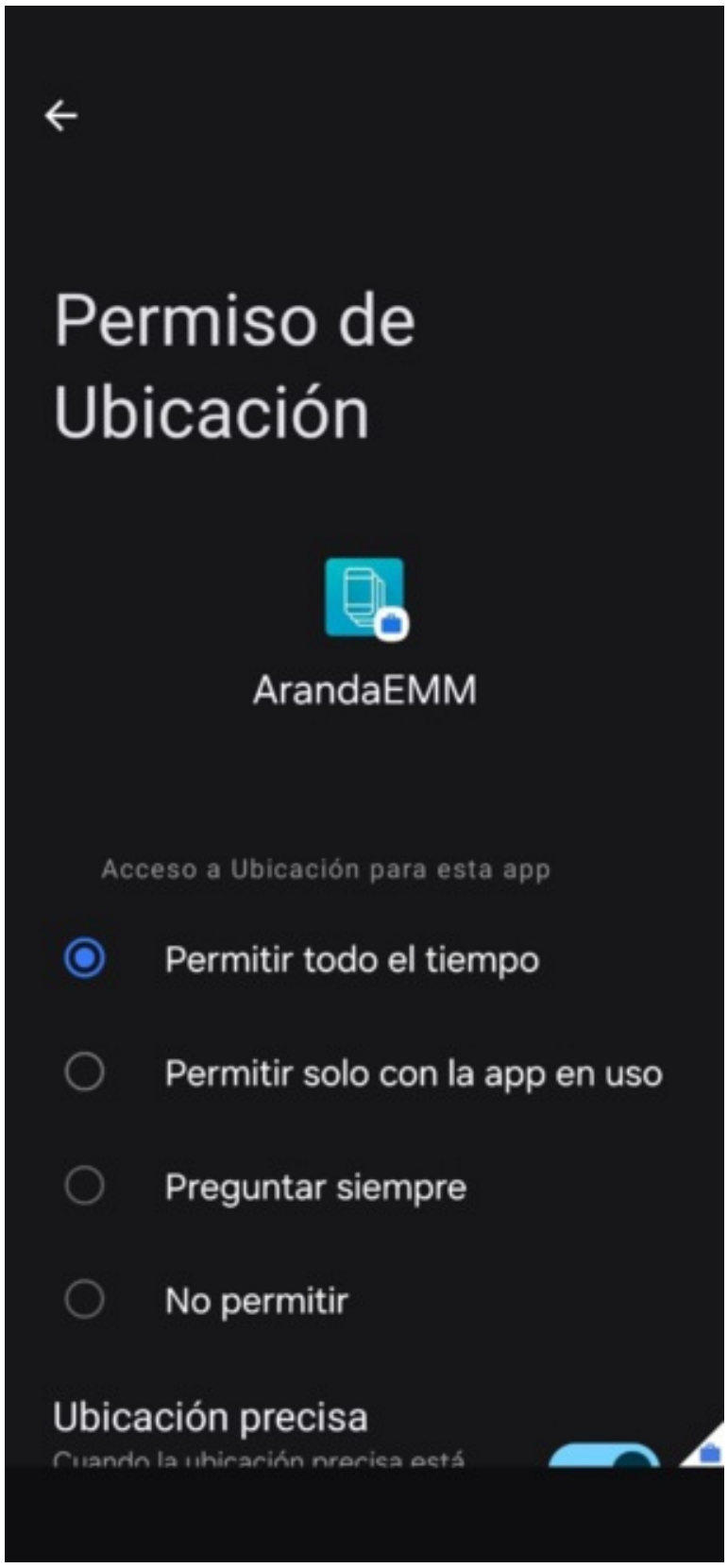


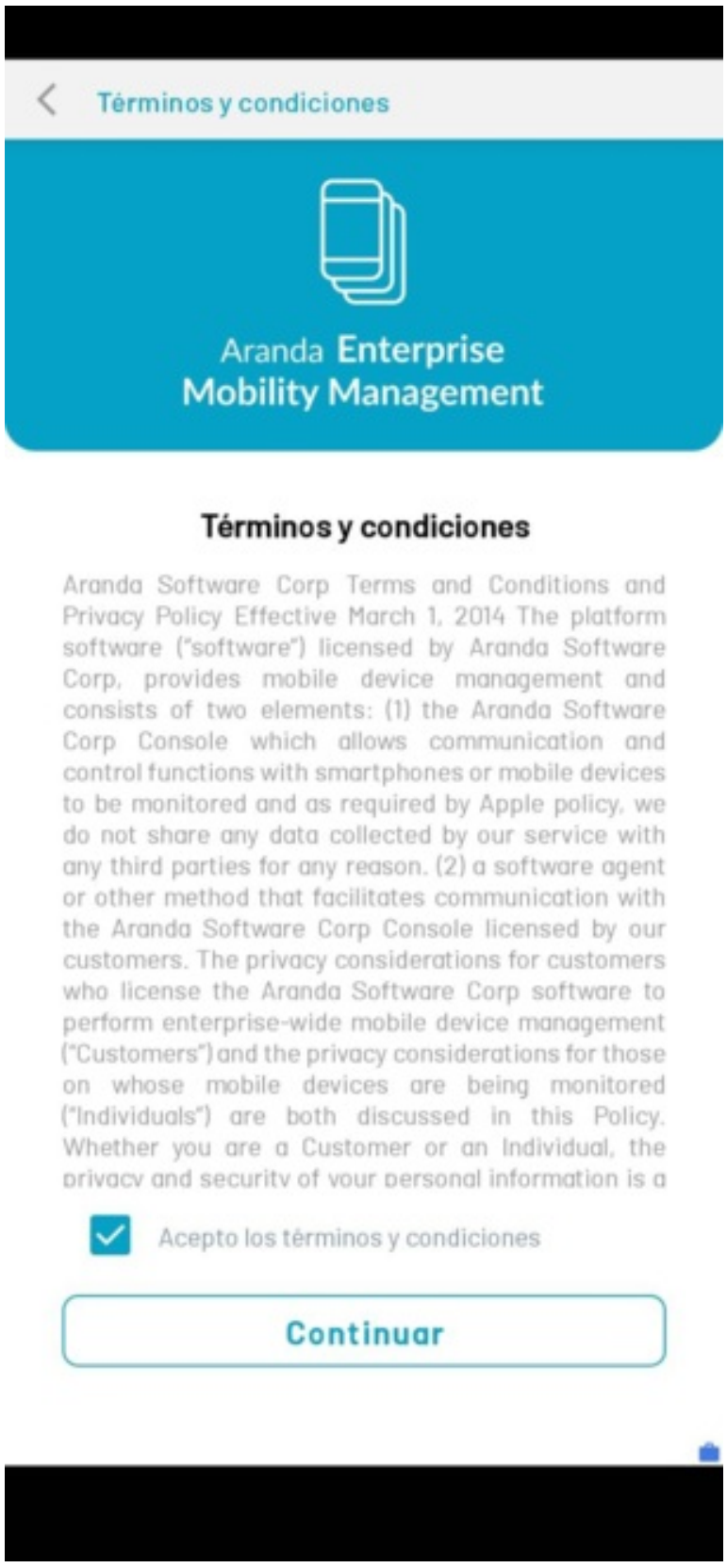
Después de que se realice este proceso (Se lea el QR o se ingrese la URL de forma manual), se habilitará para que ingrese el usuario y la clave para iniciar sesión



Después de que el inicio de sesión es correcto, se deben de aceptar el permiso de ubicación y términos y condiciones de la aplicación móvil de AEMM

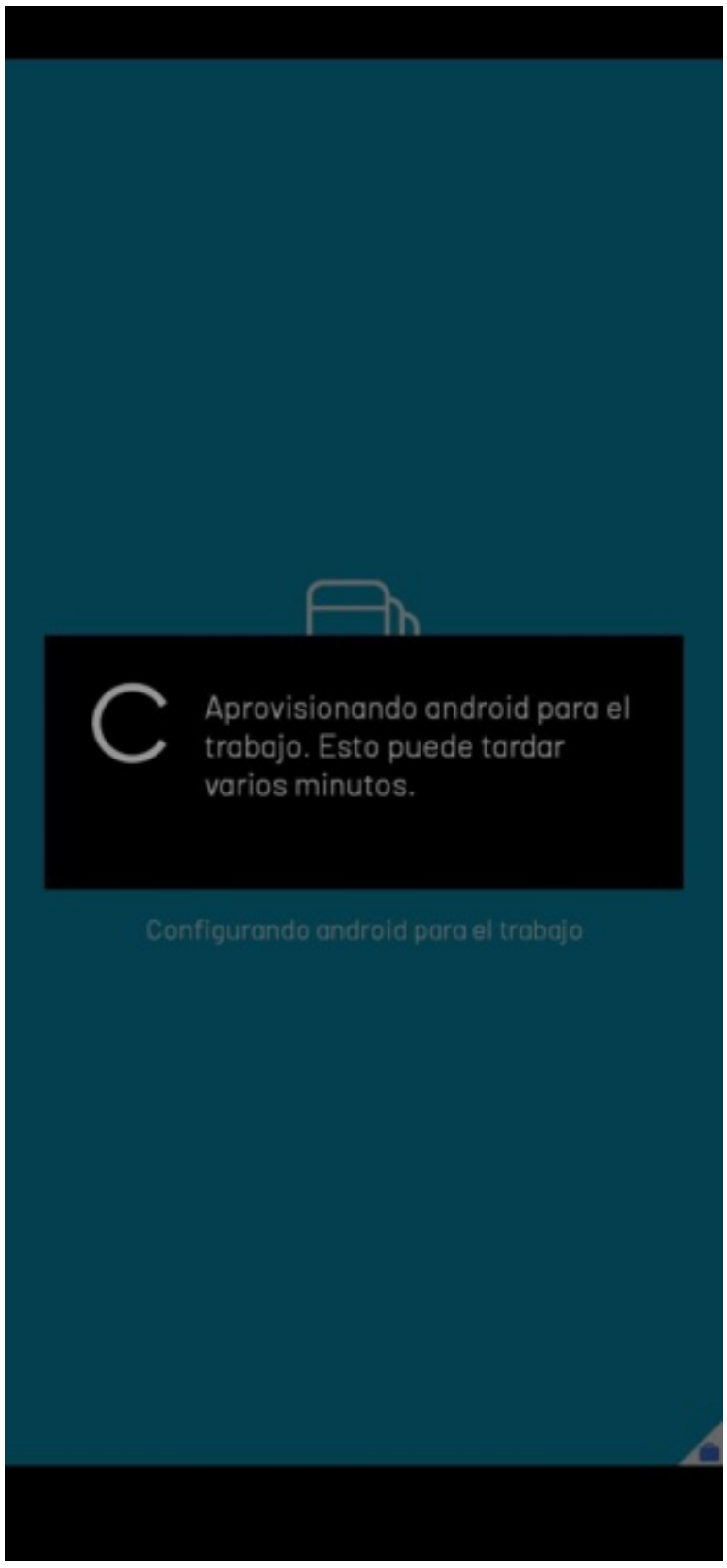

Autenticación
Aranda Enterprise
Mobility Management
¿Permitir que ArandaEMM acceda a la ubicación de este dispositivo?
Precisa
Aproximada
Mientras la app está en uso
Solo esta vez
No permitir


Permiso de Ubicación
ArandaEMM
Acceso a Ubicación para esta app
Permitir todo el tiempo
Permitir solo con la app en uso
Preguntar siempre
No permitir
Ubicación precisa

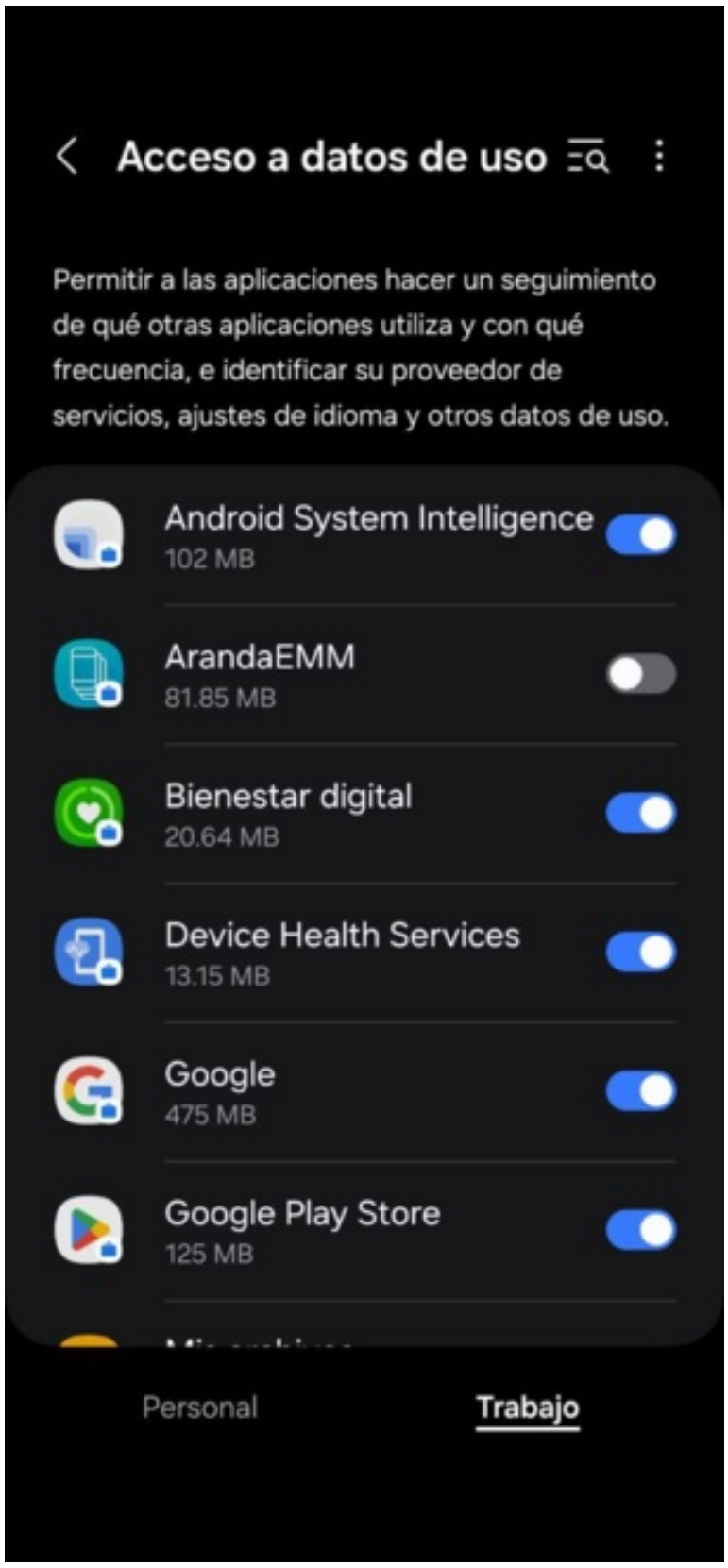


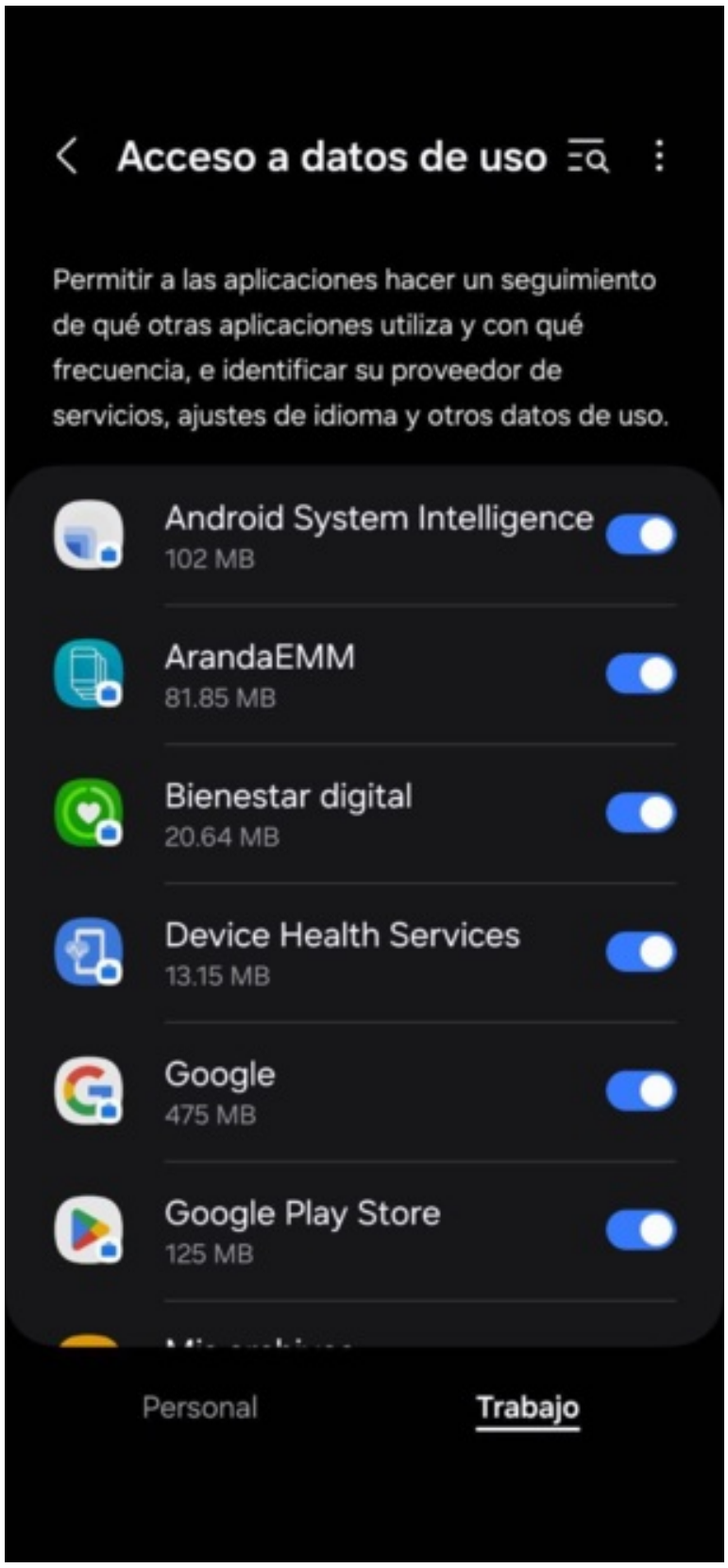
Después de que se de clic al botón **Continuar** de la pantalla de términos y condiciones, se empieza a realizar el proceso de aprovisionamiento del dispositivo. En este proceso, se realiza la vinculación a la consola de AEMM y a gestionar todo lo necesario para que se reconozca a nivel de los servicios de Googl (Android Enterprise)

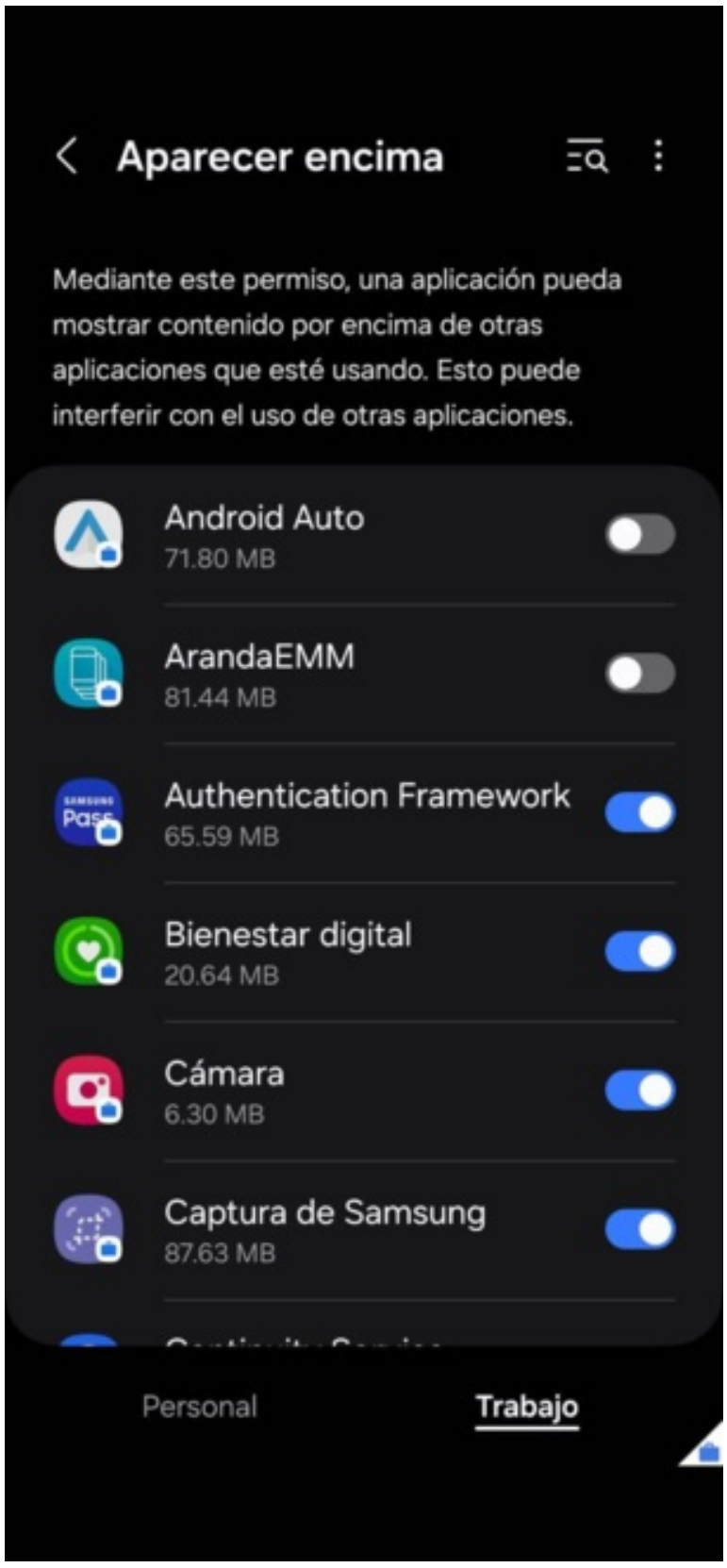

Autenticación
Aranda Enterprise
Mobility Management
Aranda EMM usará su ubicación asi esta se encuentre cerrada o en segundo plano, para poder realizar seguimiento del dispositivo, monitoreo de Geocercas y también en caso de pérdida o robo.
Aceptar
Iniciar sesión

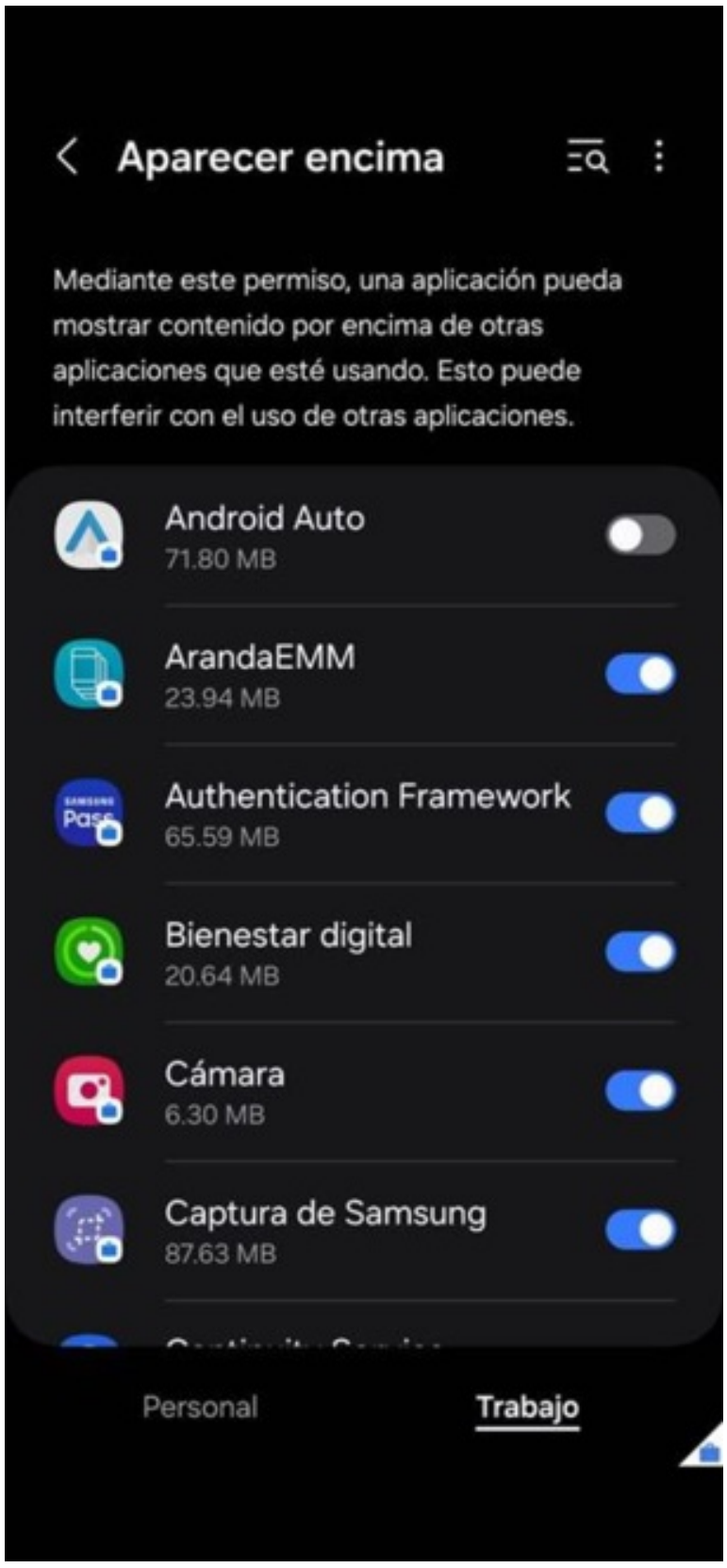


Después de este proceso, se debe de habilitar el permiso de acceso a datos de uso y el permiso de aparecer encima para la aplicación **Aranda**EMM


Acceso a datos de uso
Permitir a las aplicaciones hacer un seguimiento de qué otras aplicaciones utiliza y con qué frecuencia, e identificar su proveedor de servicios, ajustes de idioma y otros datos de uso.
Android System Intelligence
102 MB
ArandaEMM
81.85 MB
Bienestar digital
20.64 MB
Device Health Services
13.15 MB
Google
475 MB
Google Play Store
125 MB
Personal
Trabajo


Acceso a datos de uso
Permitir a las aplicaciones hacer un seguimiento de qué otras aplicaciones utiliza y con qué frecuencia, e identificar su proveedor de servicios, ajustes de idioma y otros datos de uso.
Android System Intelligence
102 MB
ArandaEMM
81.85 MB
Bienestar digital
20.64 MB
Device Health Services
13.15 MB
Google
475 MB
Google Play Store
125 MB
Personal
Trabajo


Aparecer encima
Mediante este permiso, una aplicación pueda mostrar contenido por encima de otras aplicaciones que esté usando. Esto puede interferir con el uso de otras aplicaciones.
Android Auto
71.80 MB
ArandaEMM
81.44 MB
Authentication Framework
65.59 MB
Bienestar digital
20.64 MB
Cámara
6.30 MB
Captura de Samsung
87.63 MB
Personal
Trabajo



Si la vinculación fue exitosa, se mostrará la información básica del dispositivo

Vinculación Masiva

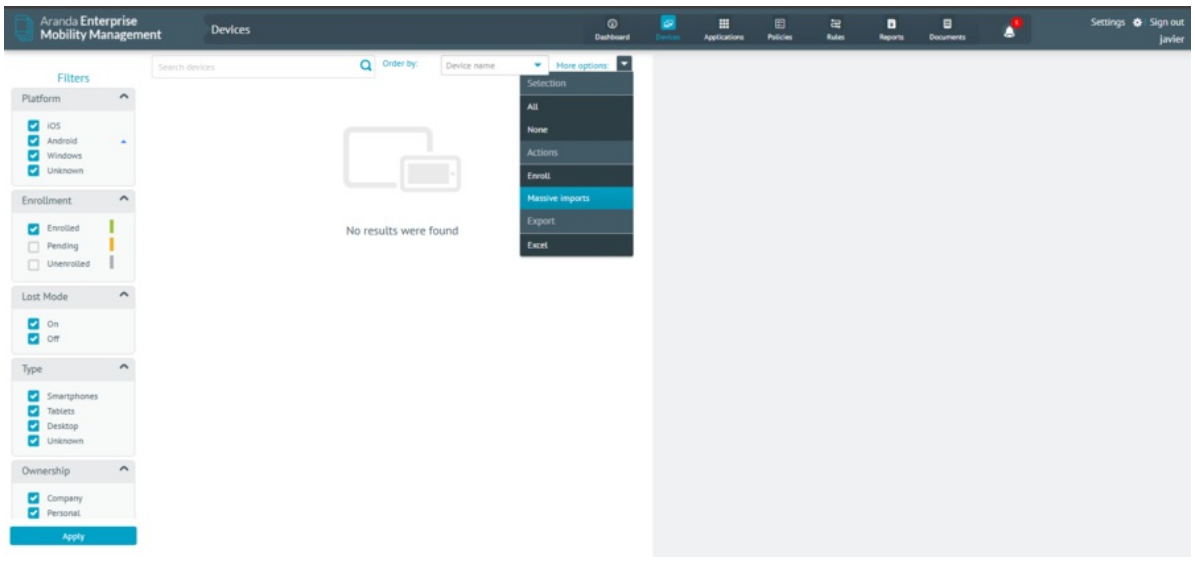
Consta de un registro de información a la consola AEMM por medio de un archivo plano CSV sencillo, el cual contiene la información necesaria para realizar la vinculación de uno o más dispositivos. Este proceso puede ser monitoreado y gestionado desde la consola AEMM y ayuda a reducir tiempos al momento de realizar la vinculación de un alto número de dispositivos.

Pasos para realizar el proceso de vinculación masiva

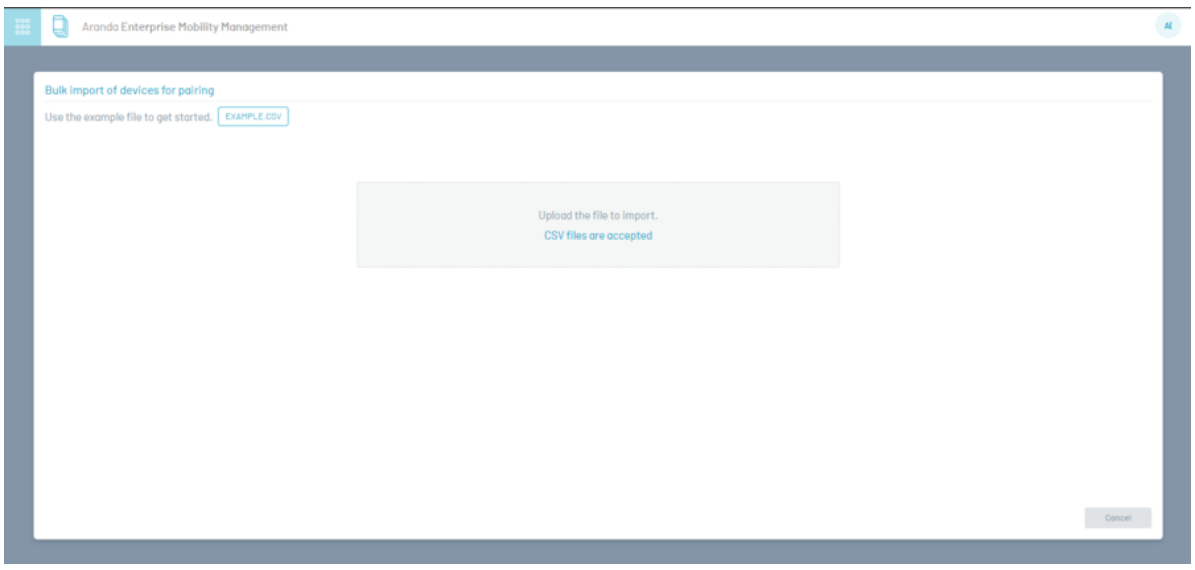
I. Cargue de plantilla para la vinculación masiva

Por medio del cargue de un archivo plano CSV delimitado por punto y coma (;), el sistema permite especificar la información requerida para la inscripción (vinculación) de los dispositivos en la consola AEMM. Este proceso se realiza de la siguiente manera:

Navegue hasta la opción de dispositivos (Devices)-> Más opciones-> Acciones-> Importación Masiva



Se muestra la pantalla en donde se debe de realizar la importación del archivo plano que contiene la información de los dispositivos a vincular



En el botón **"EJEMPLO.CSV"** se puede descargar el archivo plano de ejemplo y en este archivo encontrará la siguiente estructura:

Estructura del archivo	Descripción
IMEI:	Número (IMEI) único del dispositivo.
User:	Nombre de usuario con el que quedaría asociado el dispositivo.
Domain:	Dominio al cual pertenece el usuario.
UseSameUser:	Puede tener 2 valores: 1 ó 0.
-Valor 1:	**SOLO APLICA** si se envía en la primera fila (PRIMER registro del archivo) con valor 1, este campo hace que el sistema tome automáticamente la vinculación de todos los dispositivos con el mismo usuario que se configuró en la primera fila. Pero si ese valor se coloca en una fila diferente a la primera, el sistema no lo tiene en cuenta y siempre va validar el usuario por fila.
-Valor 0	Si se envía en 0 valida el campo **User**, por cada fila o registro.
ApplyTyC:	Puede tener 2 valores: 1 ó 0.
-Valor 0	Se identifica si el usuario va a visualizar los términos y condiciones en los dispositivos que se van a vincular.
-Valor 1	Si se envía en 1 es que los términos y condiciones fueron aceptados de forma automática, entonces al continuar desde el agente en los dispositivos, no van a visualizar la pantalla para aceptar términos y condiciones.

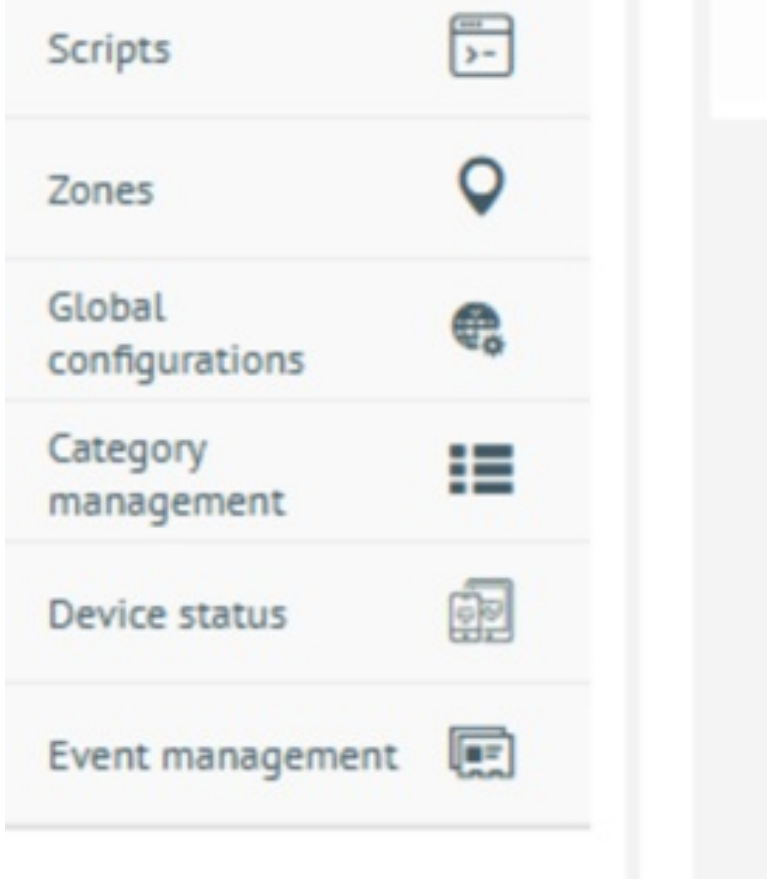
Ejemplo:

IMEI	user	domain	useSameUser	applyTyc
123456789123456	administrator	Aranda	0	1

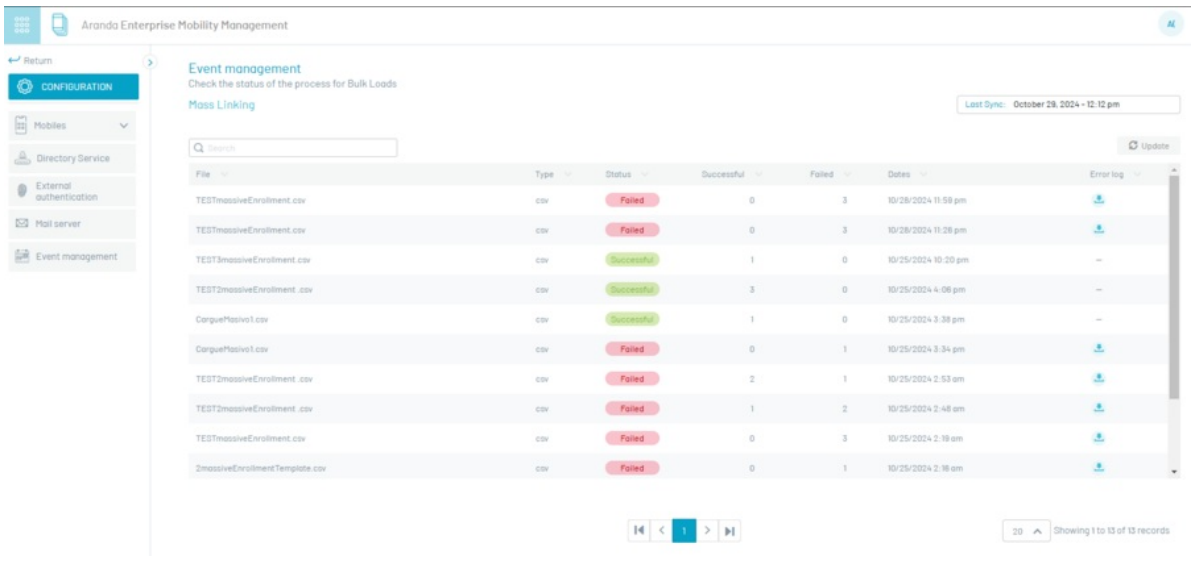
II. Visualización de resultados

El procesamiento de los datos se realiza en segundo plano, es decir; el usuario podrá navegar mientras el sistema carga la información de forma transparente para el usuario.

El administrador puede ir a configuraciones-> preferencias-> Gestión de eventos.

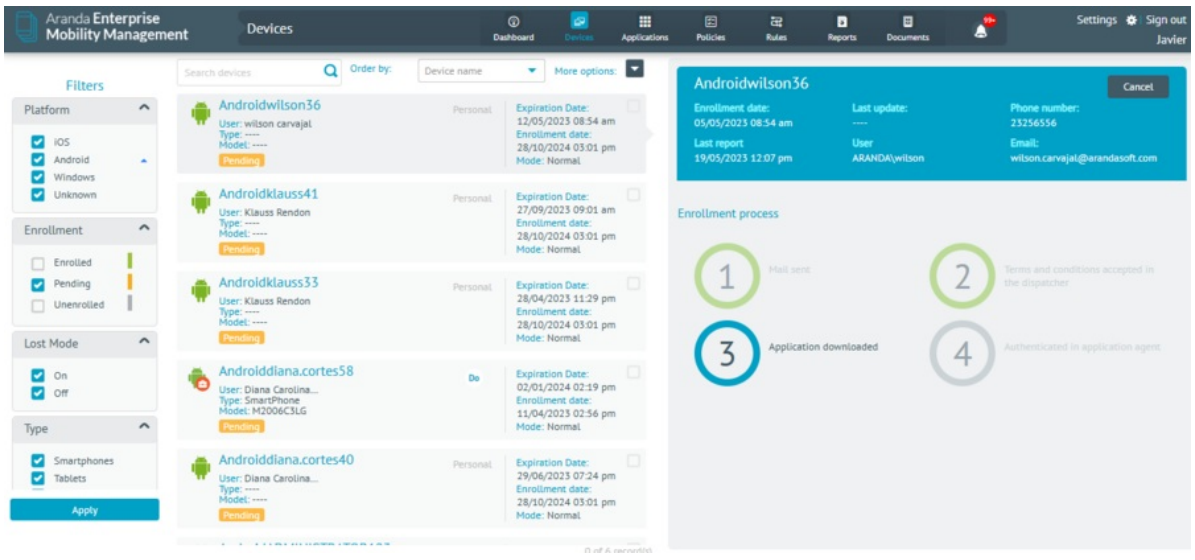


De acuerdo al proceso realizado puede filtrarlo por nombre del archivo, fecha o su estado. El sistema le informa al usuario cuantos registros fueron exitosos (ver detalles en dispositivos) y registros fallidos, para estos registros fallidos el usuario podrá descargar un archivo, donde podrá observar los fallos que se encontraron al momento de procesar la información cargada. Estos dispositivos no pudieron ser vinculados, por lo tanto el usuario debe cargar únicamente estos registros, con las correcciones indicadas por el sistema.



III. Consultar los dispositivos que están en proceso de vinculación.

El usuario puede observar los dispositivos que se encuentran vinculados o en proceso (en estado pendientes) desde el modulo de dispositivos.



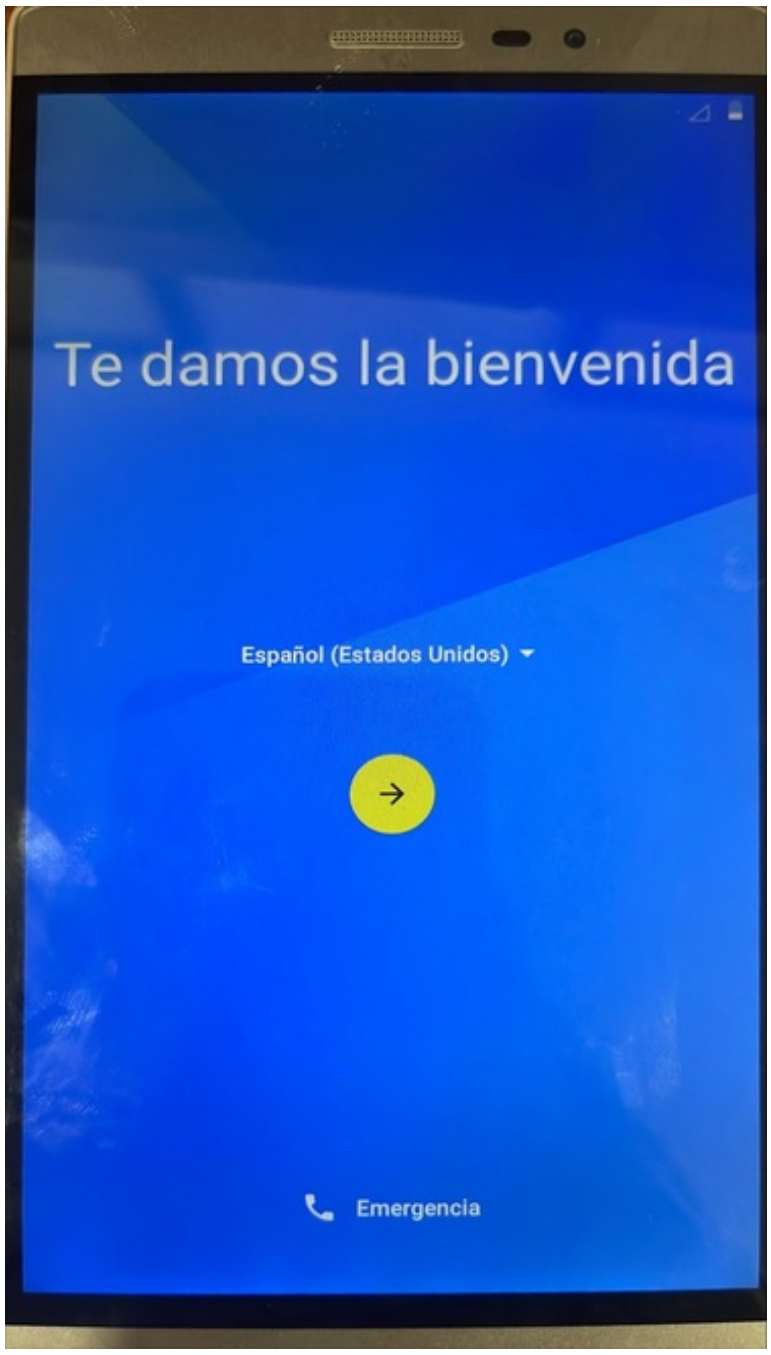
IV. Resultados de la vinculación desde los dispositivos:

- Dispositivos (con los términos y condiciones fueron aceptados desde la configuración del archivo): El usuario cuando ingresa al agente de AEMM desde el dispositivo, otorgando los permisos requeridos, cuando finalice el proceso el usuario podré observar el Home de la aplicación , consola a la que fue vinculada, política y reglas configuradas. Su vinculación fue exitosa.
- Dispositivos (sin los términos y condiciones que NO fueron aceptados desde la configuración del archivo): El usuario cuando ingresa al agente de AEMM desde el dispositivo, debe aceptar los términos y condiciones, esperar el aprovisionamiento, otorgar los permisos requeridos, cuando finalice el proceso el usuario podré observar el Home de la aplicación , consola a la que fue vinculada, política y reglas configuradas. Su vinculación fue exitosa.

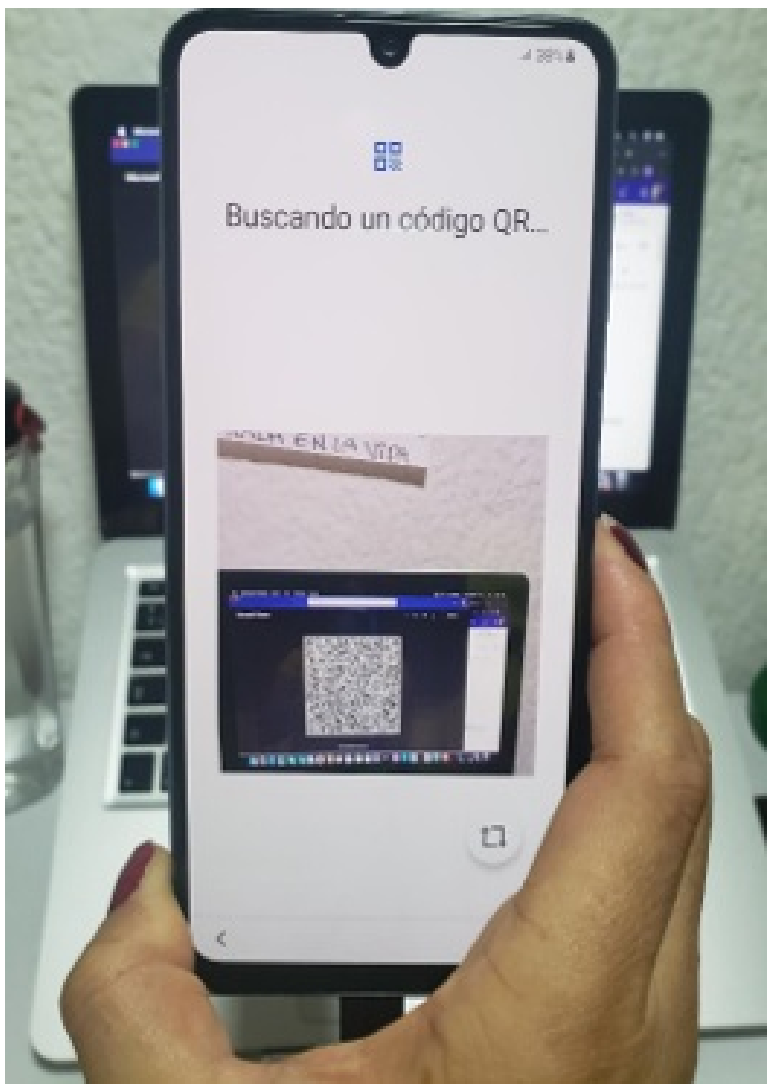
Vinculación por medio de QR

Precondiciones:

El dispositivo debe estar condiciones de fábrica en la pantalla inicial de bienvenida Actividades realizadas. El usuario debe realizar 7 touch en la pantalla blanca



Por medio de un mensaje se informará al usuario que falta un número de touch o pulsado para activarse configuración mediante QR, se puede visualizar la apertura de captura QR, escanear el QR correspondiente al proveedor de cada dispositivo (ver cuadro)

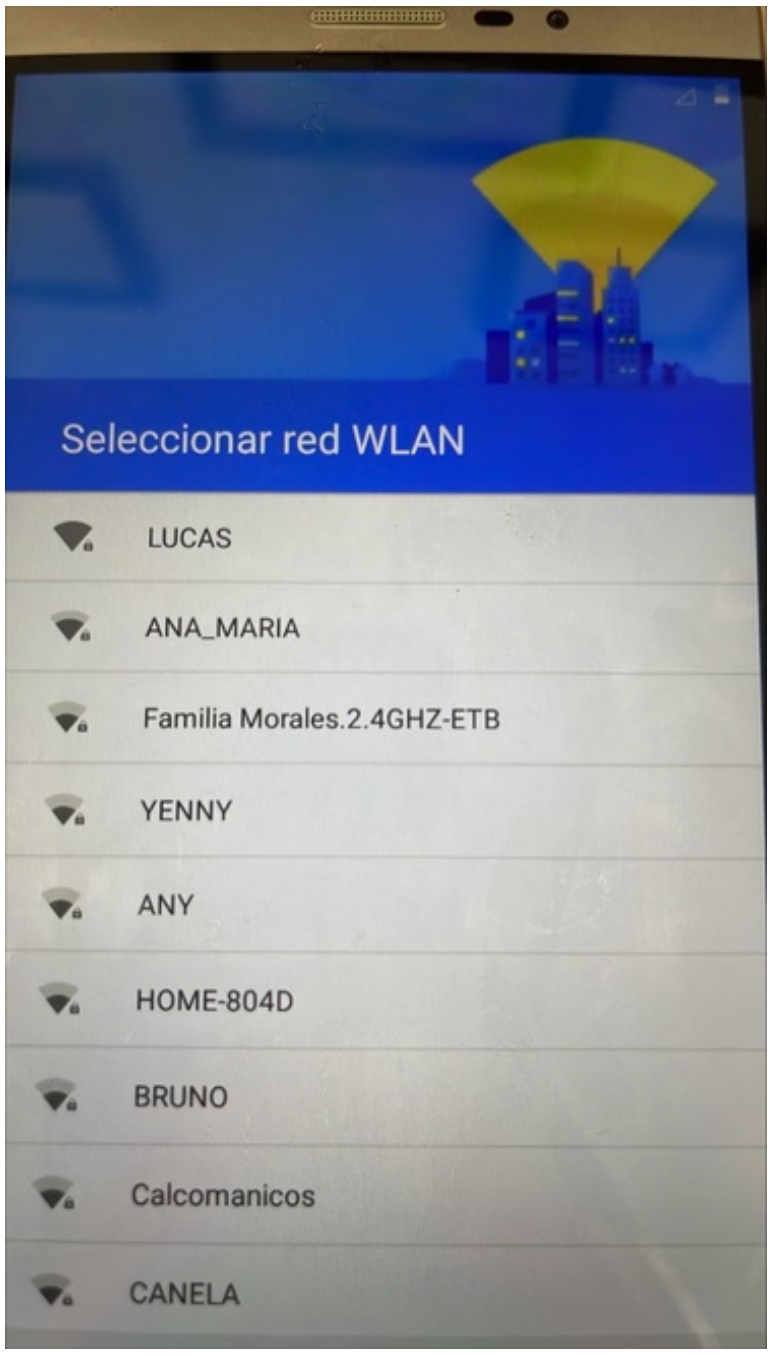


Debe tener en cuenta si su dispositivo es:

Samsung (Agente Knox)

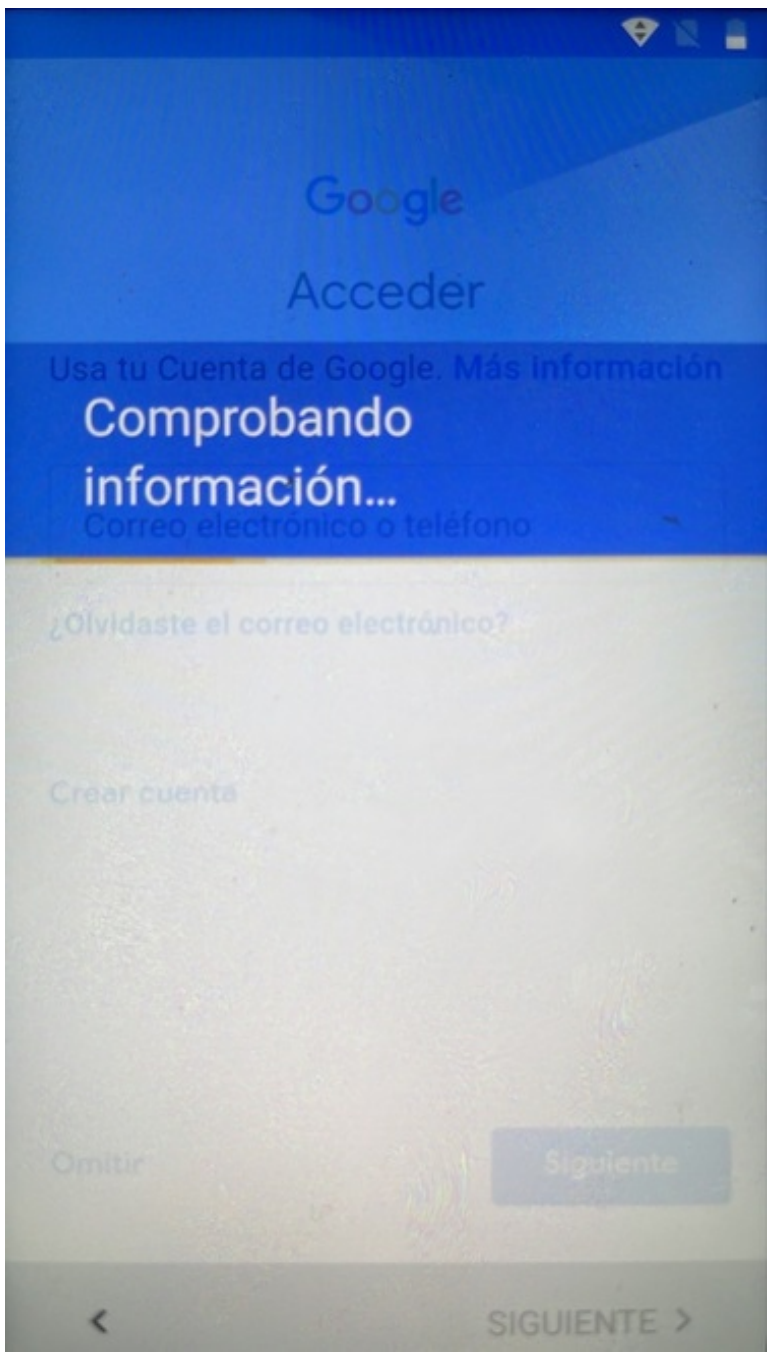
Agente genérico

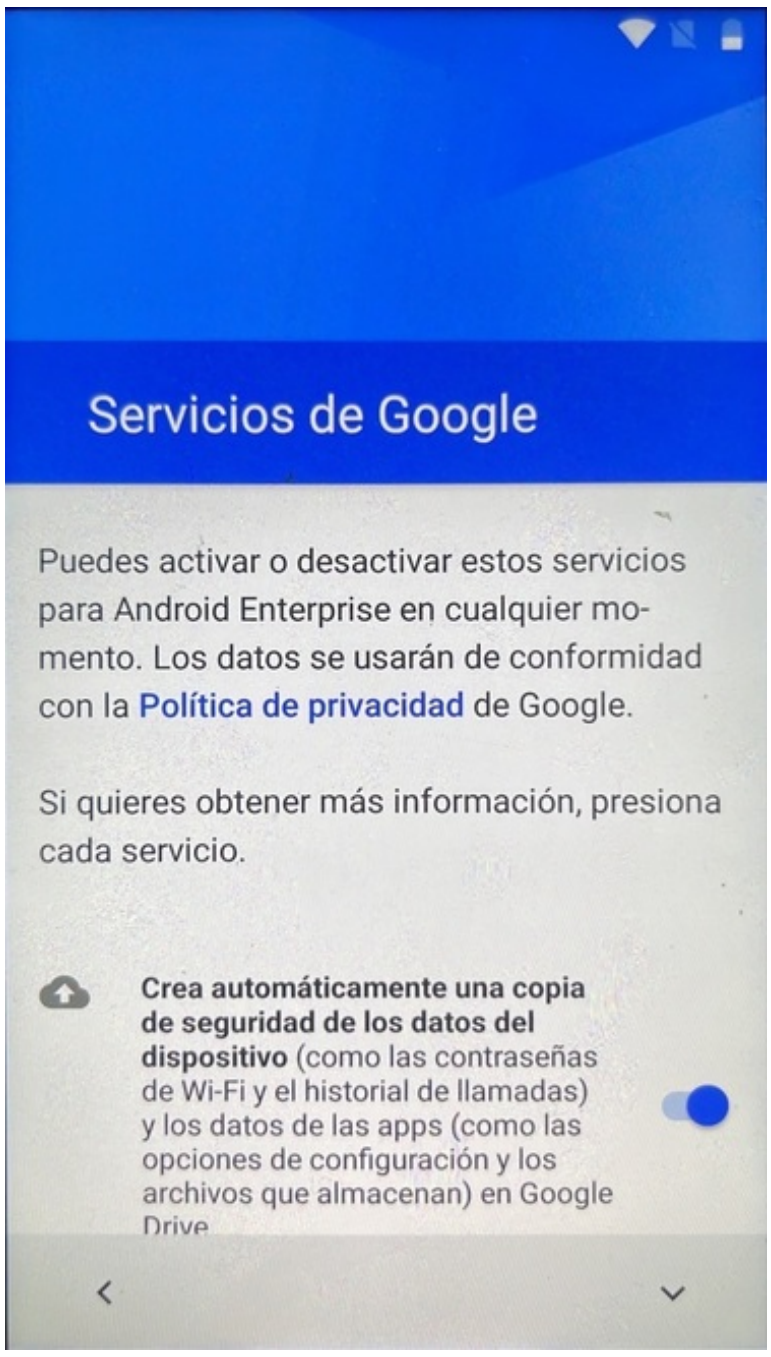
Debe realizar el ingreso de una red, por favor tenga presente que está red no este configurada con restricciones de descarga



En las siguientes imágenes el dispositivo le informará el proceso de instalación que se realizará por parte del EMM Aranda


moto
Sobre tu privacidad
Recolectamos y entregamos la información de uso para mantener el software actualizado, proporcionar asistencia técnica personalizada y ayudarnos a mejorar nuestros productos y servicios.
Selecciona "Aceptar y continuar" para usar la configuración actual o cambiar tus Configuraciones de privacidad.
ACEPTAR Y CONTINUAR

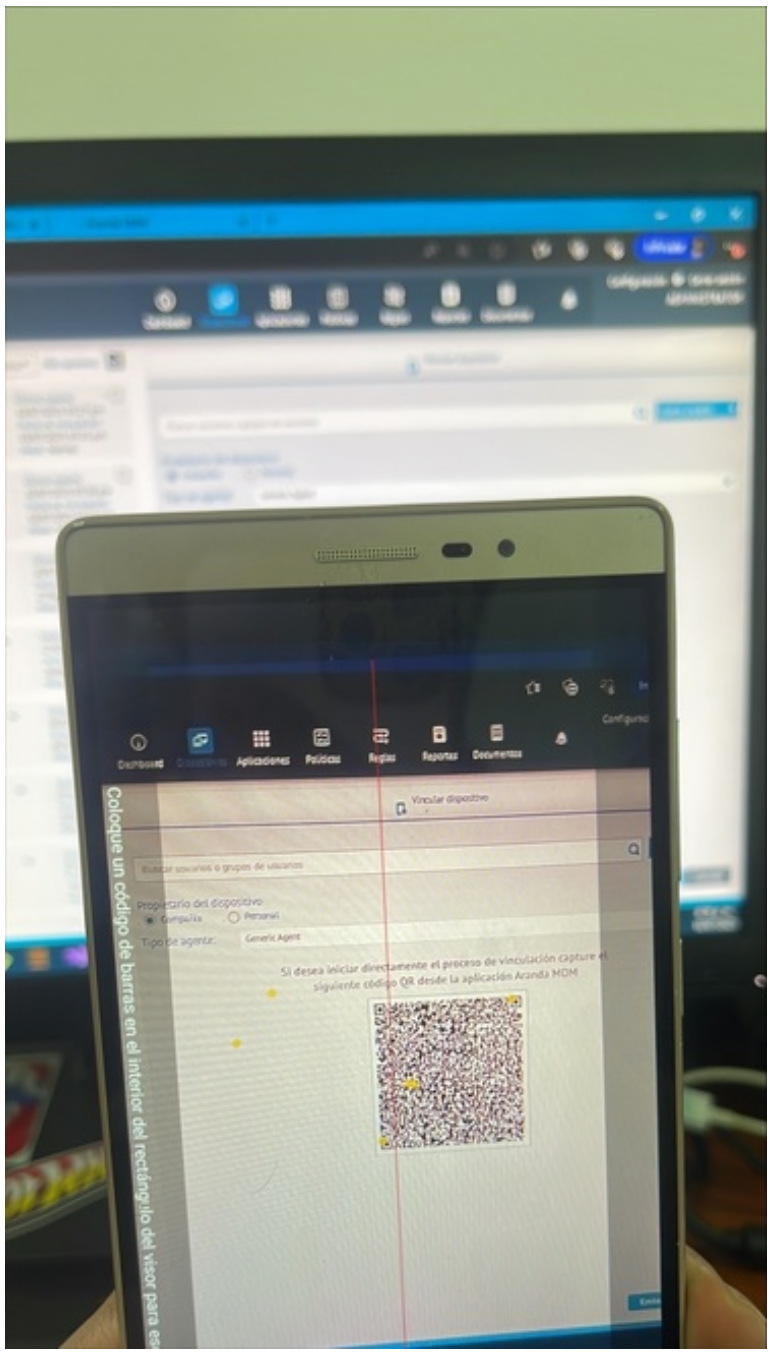

Google
Acceder
Usa tu Cuenta de Google. Más información
Comprobando información...
Correo electrónico o teléfono
¿Olvidaste el correo electrónico?
Crear cuenta
Omitir
Siguiente
SIGUIENTE

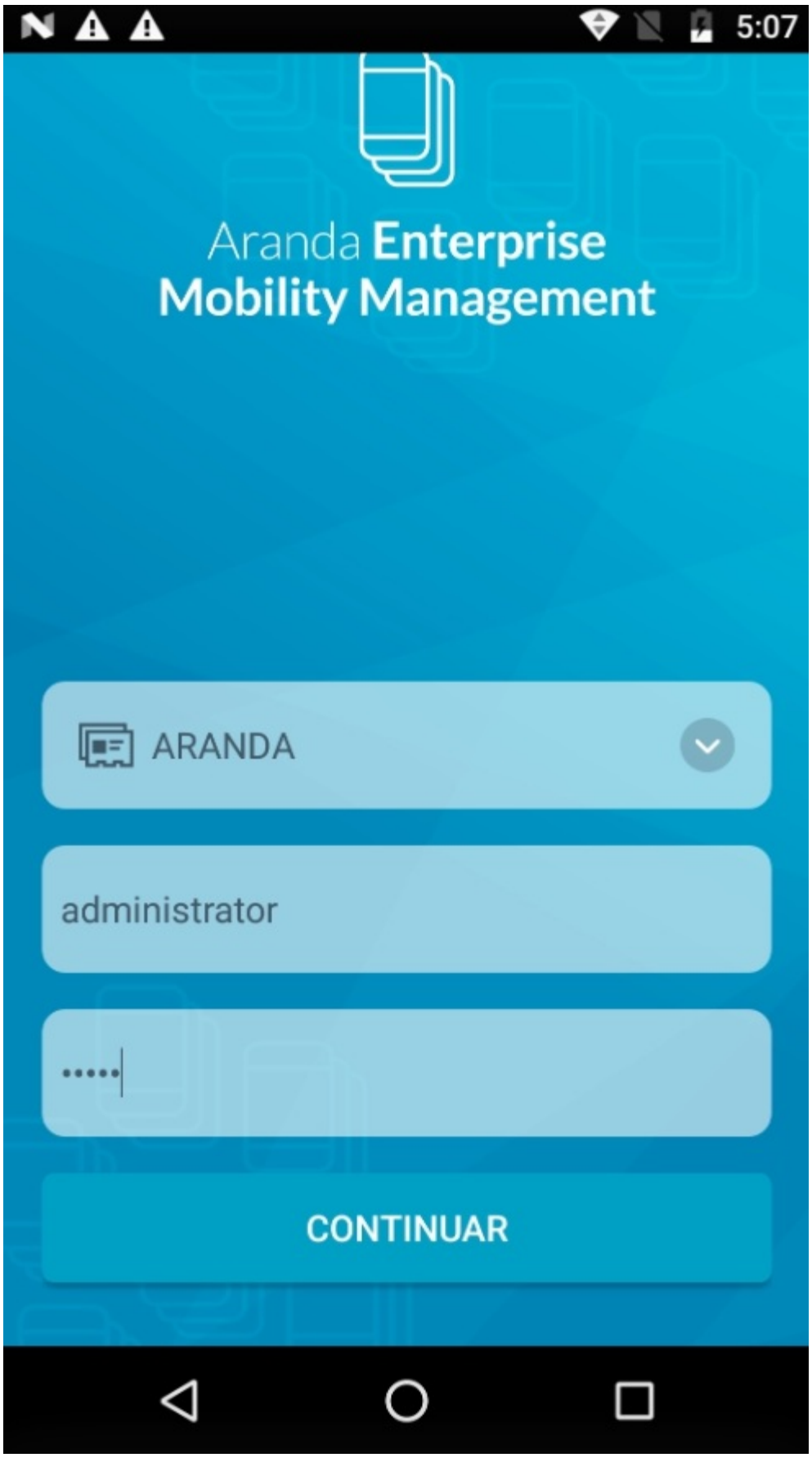


De igual forma permisos propios del dispositivo.

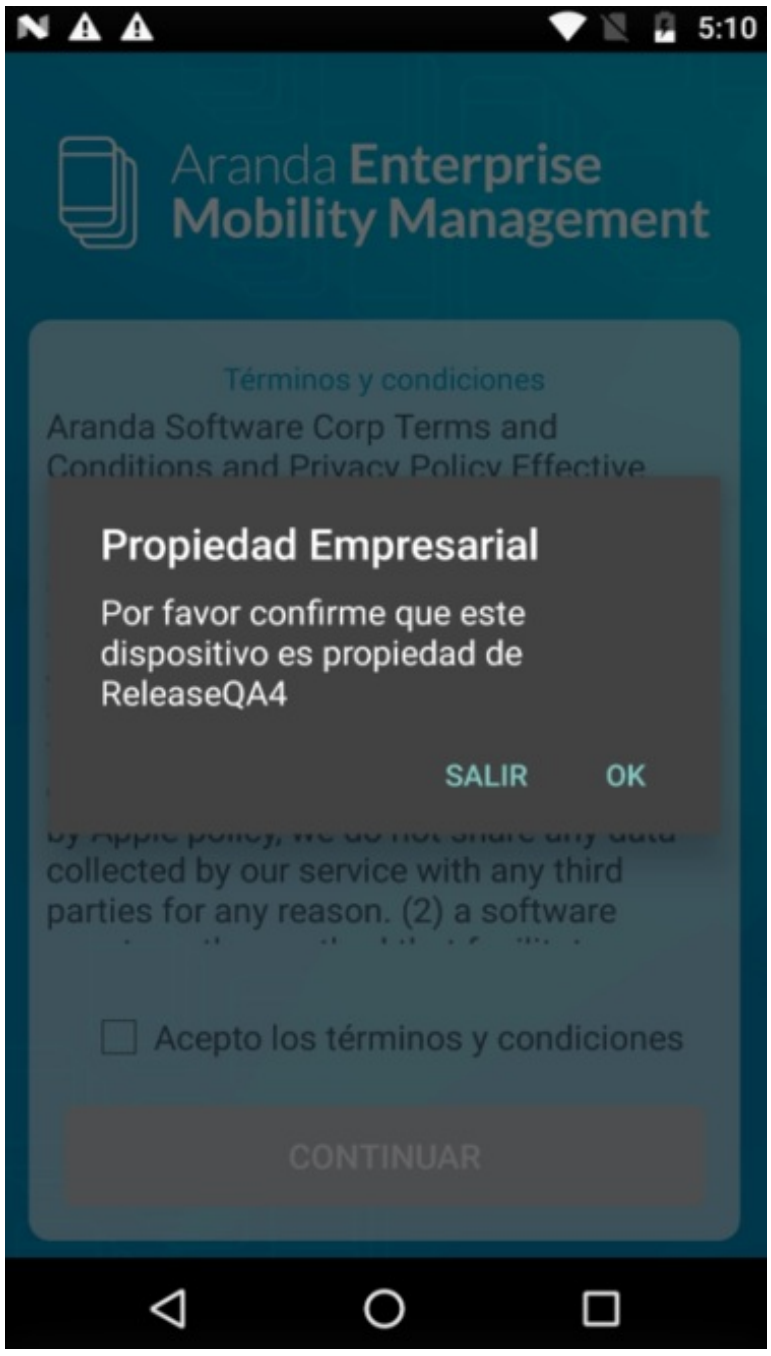
Cuando finalice el proceso de instalación, ingrese al agente ArandaEMM, nos mostrará las opciones de vincular, seleccionar Escanear código

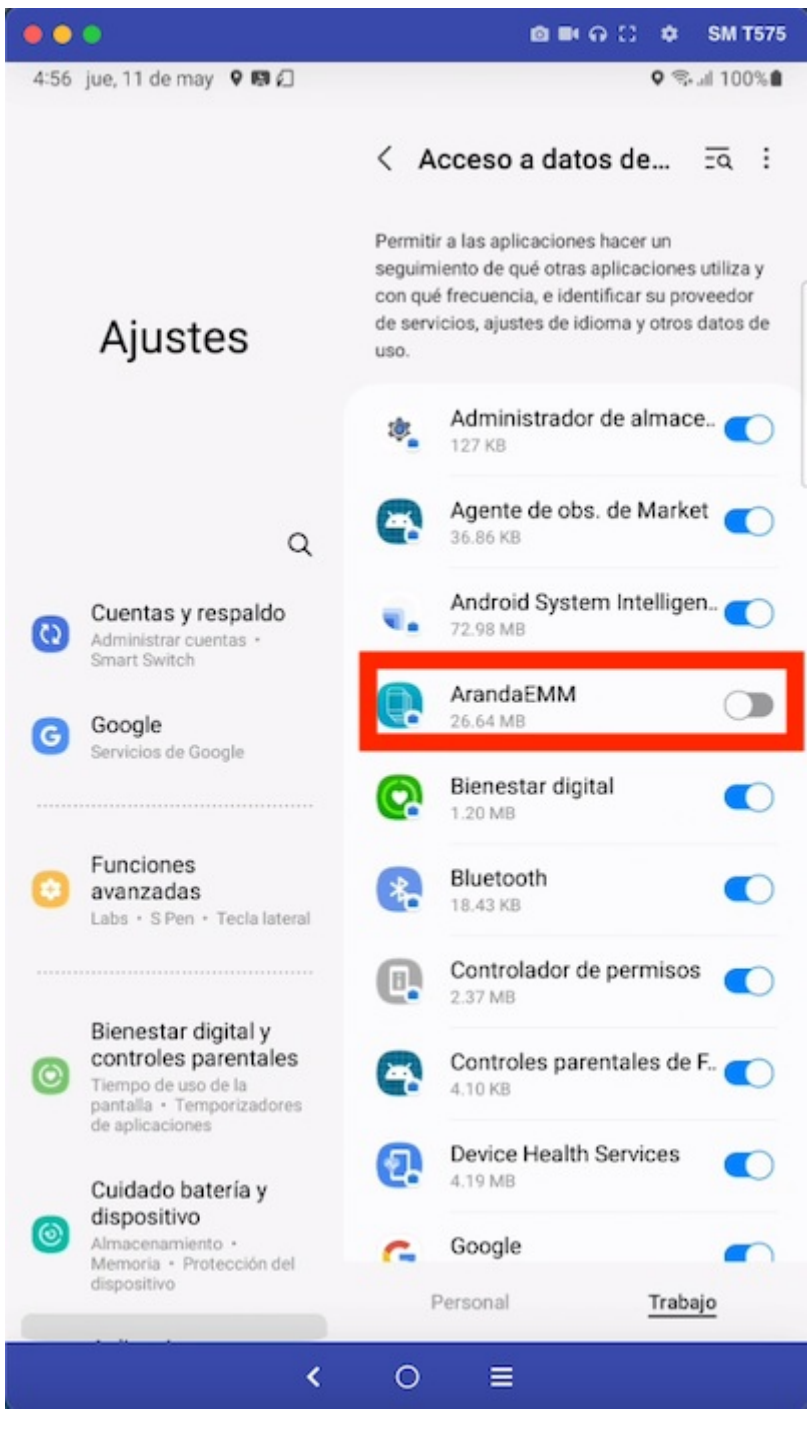
Se debe realizar el escaneo del código QR de la consola que requiere vincular e ingresar usuario



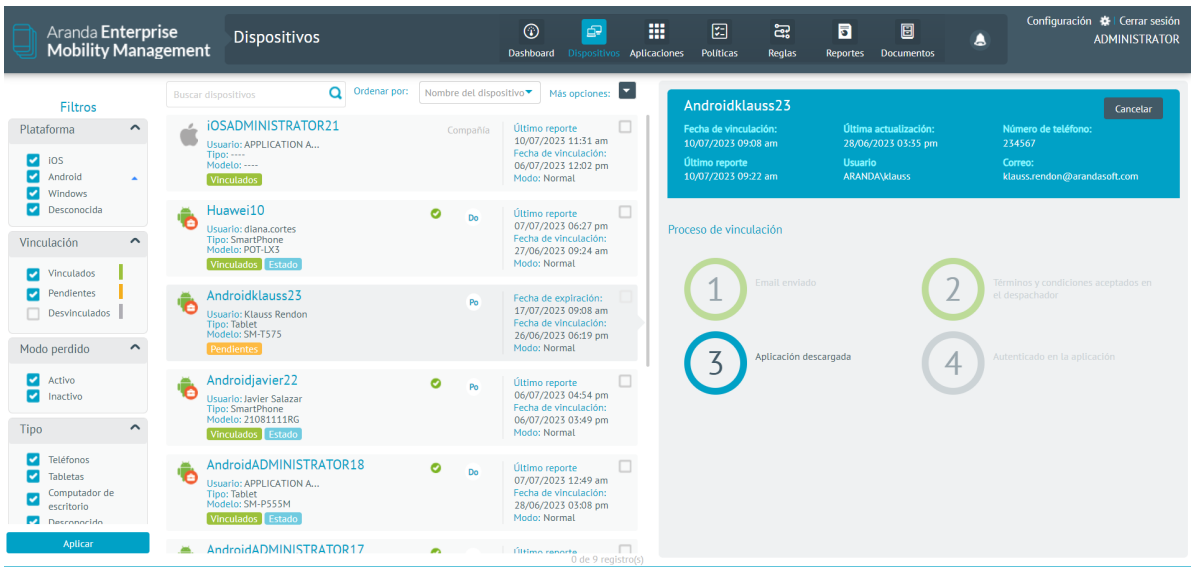


Continuar otorgando los permisos requeridos, como se muestra en algunas de las siguientes imágenes

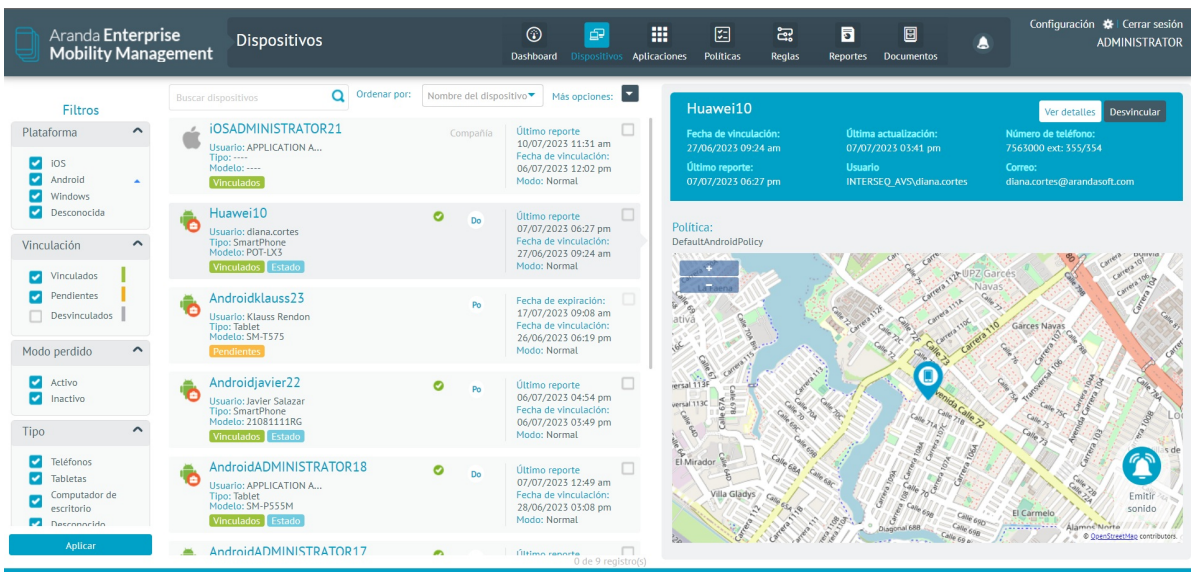




Desde consola puede observar quienes se encuentra en proceso de vinculación-> desde el módulo Dispositivos-> filtro Pendientes



Al finalizar el proceso de vinculación el dispositivo le mostrará información del IMEI, versión de agente, servidor vinculado y demás información. De igual forma se valida en consola su vinculación.



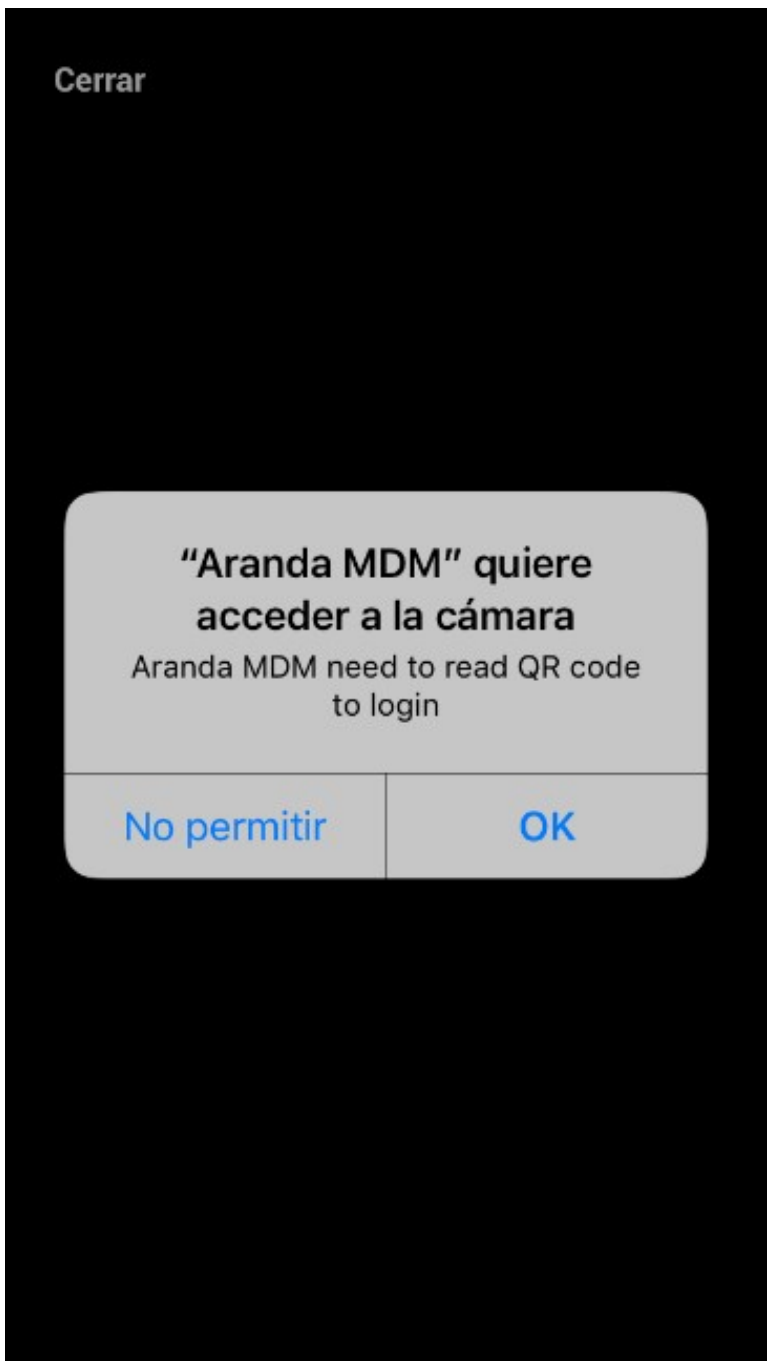
Tipos de Vinculación iOS

Vinculación Clásica en iOS

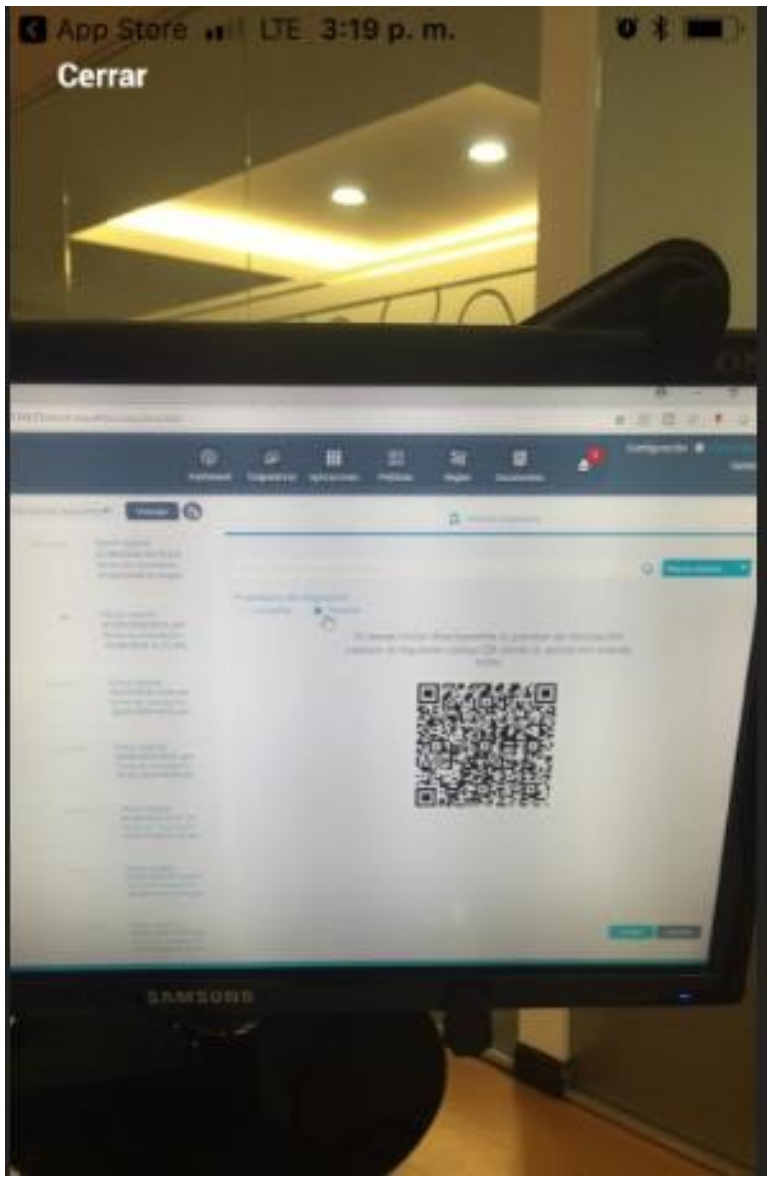
Para iOS están dos alternativas para la vinculacion:

- Ingresar código QR
- Ingresar URL de Servidor

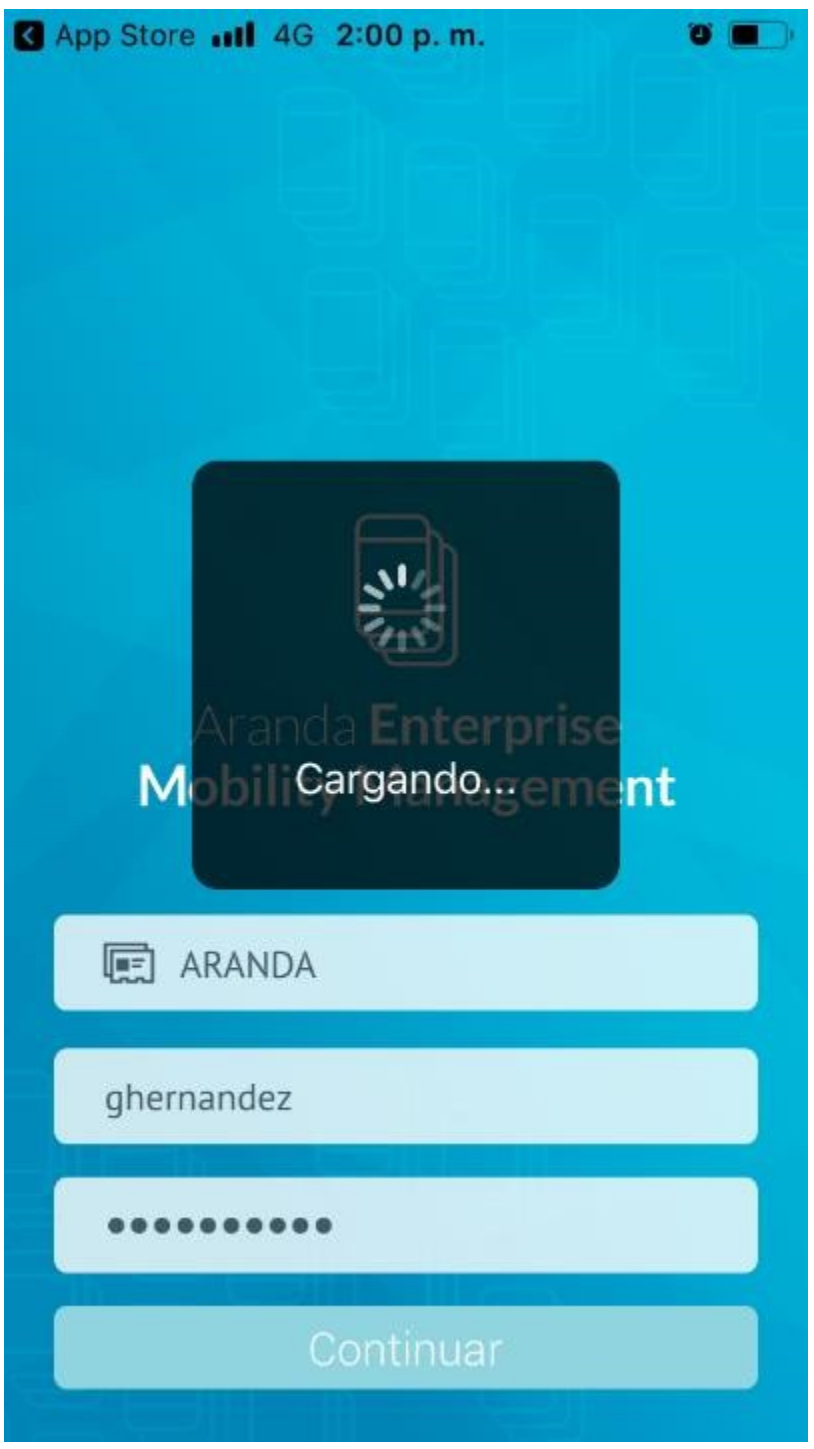
En este caso la opción escogida fue ingresar código QR, después pues de este paso usted observará la siguiente pantalla.



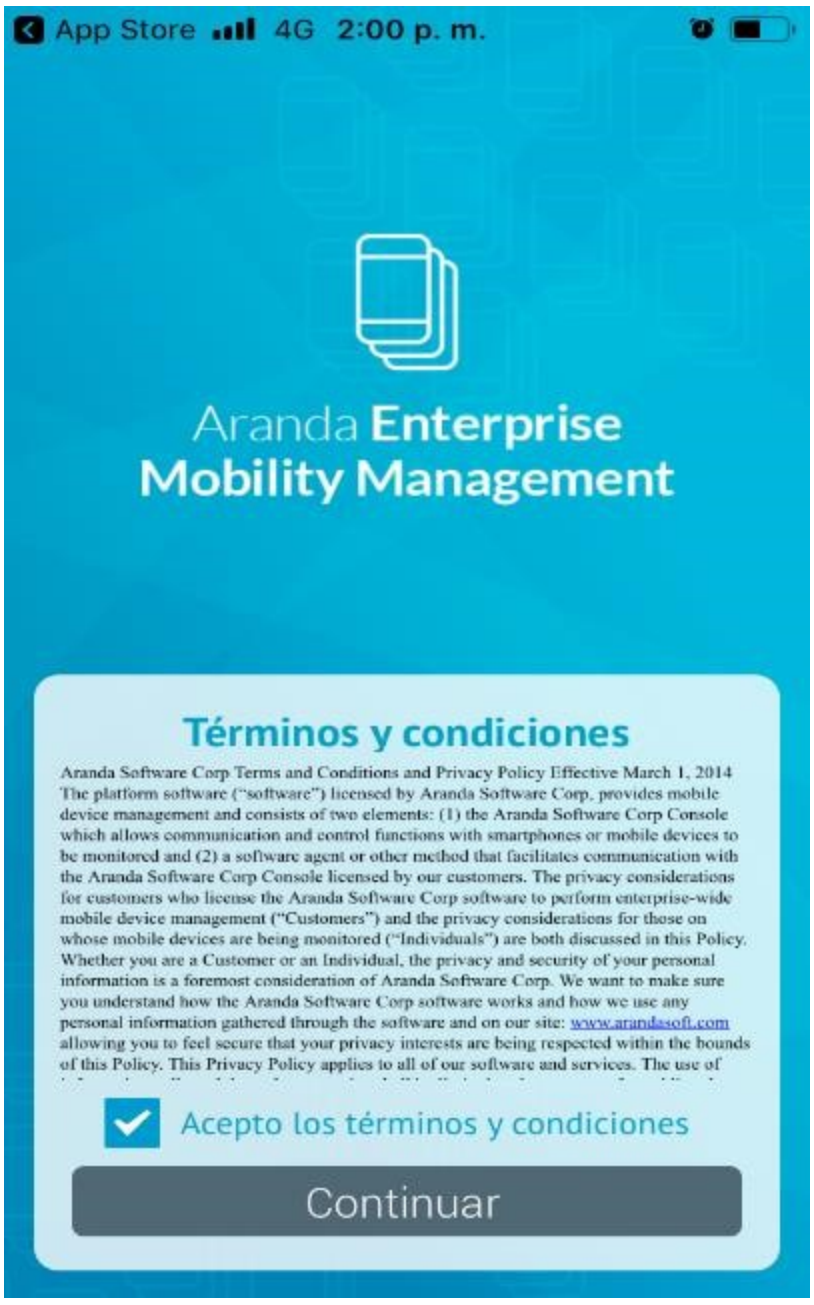
Escanee el código QR desde la consola web de Aranda Mobile Device Management



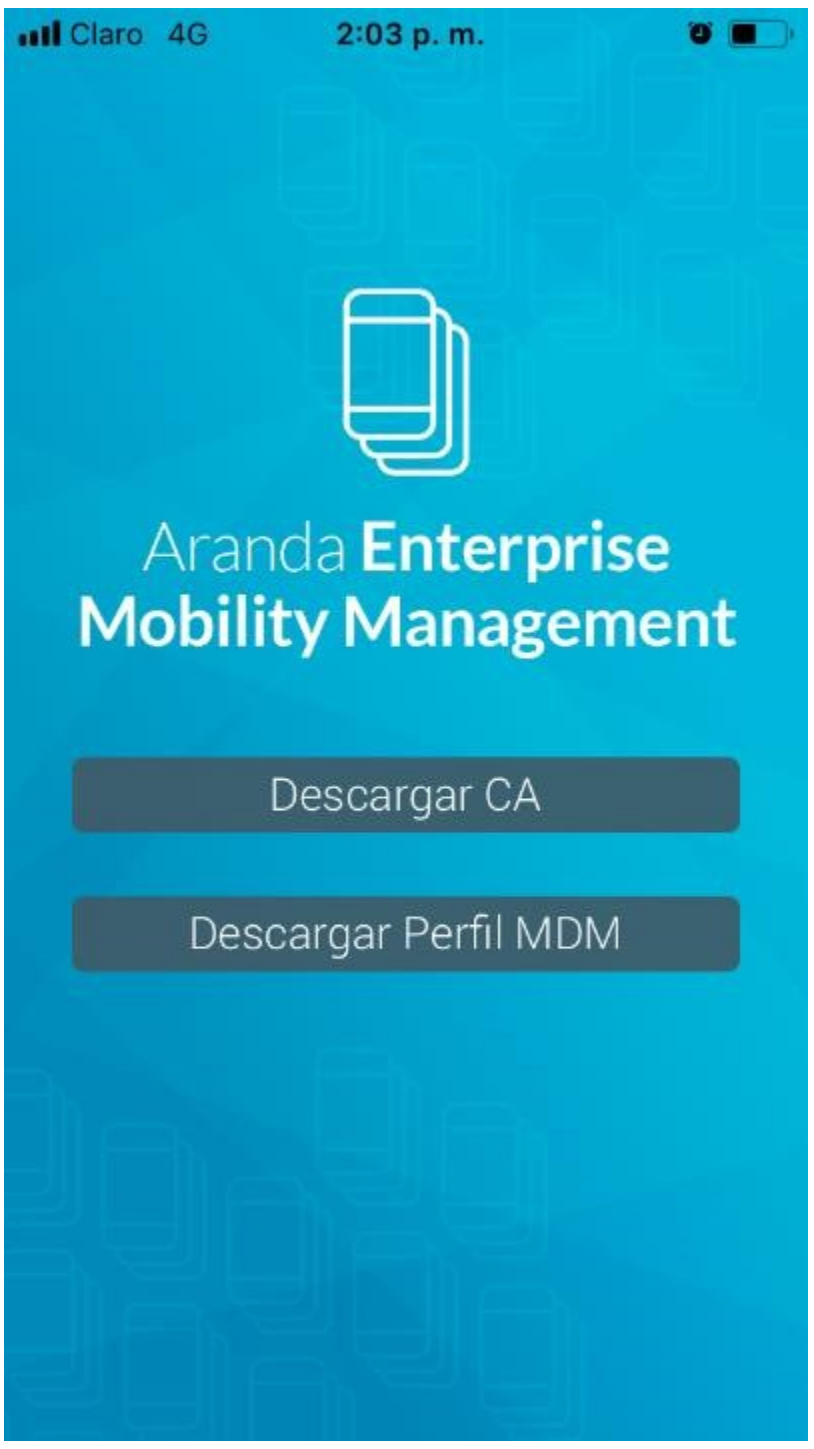
Llene los espacios con el usuario y contraseña previamente creado por el administrador, y luego de clic en **continuar**.



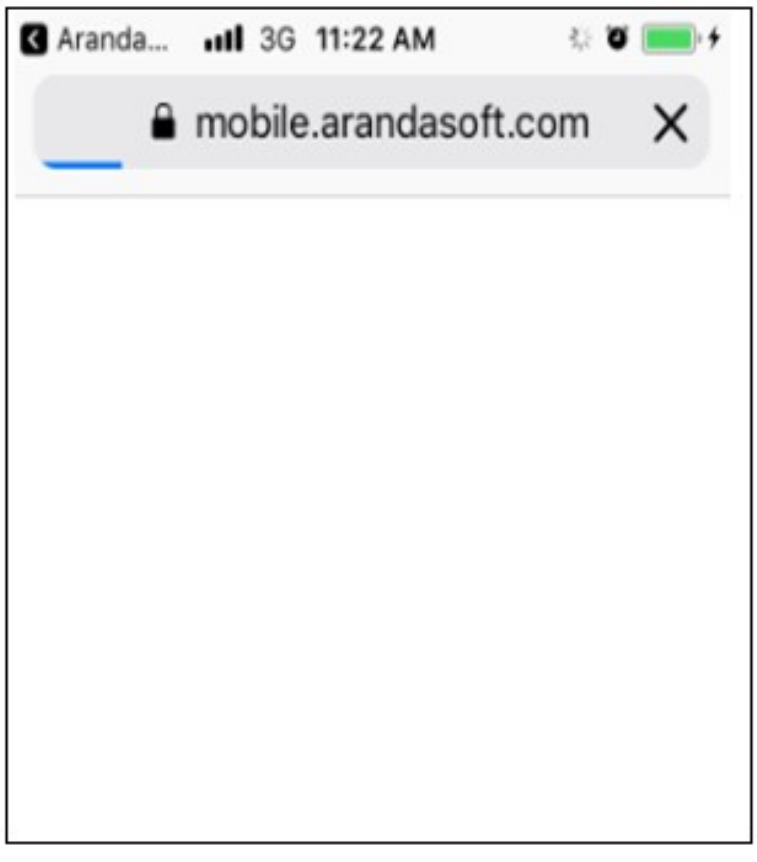
Después de esto acepte los términos y condiciones y de clic en **continuar**.



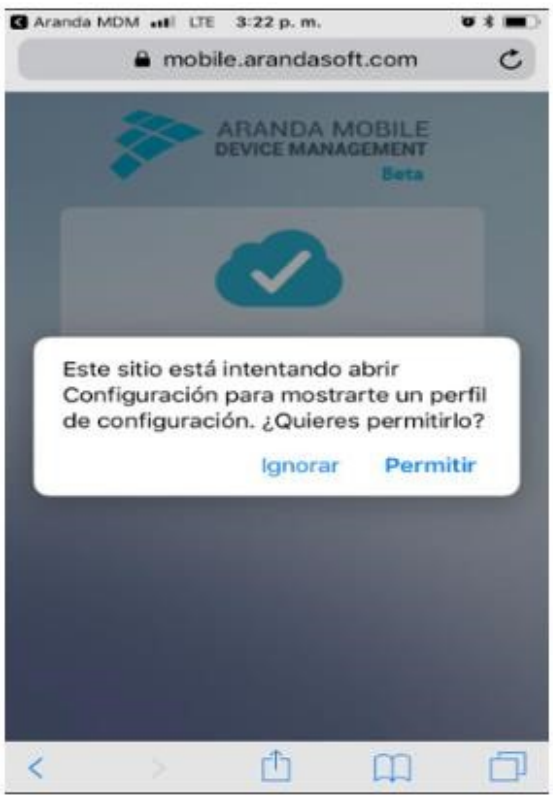
El siguiente paso es para descargar e instalar el certificado. Por favor de clic en **Descargar CA**



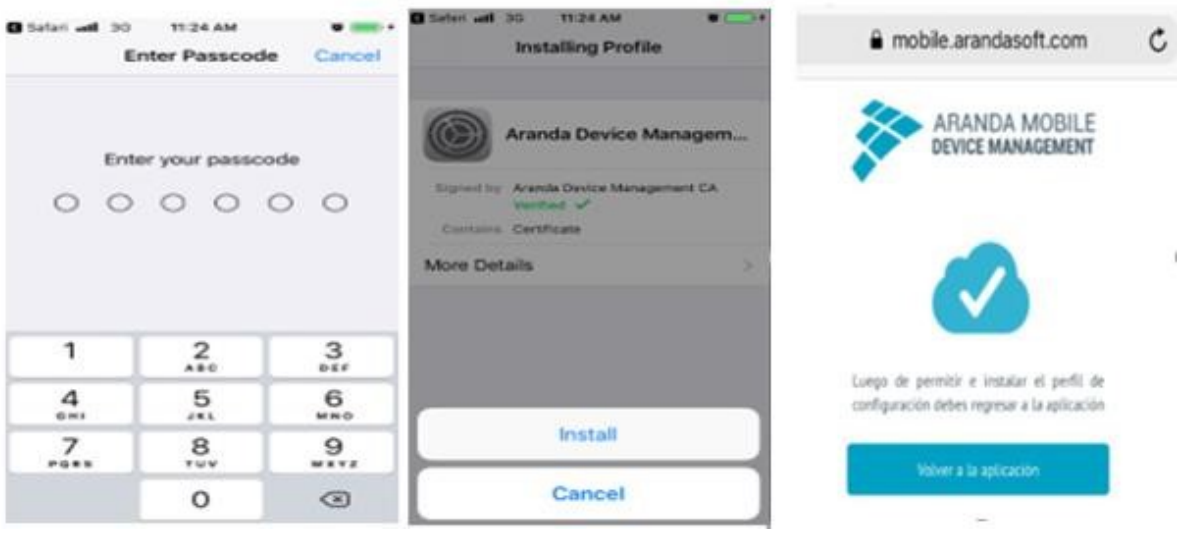
Después de esto usted será direccionado al sitio seguro **mobile.arandasoft.com** para instalar el certificado.



Por favor complete los siguientes pasos para continuar:



Por favor de clic en OK



Si su dispositivo tiene contraseña, por favor digítela y luego de clic en **Instalar**

De clic en **permitir**

Después de esto, por favor seguir los siguientes pasos para instalar el perfil.

Por favor complete los siguientes pasos y culmínelos dando clic en **abrir**

La siguiente imagen es presentada para descargar e instalar un perfil de iOS que le permite a estos dispositivos ser vinculados. De clic en **Descargar Perfil EMM** y luego de clic en **permitir.**

Finalmente, cuando usted observa la siguiente imagen, su perfil ha sido instalado y su dispositivo vinculado exitosamente y podrá ser controlado desde la consola web

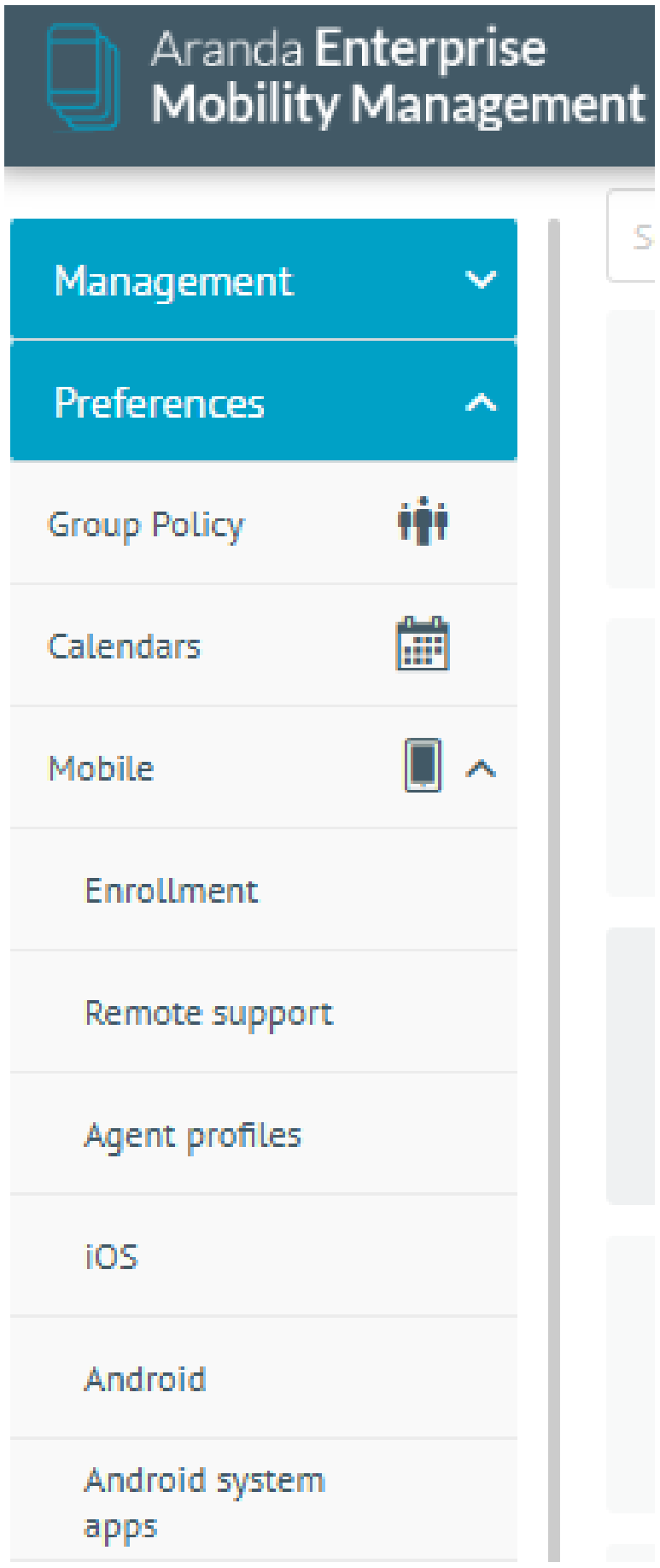
Vinculación por ABM en iOS

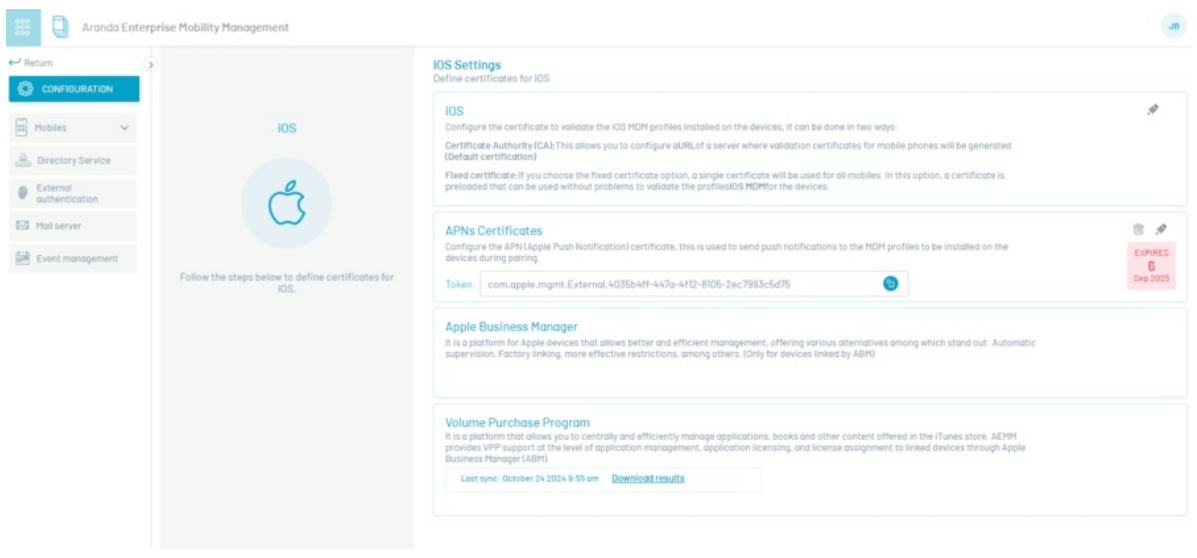
Módulo para Apple Business Manager (ABM):

Podrá encontrar la funcionalidad de ABM en las configuraciones de la herramienta donde podrá vincular la consola de administración de dispositivos AEMM con el programa Apple Business Manager, logrando realizar la gestión de dispositivos con el sistema operativo iOS para el programa descrito.

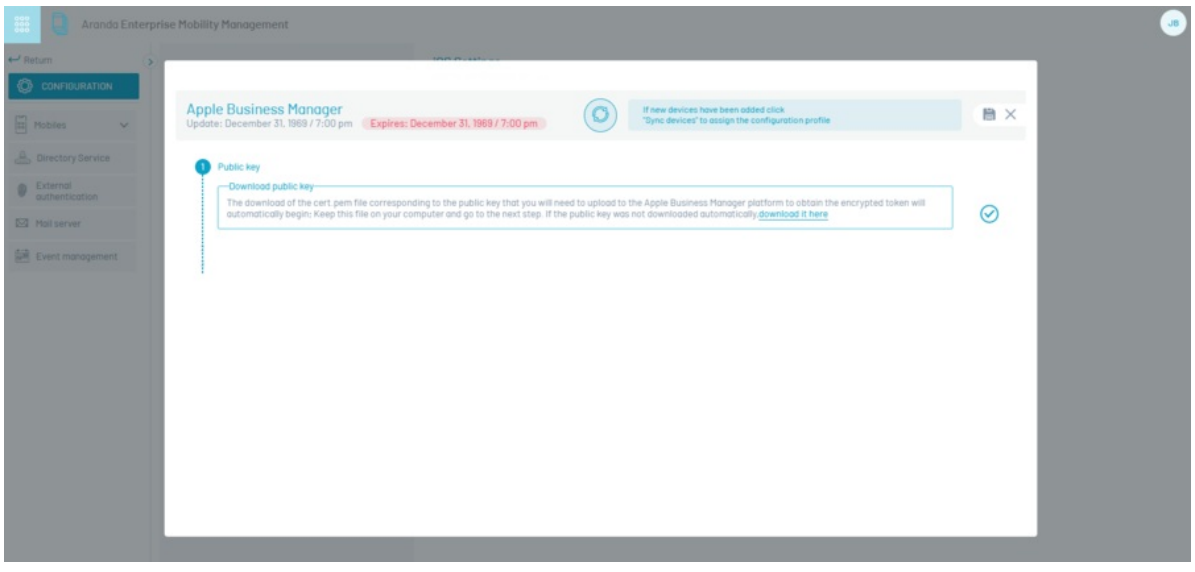
Vinculación de AEMM con Apple Business Manager

Para acceder a la configuración de Apple Business Manager en la consola AEMM, ingrese a la opción **Configuración**, y en el menú principal seleccione la opción **Preferencias**. Del sub menú desplegable, seleccione la opción **Móviles**, y en el siguiente menú seleccione la opción **iOS**.





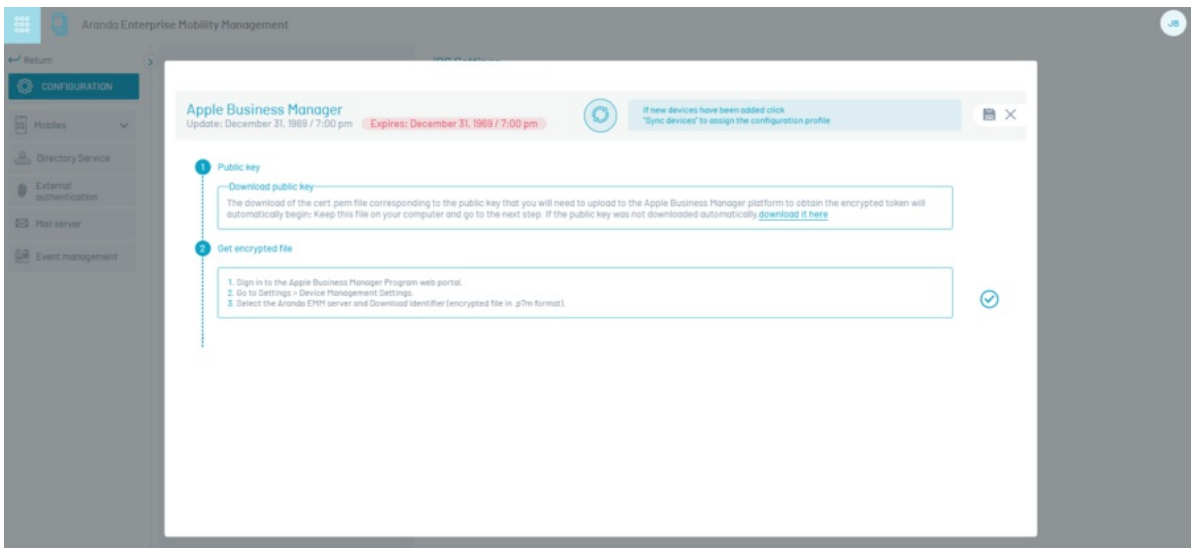
En la ventana de configuración de dispositivos iOS, haga clic en el botón **NUEVO** en la pestaña Apple Business Manager



El proceso de configuración consta de tres pasos:

1. El primer paso es descargar la llave pública de la consola AEMM. La descarga iniciará automáticamente; en caso de no iniciarse, haga clic en la opción de descarga.

Se descargará el archivo MDM_ Aranda Software Corp_Certificate.pem, guárdelo en un lugar seguro y haga clic en Siguiente.

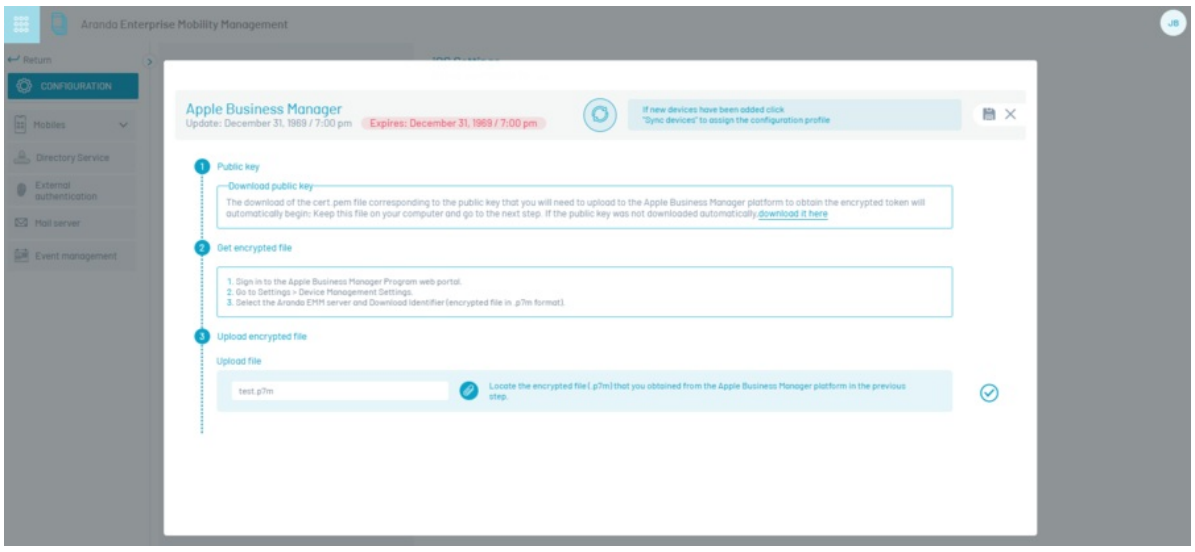


2. El segundo paso le dará las indicaciones correspondientes para vincular la consola AEMM con la llave pública descargada en el paso anterior, en la consola de administración de Apple Business Manager.

Ingresar a ABM https://business.apple.com/

Luego de realizar el proceso en la consola de administración de Apple Business Manager, haga clic en Siguiente.

3. El tercer paso consiste en cargar a la consola AEMM el archivo de extensión .p7m descargado de la consola de administración de Apple Business Manager. Haga clic en el botón Seleccionar archivo y cargue el archivo de extensión .p7m Después de seleccionar el archivo, haga clic en el botón Cargar archivo encriptado.



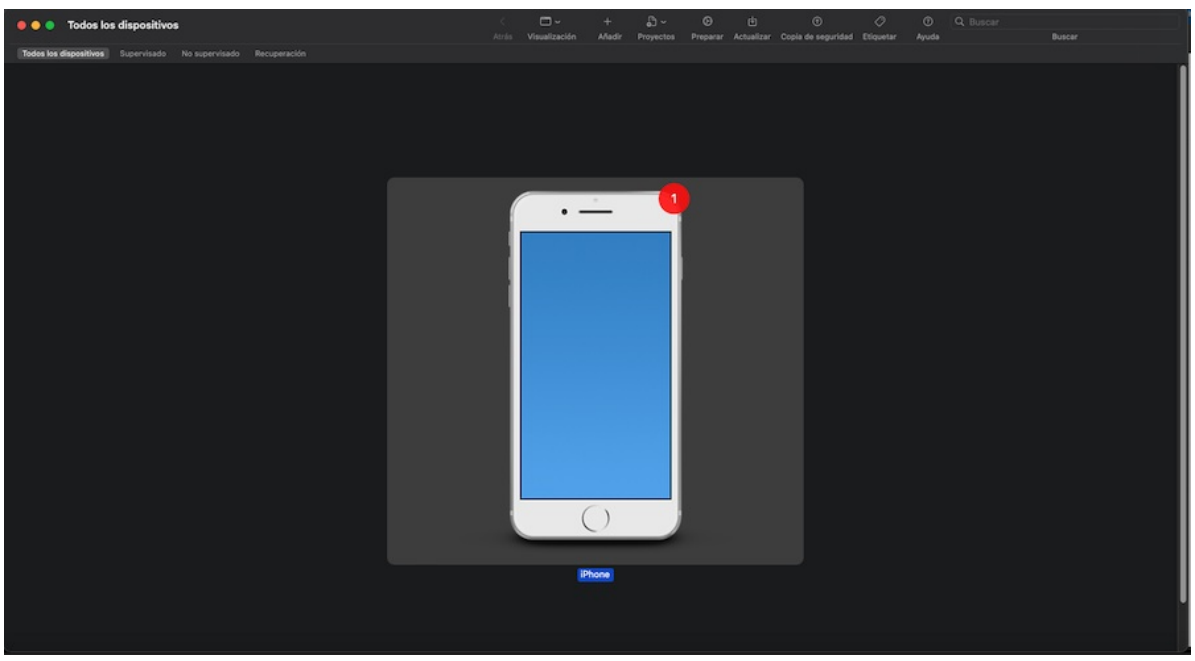
Finalmente, la consola mostrará que la vinculación entre la consola AEMM y Apple Business Manager finalizó correctamente.

Vinculación de dispositivos

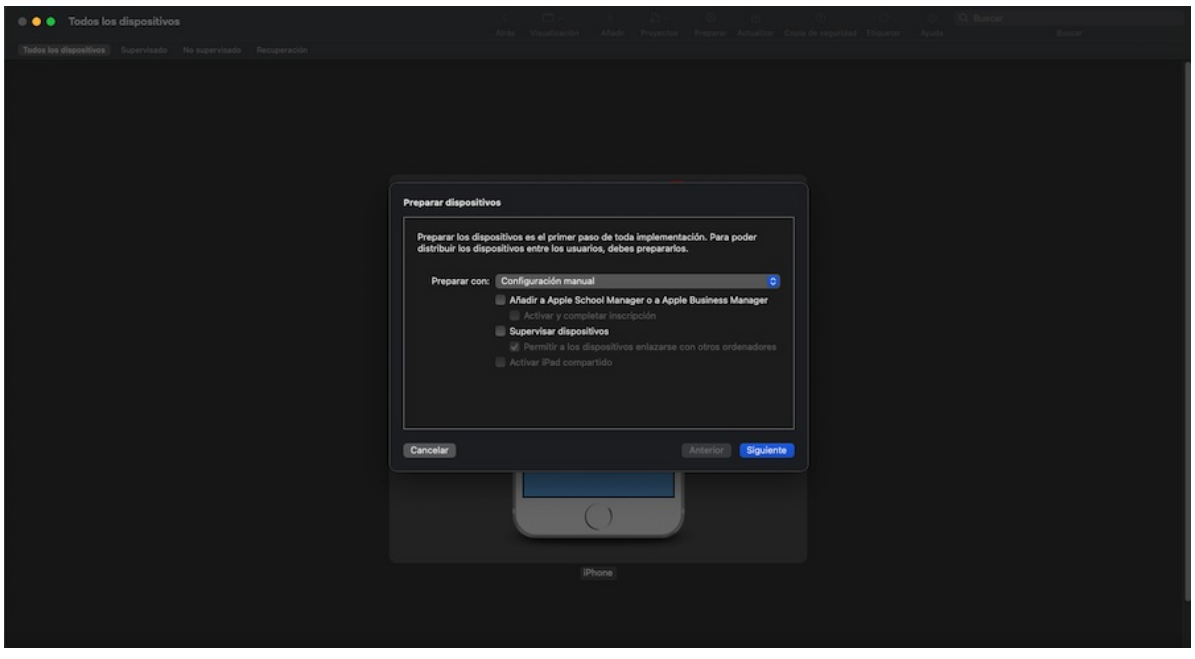
Existen dos formas de agregar los dispositivos a la consola de administración de ABM: una forma automática que se usa cuando los dispositivos han sido adquiridos bajo el programa de ABM y se cuenta con el ID de la compra o el ID del distribuidor y con esto se asocian los dispositivos de esa compra a la consola de ABM; y la otra forma es manual, agregando dispositivo por dispositivo cuando estos no fueron comprados bajo el programa.

Vinculación por medio de Apple Configurator 2

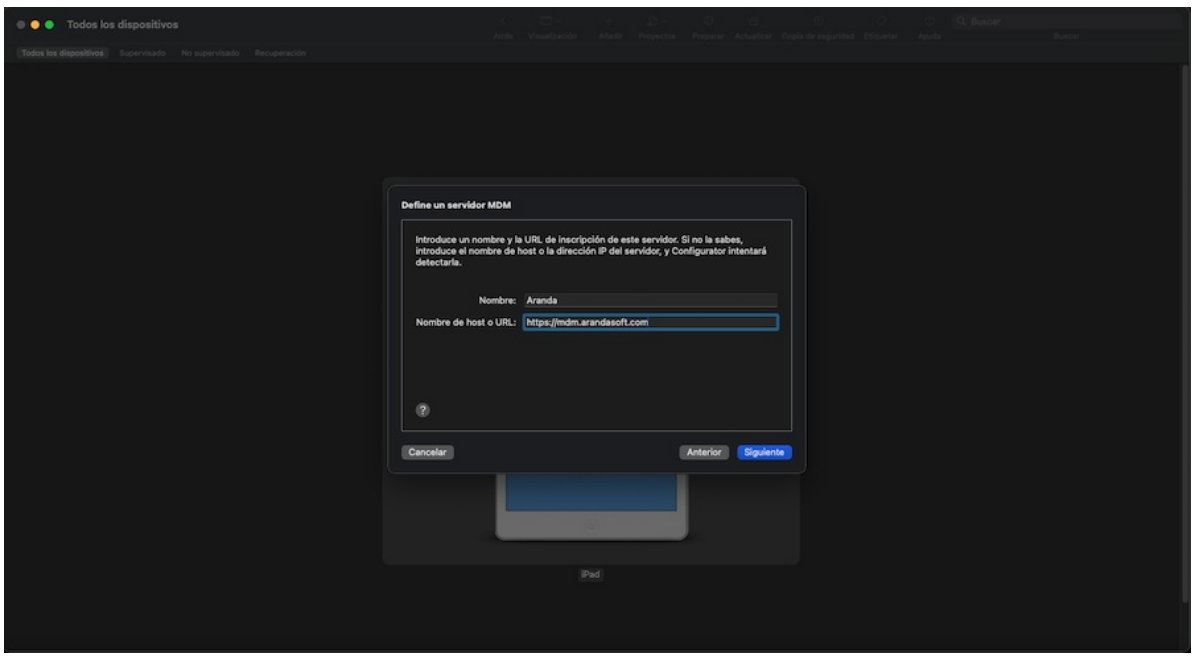
En esta guía se explica la forma manual usando el programa Apple Configurator 2 desde un Mac, conectando el dispositivo por medio de su cable USB a la computadora. Seleccione el dispositivo en el Apple Configurator y seleccione la opción Preparar.



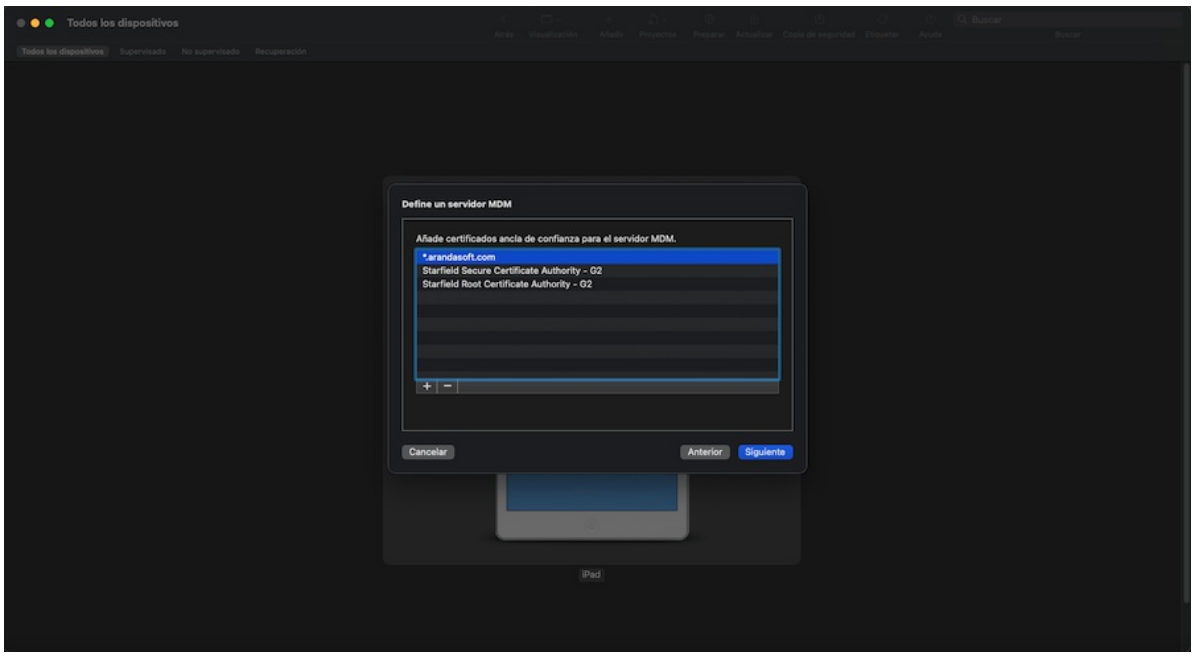
Seleccione las opciones como se muestra en la siguiente imagen y haga clic en siguiente:



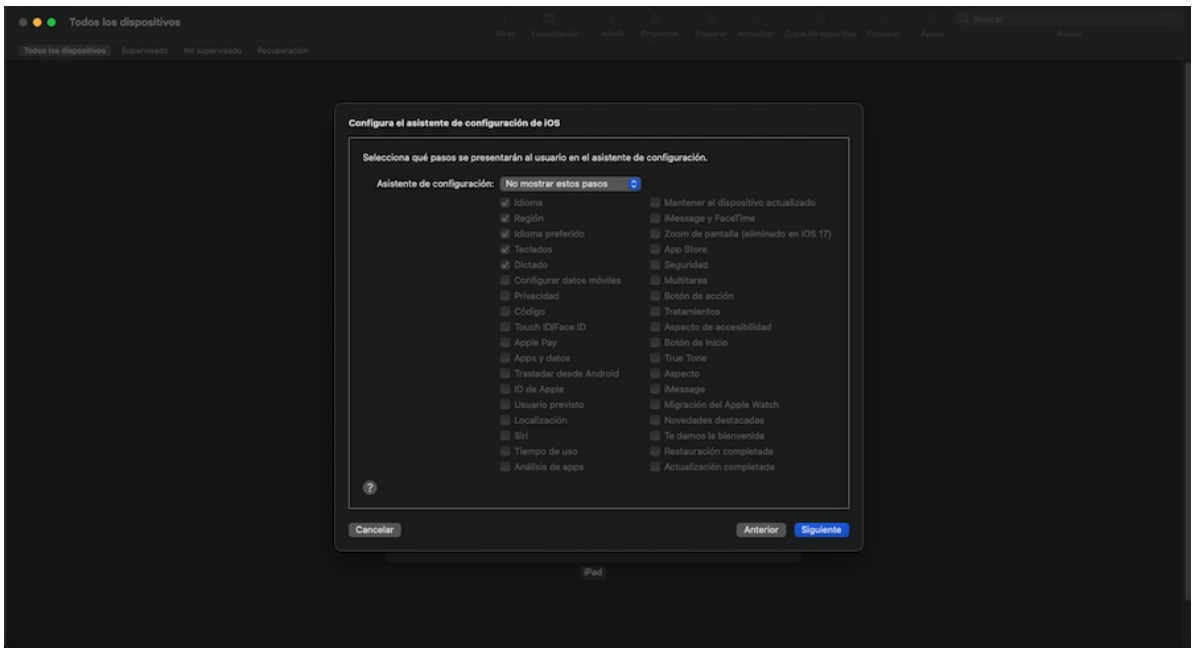
En la siguiente ventana ingrese el nombre y la URL de inscripción en el programa de ABM del cliente, en caso de no conocer estos datos, escriba un nombre y una URL que hagan alusión a la empresa para que automáticamente Apple Configurator lo busque entre los inscritos al programa. Para el ejemplo en esta guía se buscó la inscripción que tiene Aranda con ABM. Haga clic en Siguiente.



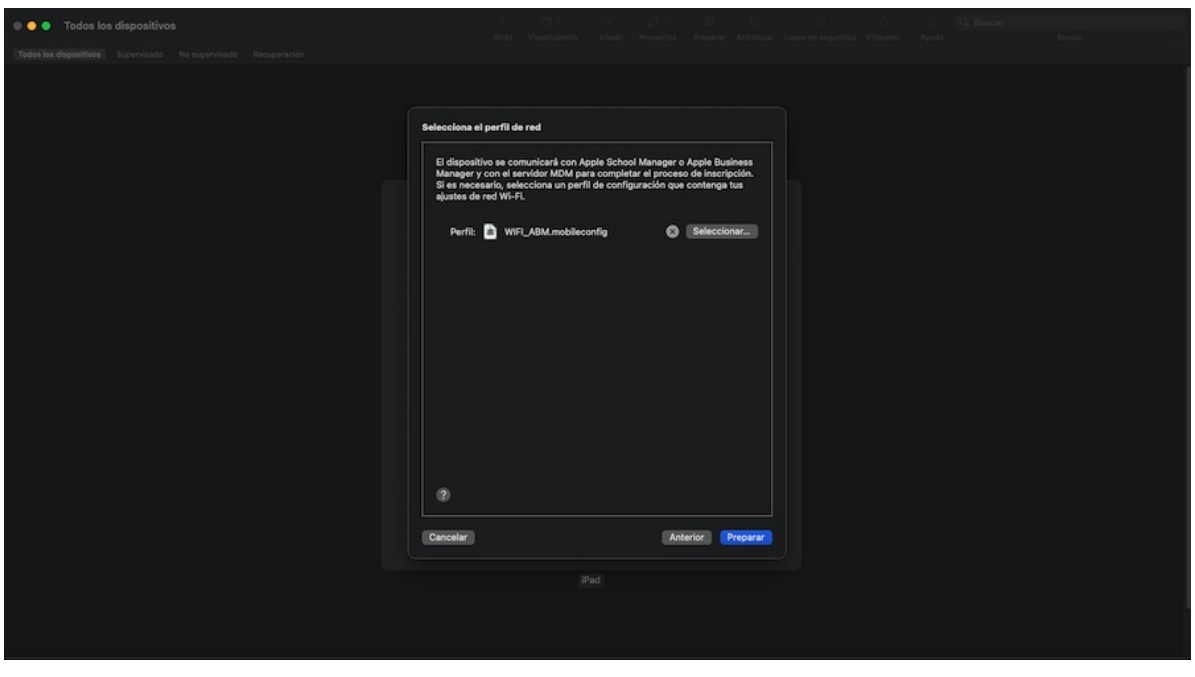
El programa busca coincidencias con los inscritos , seleccione el que crea que corresponde y luego haga clic en Siguiente.



La siguiente pantalla no es relevante, haga clic en Siguiente.

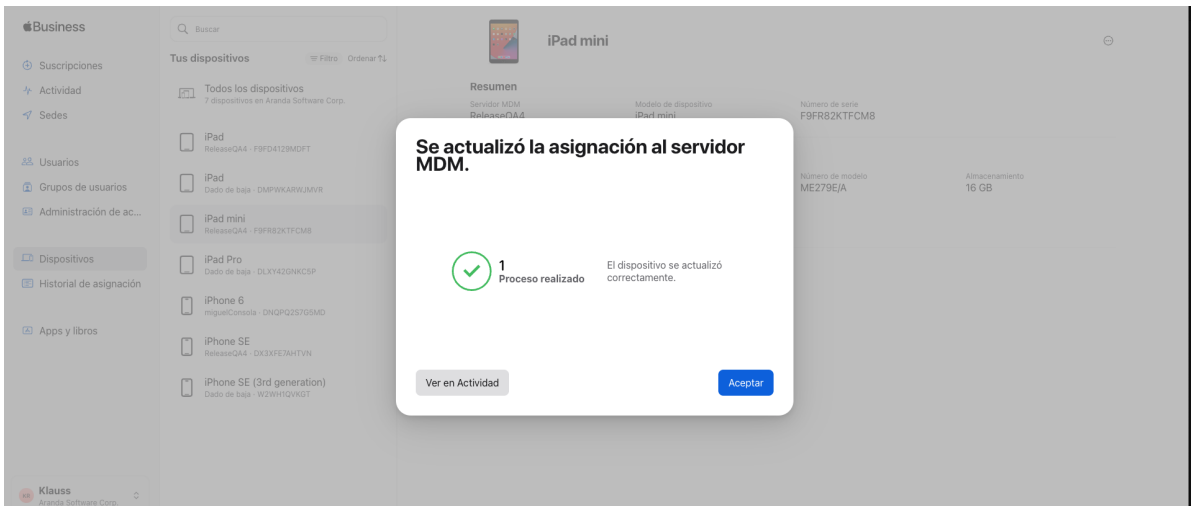


En la siguiente ventana es importante crear un perfil de WiFi y cargarlo porque el dispositivo necesita internet para comunicarse con el programa de inscripción de dispositivos. Para crear un perfil, el mismo Apple Configurator da la opción en el menú Archivo ⍰ Nuevo Perfil y allí se llena el formulario para el Wifi, luego dirigirse a Archivo ⍰ Guardar. Cargue el perfil de WiFi y elija la opción Preparar. Espere hasta que el programa complete los pasos de preparación.

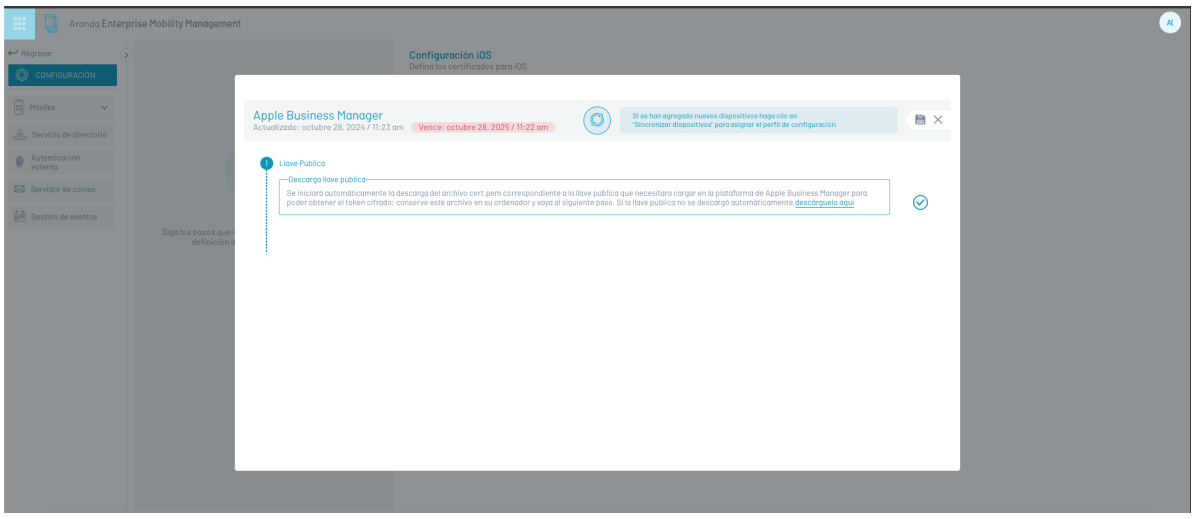


Los demás dispositivos puede conectarlos al Mac, como ya el Apple Configurator está configurado, solo haga clic en Siguiente sin configurar nada más. Una vez terminado el proceso de Apple configurator2, regrese a la plataforma de ABM, y en la opción Configuración, busque Apple Configurator2 en la lista de servidores MDM para confirmar la cantidad de dispositivos que se agregaron con Apple configurator2.

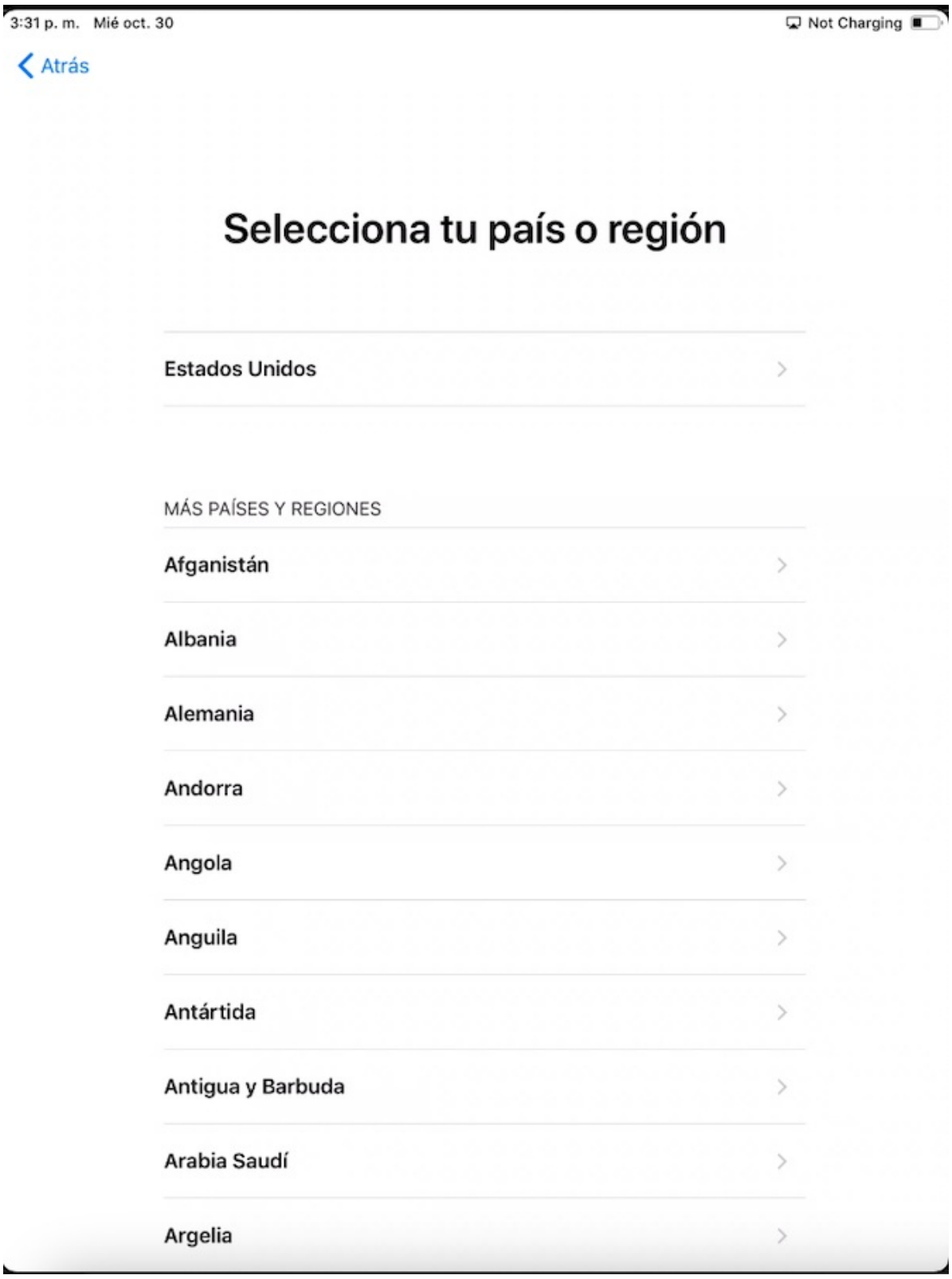
Diríjase a la opción Asignación de dispositivos para asignar el o los dispositivos al MDM, en este caso a AEMM Test. Escriba los seriales de los dispositivos directamente o cargue el listado de seriales mediante un archivo CSV. Haga clic en Aceptar.



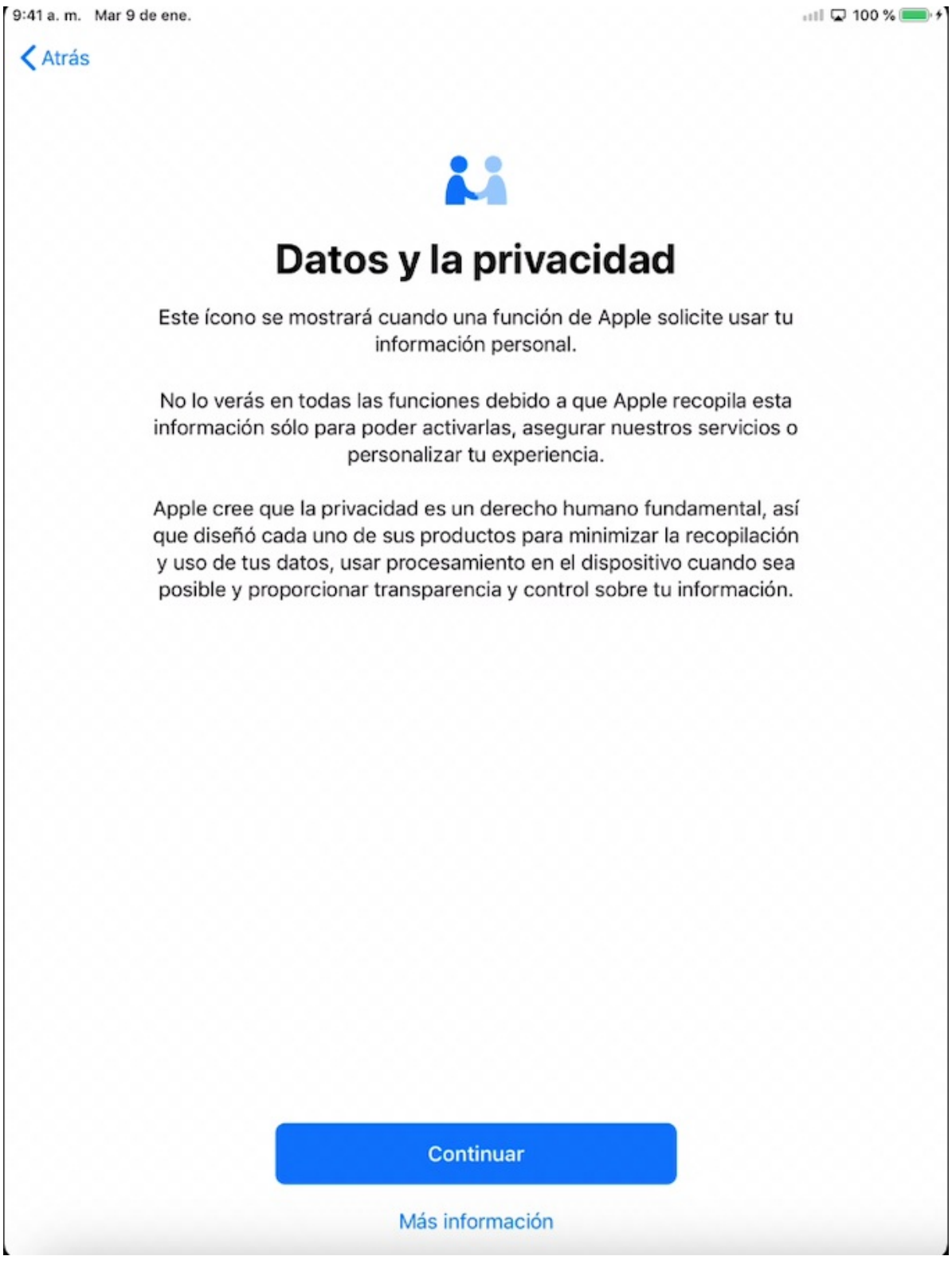
Luego del proceso en la consola de administración de Apple Business Manager, diríjase a la ventana de configuración de Apple Business Manager en la consola de AEMM (Configuración ⍰ Preferencias ⍰ Móviles ⍰ iOS ⍰ Tab Apple Business Manager) y haga clic en el botón Sincronizar Dispositivos).



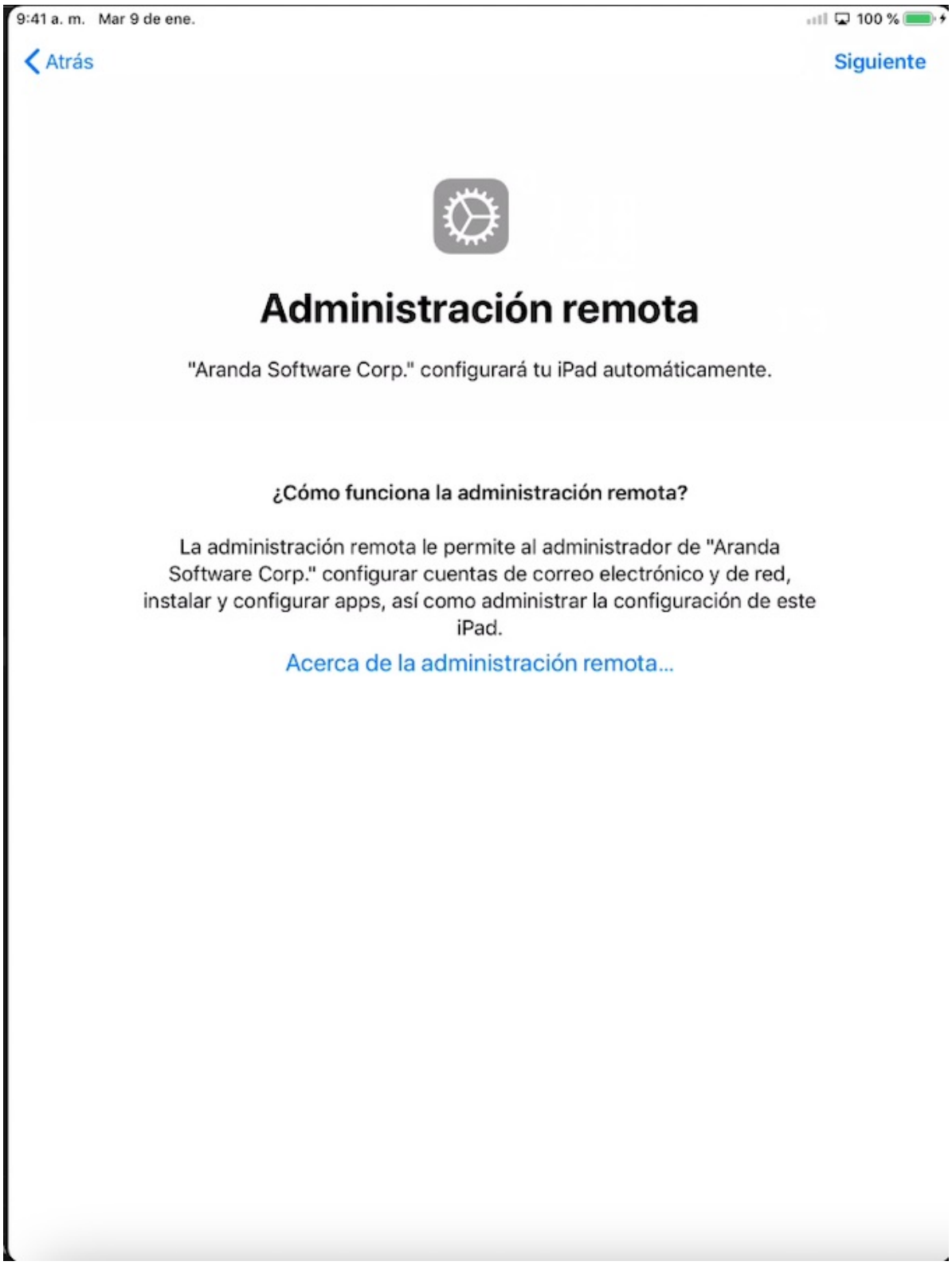
3) Proceso de vinculación en el Dispositivo Como el dispositivo se encuentra en condiciones de restauración de fábrica, seleccione el idioma deseado y el País o Región -> seleccionar en la opción siguiente.



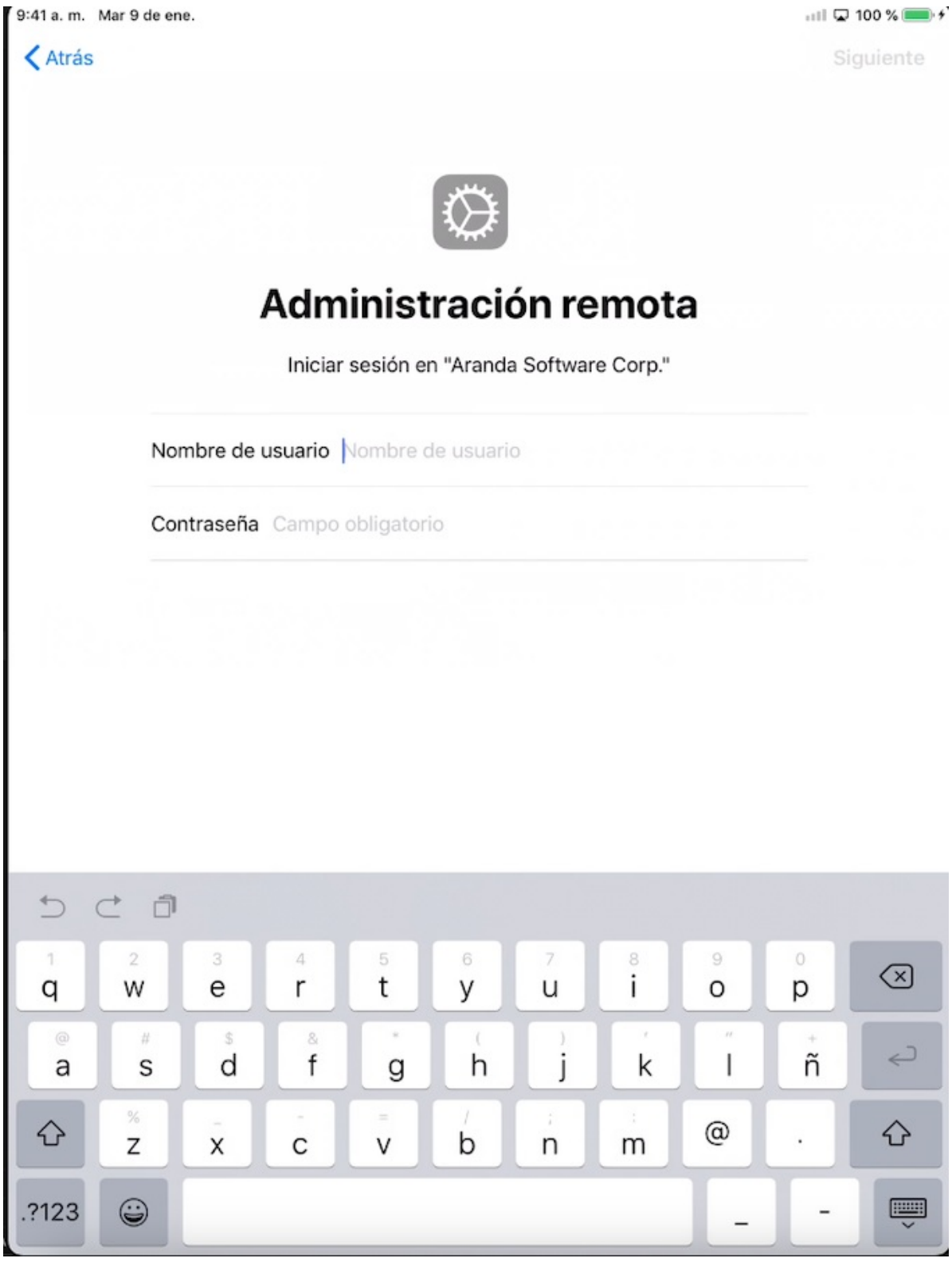
Realice la configuración de WiFi -> Seleccionar en la opción siguiente -> Se visualizará Datos y Privacidad seleccione el botón Continuar.



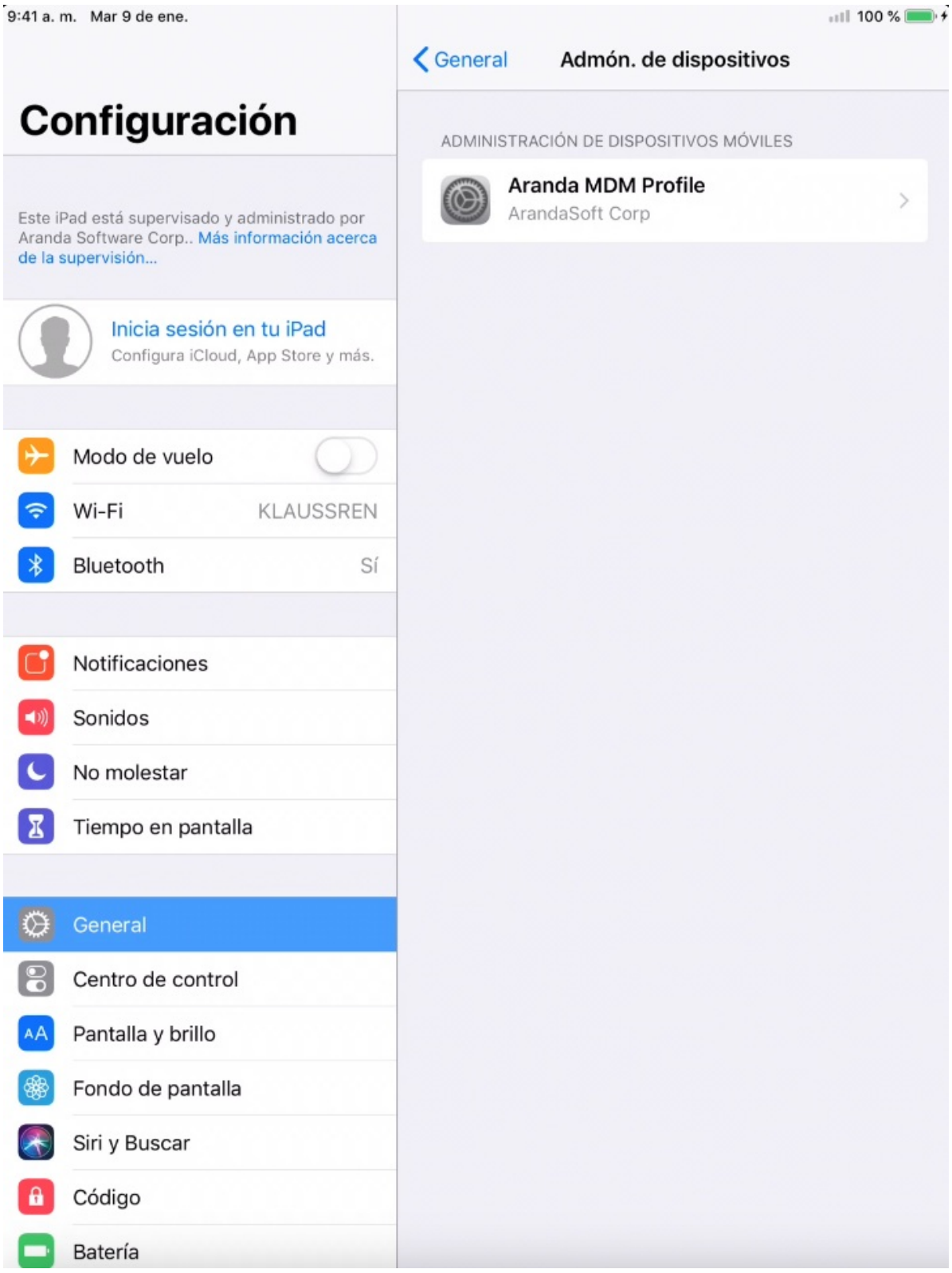
Inmediatamente visualizará la pantalla de Administración Remota, donde aparece la empresa administradora y la autorización de permisos sobre el dispositivo. Haga clic en Siguiente.



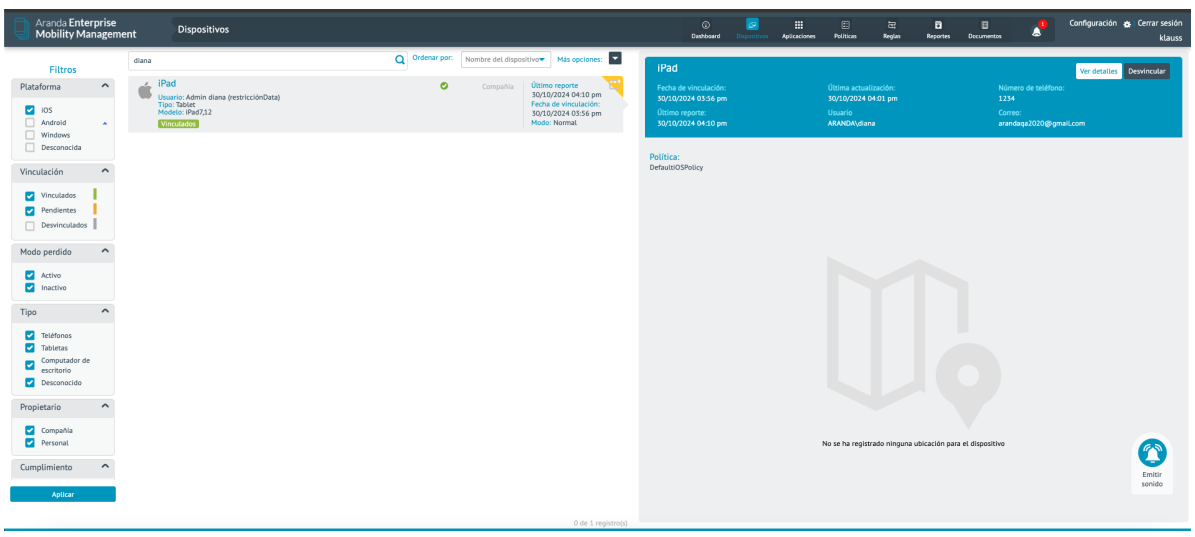
En la pantalla del login de administración remota ingrese el usuario y la contraseña. Si su conexión es exitosa, aparecerá el mensaje "Instalando configuración de software" (el cual está instalando el perfil de Aranda). Si su conexión falla, el sistema le informa la posible causa (ingreso incorrecto de datos de usuarios, conexión fallida, entre otros).



Cuando termine la configuración e instalación de Aranda Software, continúe con la configuración requerida por el dispositivo, al terminar dicha instalación debe dirigirse a Configuración-> General-> Perfil, con el fin de verificar la instalación del agente.



Al finalizar el proceso en el dispositivo, ya podrá ver el dispositivo vinculado en la consola AEMM en el listado de Dispositivos.



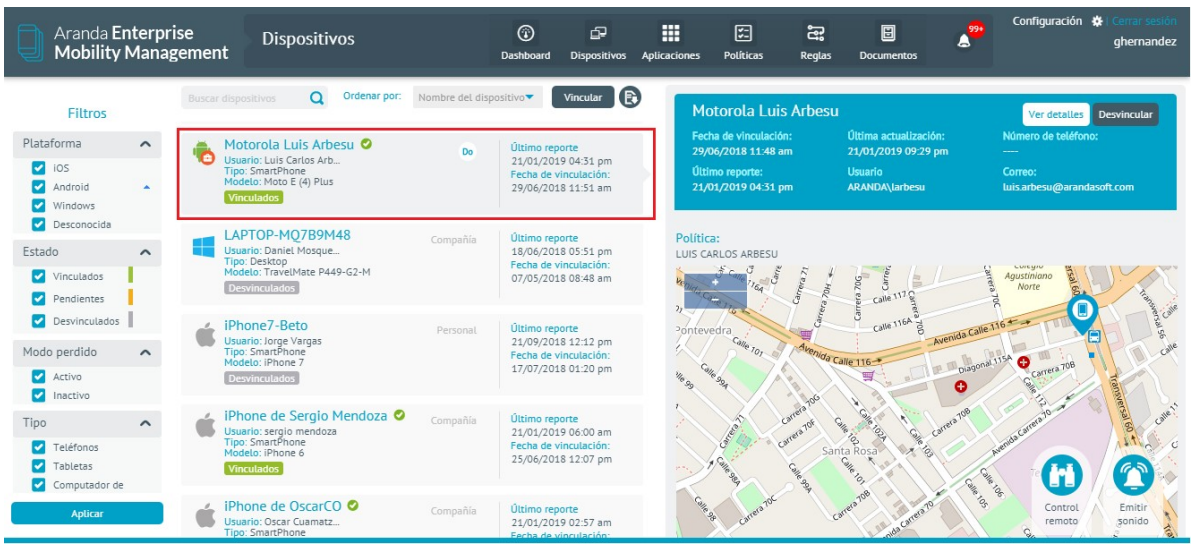
En este listado usted observará una marca amarilla, la cual le indica que el dispositivo se encuentra vinculado a la consola por medio de la instalación del perfil, pero le hace falta la instalación del agente. Al ingresar al dispositivo vinculado por ABM, en la pestaña de actividades podrá observar la ejecución de comandos y en la opción de comandos pendientes habrá unos sin ejecutar, estos últimos se ejecutarán cuando el agente se instale y así terminar el proceso de vinculación correctamente. Nota: antes de enviar a instalar el agente desde la consola valide que el comando de configuration, fue procesado exitosamente

Desvinculación

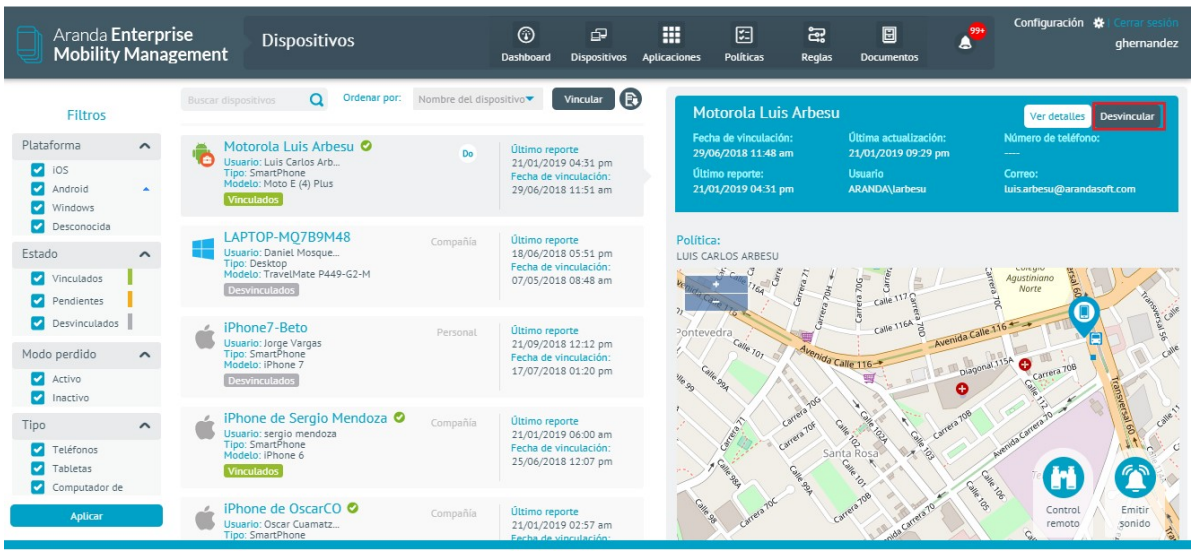
La desvinculación de un dispositivo se puede hacer desde la consola web o desde el dispositivo.

Desde la consola Web

Cuando un dispositivo se encuentra vinculado, este se puede identificar desde la consola web mediante una marca de color verde ubicada en la parte izquierda de la lista de dispositivos.



Para desvincular un dispositivo, selecciónelo de la lista de dispositivos, y de clic en **Desvincular** ubicado en el panel del lado derecho de la consola web. El sistema le preguntará que confirme si desea desvincular el dispositivo.



Si la desvinculación se hace por este procedimiento se debe esperar unos minutos para que el dispositivo reciba la notificación de que fue desvinculado.

Desde el dispositivo

Para desvincular un dispositivo desde la aplicación móvil, despliegue el menú de opciones lateral y seleccione Configuración.

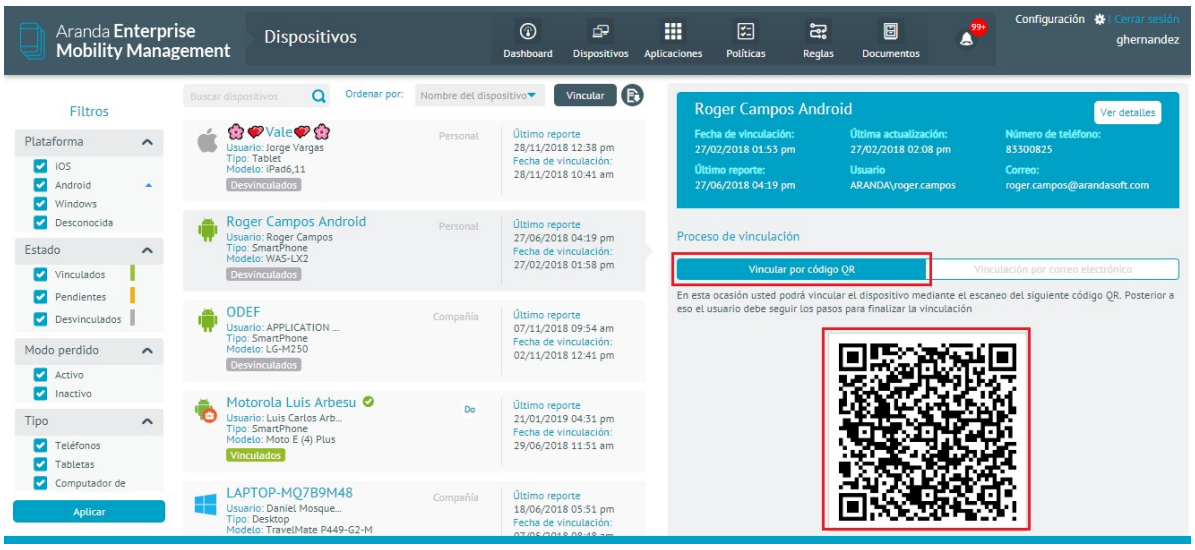
En la vista de **Configuración**, seleccione la opción **Desvincular dispositivo**, la aplicación despliega la pantalla donde

está la opción para desvincular, si da clic en el botón **Desvincular**, la aplicación mostrará un mensaje de alerta para confirmar el proceso que se va a hacer.

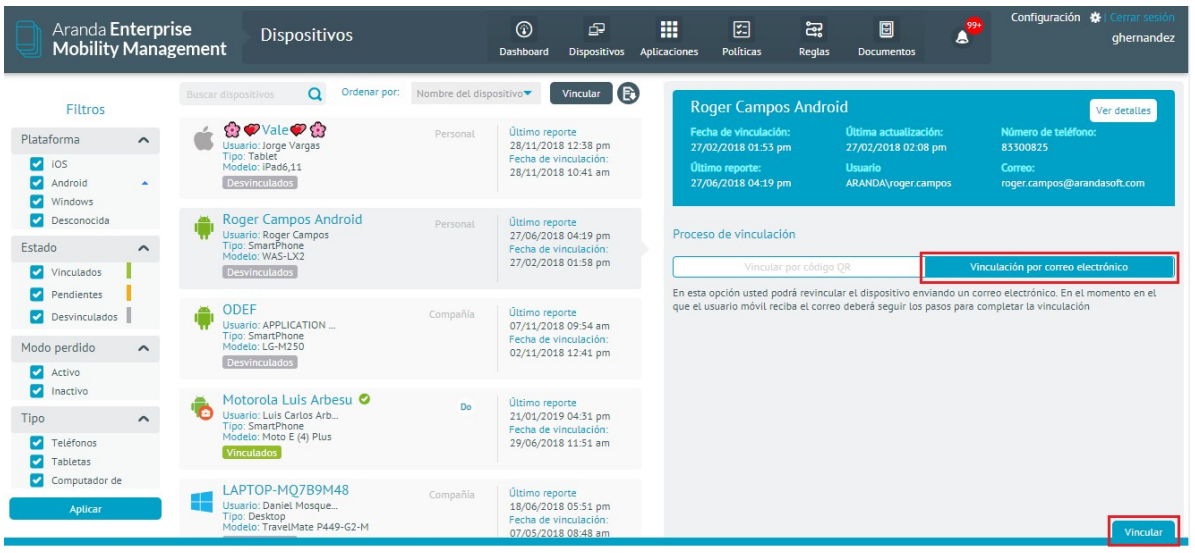
Si el usuario confirma la desvinculación, la aplicación muestra un mensaje informativo y deja a la aplicación en la ventana inicial del proceso de enrolamiento.

Revinculación

Para volver a vincular un dispositivo lo puede hacer desde la consola escaneando el código QR generado para cada dispositivo el cual contiene la información del usuario.



También puede volver a vincular un dispositivo enviando un correo electrónico escogiendo la opción Vinculación por correo electrónico del selector y dando clic en Vincular.



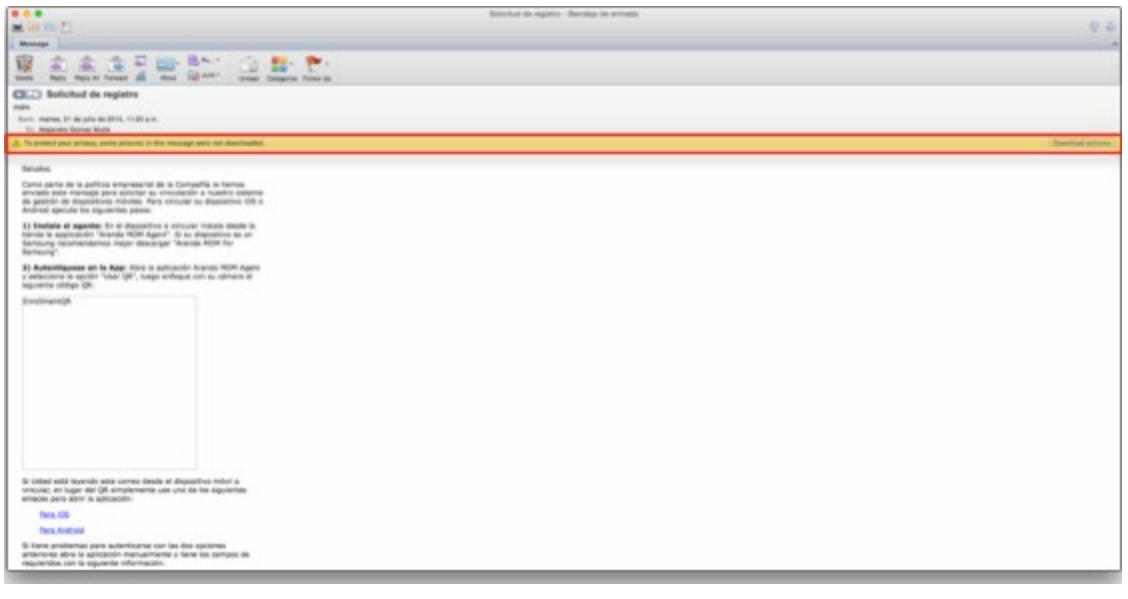
Problemas Comunes de Vinculacion

El correo no llega

En ocasiones puede ocurrir que el correo se demore unos minutos en llegar debido a que este debe pasar por un servidor saliente y otro entrante, lo que se traduce en dos procesos cuya velocidad depende de las peticiones que se hagan sobre los servidores y de la velocidad de la conexión a internet.

Cuando abro el correo, la imagen con el código QR no aparece

Esto puede presentarse por dos razones: porque el servidor de correos bloquea las imágenes de correos entrantes, en este caso se debe realizar la autorización para descargar las imágenes adjuntas al correo.



O porque la imagen aún no ha cargado, en este caso se debe esperar un momento más para que la imagen cargue o refrescar el correo.

La aplicación presenta un mensaje de error de conexión

Esto se debe a que el dispositivo no está conectado a ninguna red o su conexión es muy débil, debe tratar de buscar una conexión más estable o desactivar y volver a activar la conexión existente.

El despachador web no redirige el dispositivo para instalar el perfil (aplica solo para dispositivos iOS)

Dependiendo de la velocidad de la descarga del perfil desde el despachador, este redireccionamiento puede demorarse unos segundos, se puede verificar si la descarga se está realizando con el indicador de actividad del dispositivo ubicado en la parte superior.

La aplicación presenta un mensaje de error para descargar el perfil (aplica solo para dispositivos iOS).

Este mensaje se puede presentar porque el perfil aún no ha sido descargado o porque ya se descargó, pero aún no hay una respuesta de confirmación del servidor. Para verificar si el perfil ya fue instalado, de clic en **Ajustes -> General -> Perfil**, si el perfil se encuentra instalado y el mensaje continúa apareciendo, se debe esperar un momento mientras el servidor procesa la información.

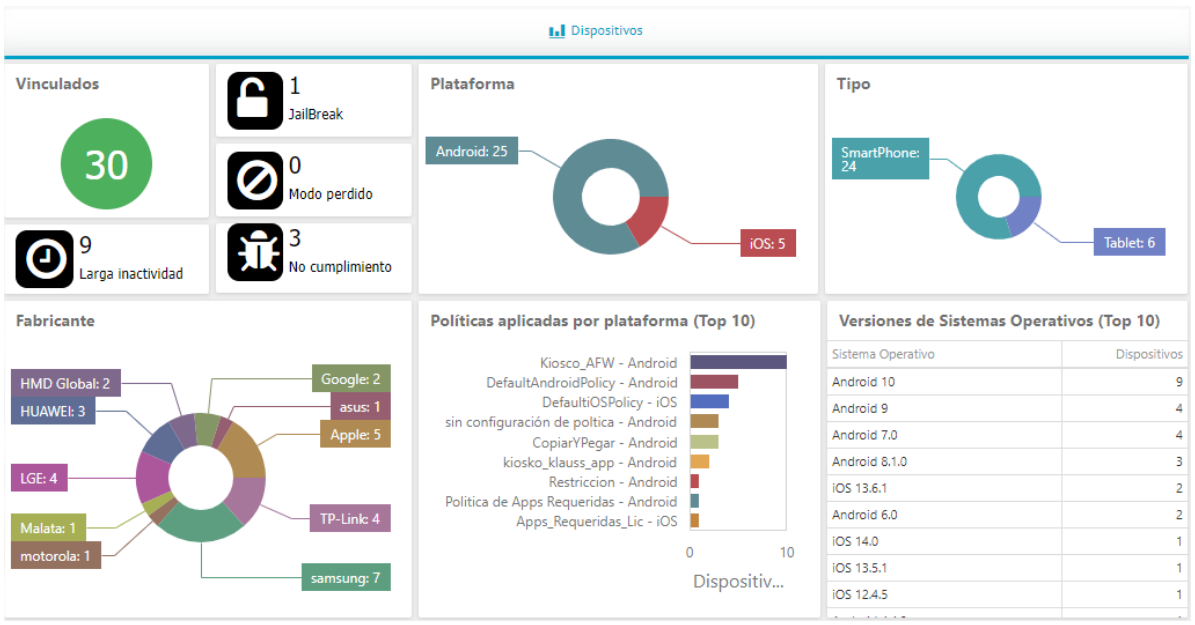
Dashboards

¿Qué son los Dashboards?

La sección de inicio de la plataforma, por defecto es la sección de Dashboard, es decir, apenas se inicia sesión en la plataforma para un usuario que tiene permisos de acceso a Dashboard es redirigido a esta sección. Dentro de la sección de Dashboard se puede consultar información estadística de forma rápida que nos muestra un pequeño resumen de las tendencias respecto a los datos de los dispositivos que se administran desde la consola. Cada uno de los tableros y sus respectivos gráficos son configurables desde la base de datos y se actualizan a partir de la lógica de negocio de la aplicación. Es posible acceder a Dashboard en cualquier momento desde la opción del menú principal de la consola de administración.

Dashboard de Dispositivos

El Dashboard de dispositivos presenta información estadística y de conteo para los dispositivos actualmente vinculados al servidor AEMM.

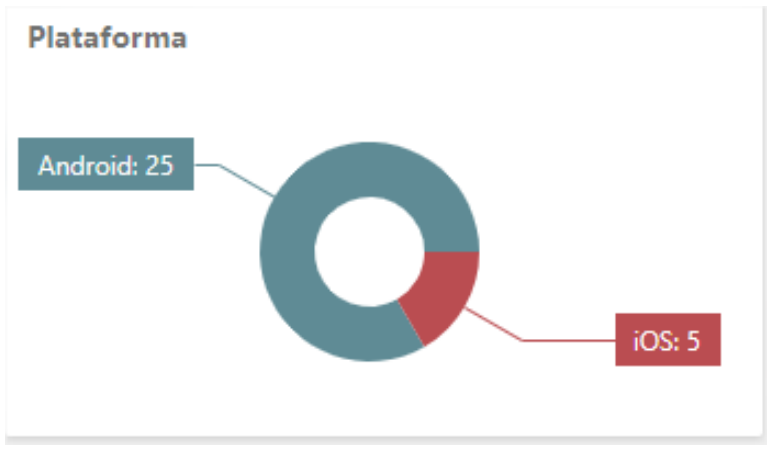


Descripción de cada elemento

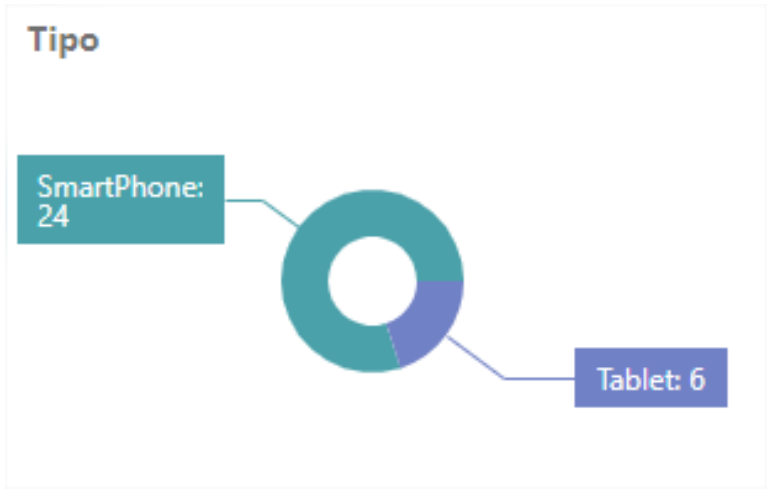
- Cantidad de dispositivos vinculados actualmente
- Cantidad de dispositivos con seguridad quebrantada (root y jailbreak).
- Cantidad de dispositivos en modo perdido
- Cantidad de dispositivos con larga inactividad

  Cantidad de dispositivos que incumplen la política asignada.
-

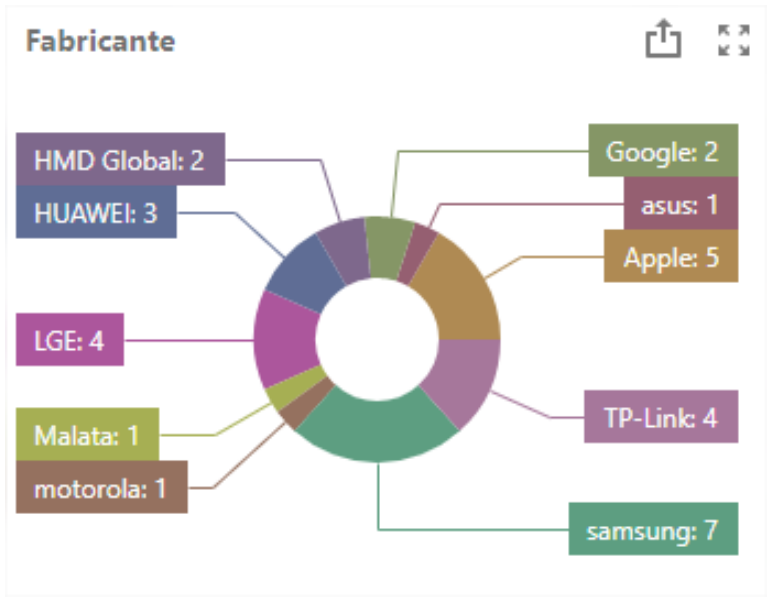
- Cantidad de dispositivos vinculados por plataforma



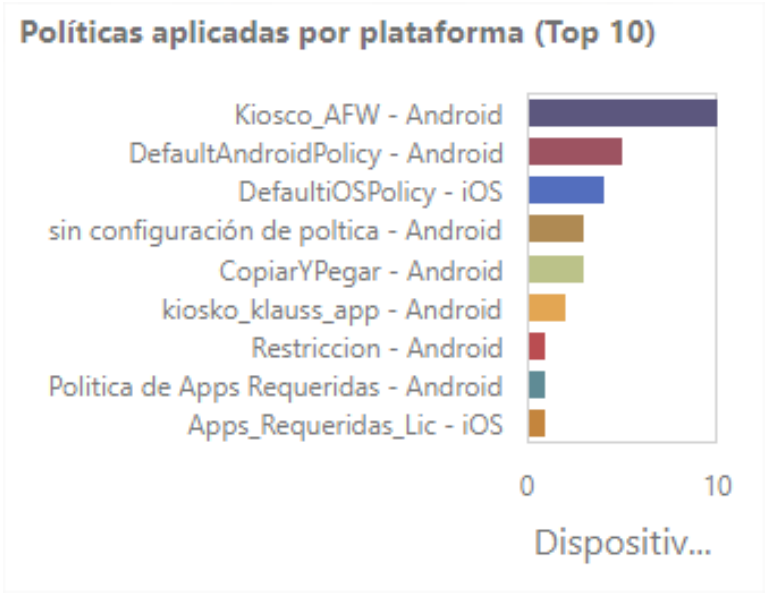
- Cantidad de dispositivos por tipo



- Cantidad de dispositivos por fabricante



- Cantidad de dispositivos por política



- Cantidad de dispositivos por versión de sistema operativo

Versiones de Sistemas Operativos (Top 10)

Sistema Operativo	Dispositivos
Android 10	9
Android 9	4
Android 7.0	4
Android 8.1.0	3
iOS 13.6.1	2
Android 6.0	2
iOS 14.0	1
iOS 13.5.1	1
iOS 12.4.5	1

Dashboard de Consumos

El Dashboard de consumos presenta información estadística y consolidada correspondiente a consumos de datos y voz de los dipositivos con un plan de consumo respectivo asignado actualmente.

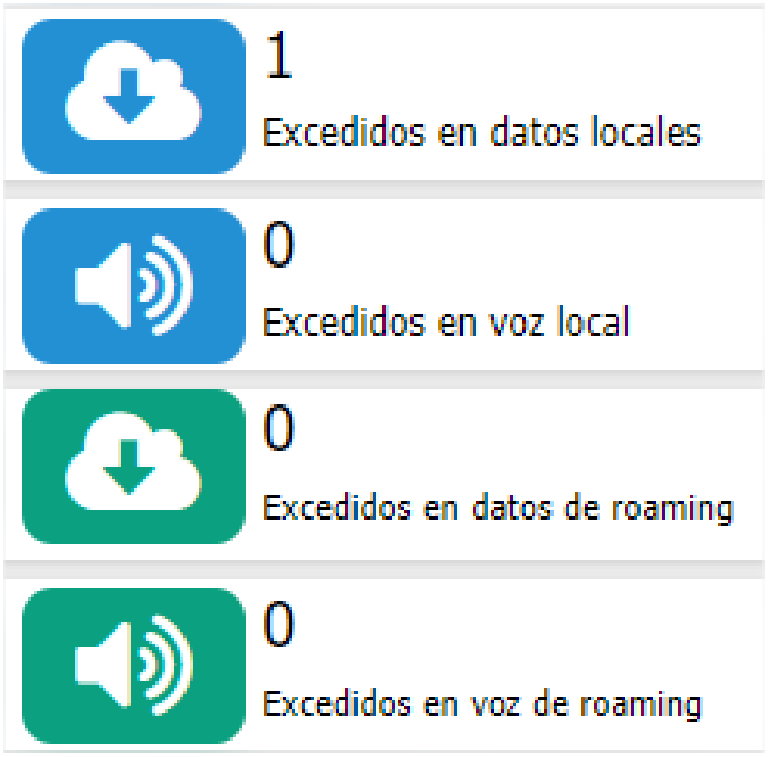
Descripción de cada elemento

- Cantidad de dispositivos con plan de consumo asignado

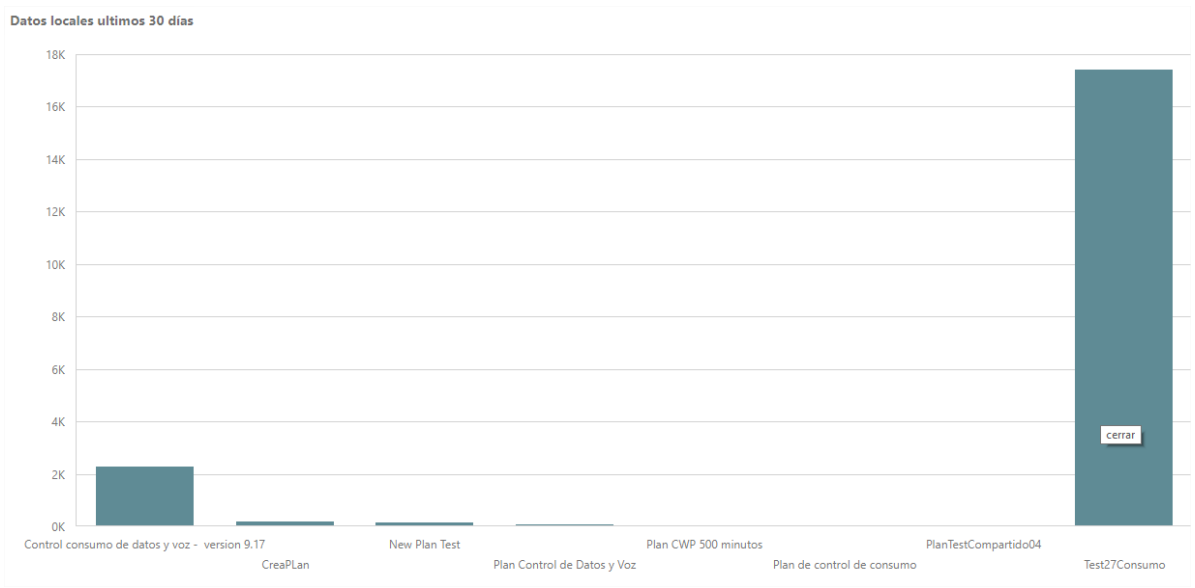
- Cantidad de dispositivos por plan de consumo

- Cantidad de dispositivos por Operador

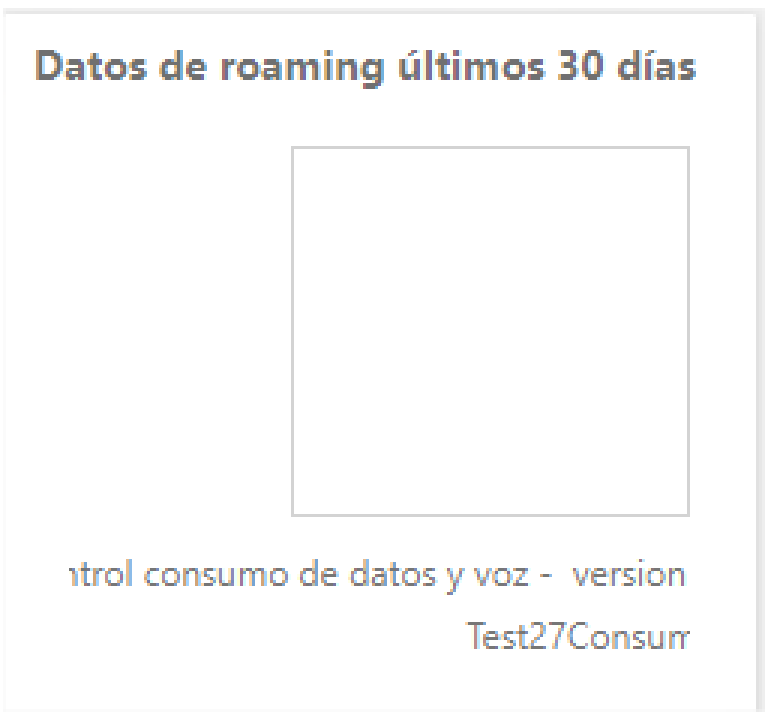
- Cantidad de dispositivos con consumos excedidos en: Datos Locales Voz Local Datos en Roaming Voz en Roaming



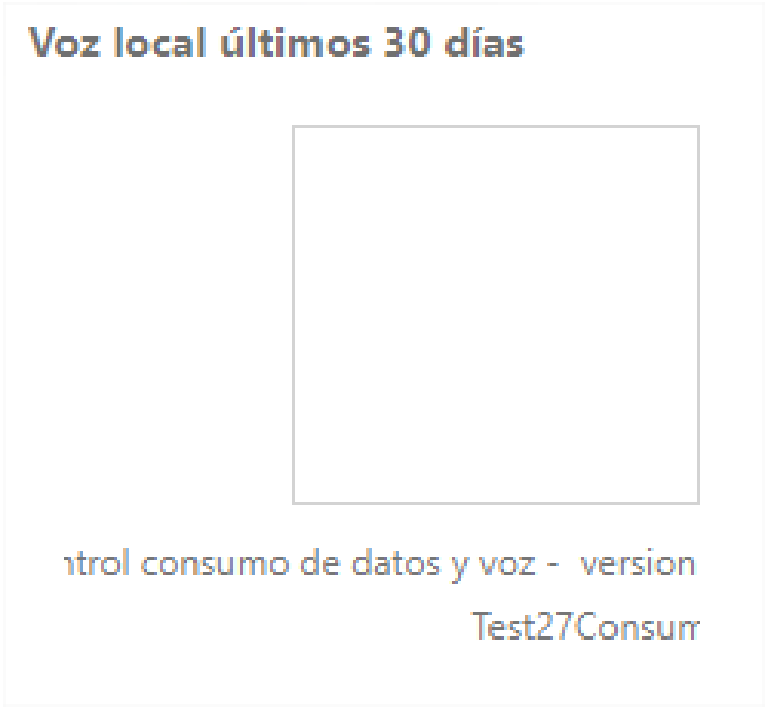
- Consumos de Datos locales por plan en los últimos 30 días



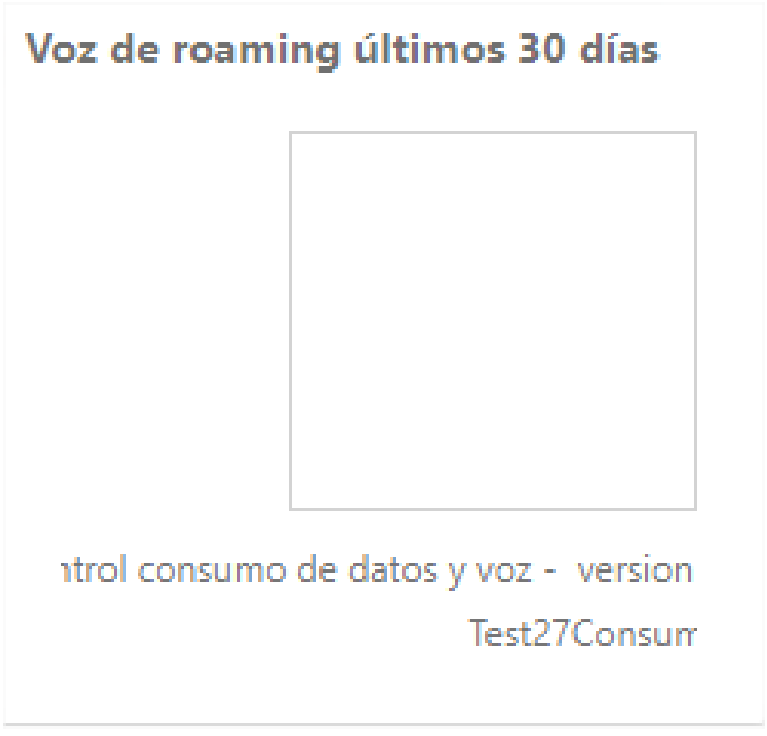
- Consumos de datos en roaming por plan en los últimos 30 días



- Consumo de voz local por plan en los últimos 30 días



- Consumo de voz en roaming por plan en los últimos 30 días



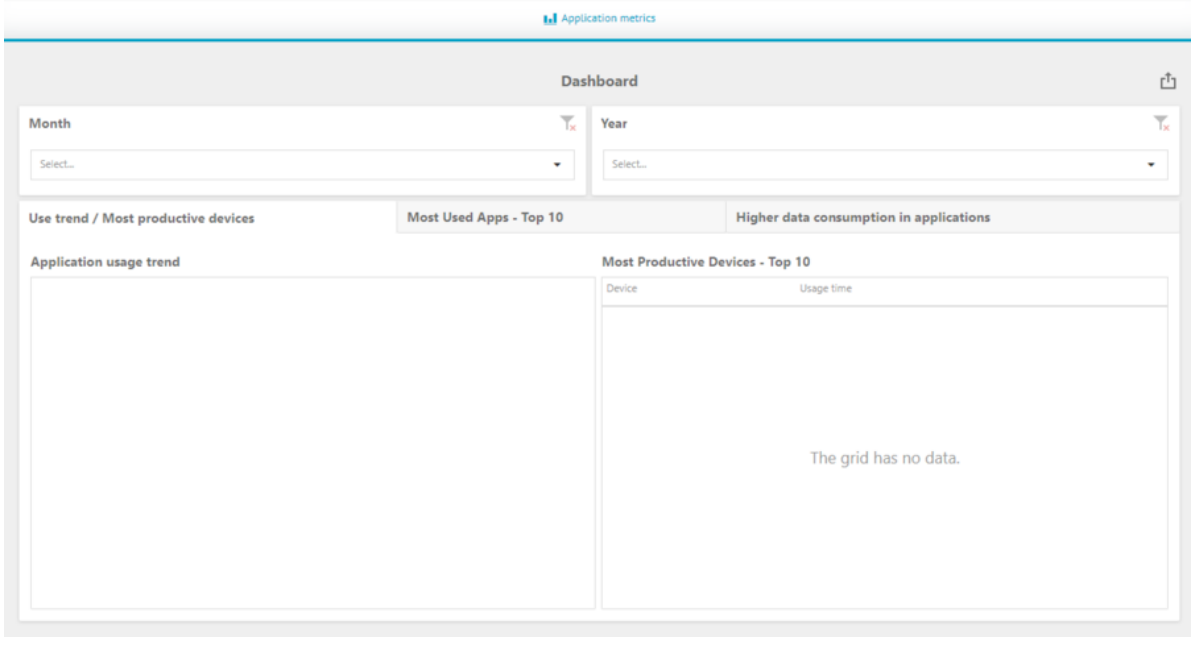
Dashboard de Métricas de Aplicaciones

El Dashboard de métricas de aplicaciones está destinado a presentar información estadística consolidada relacionada con la utilización de aplicaciones móviles y el consumo de datos móviles de las mismas.

El dashboard está orientado a brindar información acerca de la productividad en relación al uso de aplicaciones marcadas como productivas.

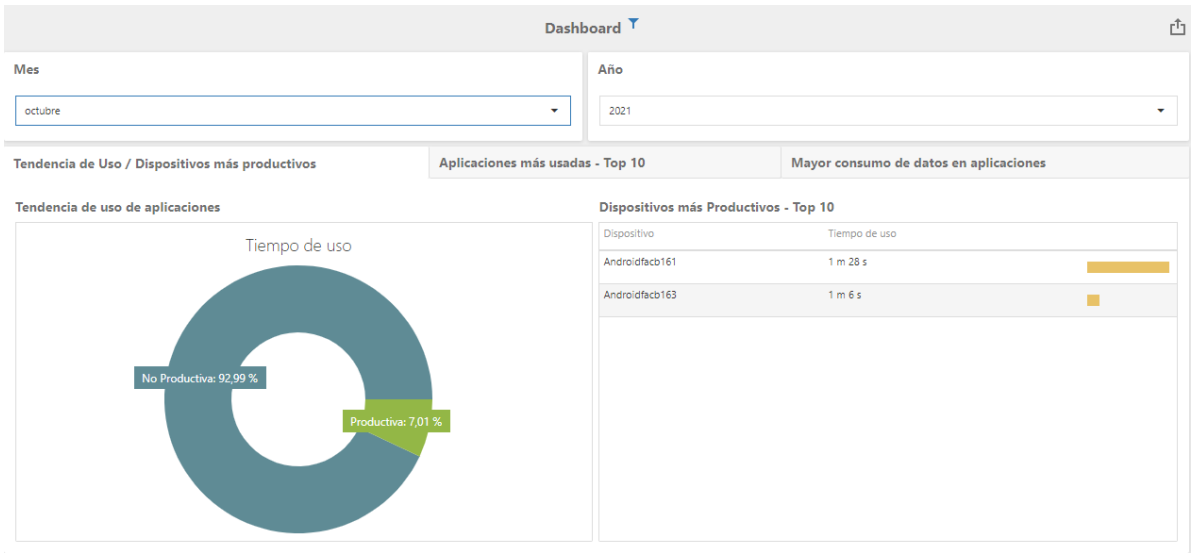
A continuación se detalla cada uno de los elementos del dashboard de métricas de aplicaciones.

Filtro principal



En este filtro se presetan listas desplegables correspondientes al mes y al año en que se desean que se filtren las gráficas de cada uno de los dashboards. Los valores cargados en las listas desplegables corresponden a lo existente en la base de datos reportado por los dispositivos en relación a uso y consumo de datos de aplicaciones.

Dashboard de Productividad



Se presentan dos elementos:

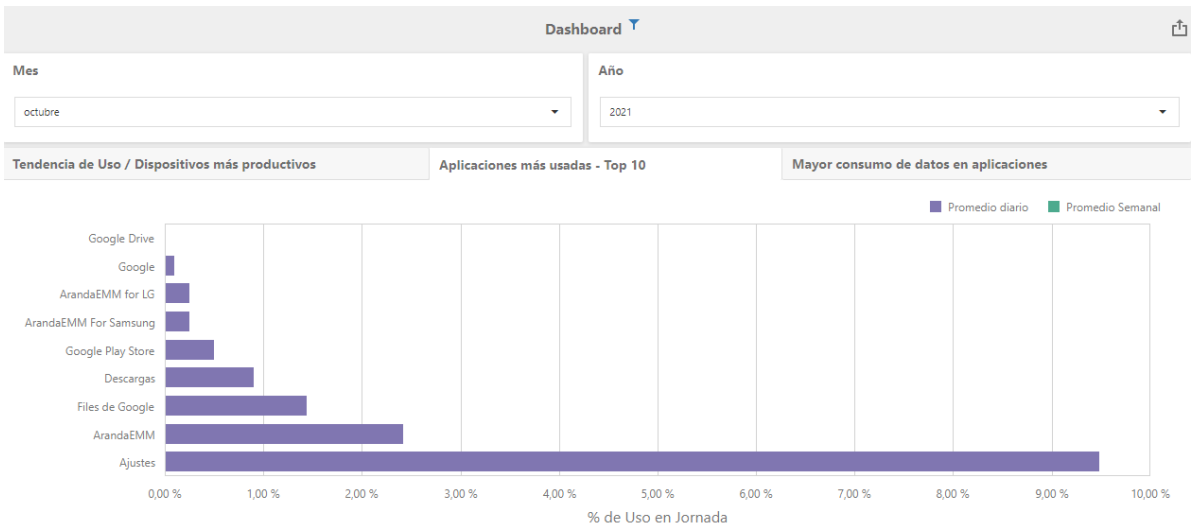
Diagrama Circular de Uso Productivo

En este diagrama se grafica comparativamente el uso de aplicaciones productivas versus las aplicaciones no productivas, en porcentaje

Lista de Dispositivos Productivos

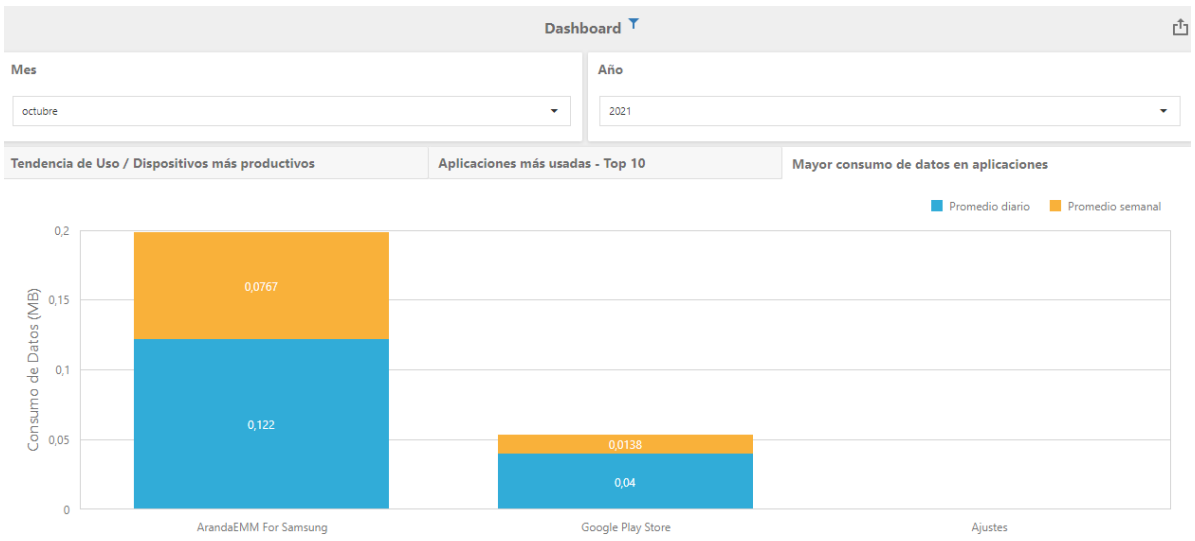
Se presenta un Top 10 de los dispositivos con más uso de aplicaciones marcadas como productivas.

Dashboard de Aplicaciones más usadas



Se presenta un diagrama de barras ordenado de menor a mayor de las aplicaciones más usadas con promedios diario y semanal.

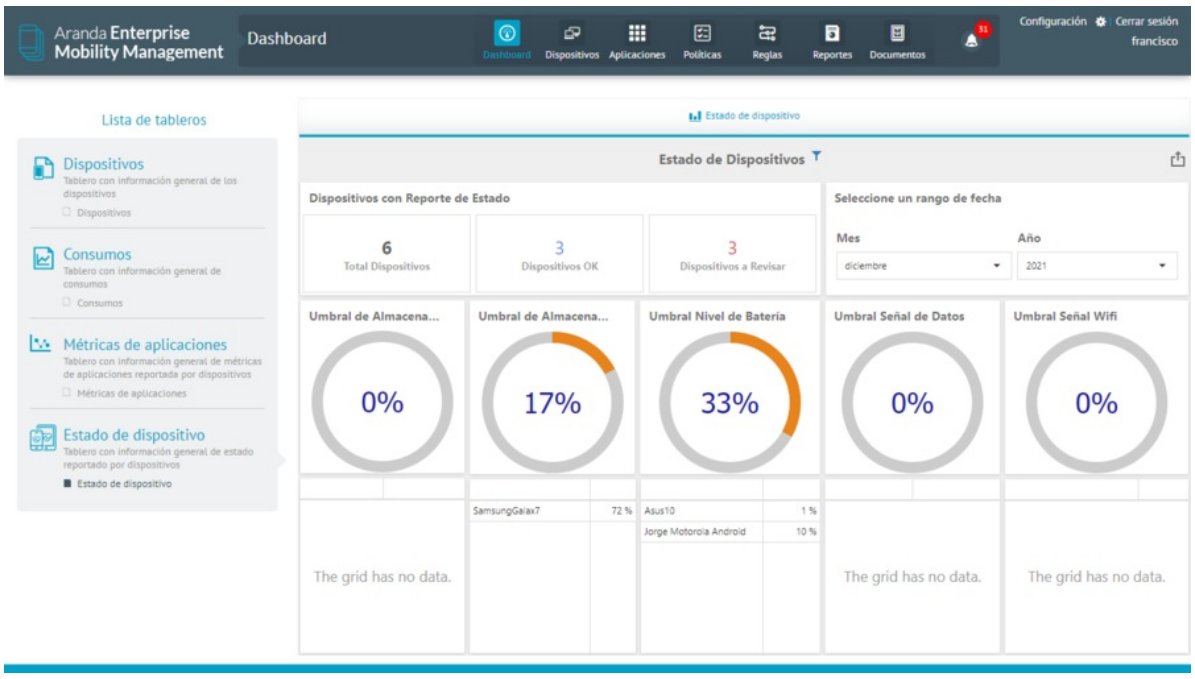
Dashboard de Consumo de Datos de Aplicaciones



Se presenta un histograma ordenado de mayor a menor de las aplicaciones con mayor consumo de datos, en promedios semanal y diario.

Dashboard de Estado del Dispositivo

El dashboard de reporte de estado de los dispositivos está destinado a presentar información consolidada del estado de los dipsositivos, de acuerdo a los reportes de estado periódicos generados.



Para visualizar el tablero con la información general del estado reportado por el dispositivo, ingrese a la consola de Inicio de AEMM, en el menú encabezado seleccione la opción **Dashboard**, en la sección Lista de tableros del menú principal, seleccione la opción **Estado del Dispositivo** y habilite el check correspondiente. En la Vista Detalle podrá visualizar los dispositivos con reporte de estado teniendo en cuenta los siguientes criterios:

Filtro principal

En este filtro se presetan listas desplegables correspondientes al mes y al año en que se pueden filtrar cada uno de los gráficos. Los valores cargados en las listas desplegables corresponden a lo existente en la base de datos reportado por los dispositivos en relación a los reportes de estado recibidos.

Conteos

En la Vista detalle del estado de dispositivos podrá visualizar la cantidad de dispositivos registrados:

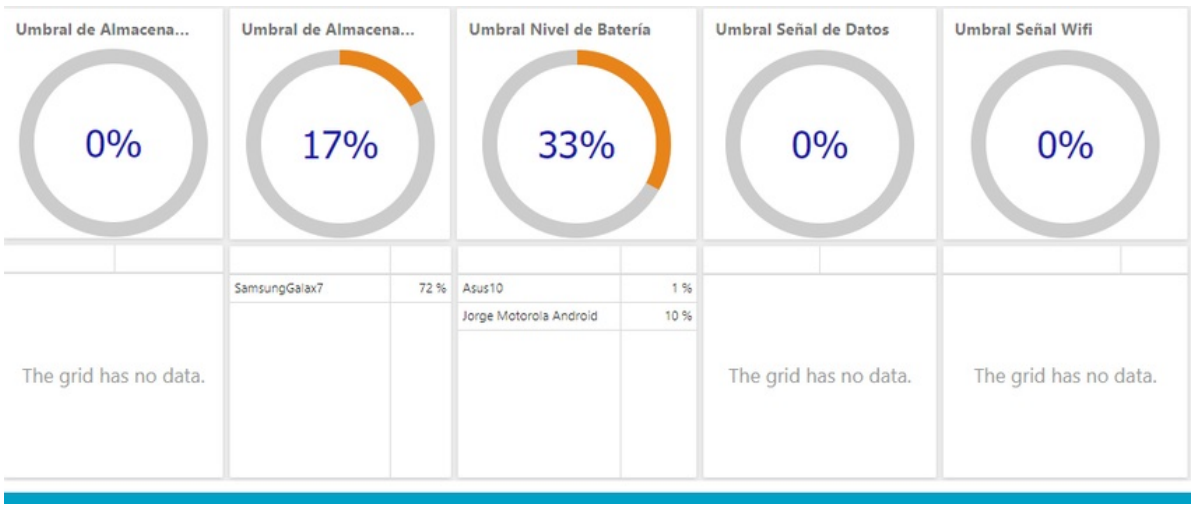
- Total Dispositivos: Dispositivos con al menos un reporte de estado.
- Dispositivos Ok: En todas las categorias reportan valores que superan los umbrales configurados.
- Dispositivos a revisar: Dispositivos que en al menos una categoría no superan el umbral configurado.

Gráficos y Tablas detalle

En la Vista detalle del estado de dispositivos podrá visualizar los gráficos de representación del umbral por tipo de dato:

Tipo de Dato	Descripción
Umbral de Almacenamiento Interno:	Porcentaje de Dispositivos que reportan almacenamiento interno usado mayor al umbral configurado
Umbral de Almacenamiento Externo:	Porcentaje de Dispositivos que reportan almacenamiento externo usado mayor al umbral configurado.
Umbral Nivel de Batería:	Porcentaje de Dispositivos que reportan un nivel de batería menor al umbral configurado.
Umbral Señal de Datos:	Porcentaje de Dispositivos que reportan una intensidad de señal de datos menor al umbral configurado.
Umbral Señal Wifi:	Porcentaje de dispositivos que reportan una intensidad de señal Wifi menor al umbral configurado.

Bajo cada gráfico se presenta la tabla que detalla cada uno de los dispositivos que tienen reportes que no satisfacen los umbrales en cada categoría.

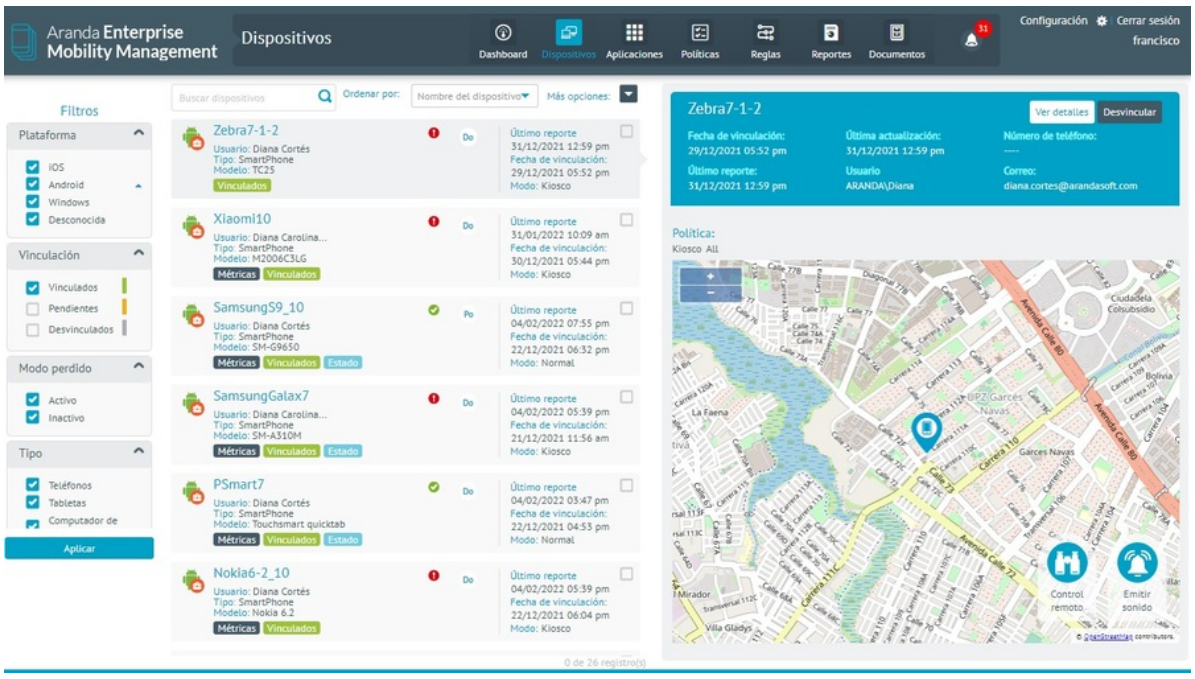


Dispositivos

Módulo Dispositivos

Una vez se completa el proceso de vinculación, un dispositivo podrá ser consultado y gestionado desde la consola de administración de Aranda ENTERPRISE MOBILE MANAGEMENT AEMM.

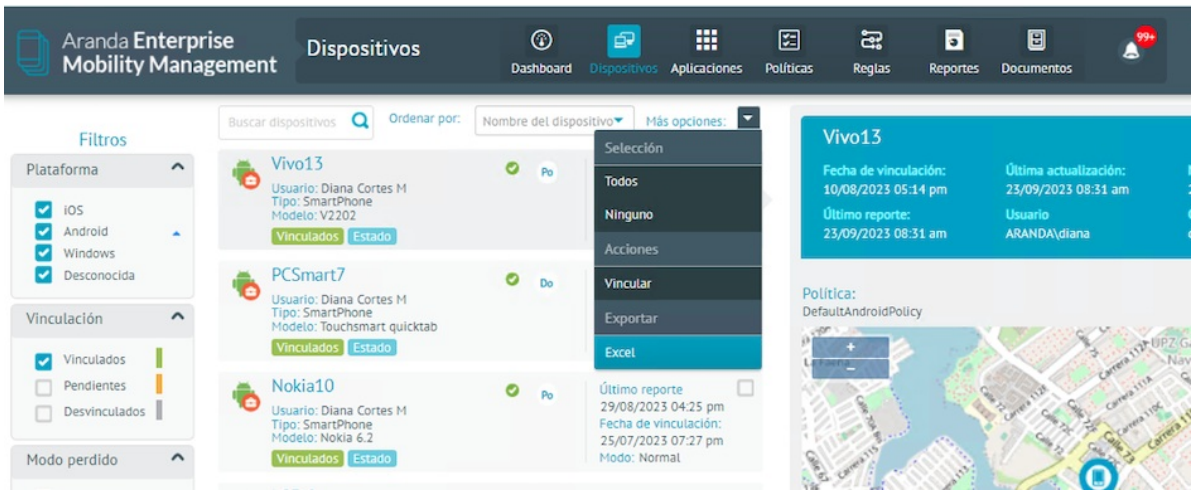
1. Para visualizar la información reportada por el dispositivo, ingrese a la consola de Inicio de AEMM, en el menú encabezado seleccione la opción **Dispositivos**, en la sección filtros del menú principal podrá personalizar la consulta seleccionando los criterios asociados a la información general del dispositivo vinculado.



Los criterios de consulta están agrupados por categorías y podrá personalizar los siguientes filtros:

Filtros	Descripción
Tipo:	Este filtro define el tipo de dispositivo (Smartphone, Tablet, desktop).
Propietario:	Hace referencia a la propiedad del dispositivo (del usuario, de la compañía).
Estado:	Este filtro establece el estado del dispositivo (vinculado, desvinculado, pendiente).
Plataforma:	Este filtro presenta las plataformas asociadas al dispositivo (iOS, Android).
Vinculación:	Este filtro presenta la vinculación de los dispositivos (vinculados, desvinculados, pendientes).
Cumplimiento:	Este filtro presenta el dispositivo con políticas relacionadas (de acuerdo o no con la política aplicada).
Métricas:	Este filtro define el estado de métricas (activado/desactivado).
Reporte de estado:	Este filtro presenta el estado del dispositivo (activo/inactivo)
Grupos:	Este filtro presenta los grupos asociados al dispositivo.

2. Después de definir los filtros de consulta, seleccione el botón **Aplicar**. En la vista de información podrá visualizar los dispositivos relacionados a los criterios definidos. seleccione un dispositivo en estado vinculado y en la vista detalle podrá visualizar en el mapa la información básica del elemento seleccionado. De igual forma el admisnitrador de consola puede realizar la descarga de un archivo .xls, el cual detalla la siguiente información:

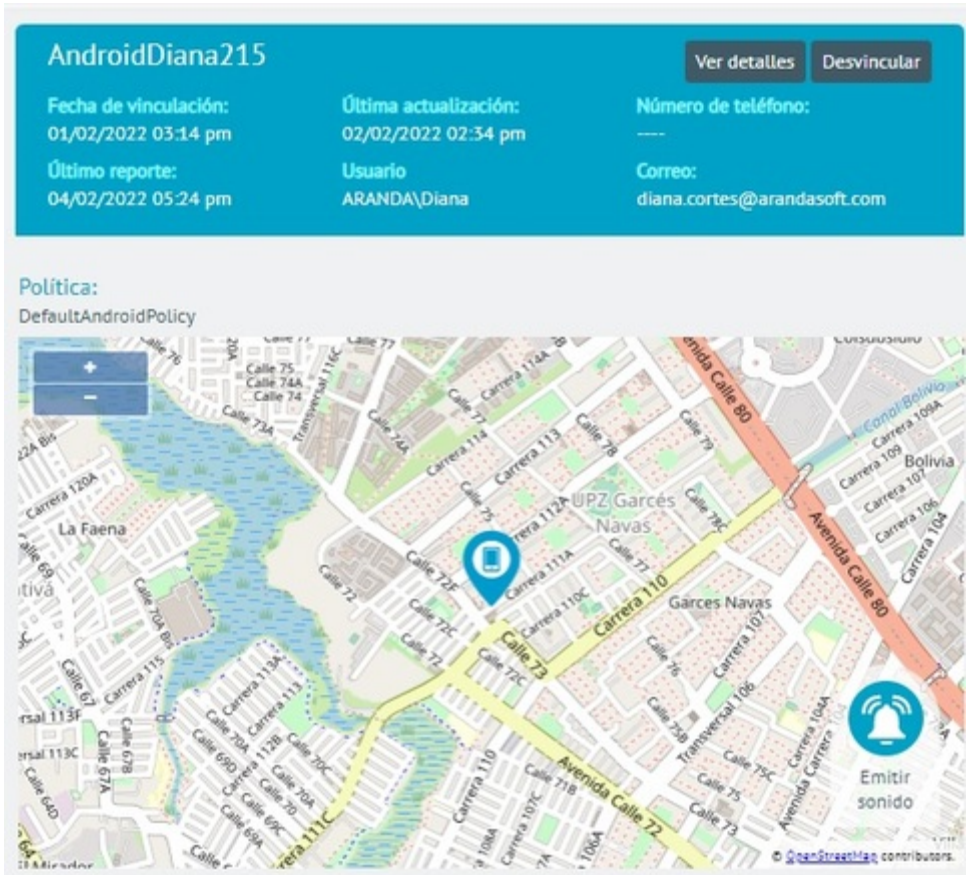


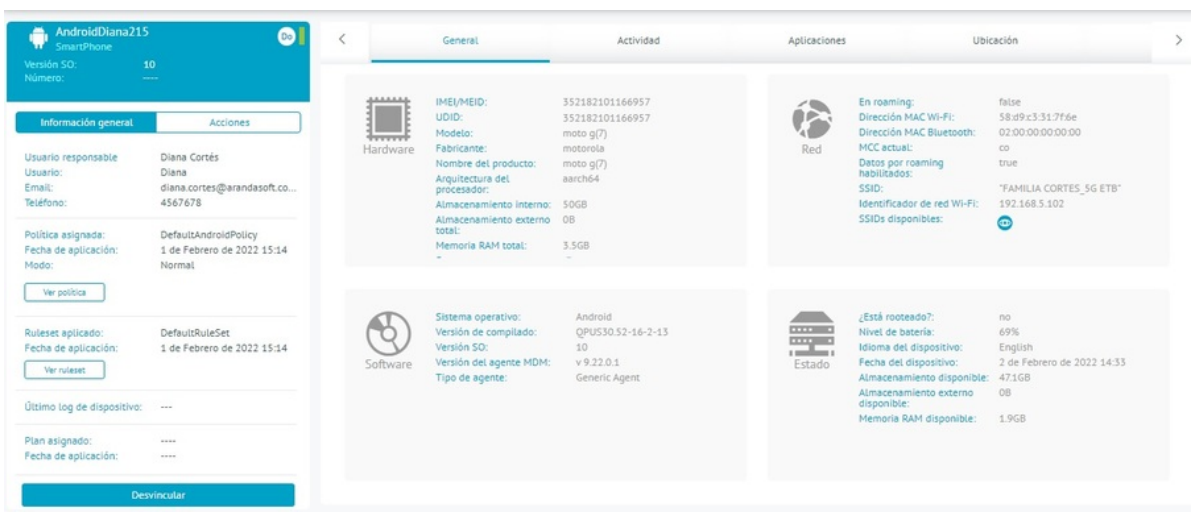
Campos más relevantes

Detalles

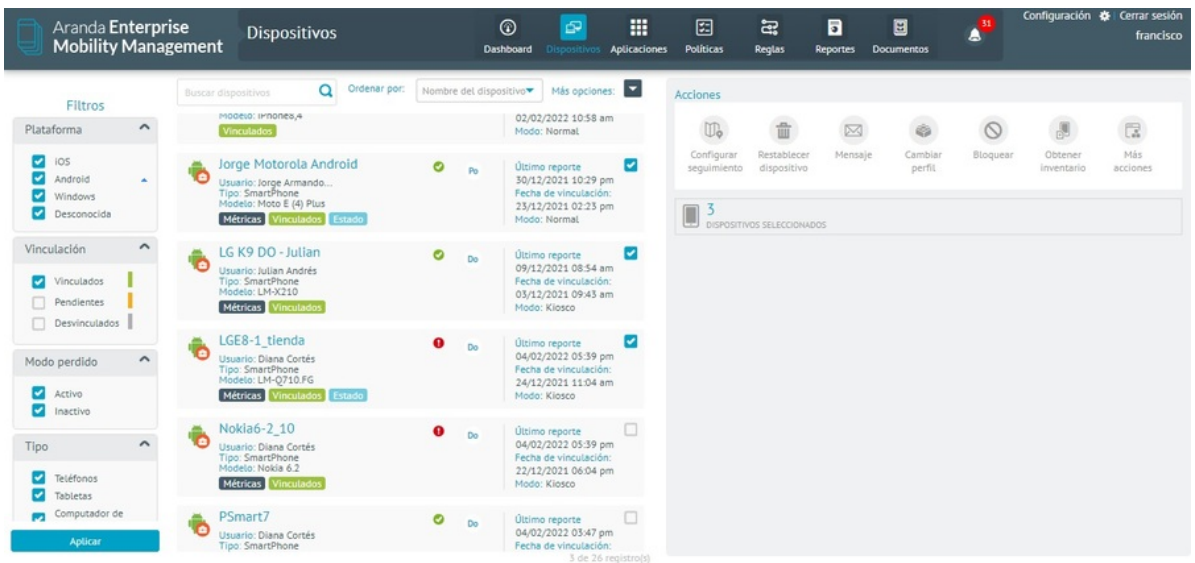
- Nombre del dispositivo
- Plataforma
- Número de serial
- IMEI
- Modelo del dispositivo
- Sistema operativo
- Almacenamiento interno
- Serial de la SIMM
- Otros campos

3. seleccione la opción "**Detalles**" para visualizar a la hoja de vida del dispositivo.





4. En la vista de información del dispositivo podrá seleccionar uno o varios dispositivos vinculados y configurar diferentes acciones disponibles como:

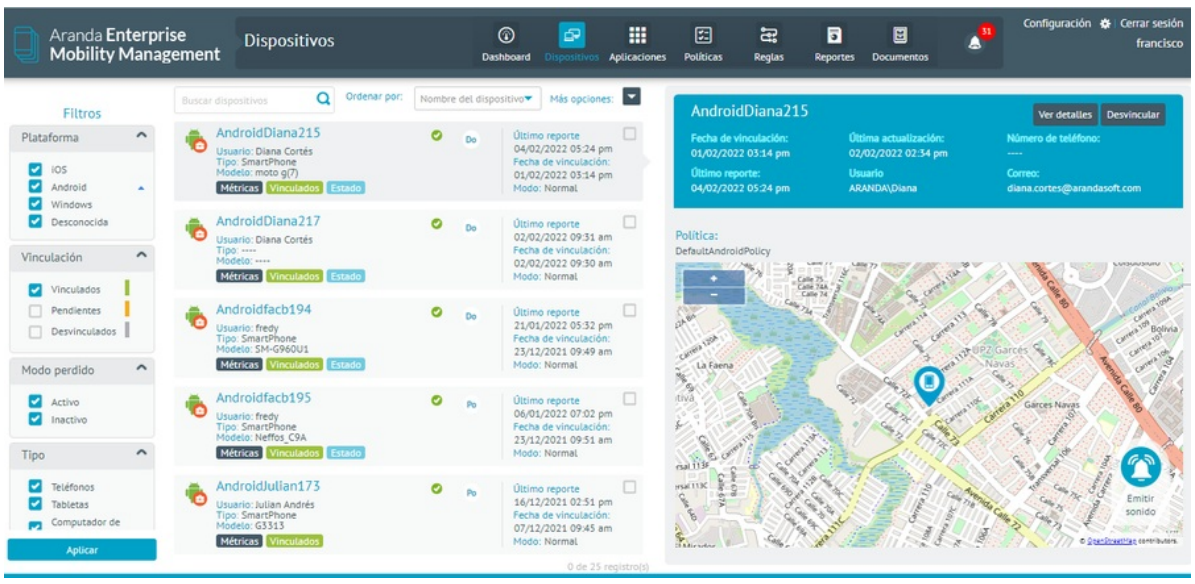


- Configurar seguimiento
- Reestablecer Dispositivo
- Mensaje
- Cambiar Perfil
- Bloquear
- Obtener Inventario
- Más opciones

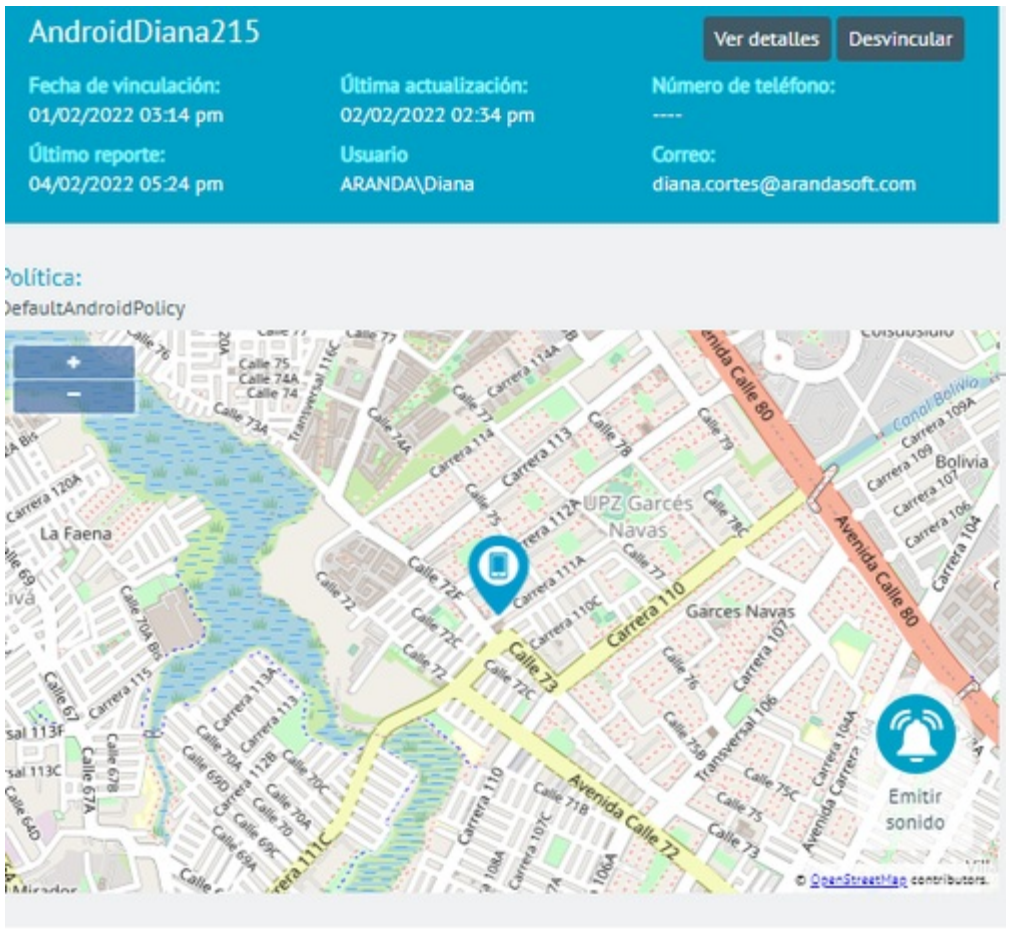
Hoja de vida de dispositivo

Visualizar Hoja de Vida del dispositivo

1. En la vista de información de la consola de inicio de AEMM ,podrá visualizar los dispositivos relacionados con los criterios definidos. Seleccione un dispositivo en estado vinculado y en la vista de detalle podrá visualizar en el mapa la información básica del elemento seleccionado.



2. Seleccione la opción “**Ver Detalles**” para visualizar a la hoja de vida del dispositivo. se carga la información detallada del dispositivo en particular, lo que se denomina **Hoja de vida dispositivo**



3. En la hoja de vida del dispositivo podrá visualizar la información principal del dispositivo y categorías asociadas al dispositivo.

Información principal del dispositivo

En esta sección se presenta información general relevante del estado actual del dispositivo.

En la parte superior de esta sección se presenta la siguiente información básica:

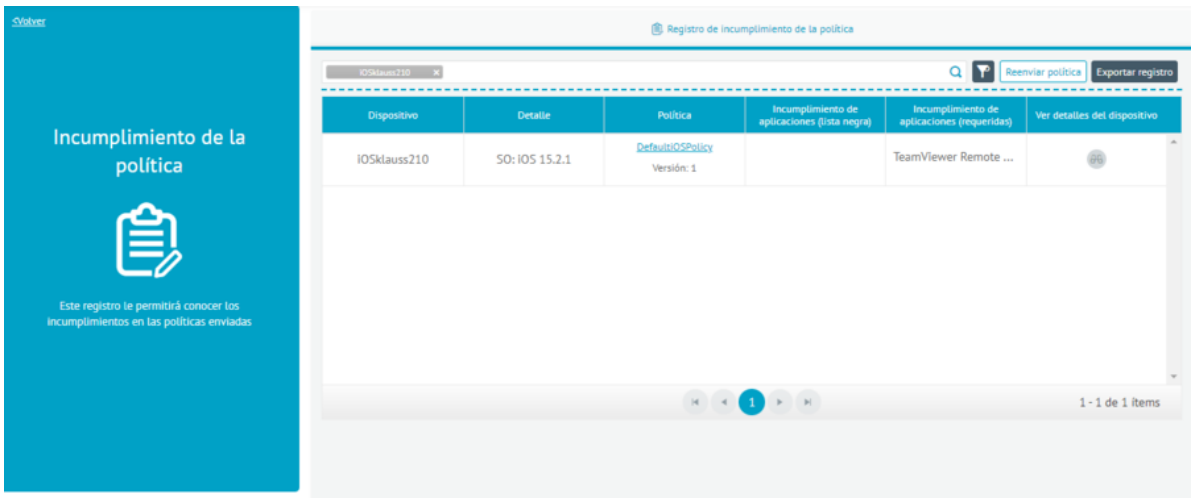
Nombre	Descripción
Ícono	Ícono de la plataforma del dispositivo (Android, iOS o Windows)
Nombre	Nombre del dispositivo
Tipo	Tipo del dispositivo (SmartPhone, Tableta o WorkStation)
Versión	Versión del Sistema Operativo instalado en el dispositivo
Número	Número de teléfono de la SIM activa en el dispositivo (Si está disponible)

A su vez esta sección tiene dos sub-secciones a saber:

Información General

Nombre	Descripción
Usuario responsable	Usuario asociado actualmente al dispositivo.En la opción de comandos individuales el administrador puede cambiar de usuario responsable; Tiene la opción de cambiar de grupo (a un nuevo usuario responsable) o que permanezca en el grupo ya asociado(es decir que no se haga ajuste de grupo, solo usuario responsable).
Política asignada	Nombre de la política actualmente aplicada al dispositivo.
Fecha de Aplicación	Fecha y hora en la que se aplicó la política al dispositivo.
Ver política	Acceso directo a la política aplicada.
Icono de cumplimiento	Aparece en Rojo, no cumple; No aparece: cumple.
Ruleset aplicado	Nombre del conjunto de reglas aplicado.
Fecha de aplicación	Fecha y hora en la que se aplicó el conjunto de reglas al dispositivo.
Ver ruleset	Acceso directo al conjunto de reglas aplicado.
Último log de dispositivo	Último log recibido del dispositivo y disponible para descarga.
Plan asignado	Nombre del plan de consumo asignado al dispositivo.
Fecha de aplicación	Fecha y hora en la que se aplicó el plan de consumo al dispositivo.
Perfil de agente	Nombre del perfil de agente aplicado al dispositivo.
Fecha de vinculación	Fecha y hora de vinculación del dispositivo en la instancia en cuestión de Aranda ENTERPRISE MOBILE MANAGEMENT AEMM.
Última actualización	Fecha y hora de la última actividad realizada en el dispositivo.
Último reporte	Fecha y hora de la última vez que el dispositivo se reportó al servidor AEMM.
Contenido bloqueado	Indica si el usuario tiene acceso o no a los archivos ycarpetas almacenados en la sección de documentos por medio de la aplicación Content Management.

En caso que el dispositivo, en la subsección Política asignada, presente el mensasje incumplimiento de la política, podrá hacer clic en dicho ícono y acceder al detalle del incumplimiento de la política:



En esta sección se podrán visualizar las aplicaciones que hacen que el dispositivo incumpla la política que actualmente tiene aplicada.

También se presentan las siguientes opciones:

- **Filtro**: Se pueden filtrar el listado presentado, por sistema operativo y política.
- **Reenviar política**: Encola un comando de política al dispositivo en cuestión con la política aplicada actualmente.
- **Exportar registro**: Exporta el listado presentado a un archivo Excel.

Acciones (Comandos)

Las acciones corresponden a comandos que se envían al dispositivo para que este a su vez los ejecute y reporte el resultado al servidor de Aranda ENTERPRISE MOBILE MANAGEMENT AEMM.

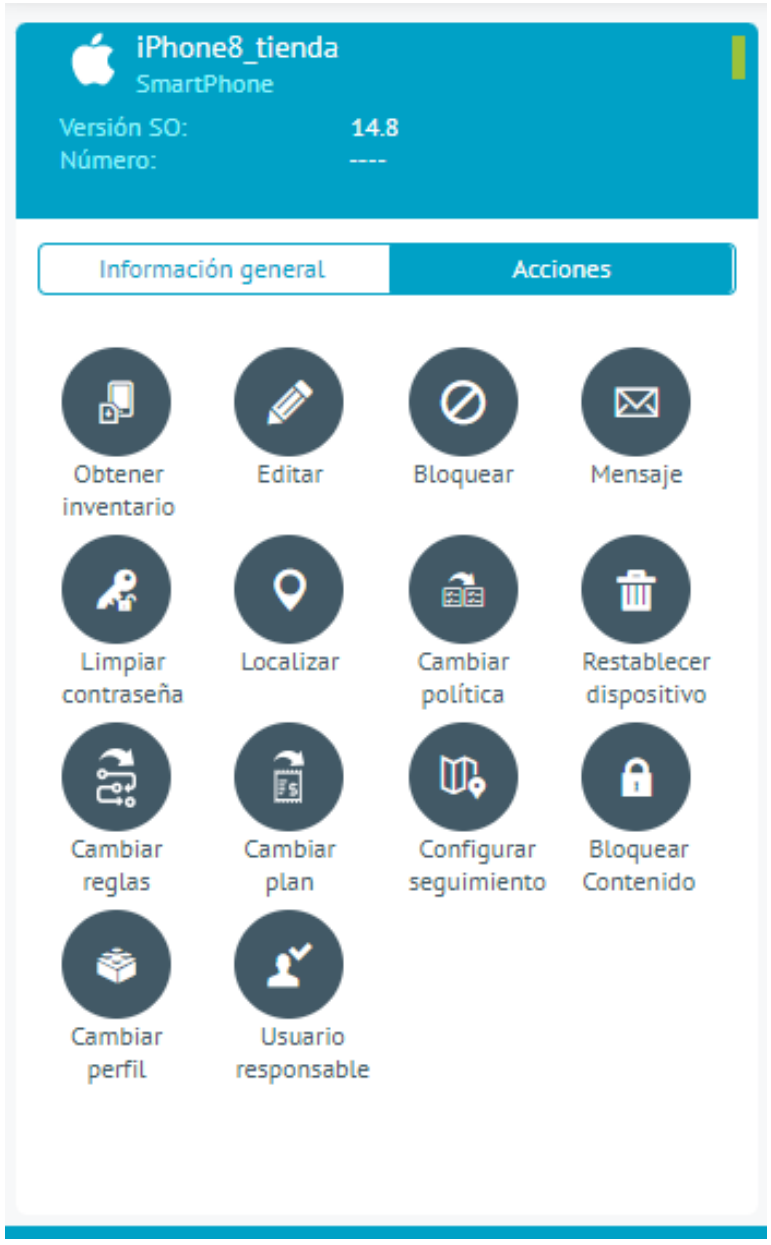
Las acciones disponibles cambian de acuerdo a la plataforma del dispositivo, a saber:

Android

Acción	Descripción
Obtener inventario	Recolecta información de Hardware, Software (aplicaciones instaladas) y ubicación actual (si está disponible).
Editar	actualizar el nombre del dispositivo, el número telefónico el tipo de propiedad (personal o compañía)
Activar modo perdido	Solo aplicable para dispositivos vinculados mediante Android For Work Device Owner. Bloquea el dispositivo para uso normal, permitiendo configurar la pantalla de bloqueo mostrada, que incluye: título, descripción, opción de seguimiento y una contraseña de desactivación del modo perdido.
Mensaje	Envía un mensaje visible en la barra de notificaciones del dispositivo y en la sección de mensajes en el agente.
Cambiar contraseña	Cambia la contraseña de desbloqueo del dispositivo, sujeta a las restricciones de contraseña que se hayan configurado en la política aplicada.
Cambiar contraseña perfil AFW	Solo aplicable para dispositivos vinculados mediante Android For Work Profile Owner. Cambia la contraseña de acceso al perfil de trabajo AFW creado en el dispositivo.
Localizar	Reporta la ubicación actual del dispositivo, siempre y cuando esté activada la localización en el dispositivo.
Control remoto	Solicita una sesión de control remoto en el dispositivo. Para control remoto completo debe del dispositivo haberse vinculado usando agentes Aranda for Samsung, Aranda for LG, Aranda for Cyrus y Aranda for Panasonic

Acción	Descripción
Cambiar política	Envía una política para ser asignada en el dispositivo.
Restablecer dispositivo	Restablece de fábrica el dispositivo.
Cambiar reglas	Envía un conjunto de reglas para ser aplicado en el dispositivo.
Cambiar plan	Envía un plan de consumo para ser aplicado en el dispositivo.
Configurar seguimiento	Envía solicitud de seguimiento al dispositivo, las opciones para seguimiento son: No seguir, Baja: Se reporta ubicación cada 60 minutos, Media: Se reporta ubicación cada 30 minutos, Alta: se reporta ubicación cada 5 minutos.
Bloquear contenido	Bloque el acceso a los contenidos al usuario responsable del dispositivo. Los contenidos bloqueados son configurados en la sección de documentos de la consola AEMM y accedidos por la aplicación móvil Content Management.
Cambiar perfil	Cambia el perfil de agente asignado al dispositivo
Usuario responsable	Cambia el usuario responsable del dispositivo.
Obtener paquetes ocultos	Solo aplicables a dispositivos vinculados mediante Android For Work Device Owner. Obtiene los paquetes que el mecanismo Android For Work oculta durante la vinculación.
Obtener Log	Obtiene el último log generado en agente instalado en el dispositivo.
Reiniciar	Reinicia el dispositivo, a menos que se encuentre una llamada en curso, en tal caso no será posible el reinicio y se reportará el error a servidor.
Métricas	Activa o desactiva la recolección de métricas de aplicaciones y la visualización de la interfaz de consulta de métricas en agentes móvil.
Estado del dipositivo	Activa o desactiva la recolección de datos de estado y su visualización en el agente instalado en el dispositivo.
Solicitar estado	Solicita al dispositivo un reporte de estado por demanda. Este comando sólo es visible si el dispositivo tiene el reporte de estado activado.
Protección Reset Android	Esta acción habilita el bloqueo de seguridad en el dispositivo al realizar el restablecimiento de fábrica
Deshabilitar protección reset Android	Esta acción elimina el bloqueo de seguridad en el dispositivo en el que se configuró la protección de restablecimiento de fábrica

iOS

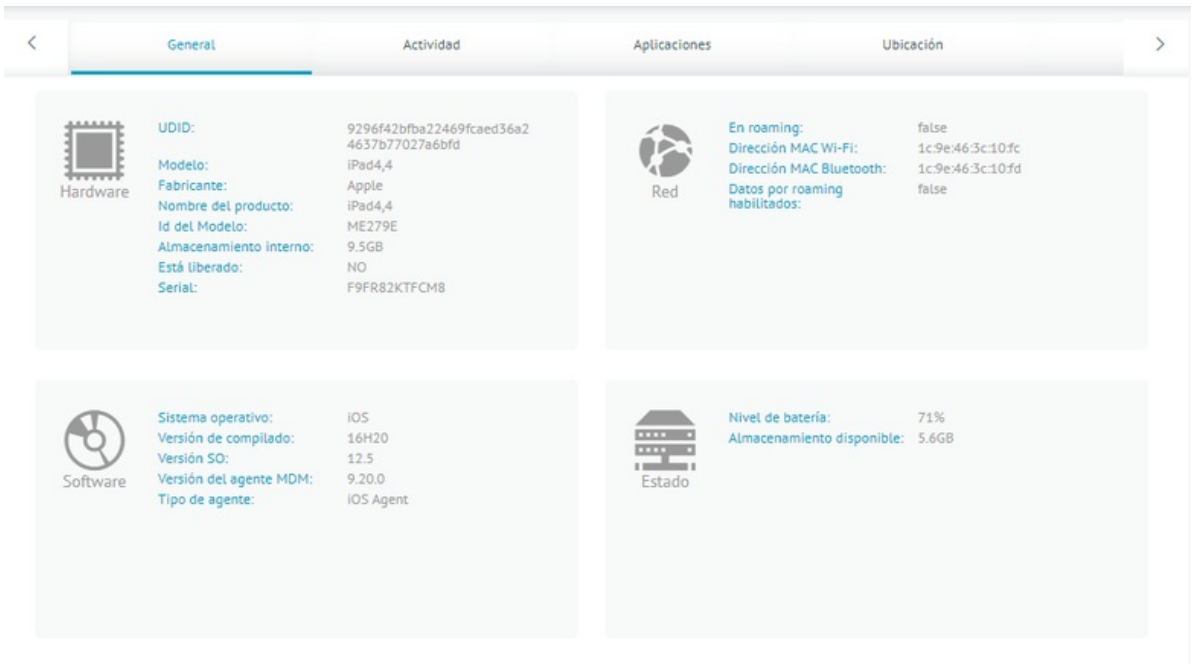

iPhone8_tienda
SmartPhone
Versión SO: 14.8
Número: ----
Información general
Acciones
Obtener inventario
Editar
Bloquear
Mensaje
Limpiar contraseña
Localizar
Cambiar política
Restablecer dispositivo
Cambiar reglas
Cambiar plan
Configurar seguimiento
Bloquear Contenido
Cambiar perfil
Usuario responsable

Nombre	Descripción
Obtener inventario	Recolecta información de Hardware, Software (aplicaciones instaladas) y ubicación actual (si está disponible).
Editar	Permite actualizar el nombre del dispositivo, el número telefónico y el tipo de propiedad (personal o compañía)
Bloquear	Bloquea el dispositivo, emulando la opresión del botón de bloqueo.
Mensaje	Envía un mensaje visible en la barra de notificaciones del dispositivo y en la sección de mensajes en el agente.
Limpiar contraseña	Quita la contraseña de desbloqueo del dispositivo
Localizar	Reporta la ubicación actual del dispositivo, siempre y cuando esté activada la localización en el dispositivo.
Cambiar política	Envía una política para ser asignada en el dispositivo.
Restablecer dispositivo	Restablece de fábrica el dispositivo.
Cambiar reglas	Envía un conjunto de reglas para ser aplicado en el dispositivo.
Cambiar plan	Envía un plan de consumo para ser aplicado en el dispositivo.
Configurar seguimiento	Envía solicitud de seguimiento al dispositivo, las opciones para seguimiento son: No seguir, Baja: Se reporta ubicación cada 60 minutos, Media: Se reporta ubicación cada 30 minutos, Alta: se reporta ubicación cada 5 minutos.
Bloquear contenido	Bloque el acceso a los contenidos al usuario responsable del dispositivo. Los contenidos bloqueados son configurados en la sección de documentos de la consola Aranda ENTERPRISE MONILE MANAGEMENT AEMM y accedidos por la aplicación móvil Content Management.
Cambiar perfil	Cambia el perfil de agente asignado al dispositivo.
Usuario responsable	Cambia el usuario responsable del dispositivo.

1. En la hoja de vida del dispositivo de la consola principal de AEMM, podrá visualizar en Categorías información asociada al dispositivo vinculado, tales como información general, actividad, aplicaciones,

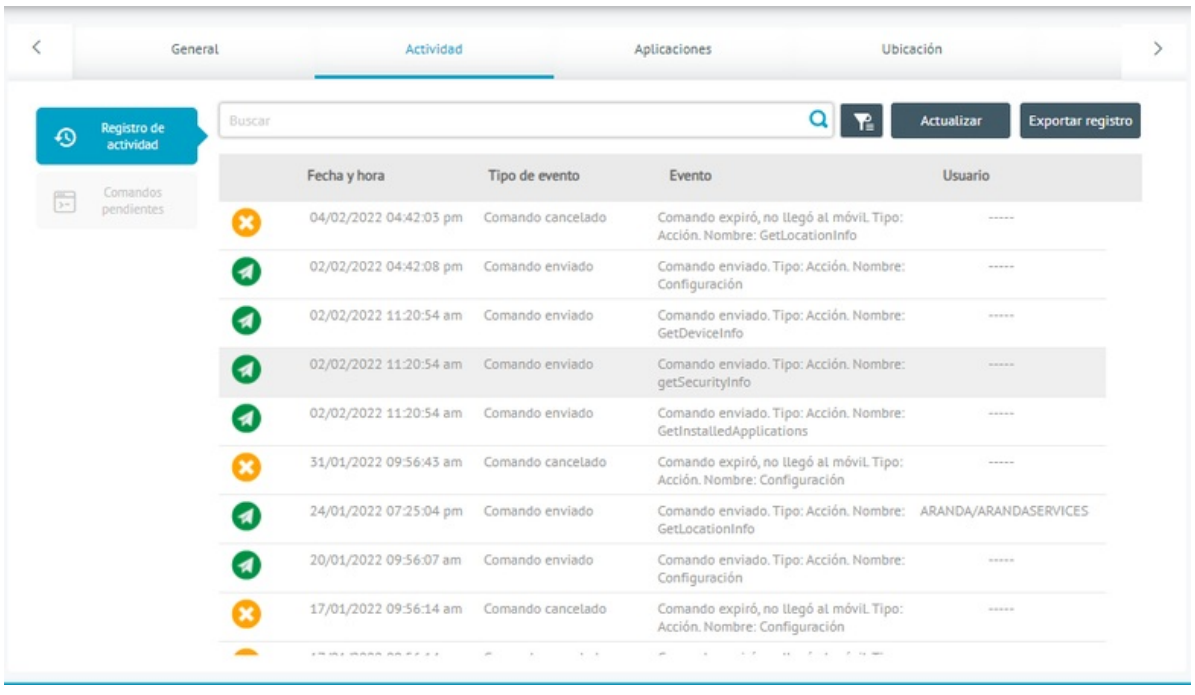
Pestaña General

Permite ver información de hardware (Fabricante, modelo, IMEI, espacio disponible, etc..), software (Sistema operativo, versión de agente, versión del SO, etc..), red (ICCID o identificador de SIM card, MAC de wifi, MAC de bluetooth, roaming habilitado, operador de la SIM card, etc.) y estado (nivel de batería, almacenamiento disponible, etc.). La cantidad de información desplegada en cada una de estas secciones varía de acuerdo a la plataforma y el fabricante del dispositivo.



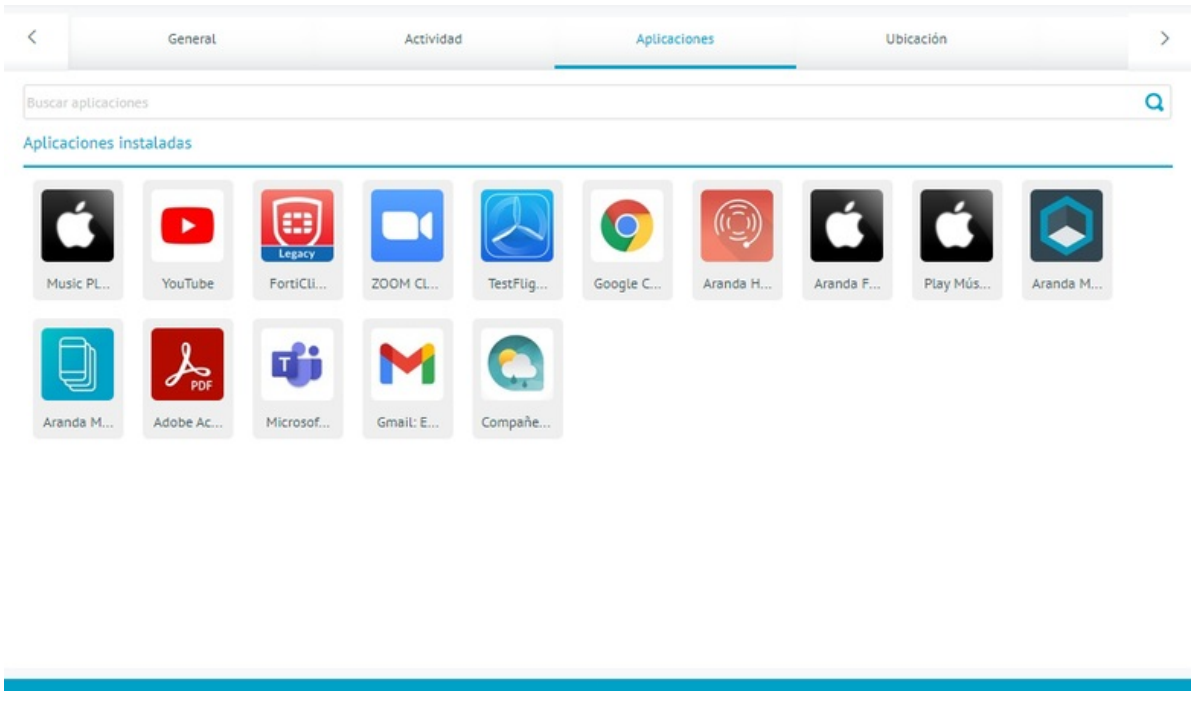
Pestaña Actividad

Permite ver un listado de todos los eventos ocurridos en el móvil, ordenados por fecha de ocurrencia. Este listado de actividad muestra el ciclo de vida de los comandos (envío, recepción en el móvil y ejecución), así como los eventos registrados (envío de localización, salida o entrada de zonas, desvinculación, etc.)



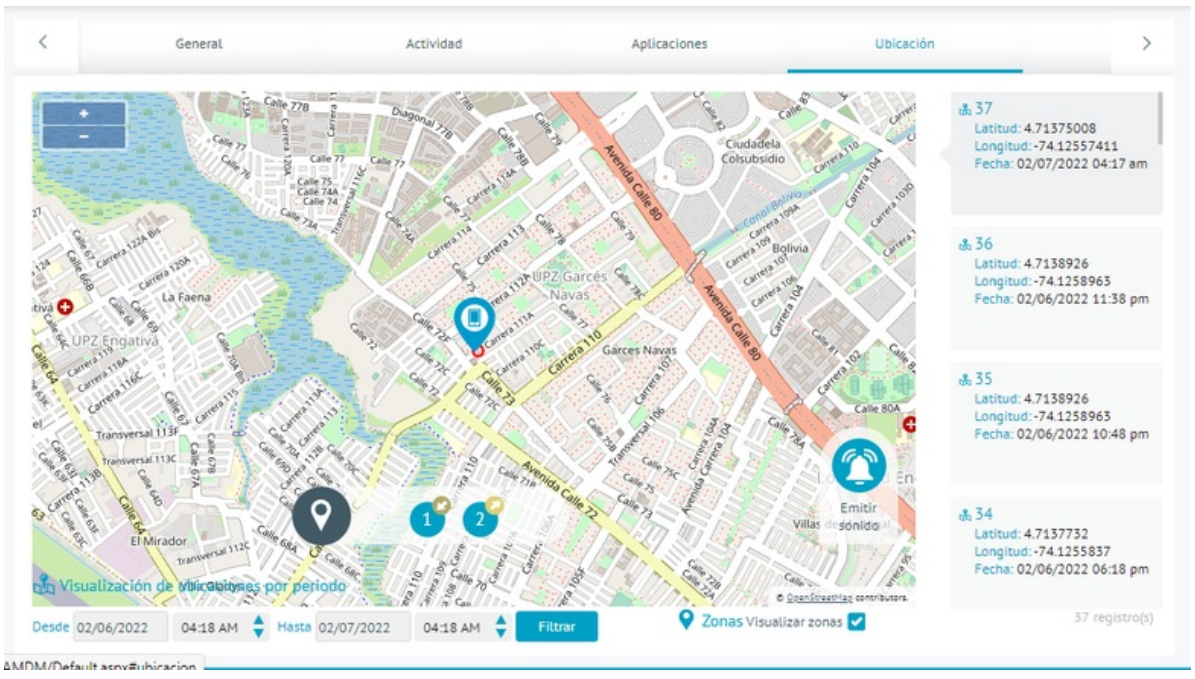
Pestaña Aplicaciones

Permite ver el listado de aplicaciones instaladas en el móvil de acuerdo al último reporte recibido. Cada aplicación permite seleccionarse en esta lista para mostrar información detallada (descripción, categoría, etc..). En esta pantalla se puede solicitar la desinstalación de la aplicación, lo cual genera el envío del comando respectivo al móvil. En Android genérico la desinstalación se realiza con la aprobación del usuario; en Samsung se desinstalan de manera silenciosa; en iOS la desinstalación ocurre de manera silenciosa pero sólo para aplicaciones instaladas desde el EMM. Desde aquí también se pueden instalar aplicaciones en el móvil. Cuando el comando de instalación se ejecuta en el móvil iOS o en Android genérico se pide automáticamente una confirmación al usuario. En móviles Samsung se muestra primero una notificación simple al usuario por algunos segundos y luego se instala sin requerir confirmación.



Pestaña Ubicación

Permite ver la localización del dispositivo en un mapa de manera clara y con todas las opciones de navegación necesarias. Desde esta pantalla se puede enviar un comando de alerta sonora para ubicar el dispositivo dentro de una oficina o algún otro espacio cerrado.



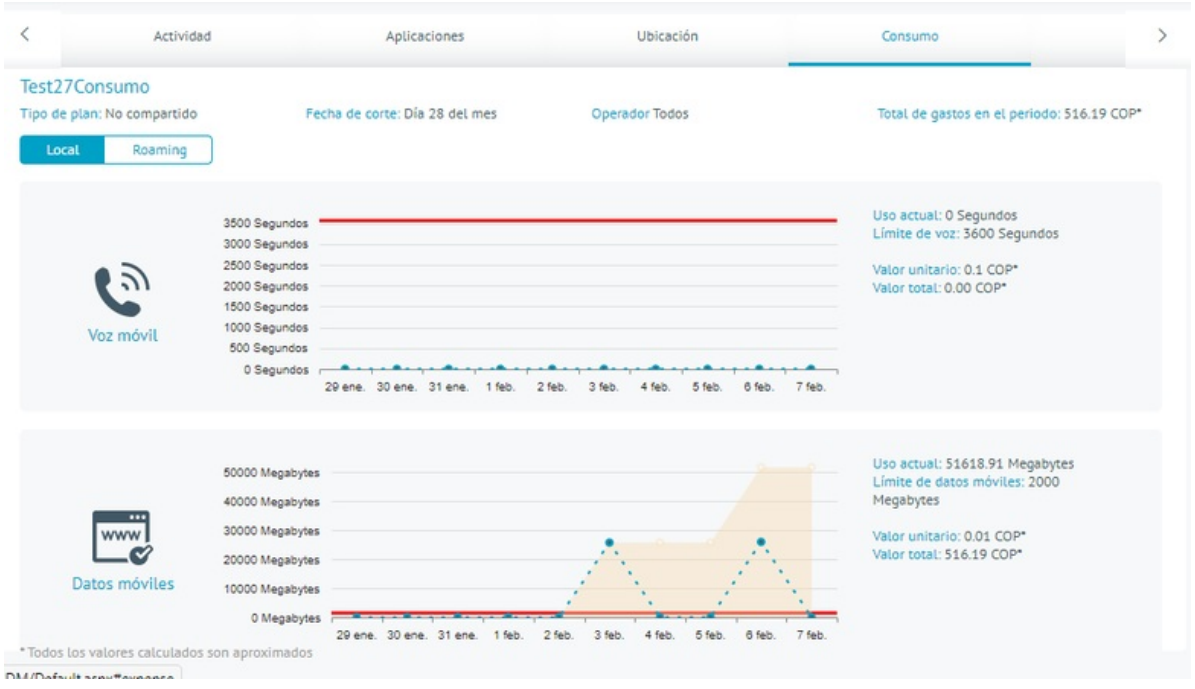
En esta pestaña se encuentra incluída la funcionalidad de **Emitir sonido**. Esto lo que hace es enviar un comando (o evento) al dispositivo el cual activa una alerta sonora. Esta funcionalidad sirve como ayuda para encontrar el dispositivo en caso de que se encuentre perdido

> ⚐ **Nota:** - Para los dispositivos Xiaomi vinculados con Profile Owner (PO) se presenta problemas con esta funcionalidad.
>
> Se recomienda que para el correcto funcionamiento del emitir sonido acceda a los permisos de las aplicaciones del perfil de trabajo. Para hacerlo debe de ir a Configuración->Aplicaciones->Administrar aplicaciones, desplegar el menú de los 3 puntos que está en la parte superior derecha y escoger la opción **Mostrar aplicaciones del espacio de trabajo**, seleccionar la aplicación **AndaEMM** que tiene un ícono de portafolio e ingresar a la opción **Otros permisos**. Habilitar los permisos **Mostrar en pantalla de bloqueo** y **Abrir nuevas ventanas mientras se ejecuta en segundo plano**.

Pestaña Consumo

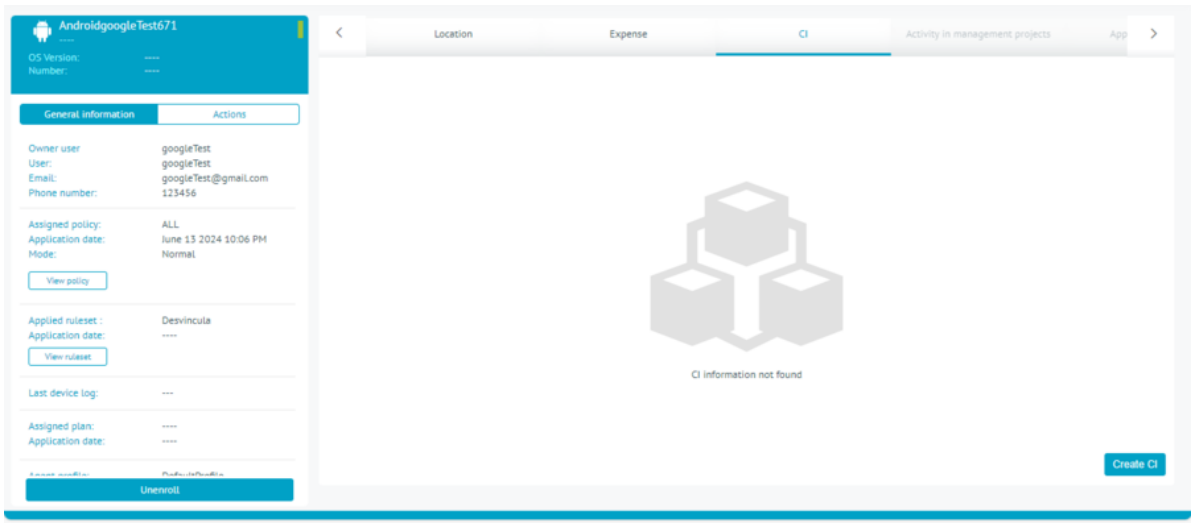
Esta opción permite ver una gráfica detallada del consumo del plan telefónico tanto de voz como de datos; también se podrá observar el plan que tiene asignado el dispositivo y ver los consumos locales de roaming, en caso de tener el servicio activado.

El consumo de voz móvil es visualizado en segundos y el plan de voz en Gigabytes.

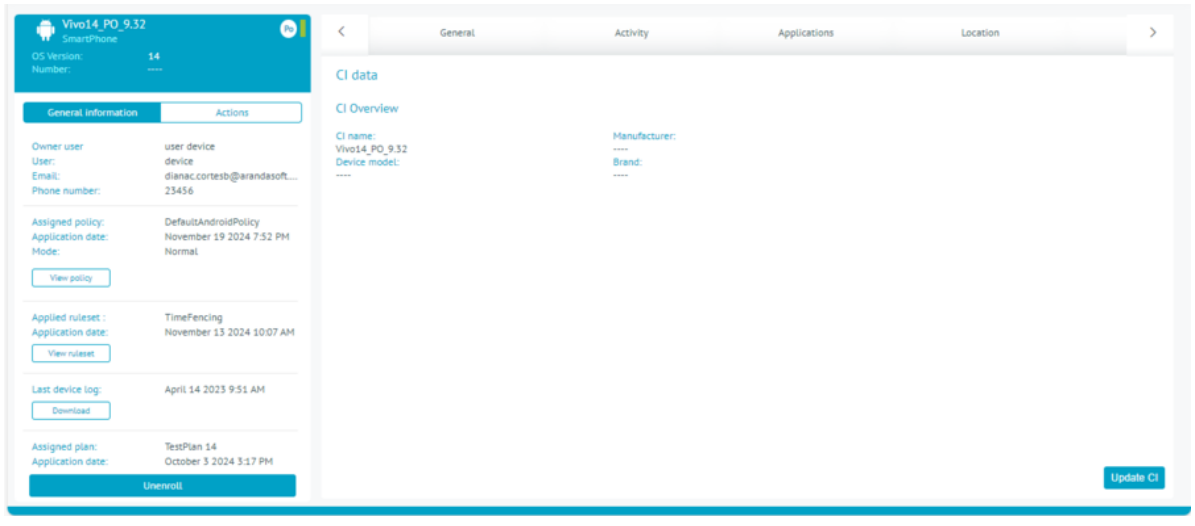


CI

En esta pestaña se presentan los datos obtenidos desde con la integración realizada con la CMDB, en caso de no existir un CI creado se puede ejecutar la creación de forma manual utilizando el botón **Crear CI**



Cuando ya existe un CI creado e integrado con la consola de AEMM se puede actualizar de forma manual utilizando el botón de **Actualizar CI**



Tener en cuenta que al momento de enviar un comando de obtener inventario o vincular un dispositivo con una configuración de CMDB activa generará las acciones de crear y/o actualizar CI respectivamente.

> ⚐ **Nota:** Al momento de desvincular un dispositivo se inactivará de forma automática el CI creado en los servicios de CMDB.

Pestaña Métricas

En esta pestaña se presentan las estadísticas basadas en métricas de consumo de datos y uso de las aplicaciones en el dispostiivo. Esta pestaña sólo se activará cuando la recolección de métricas global este activada y el dispositivo tenga activada la opcion de recolectar métricas. En la parte superior podrá seleccionar el rango de tiempo en la que se consultará la información; por defecto se carga como fecha el día actual que se valida la métrica, semana y meses.

Tabla de Detalles de Métricas Consolidada

Esta tabla presenta las aplicaciones que reportaron consumo de datos, al menos en una ocasión, o uso en el dispositivo durante el intervalo de tiempo escogido. Esta información se ordena descendentemente por la columna consumo de datos.

Columnas de la tabla:

- Aplicación: Nombre de la aplicación

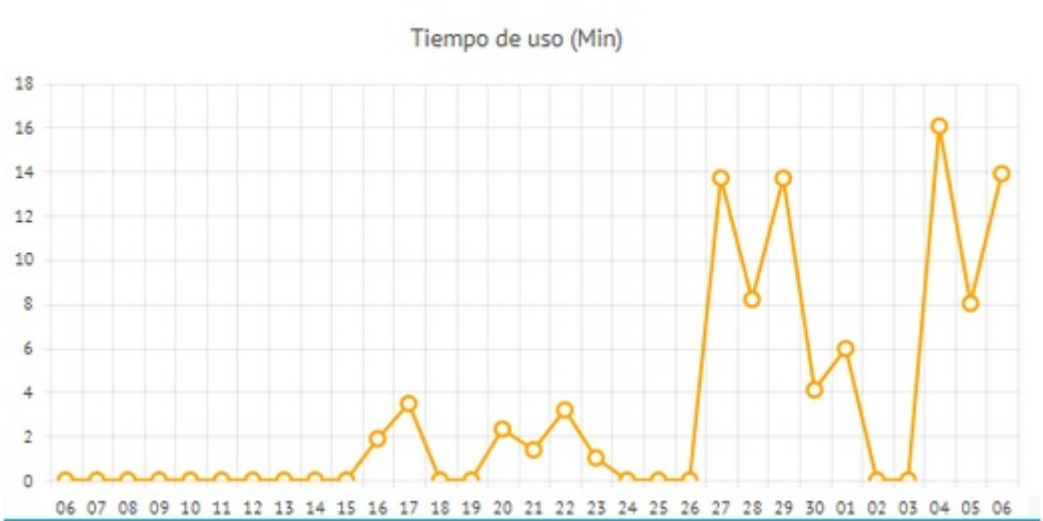
- Consumo de datos: Consumo total de datos en el intervalo de tiempo escogido
- Tiempo de uso: Tiempo de uso total en el intervalo de tiempo escogido
- Instalada: Presenta un ícono verde de verficación cuando la aplicación se reportó como instalada durante el último inventario reportado por el dispositivo; en caos contrario, se presenta un ícono rojo de "X" que indica que la aplicación no se reportó como instalada.

Al seleccionar cada fila de la tabla, se filtran automáticamente las dos siguientes gráficas de acuerdo a la aplicación seleccionada.

Gráfico de Consumo de datos vs Día

Presenta el consumo en Mega Bytes de la aplicación por cada día en el intervalo de tiempo escogido.

Gráfico de Uso vs Día



Presenta el uso de la aplicación en minutos por cada día en el intervalo de tiempo escogido.

Pestaña Estado del Dispositivo

Se presenta el estado actual de acuerdo al último reporte de estado enviado por el dispositivo.

Por cada categoría se presenta lo siguiente:

- Valor actual
- Dato actual

- Color indicativo:

- Verde: OK
- Rojo: En riesgo
- Gris: No disponible / No aplica

El color indicativo depende de los valores configurados en los umbrales para estado del dispositivo, disponible en Configuración -> Preferencias -> Estado del dispositivo

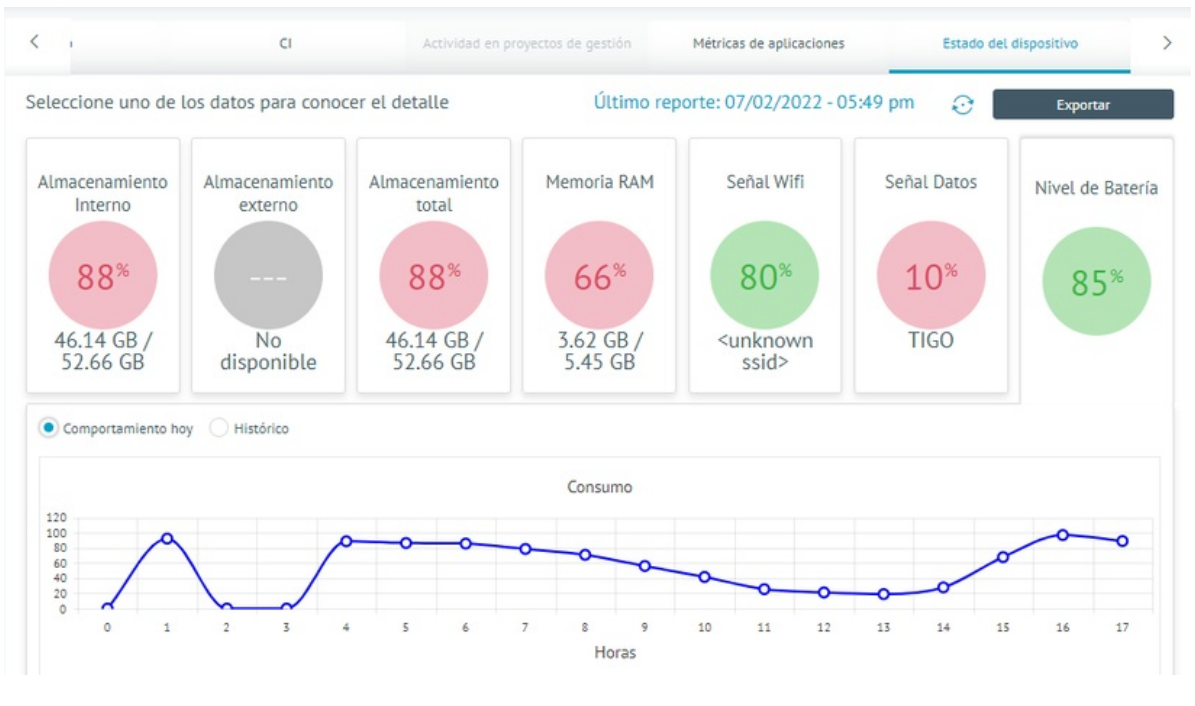
Detalle de cada Categoría

Para las siguientes categorias de reporte de estado:

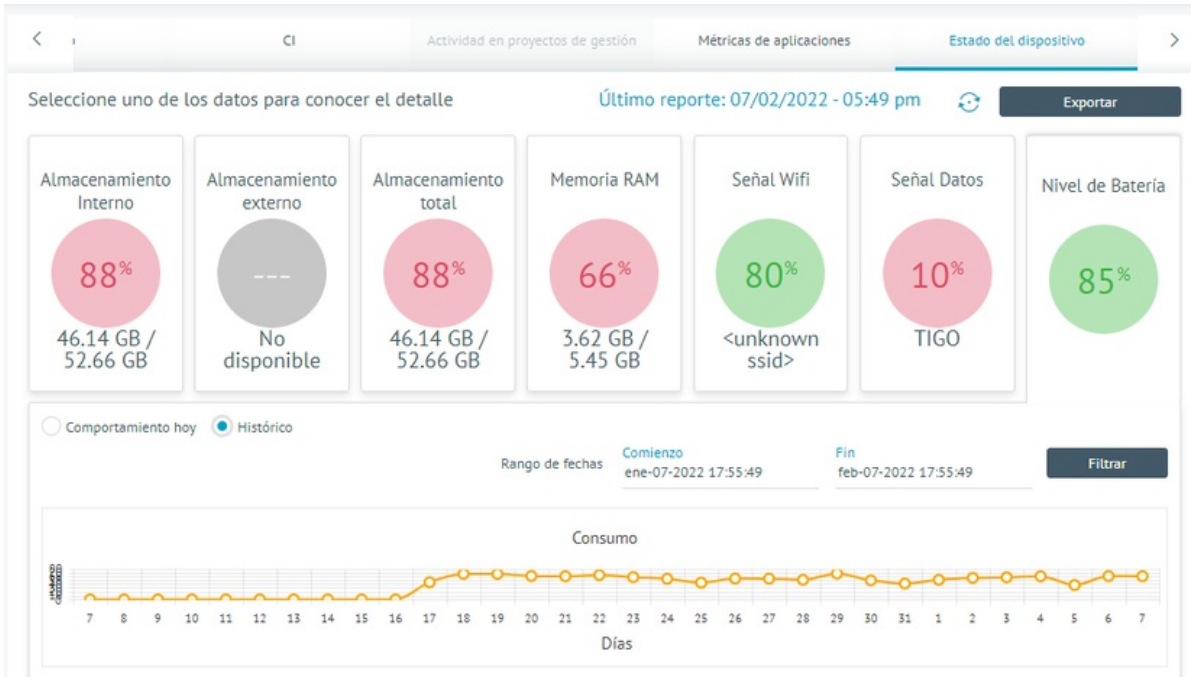
- Almacenamiento interno
- Almacenamiento externo
- Almacenamiento total
- Memoria RAM
- Nivel de Batería

Al dar clic sobre el ícono del valor actual se presentará un gráfico del comportamiento de la categoria en el tiempo, siendo posbile ver el comportamento del día de hoy, así como un dato histórico tentativo a ser filtrado por fechas.

Comportamiento para el presente día:



Comportamiento histórico



Problemas comunes en manejo de dispositivos

El comando no llega al dispositivo

Los dispositivos deben tener conexión a Internet para poder recibir los comandos. El tiempo de recepción depende mucho de la velocidad de la red en el móvil y en el canal del servidor. Si un comando no ha llegado es posible que el móvil esté apagado, o que la conexión esté lenta. En ambos casos el comando llegará cuando las condiciones cambien. Algunos comandos son procesados directamente por la aplicación agente. Si el agente fue suspendido manualmente no recibirá comandos, será necesario en este caso abrir la aplicación en el móvil para retomar la comunicación. Este problema se evidencia cuando en la línea de tiempo solo se muestra el mensaje de envío de comando.

Se envían muchos comandos y solo llega uno

Cuando se envía un comando a un móvil, el sistema automáticamente bloquea el envío de más comandos del mismo tipo, hasta que el primero termine su ciclo de vida. Se recomienda simplemente esperar a que el primero termine.

El comando de localización retorna un error

En la línea de tiempo se puede observar un error en el comando de localización cuando en el móvil el usuario decide deshabilitar la localización para la app. Esta situación escapa del control del EMM, ya que el usuario siempre es libre de decidir si quiere o no que lo ubiquen a través de su móvil.

El comando no se puede ejecutar en el momento

En la línea de tiempo se puede observar una advertencia en el comando de política cuando el dispositivo iOS no está disponible para procesar peticiones del EMM. Normalmente esto sucede cuando el dispositivo está bloqueado. Si esto sucede se recomienda esperar a que el dispositivo esté disponible y vaya automáticamente a recibir el comando. Normalmente el dispositivo queda disponible cuando el usuario enciende la pantalla.

En iOS la política llega, pero no se ve la descripción en el móvil

La descripción de la política aplicada es manejada exclusivamente por la aplicación agente. En iOS las políticas se despachan directamente al sistema operativo con un protocolo diferente. Puede que la comunicación con la aplicación agente sea más lenta en algunos casos. Cuando esto sucede se recomienda simplemente esperar. En

cualquier caso, si el usuario abre la aplicación agente, la descripción llegará.

El comando de sonido se percibe en el móvil como un comando de mensaje

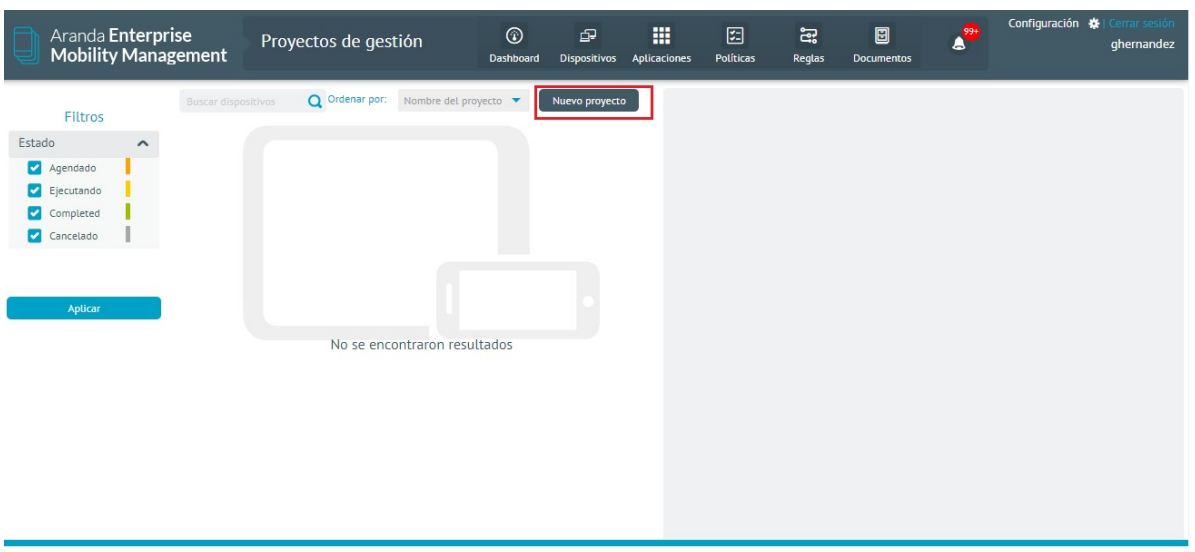
Si el dispositivo tiene deshabilitado el sonido, el comando de alerta sonora y solo se verá como un mensaje. El EMM no tiene forma de forzar la habilitación del sonido cuando el usuario lo ha impedido a propósito.

Proyectos de Gestión

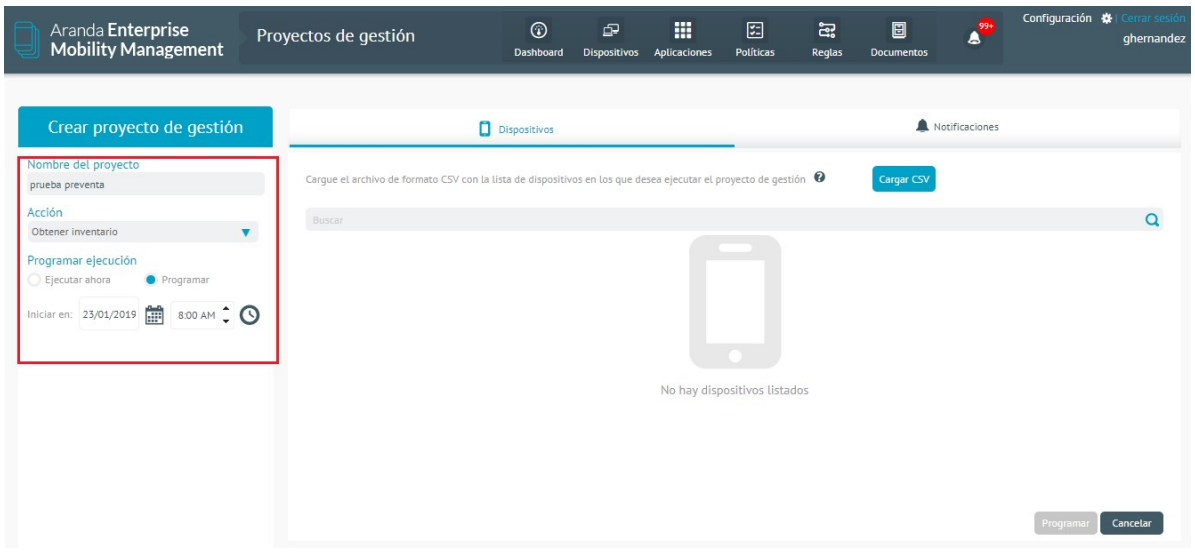
Esta función permite crear grupos (Proyectos) de dispositivos y realizar envío el envío de configuraciones a estos de manera unificada o masiva. Esto se realiza a través de la creación de un archivo .CSV con el Imei de los equipos a los cuales se les enviará la configuración.

De clic en la pestaña Dispositivos y seleccione Proyectos de Gestión.

Luego de clic en la opción **Nuevo proyecto**.

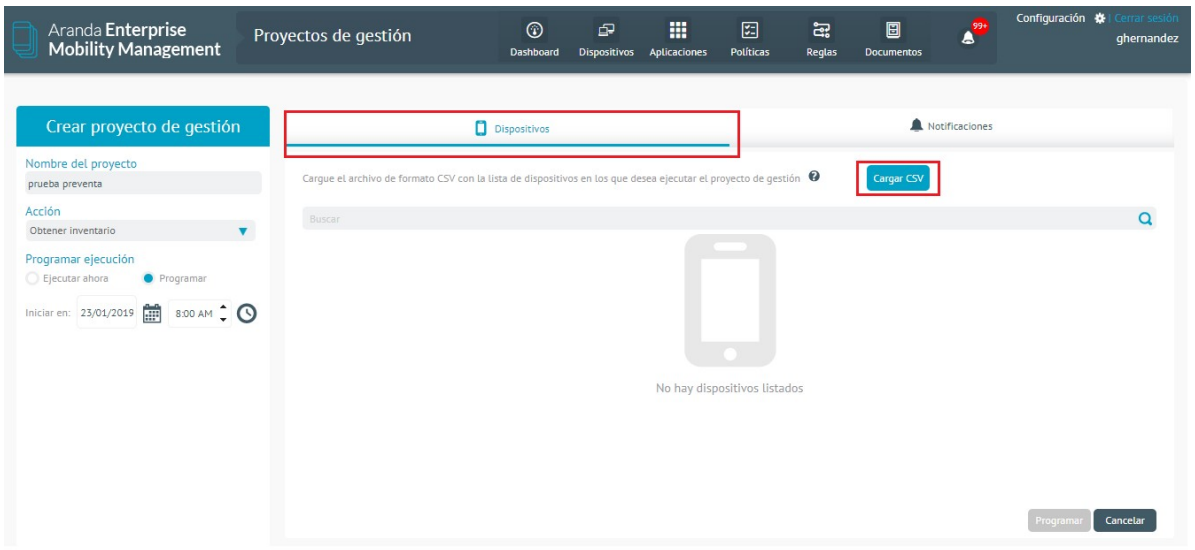


En el costado derecho, diligencie los datos del proyecto y la acción a tomar para este grupo (Dispositivos). Esta opción también le permite programar la ejecución ya sea de manera inmediata o alguna fecha y hora específica.

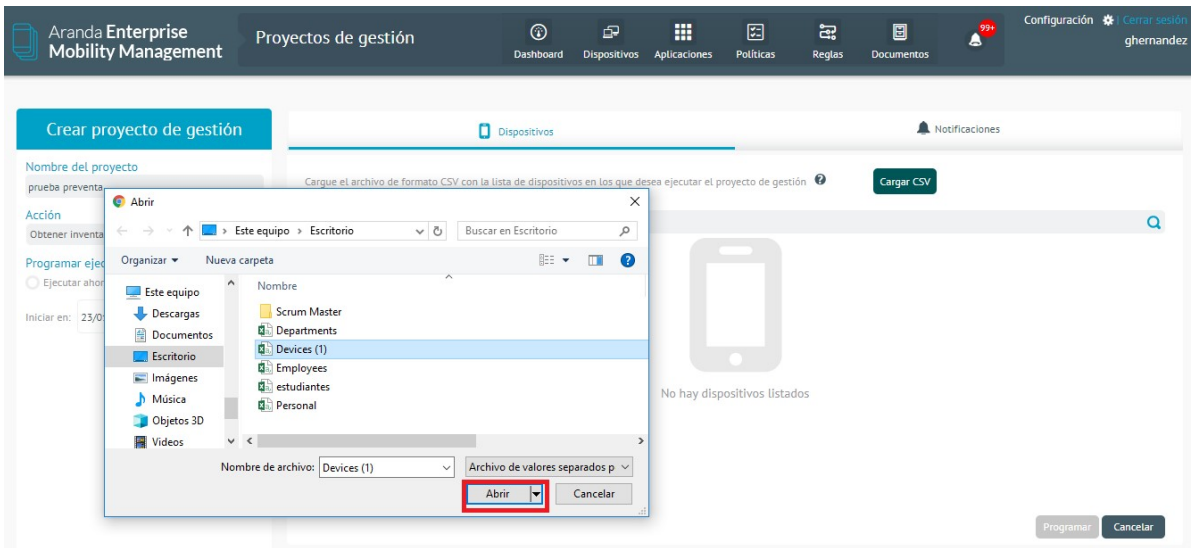


Carga de Dispositivos al Proyecto de Gestión

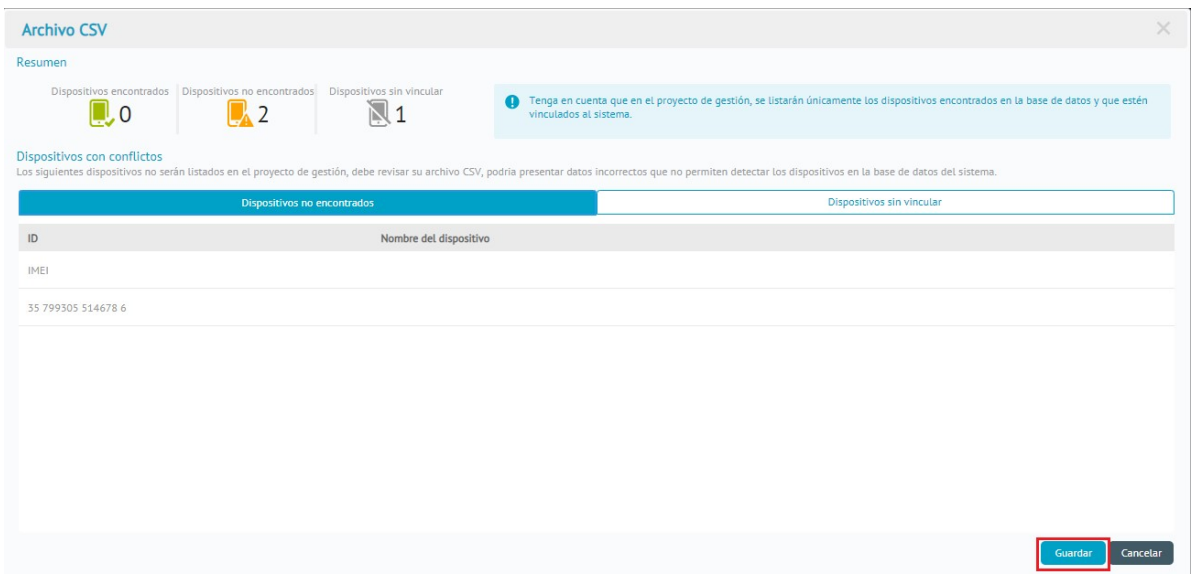
Cree el listado un archivo de Excel con los números de Imei de los dispositivos y guardarlo como archivo .csv, luego de lic en la opción Cargar CSV y cargue el archivo.



Exporte el archivo CSV en la ruta en la cual lo tenga almacenado y de clic en **Abrir**.

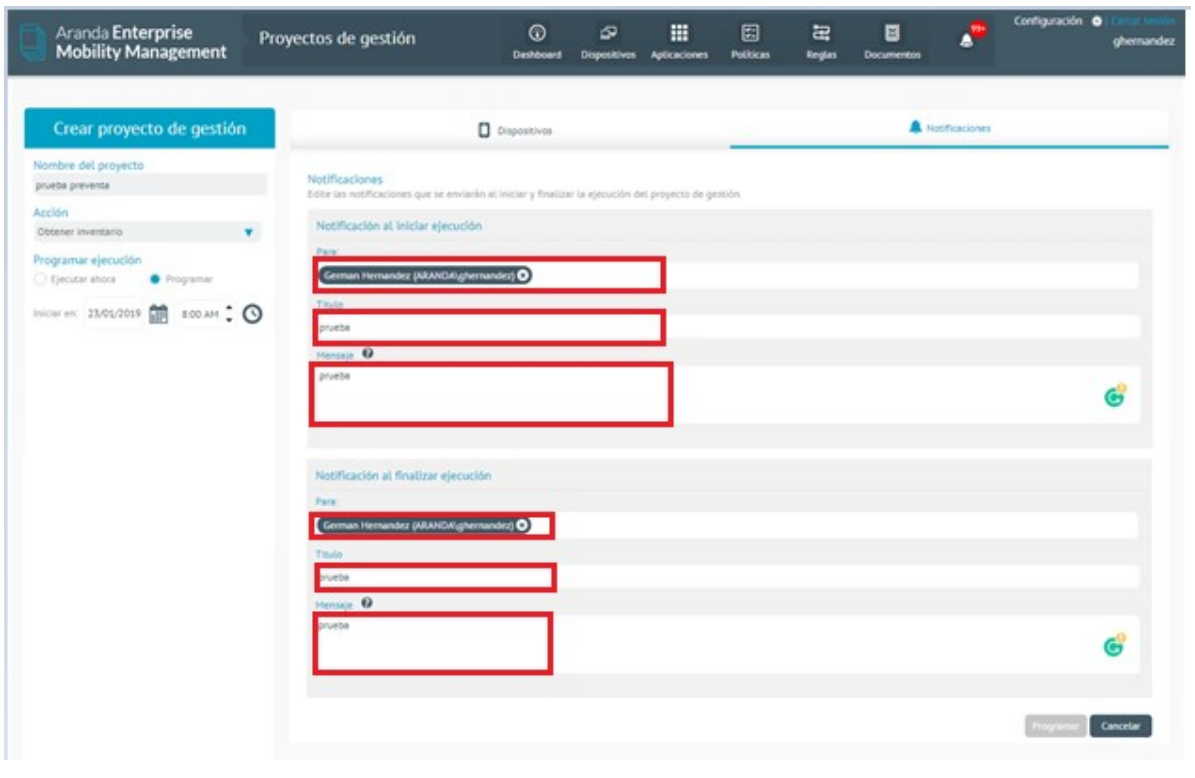


Luego de clic en **Guardar**



Configuración de Notificaciones

En esta opción, configure los usuarios a los que desea enviarle notificación cuando inicie la ejecución del proyecto al igual que cuando esta culmine.

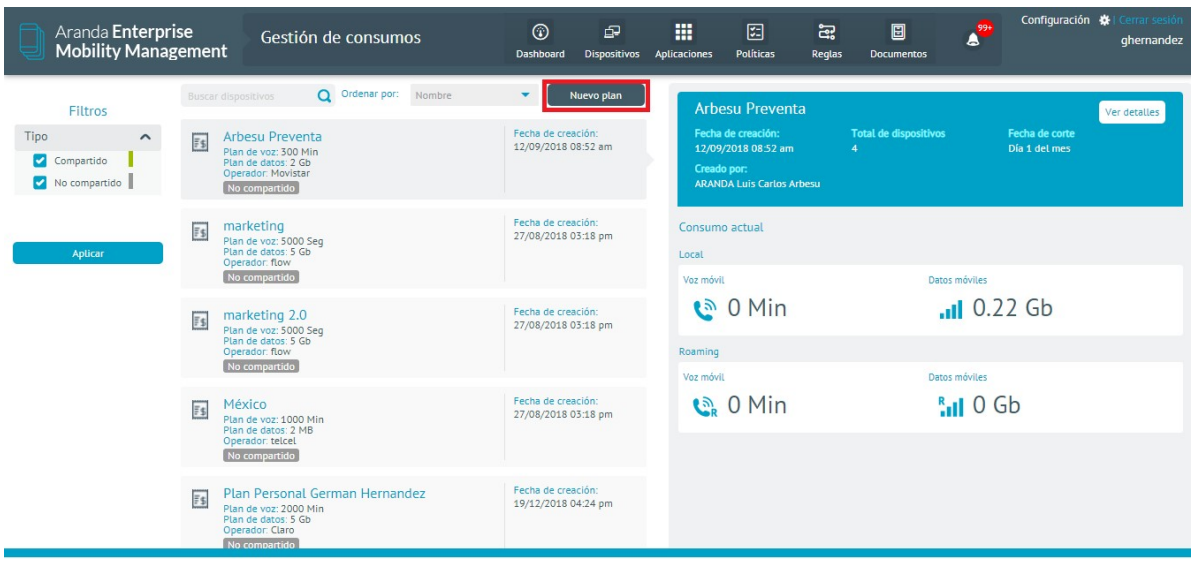


Luego de clic en **Programar**.

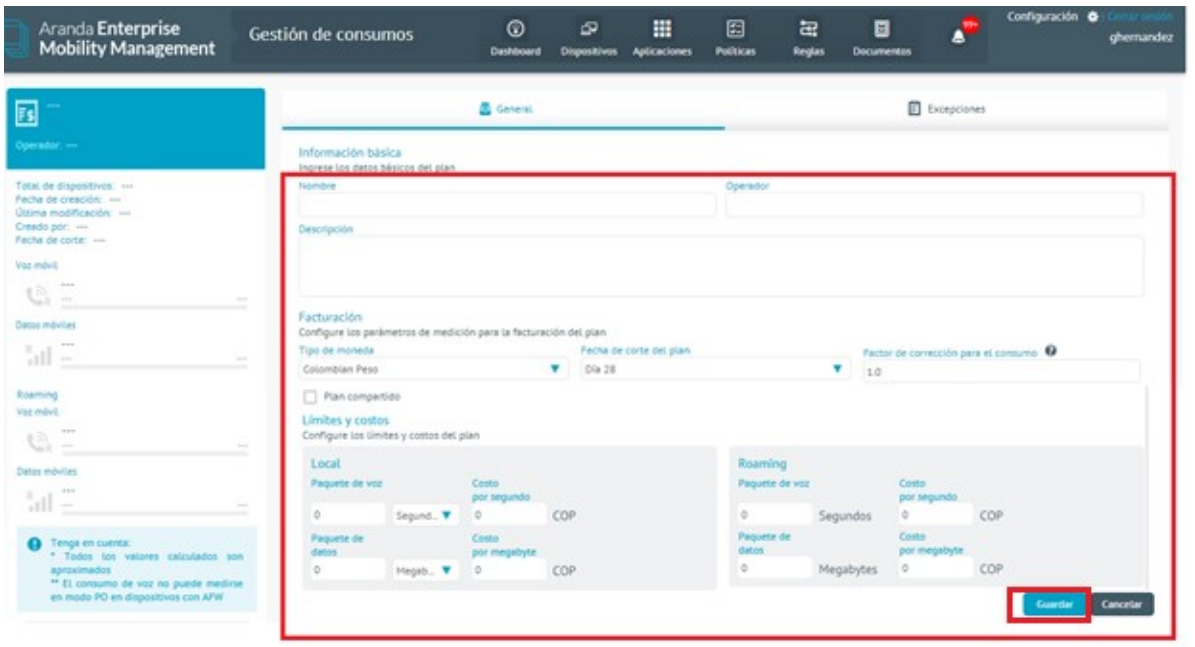
Gestión de Consumos

Esta opción se debe configurar si se desea realizar un seguimiento al consumo de voz y/o datos de un dispositivo móvil y para hacer uso del conjunto de reglas de gastos. A continuación:

Ingrese a pestaña Dispositivos y seleccione la opción **Gestión de Consumos** dentro del menú EMM y de clic en **Nuevo Plan.**



Ingrese los datos solicitados y de clic en **Guardar**.

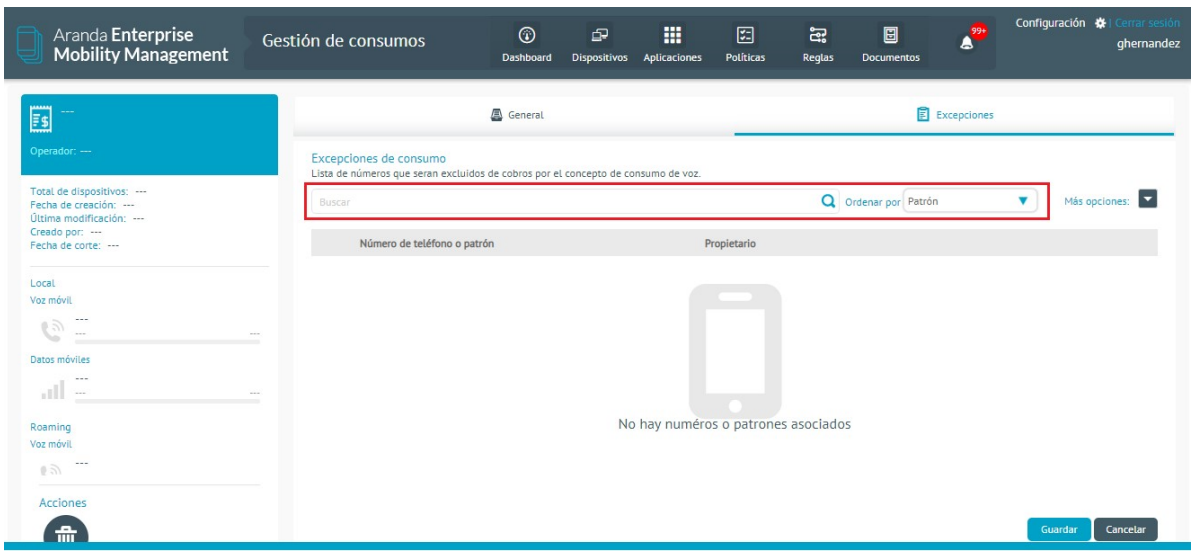


Excepciones

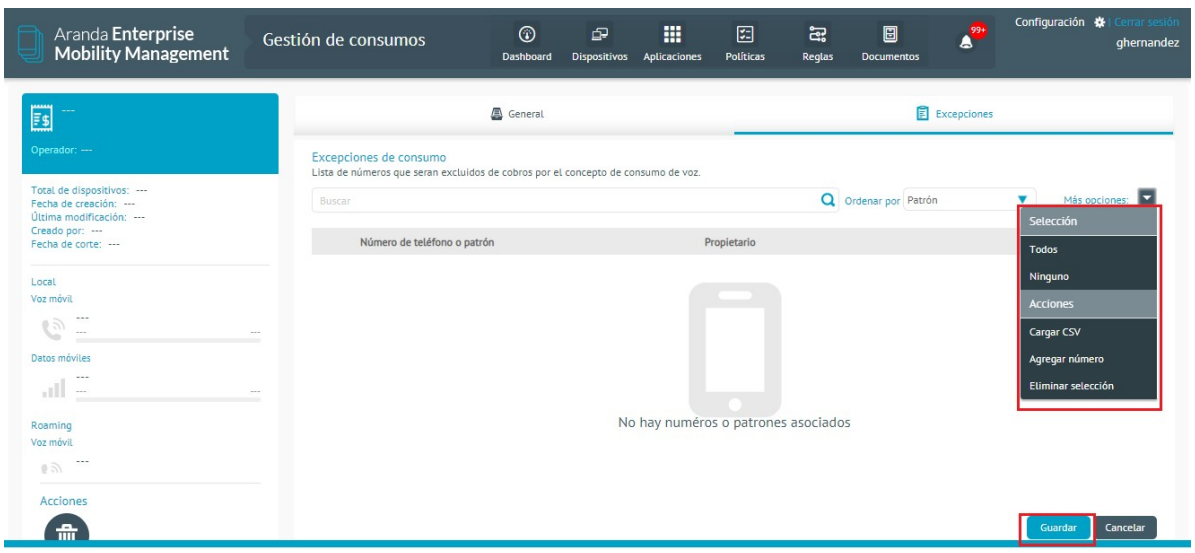
Para crear una excepción de consumo, esta se puede llevar a cabo de varias formas:

- Realizando búsqueda del número del dispositivo a través de la opción Buscar, ordenando a la vez por patrón o

propietario



- La otra opción es, seleccionar un grupo de números o dispositivos cargando un archivo CSV con el listado de dispositivos a los cuales desea realizar la excepción y luego de clic en el botón **Guardar**.



Detalle en Dispositivos Móviles

En el Agente (consola móvil AEMM) podrá acceder a la vista detalle del dispositivo donde podrá encontrar:

Campo	Descripción
Información Básica Dispositivo:	En esta sección podrá consultar datos como: la fecha del último reporte enviado al dispositivo, nombre e id del dispositivo, versión del agente instalado y referencia de la consola a la que está vinculado el dispositivo.
Acciones:	En esta sección podrá realizar las siguientes tareas: - *Desvincular*: Al seleccionar este botón se desvincula el dispositivo asociado. Esta opción sólo aplica para dispositivos PO. - *Ver Detalle*: Al seleccionar este botón podrá al detalle de la política que tiene asociado el dispositivo. - *Enviar Correo*: Al seleccionar este botón podrá enviar los logs generados al correo asociado al dispositivo.

Acciones en Dispositivos

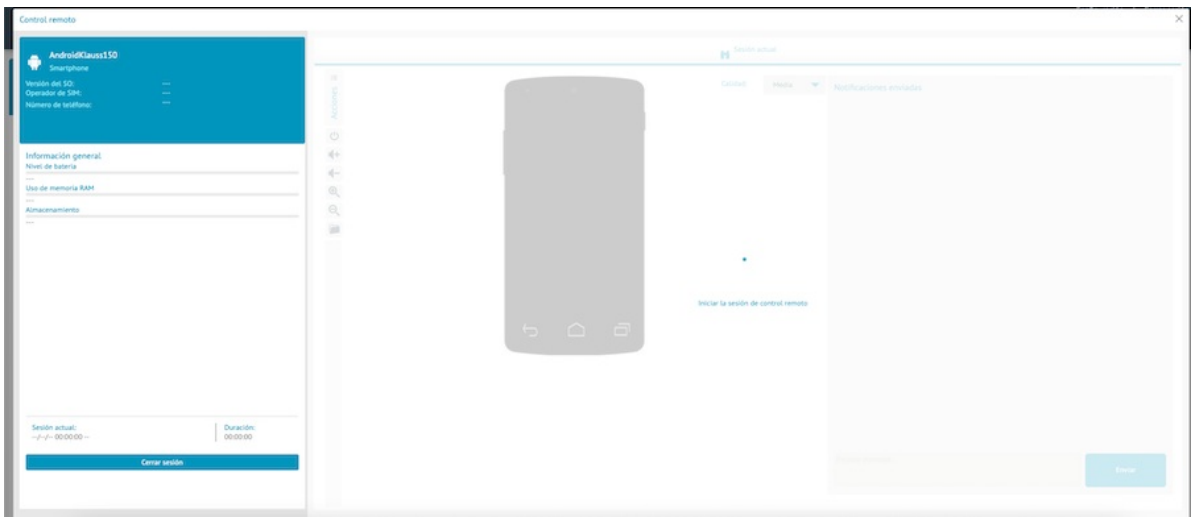
En la vista de información de la consola de inicio de AEMM ,podrá visualizar Acciones (Comandos). Las acciones corresponden a comandos que se envían al dispositivo para que éste a su vez los ejecute y reporte el resultado al servidor de Aranda ENTERPRISE MOBILE MANNAGEMENT AEMM.

Las acciones disponibles cambian de acuerdo a la plataforma del dispositivo, a saber:

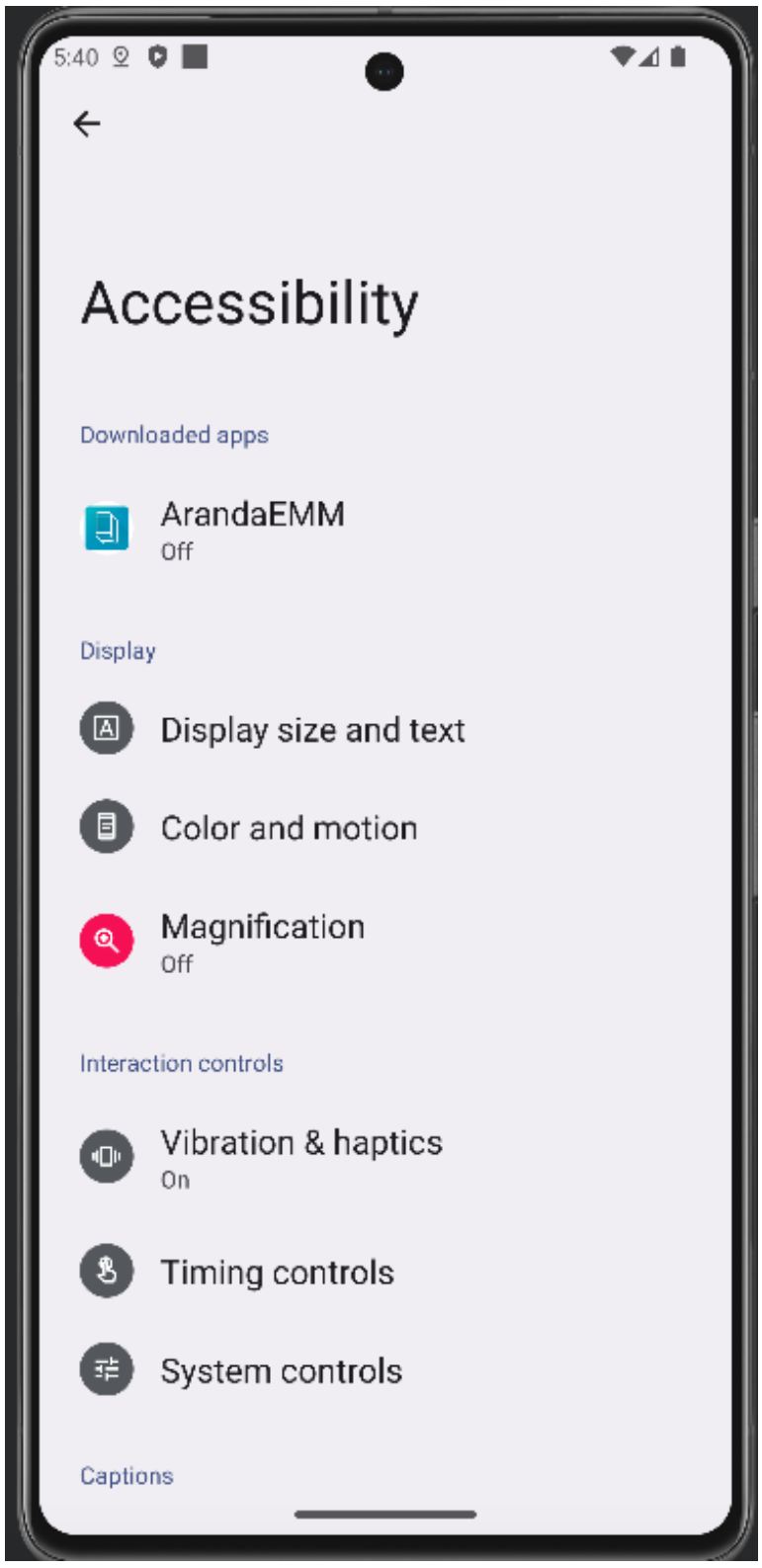
Android

Control Remoto

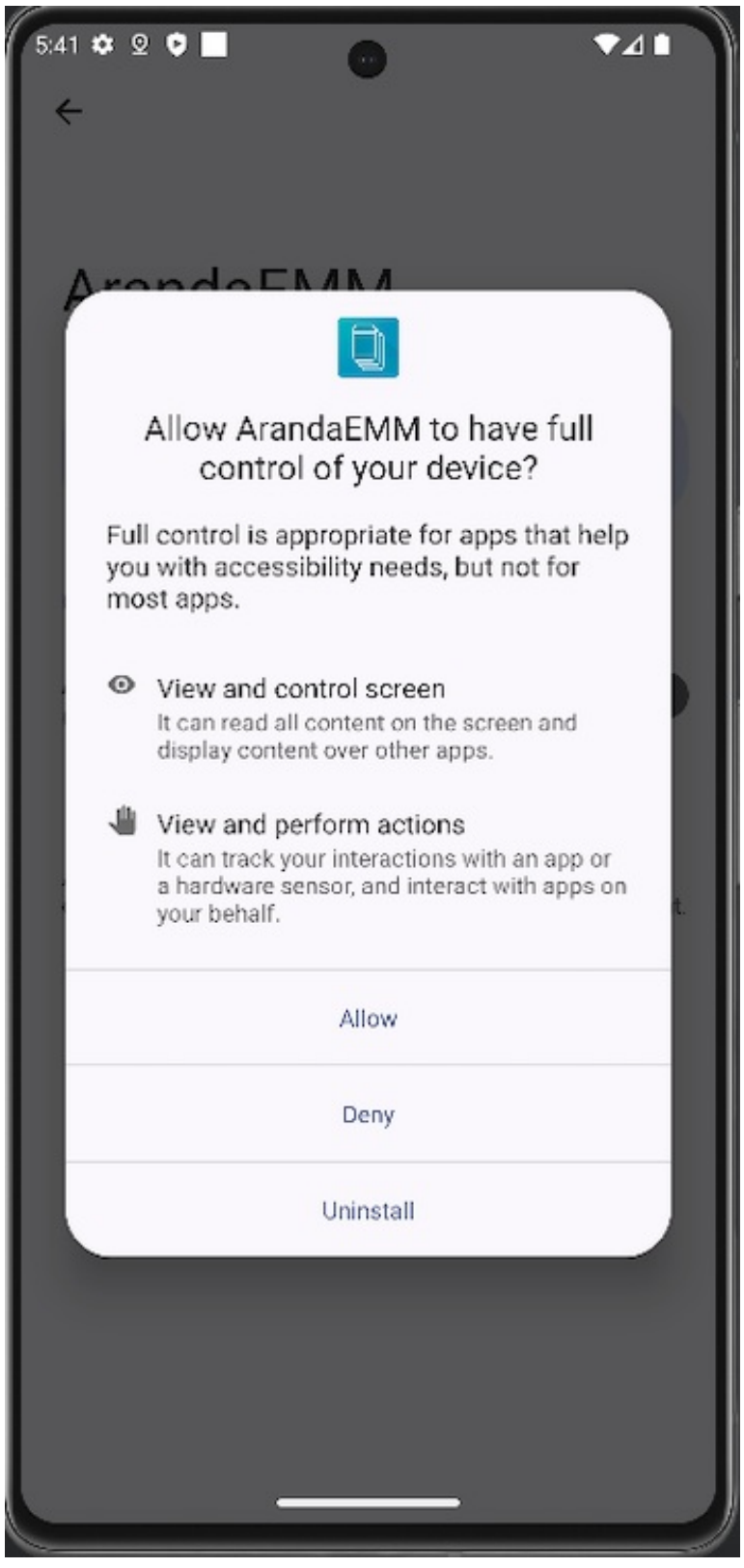
1. Solicita una sesión de control remoto en el dispositivo desde la consola AEMM .

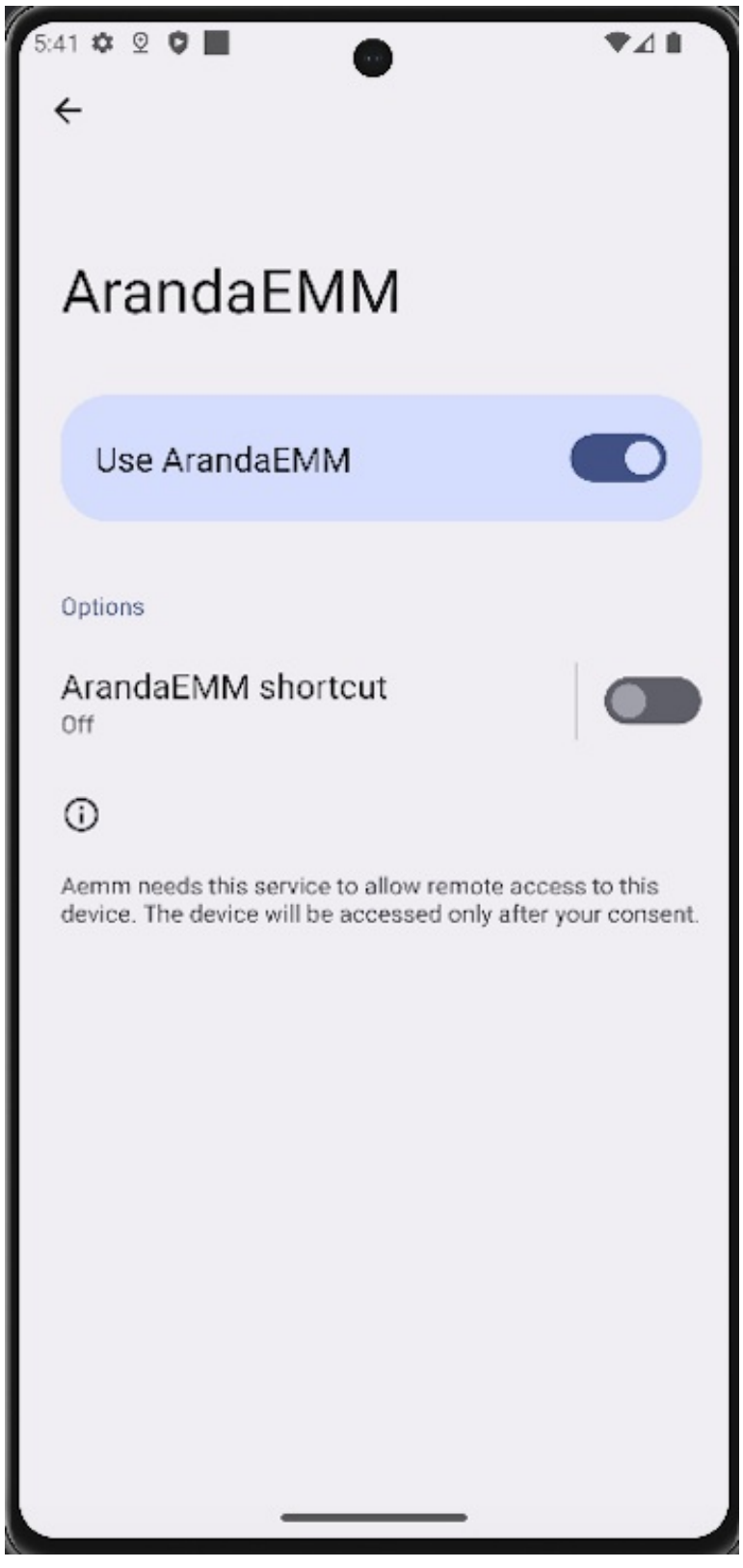


2. Esta de acción llega al dispositivo y le solicita al usuario habilitar el servicio de Accesibilidad.

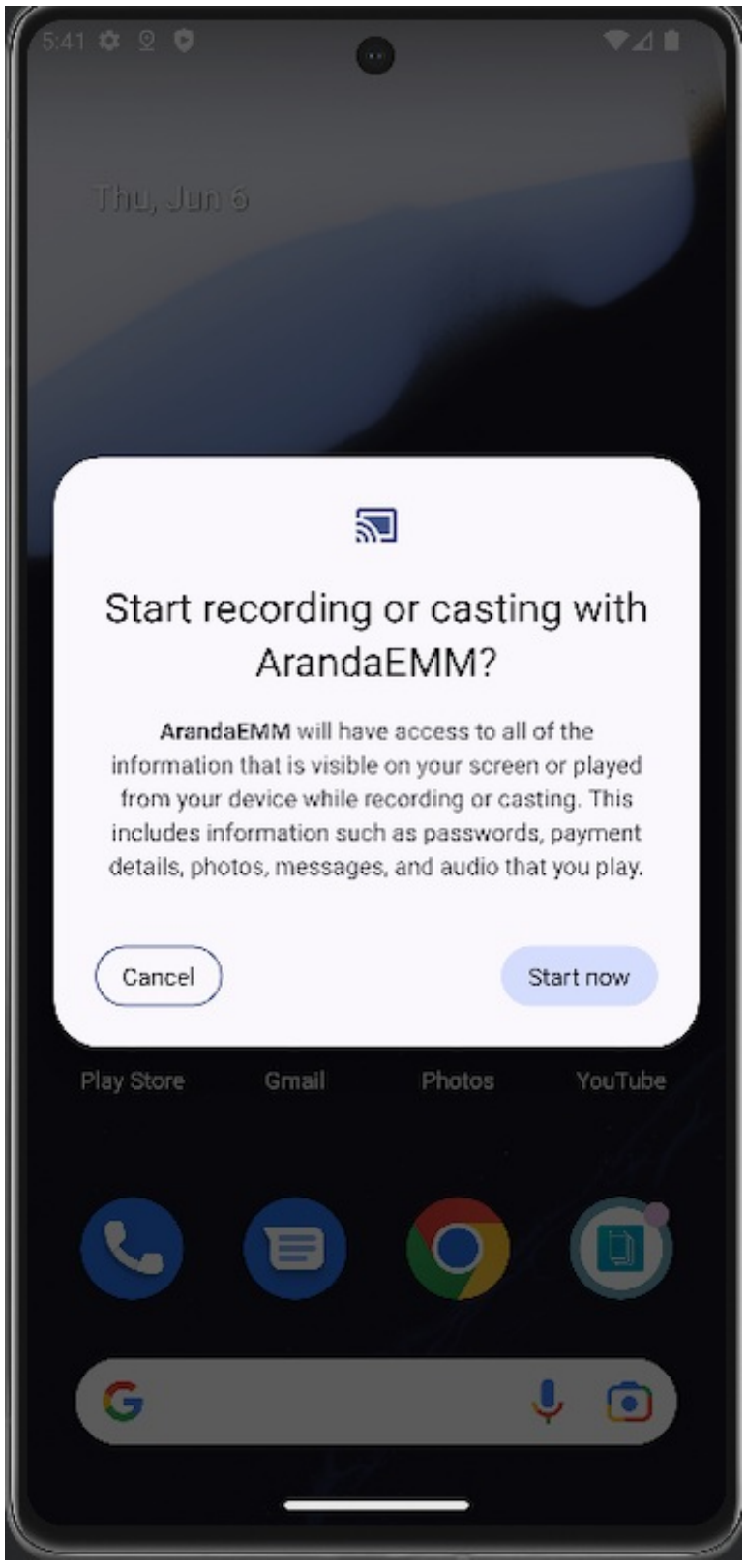


3. Habilite el servicio de accesibilidad para otorgar Control remoto completo.

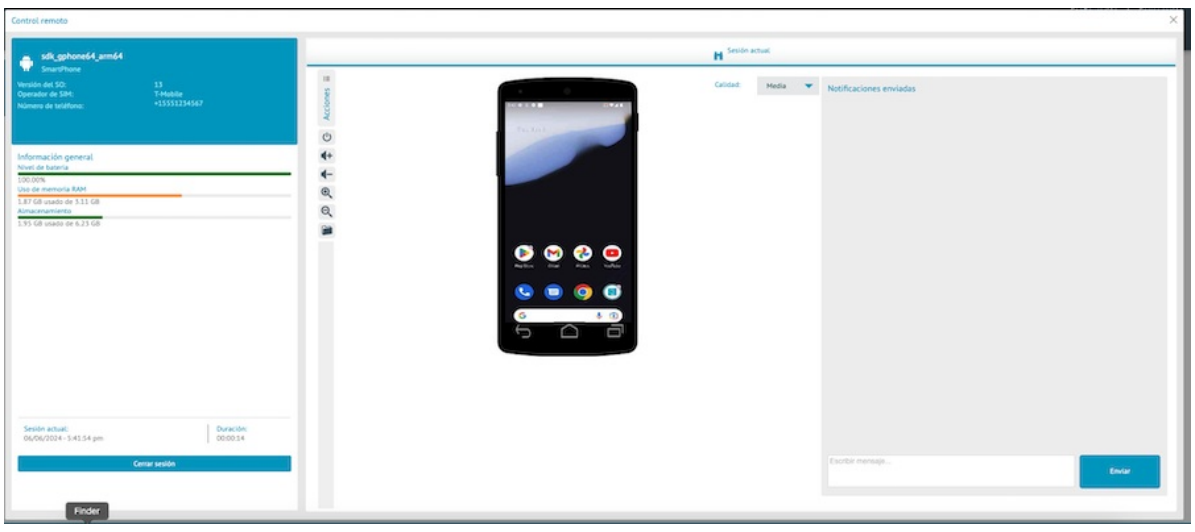

5:41
Allow ArandaEMM to have full control of your device?
Full control is appropriate for apps that help you with accessibility needs, but not for most apps.
View and control screen
It can read all content on the screen and display content over other apps.
View and perform actions
It can track your interactions with an app or a hardware sensor, and interact with apps on your behalf.
Allow
Deny
Uninstall



4. Haga clic en el botón Empezar ahora.

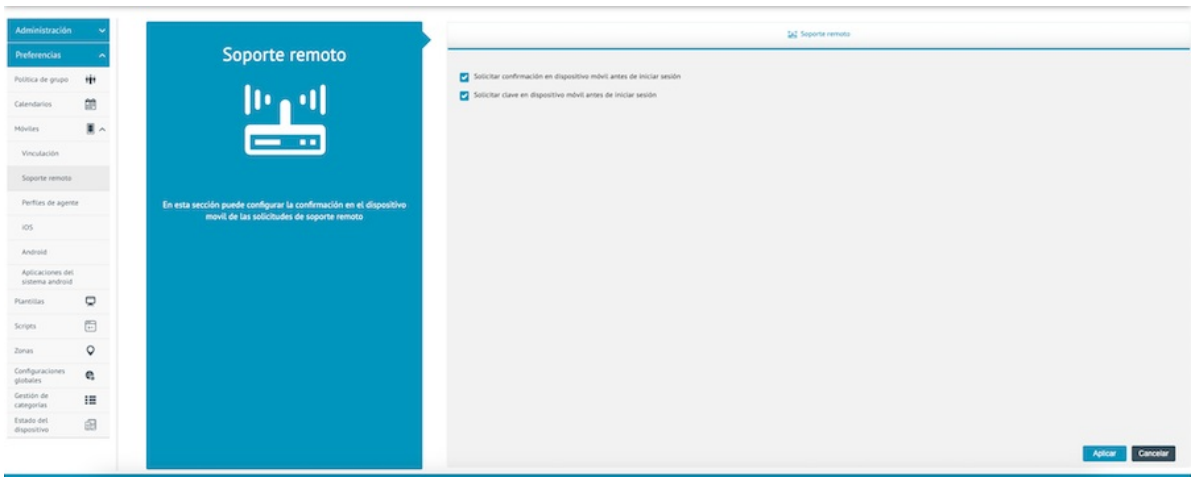


5. Al iniciar el control remoto desde la consola AEMM podrá tener control total del dispositivo.

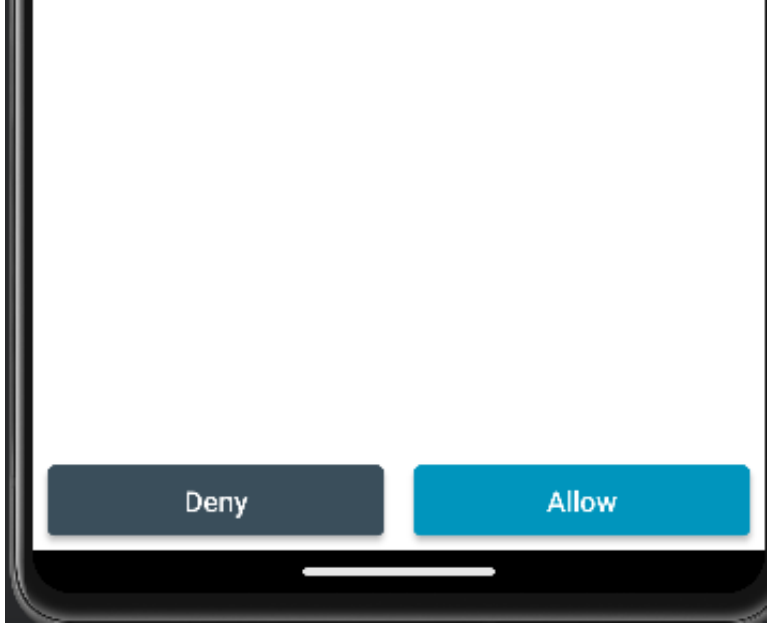


6. En la consola AEMM podrá modificar dos configuraciones en la sección Settings, Móviles, Soporte remoto, donde tendrá las siguientes opciones para solicitar el control remoto:

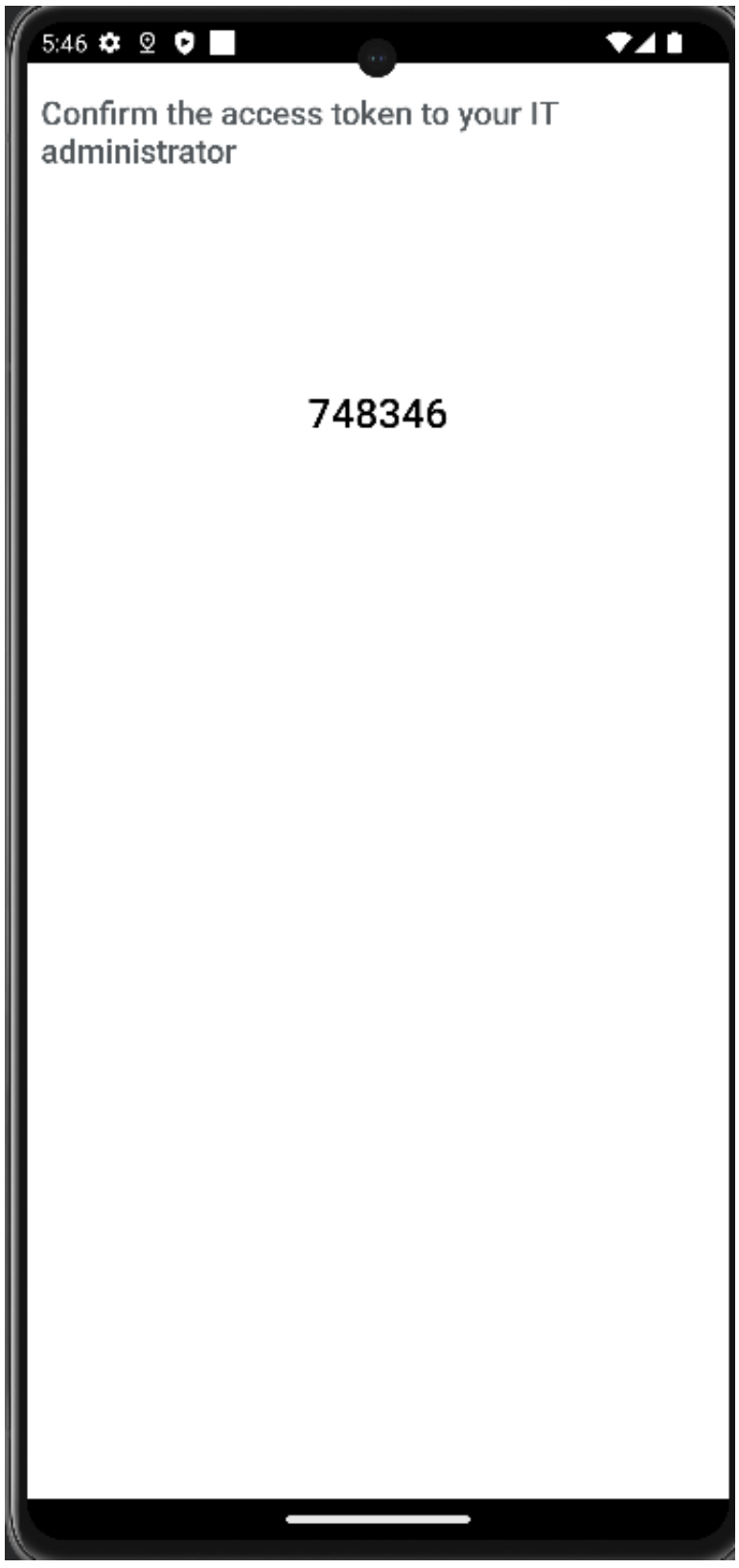
- Solicitar confirmacion en dispositivo móvil antes de iniciar sesión.
- Solicitar clave en dispositivo móvil antes de iniciar sesion.



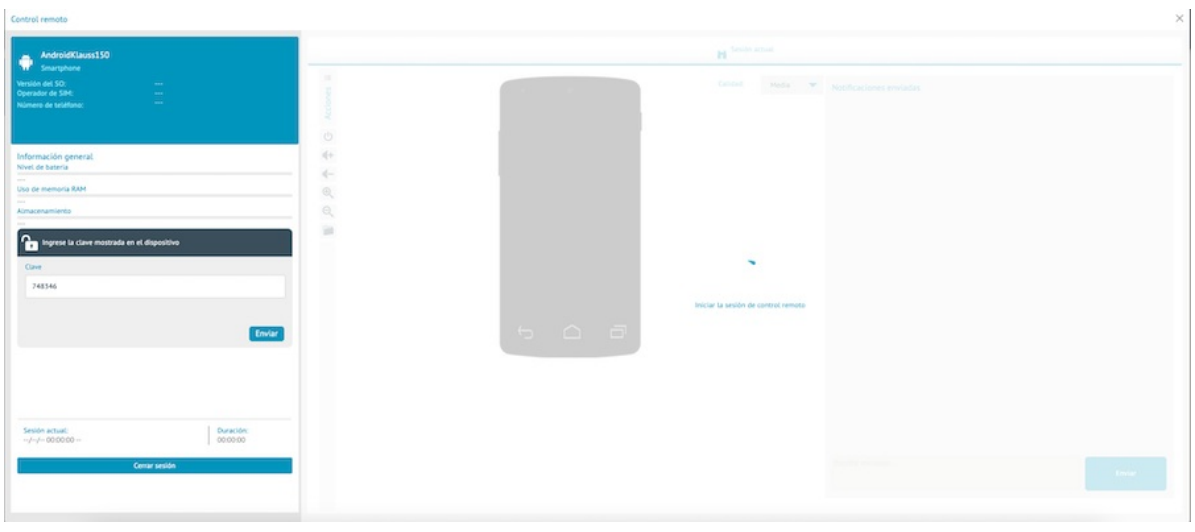
7. El comando llega al dispositivo y solicita la confirmación antes de iniciar sesión de control remoto.



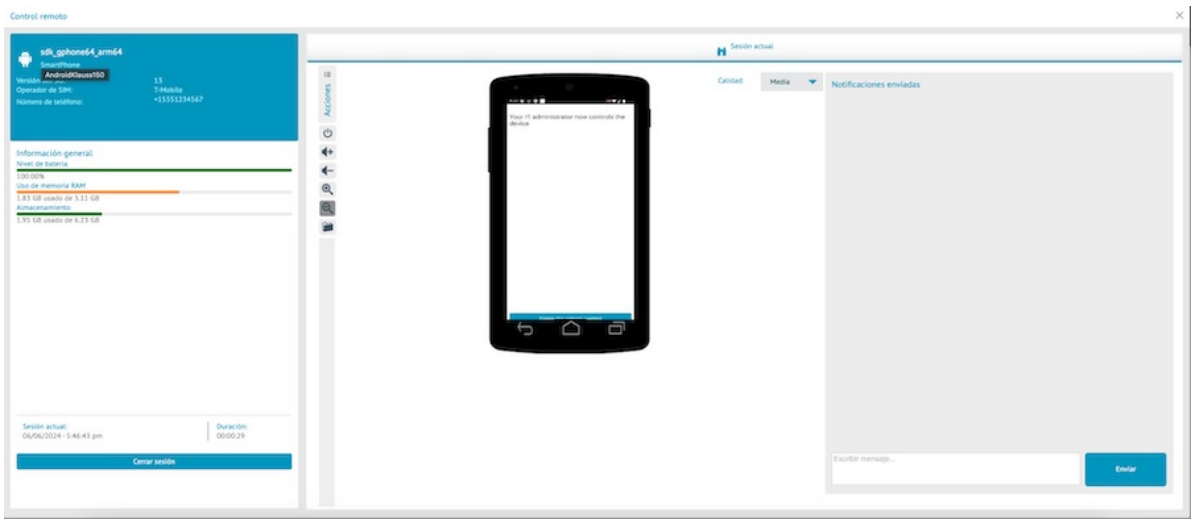
8. En el dispositivo podrá visualizar un Token para digitarlo en la consola y realizar el control remoto.



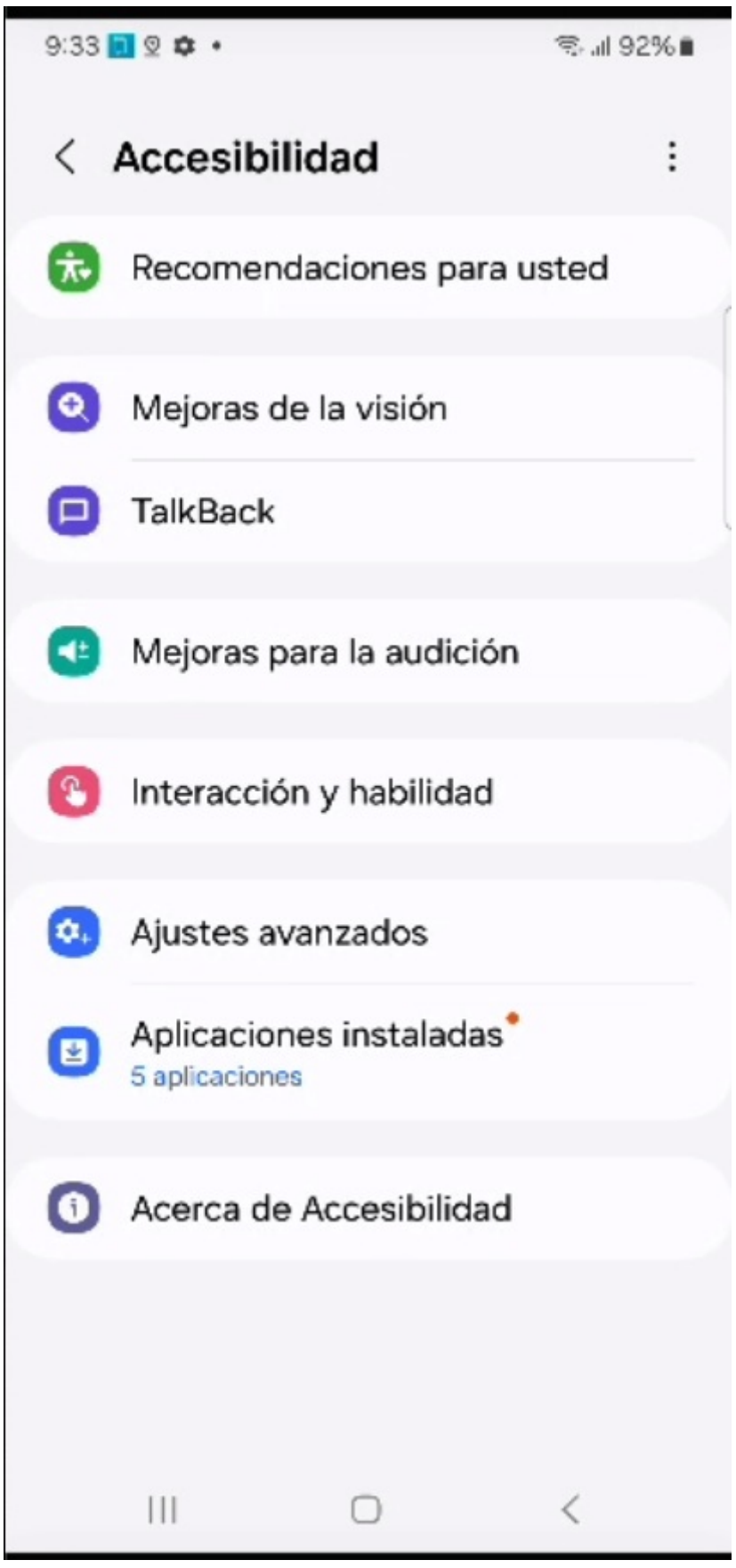
9. Ingrese el Token en la consola AEMM para realizar el control remoto.



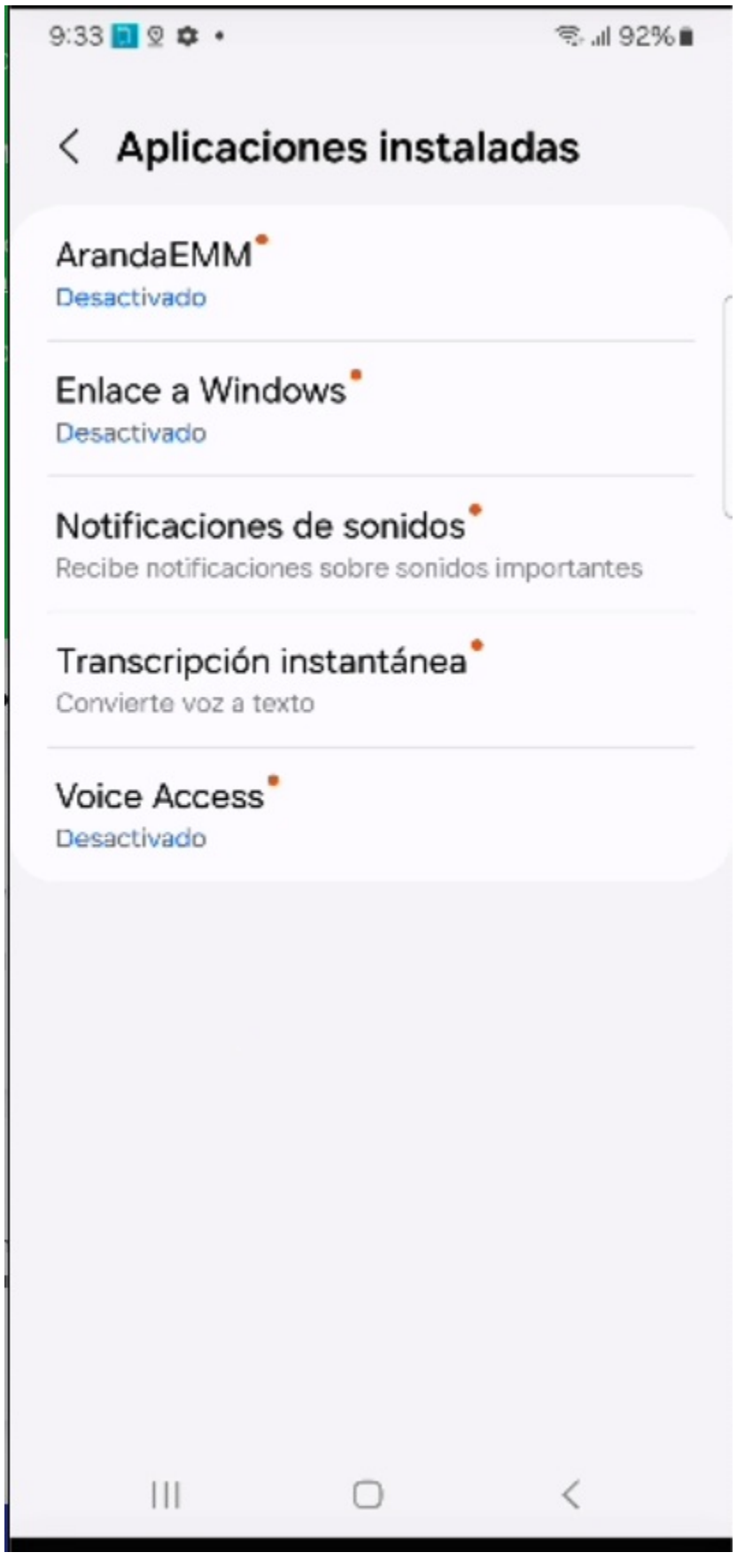
10. El control remoto ha empezado en el dispositivo.



11. La solicitud de habilitar acceso es diferente en dispositivos Samsung con Agente AEMM genérico; primero ingresa a la sección de aplicaciones instaladas, así:



12. Ingrese en Aranda AEMM



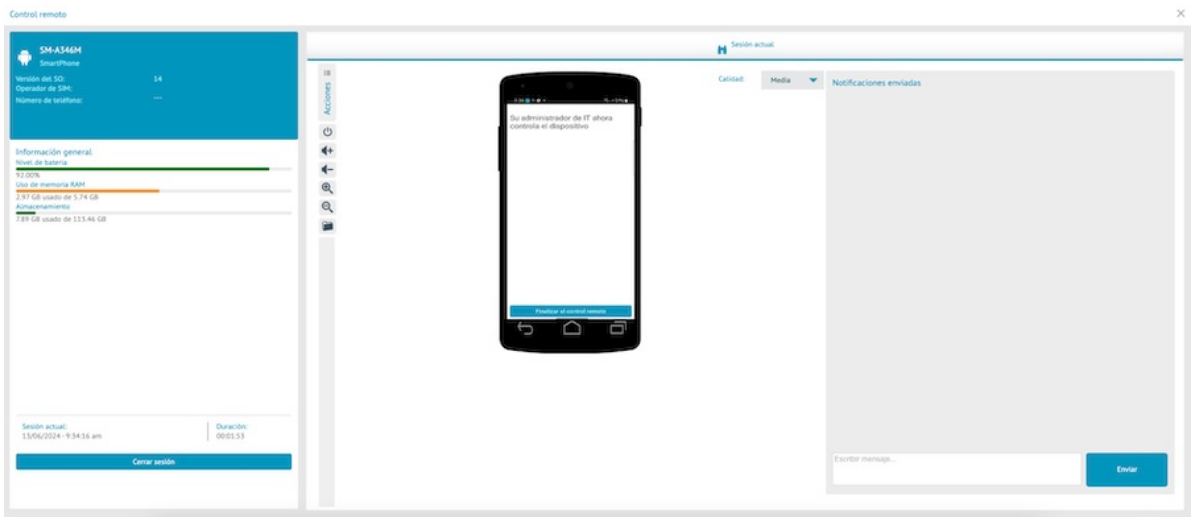
13. Haga clic en el swipe button para activar la accesibilidad.

14. Haga clic en Permitir para conceder el control total al teléfono a AEMM.

15. Haga clic en Aceptar.

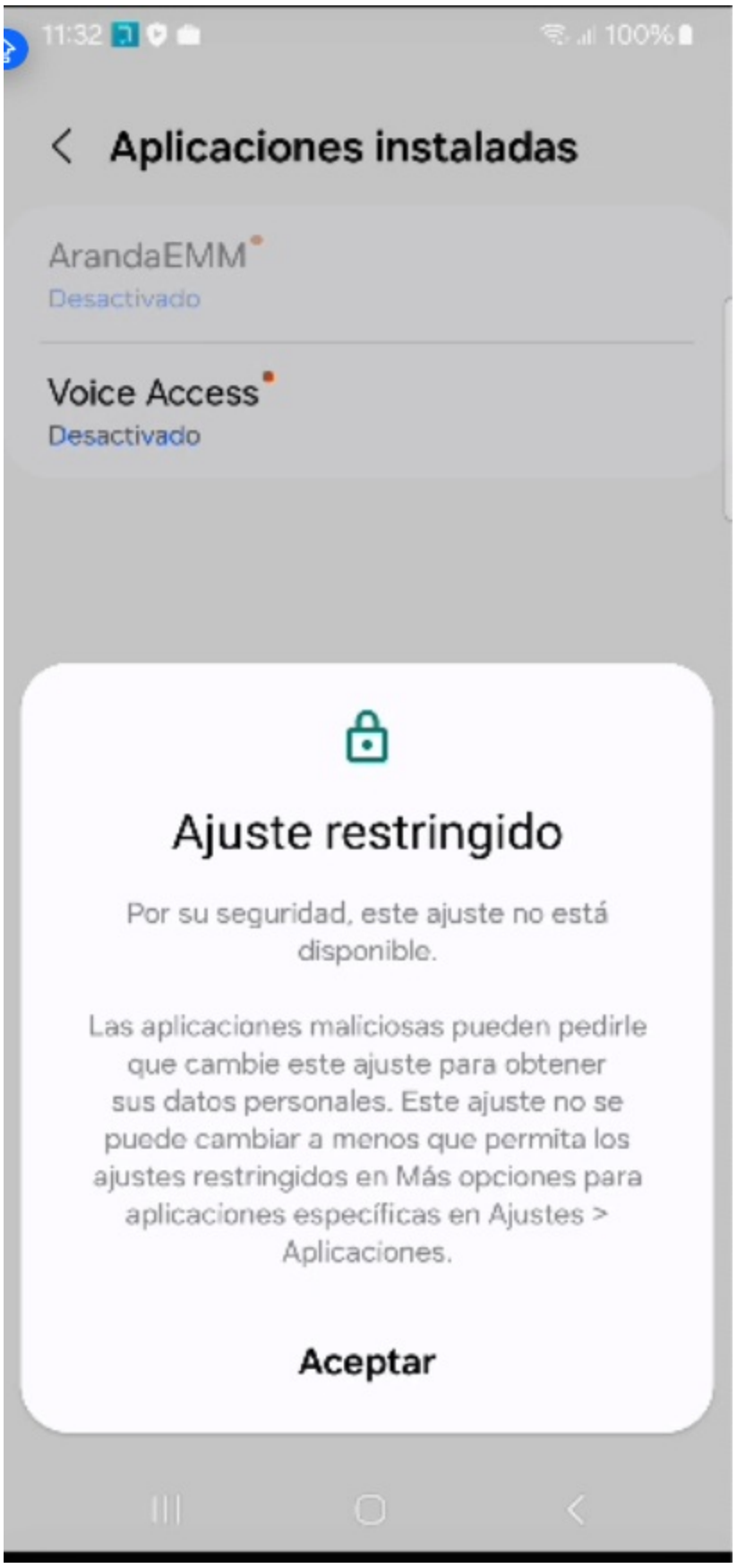
16. Haga clic en Comenzar ahora para iniciar el control remoto.

17. El control remoto ha empezado en el dispositivo.

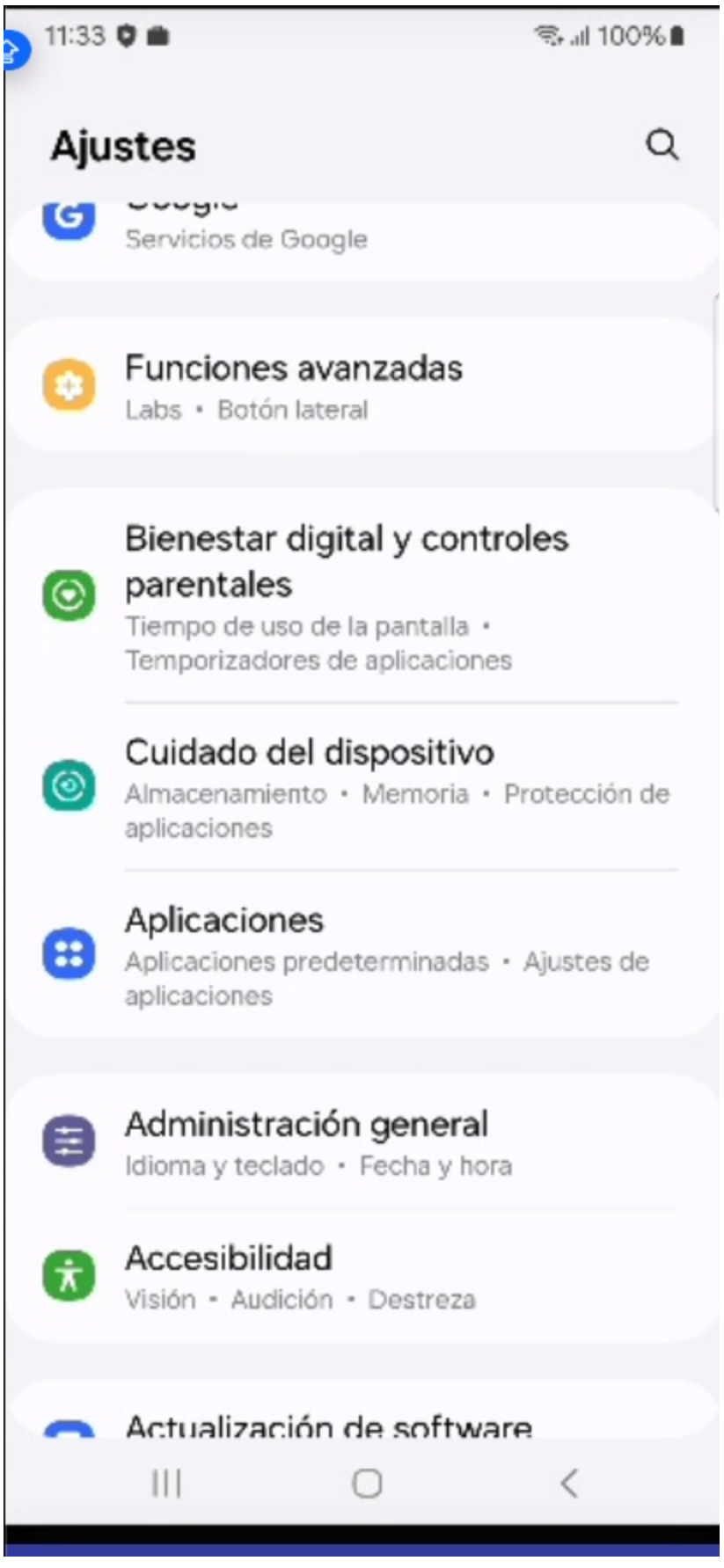


Caso para dispositivos samsung en Accesibilidad

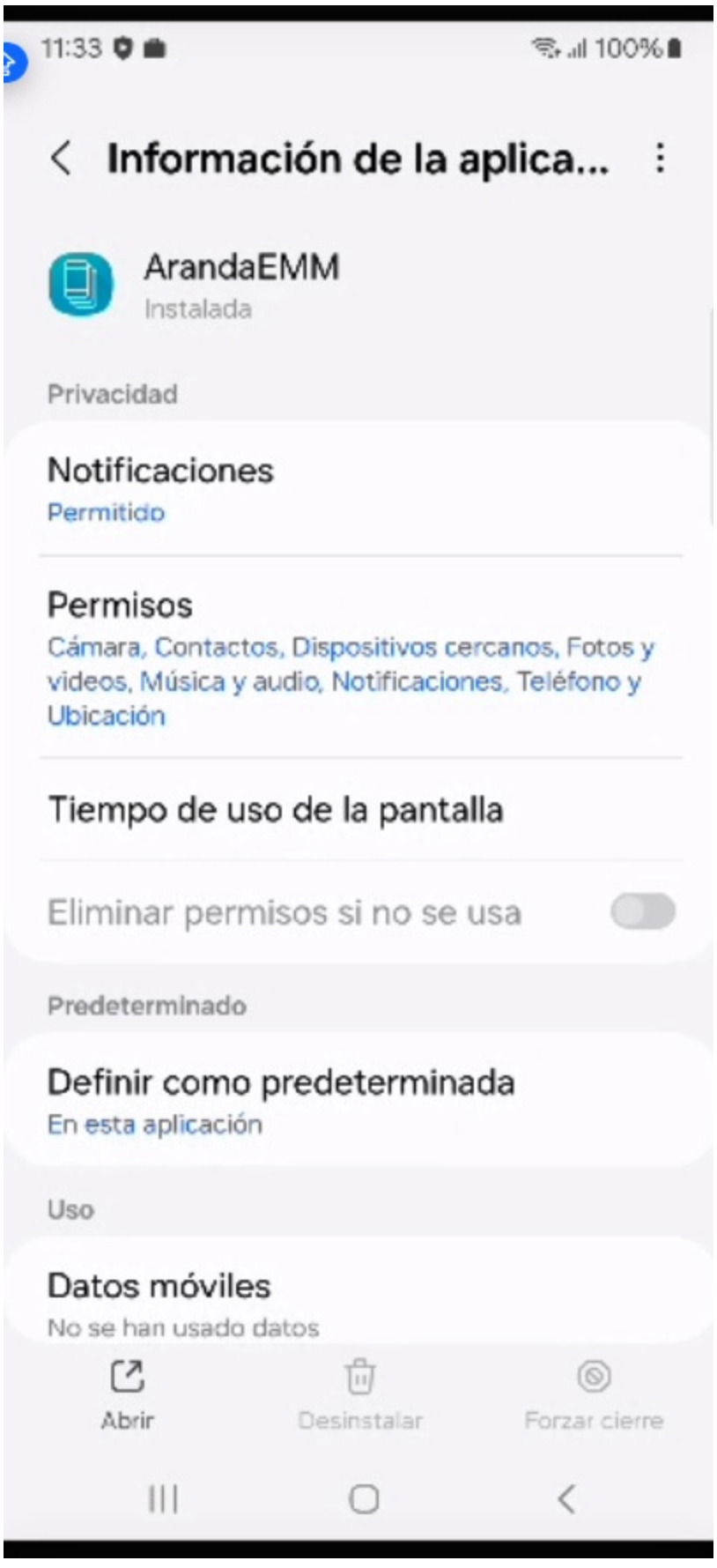
18. Si la accesibilidad está bloqueada como se muestra en la siguiente imagen, tenga en cuenta las siguientes consideraciones:



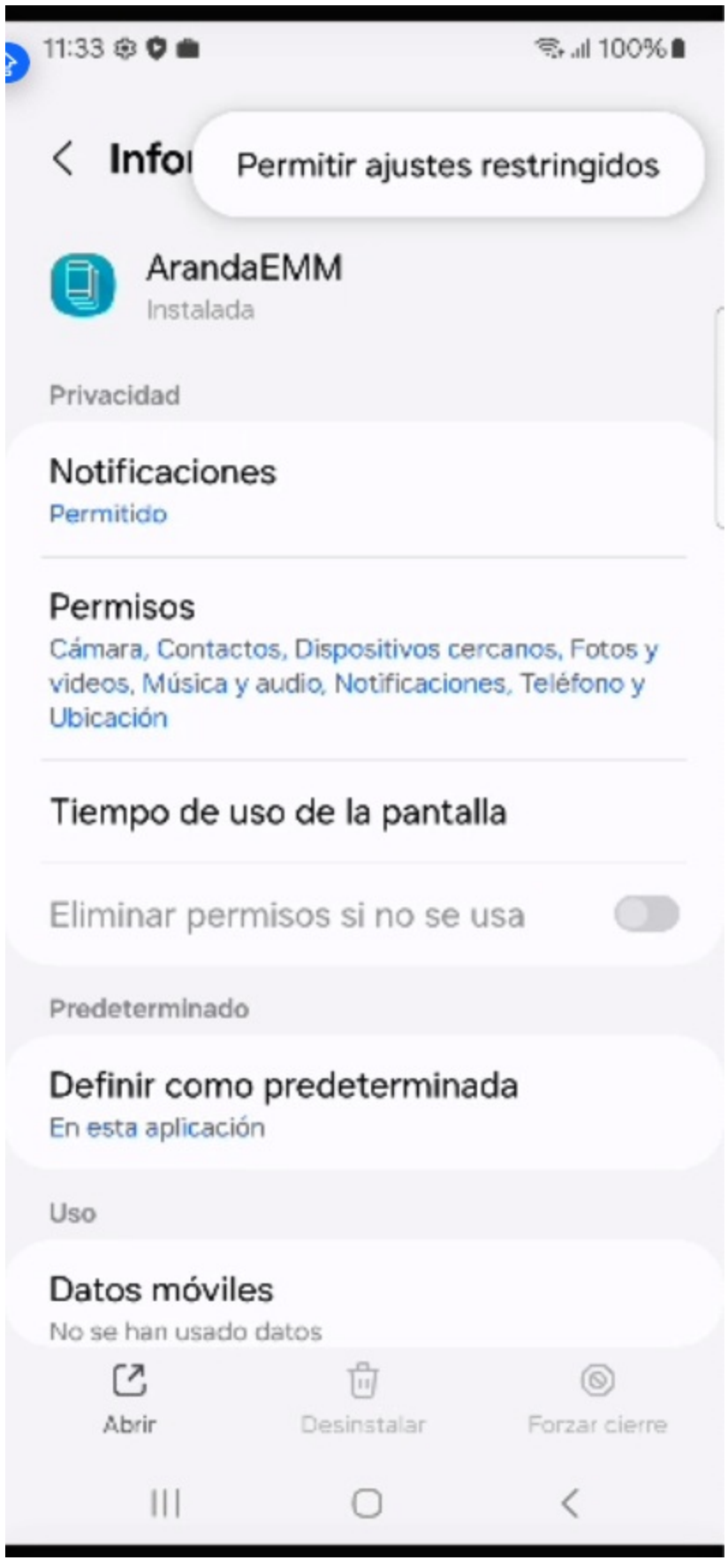
19. En Ajustes del sistema, seleccione la opción Aplicaciones y buscar la aplicación ArandaEMM.



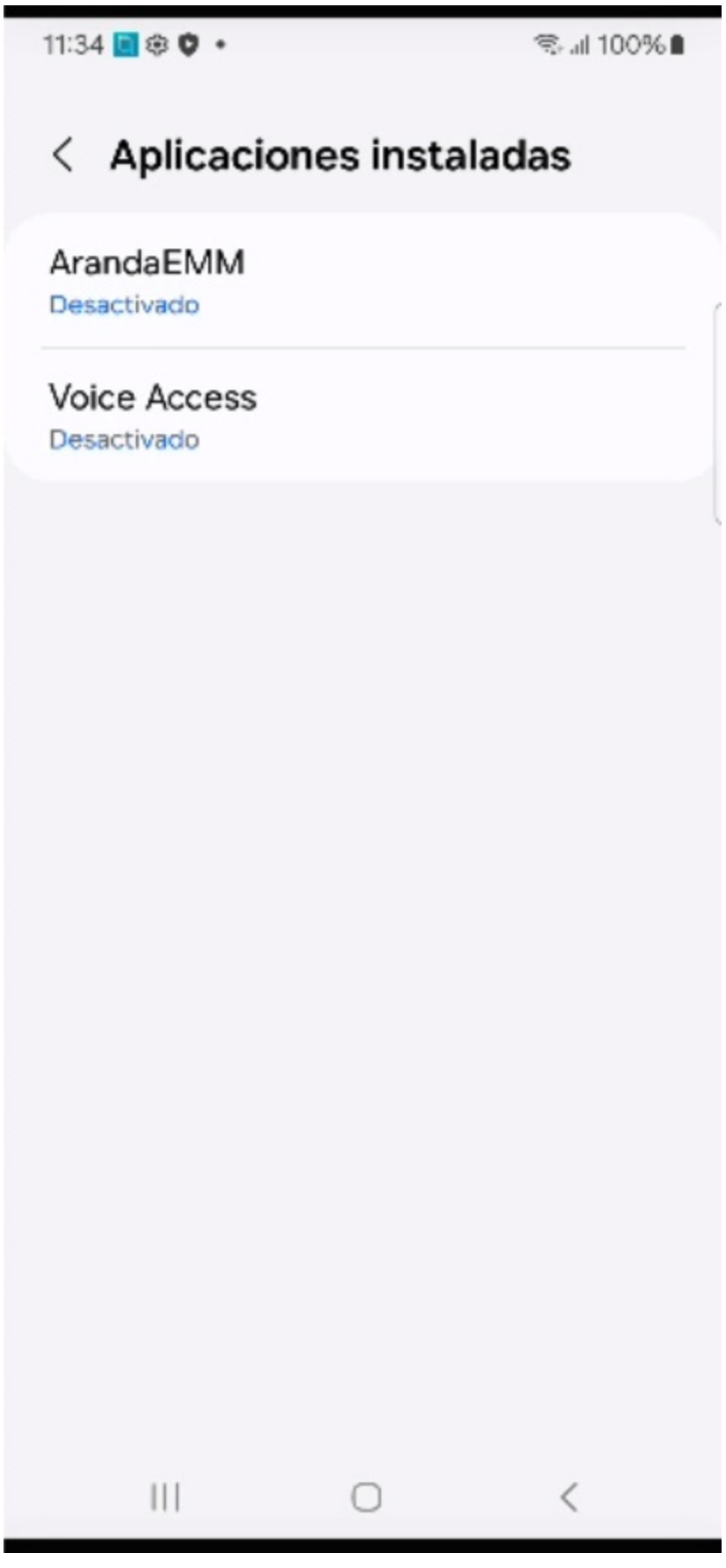
20. En el menú superior , en la información de la política, seleccione los tres puntos ....



21. Haga clic en la opción permitir ajustes restringidos.



22. Regrese a la opción de Accesibilidad y repita los pasos del punto 12 al 15 para iniciar el control remoto.

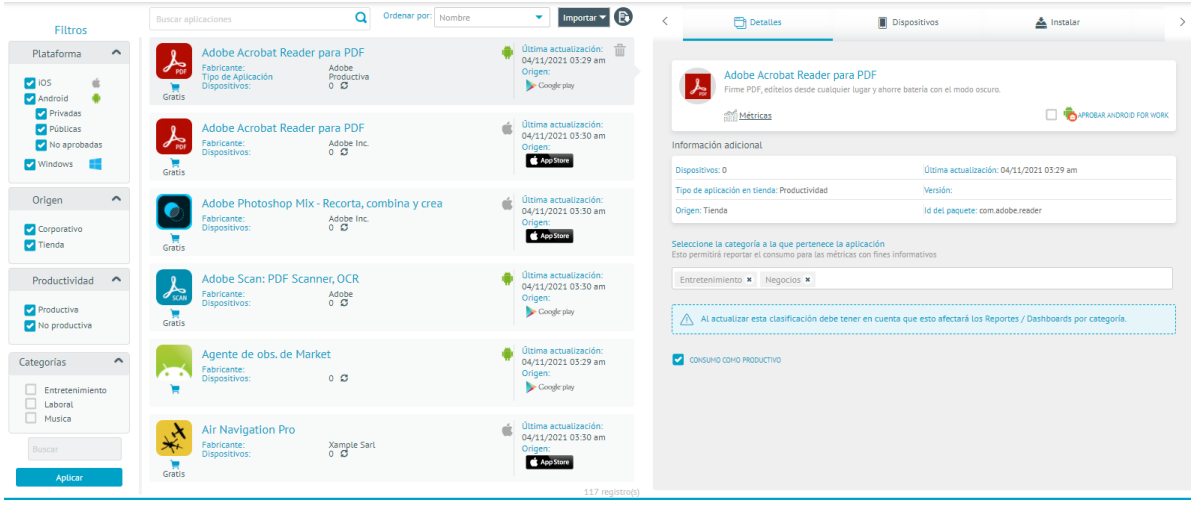


Aplicaciones

Módulo Aplicaciones

En esta sección se podrán visualizar todas las aplicaciones que se han encontrado a través de los inventarios de los dispositivos y como resultado de la importación de aplicaciones desde cada una de las tiendas (google play y app store).

La sección de aplicaciones funciona a manera de catálogo. Aquí podrá realizar acciones asociadas a cada aplicación y administrar cada una de las apps teniendo la posibilidad de realizar acciones masivas sobre todos los dispositivos (con o sin aplicación instalada).



La pantalla se divide en 3 secciones principales:

Sección Filtros

En esta sección se visuazan dos tipos de filtro; uno por tipo de plataforma, por origen de la aplicación, si está marcada como productiva y en que categoria(s) esta clasificada.

Sección Listado

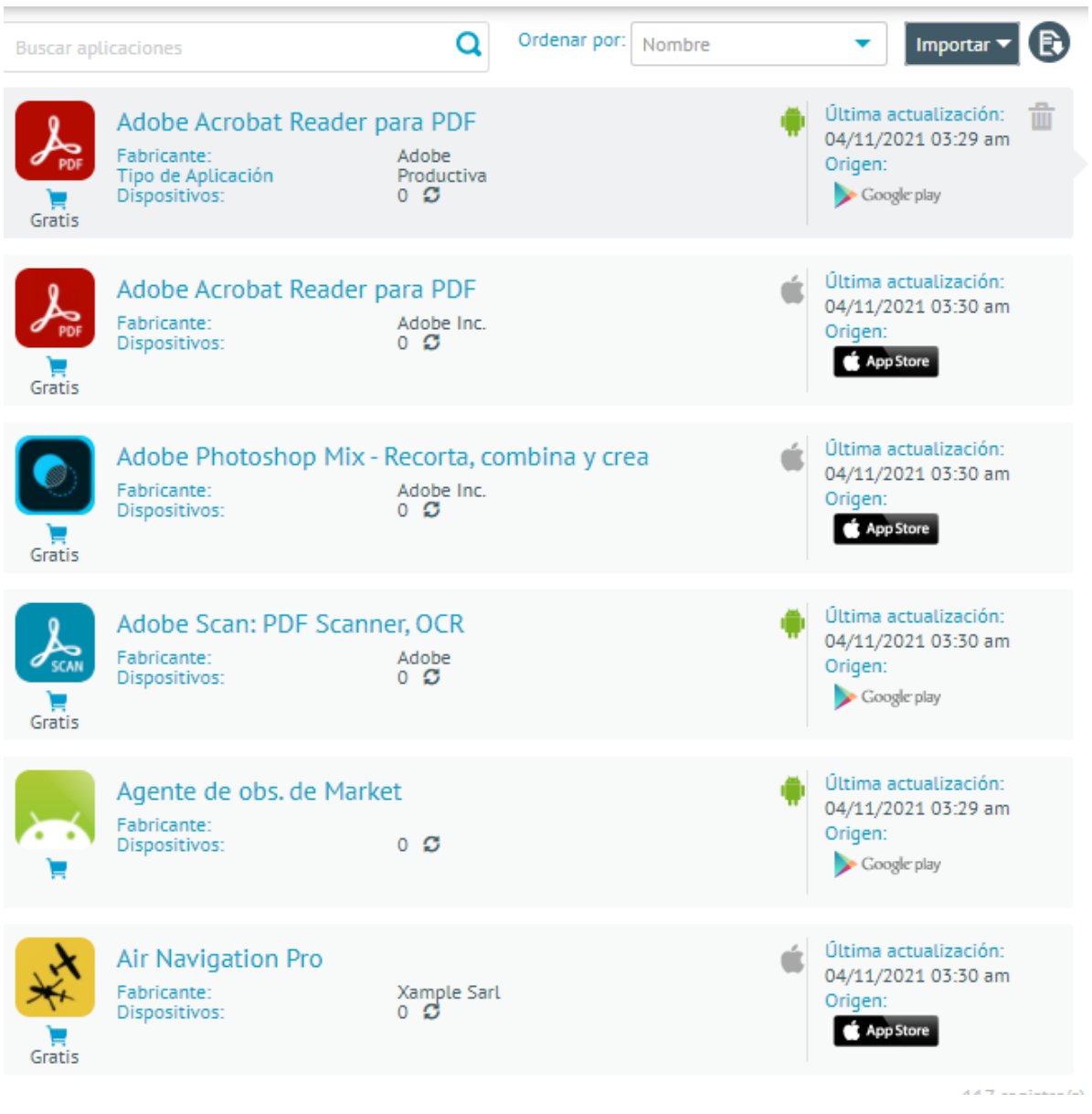
Esta seción presenta un campo de búsqueda de aplicaciones donde se podrá realizar la consulta por el nombre de las aplicación; un campo adicional permite ordenar la búsqueda que se haya realizado. También será posible importar una aplicación y subir un APK empresarial. También podrá exportar el listado generado de la consulta, utilizando el botón que encuentra en el extremo derecho de la columna . El listado generado de la consulta es un archivo de Excel.

Cada una de las tarjetas de resultados tiene la siguiente información y si está marcada como productiva:

- Nombre de la aplicación.
- Plataforma
- Cantidad de dispositivos que la tienen instalada
- Tipo de aplicaciones.
- Desarrollador de la aplicación
- Versión de la aplicación .

En el listado podrá visualizar el detalle de cada item con la ayuda del teclado..

Con el ícono de recarga, se podrá recalcular el conteo de dispositivos que ha reportado la aplicación como instalada. Esta acción sólo es posible para la aplicación seleccionada.



Importar aplicación

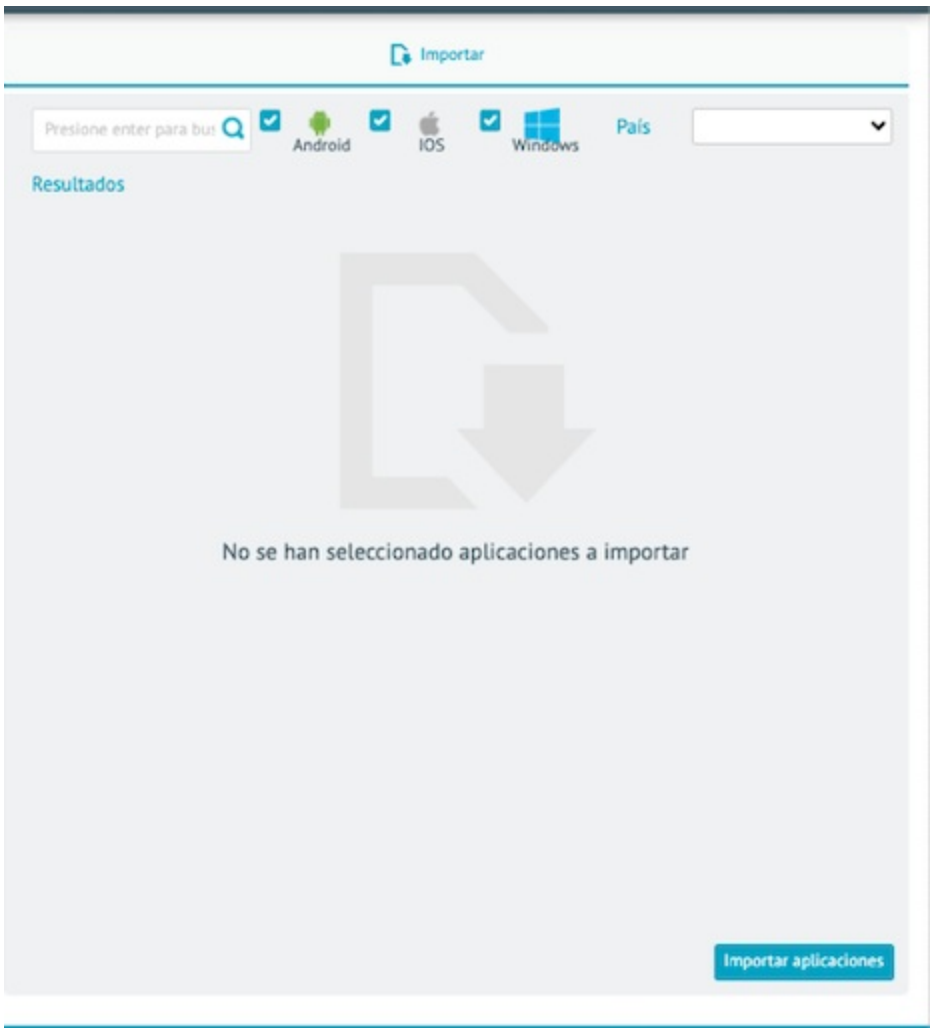
El catalogo de aplicaciones de Aranda ENTERPRISE MOBILE MANAGEMENT AEMM tiene la funcionalidad de importación de aplicaciones, lo que permite cargar aplicaciones desde tiendas públicas de aplicaciones como Google Play, ITunes y Windows Store.

Por otro lado se ofrece también la carga de aplicaciones del tipo corporativo donde podrá importar un archivo APK (Android) o IPA (iOS) para instalar directamente en los dispositivos.

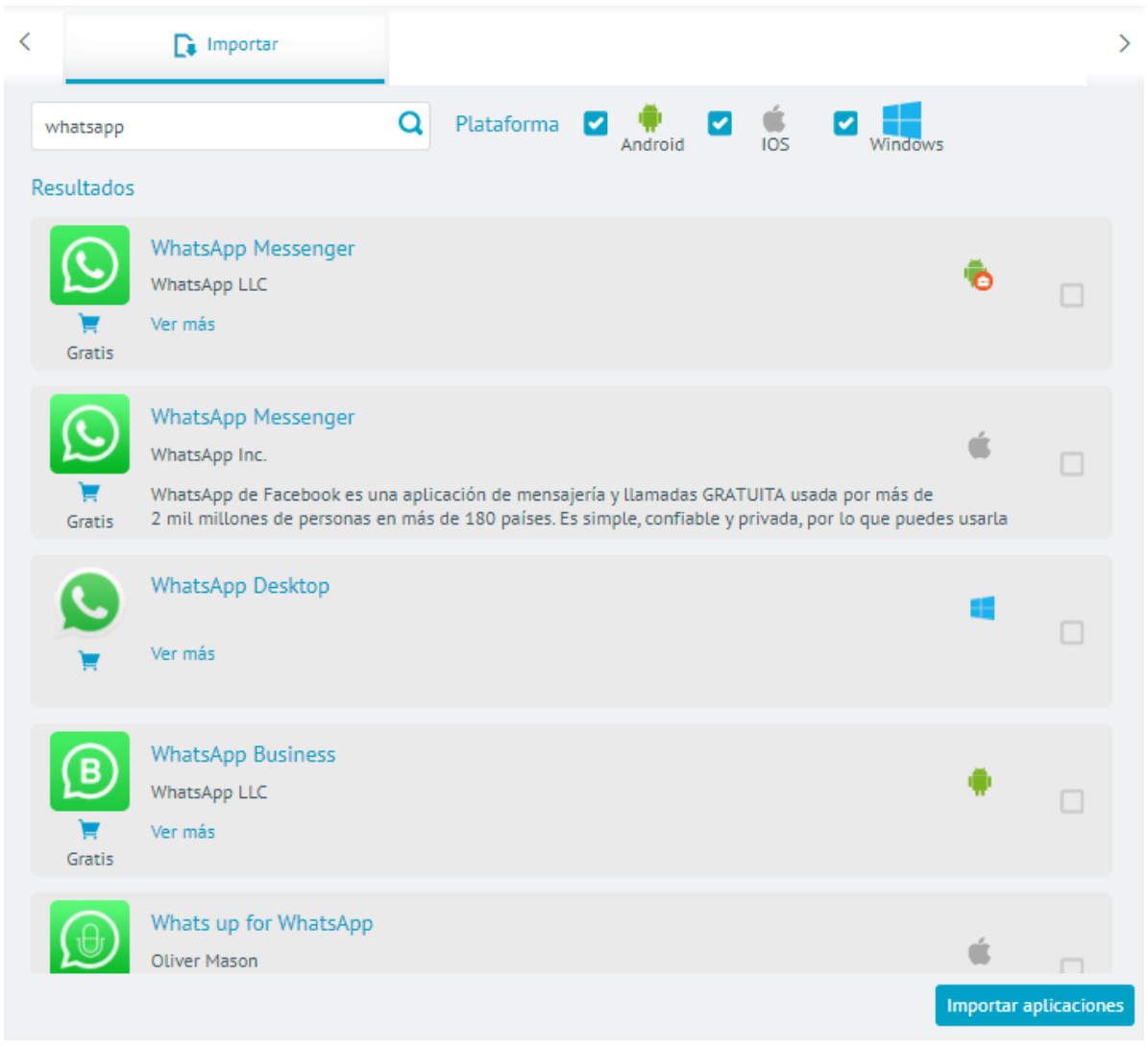
Importación desde Tienda Pública

Para acceder a este modo de importación haga click en el combo Importar, seguido de la opción Importar. En la seccion de detalles se cargará la interfaz de búsqueda e importación de apliaciones:

Descripción



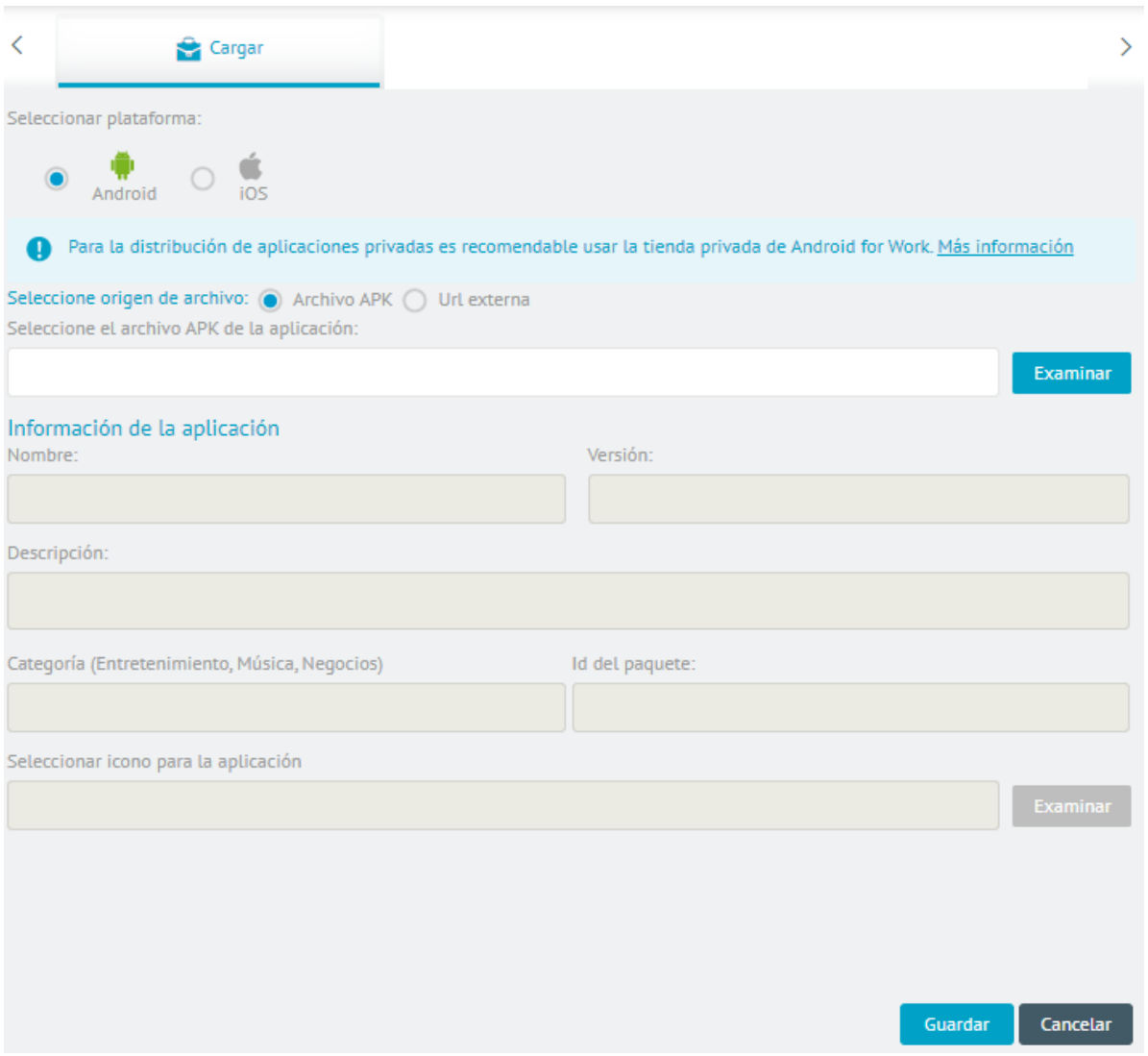
En el campo de búsqueda ingrese un criterio de consulta para buscar las aplicaciones coincidentes en las plataformas seleccionadas. Si la aplicación sólo aparece en la tienda de un país, debe seleccionarlo en el campo país (este campo solo aplica para plataforma Android), se mostrarán los resultados de búsqueda de acuerdo a la configuración de los filtros:



Posterior a seleccionar las aplicaciones que se deseen importar y identifique la opción Importar Aplicaciones. la aplicación importada quedará agregada al catálogo de Aplicaciones de Aranda ENTERPRISE MOBILE MANAGEMENT AEMM.

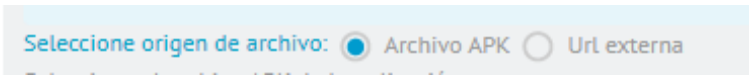
Carga de Aplicaciones usando archivos APK o IPA

Para acceder a este modo de importación, selecione elcombo Importar, seguido de la opción Cargar. Posterior a esta acción, la seccion de detalles cargará la interfaz de carga de aplicaciones corporativas:



Usando esta interfaz se podrán cargar aplicaciones usando directamente archivos APK o IPA para plataformas Android o iOS respectivamente.

Existen dos modos de carga de aplicaciones:



Modos de Carga	Descripción
Carga Directa del Archivo	En este modo se carga directamente el archivo en la consola, quedando asi ya disponible para instalación en los dipsositivos.
Carga por Url	En este modo el archivo se debe de cargar en un gestor externo de archivos como por ejemplo: DropBox, Azure Blob Storage. Este modo se recomienda cuando el archivo sea de un tamaño considerable (mayor a 30 MegaBytes) y se deseee realizar una instalación masiva a un numero considerable de dispostiivos (> 200)

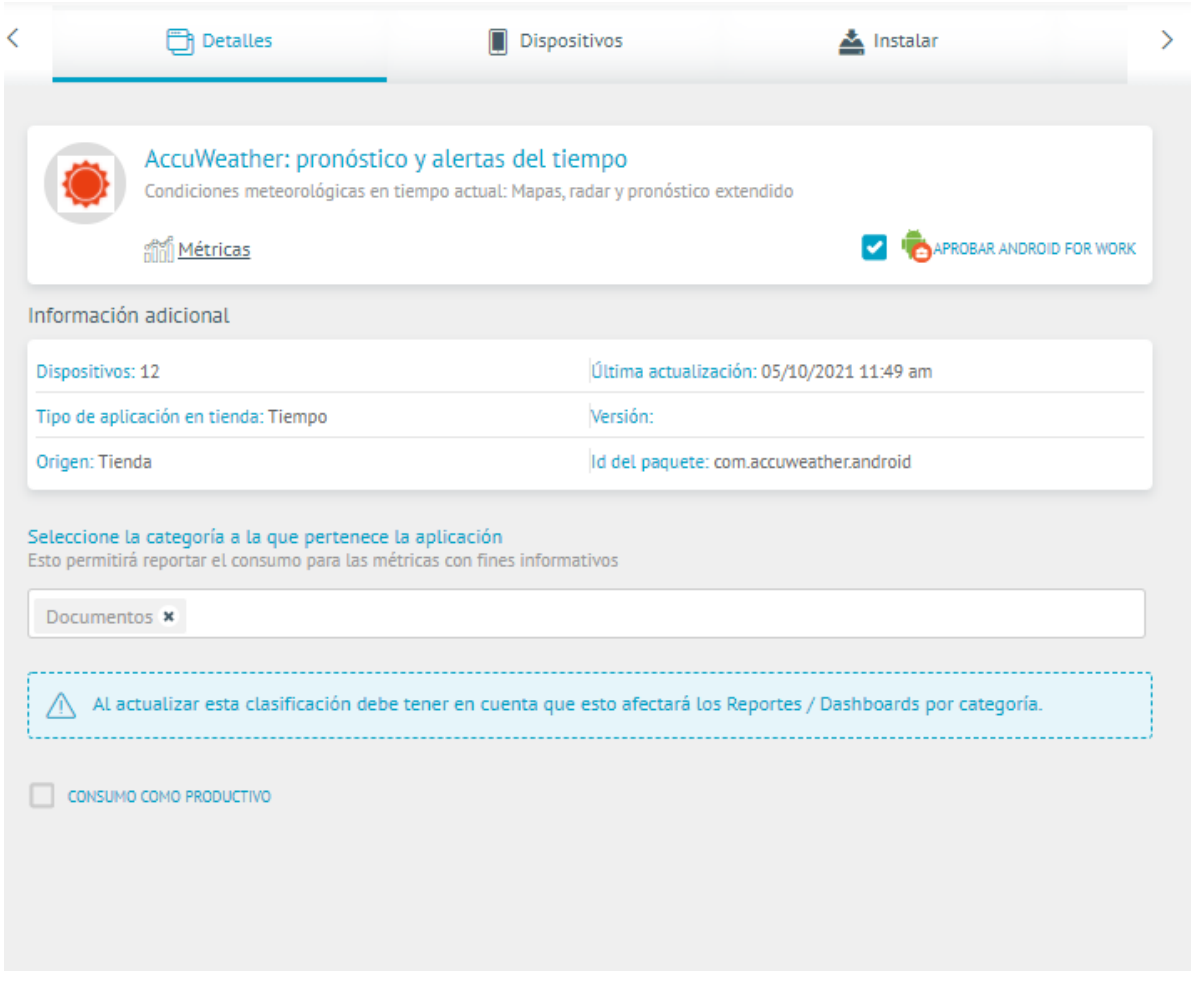
⚐ **Nota:** En ambos modos de carga la consola intentará extraer los datos del archivo/url cargado y los colocará en las casillas correspondientes.

Una vez registrados todos los datos de la aplicacion seeleccione la opción Guardar para persistir la aplicacion en el catalogo de aplicaciones de Aranda ENTERPRISE MOBILE MANAGEMENT AEMM.

Sección Detalle de la Aplicación

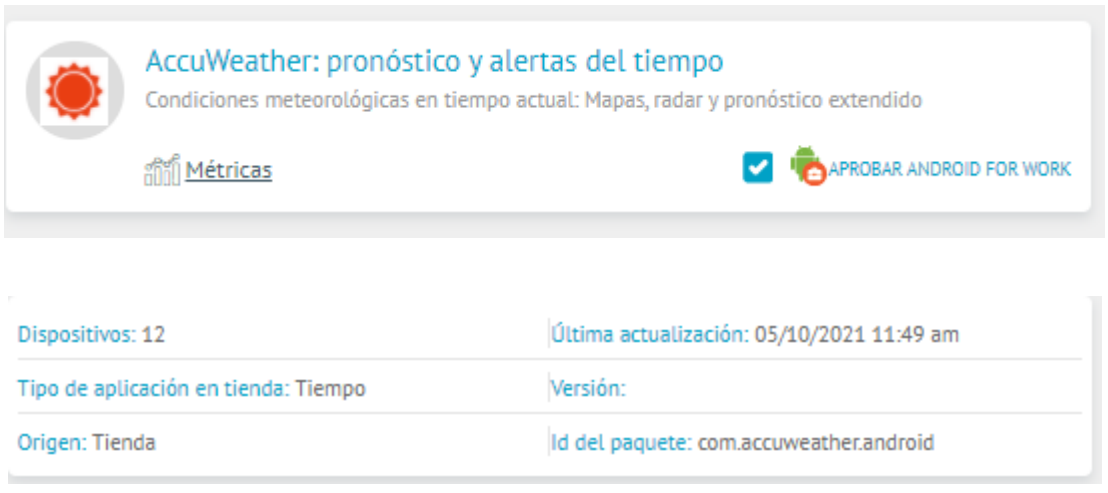
En esta sección se presentan los detalles y funcionalidades más relevantes correspondiente a cada aplicación, esta sección tiene las siguientes pestañas:

Pestaña Detalles

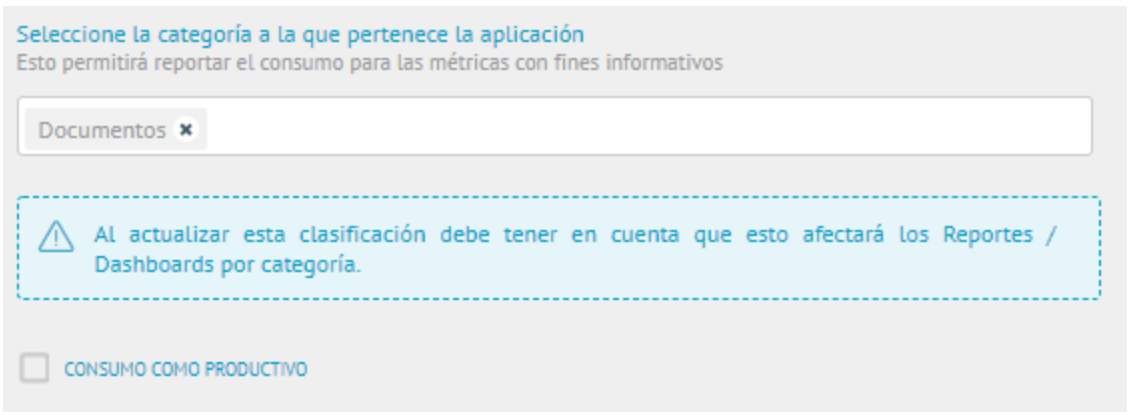


En esta pestaña se muestran los detalles y opciones generales divididas en los siguientes grupos:

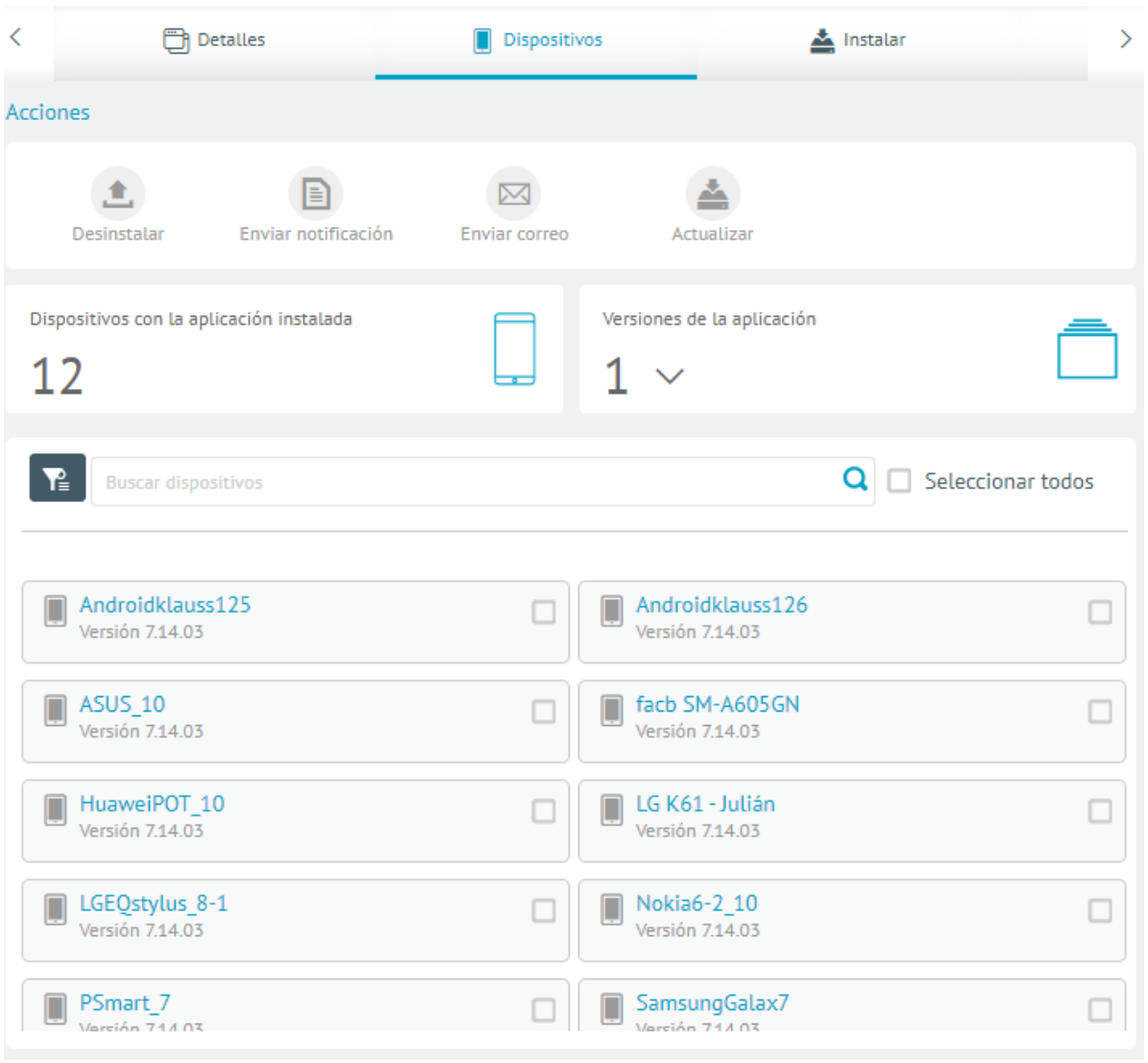
Grupos	Descripción
Tarjeta de Descripción:	Se presenta el nombre completo de la aplicación, descripción, enlace directo a la pestaña de Métricas y el checkbox para aprobar la aplicación para su uso en Android For Work (De estar activado en la consola el modo AFW)
Tarjeta Información Adicional:	Se presentan datos de conteo de dispositivos, última actualizacion desde tienda, clasificación de la aplicación, Versión, Origen, Id del Paquete.
Tarjeta Métricas:	Se presentan las categorías en que está clasificada la aplicación, además de un checkbox que marca la aplicación como Productiva. Estas categorías son las que se definen en la opción: Configuración -> Preferencias -> Gestión de Categorías. Estas categorias y los datos de consumo productivo se utilizan para los datos de métricas de aplicaciones para la sección de Dashboard de Métricas como para la Hoja de vida del dispositivo, en la pestaña métricas de aplicaciones.



El hecho de marcar una aplicación como Productiva se basa en el propio objetivo de negocio de la empresa, por ende, las aplicaciones que se marquen como productivas son las que soportan las actividades principales del objeto de negocio de la empresa.



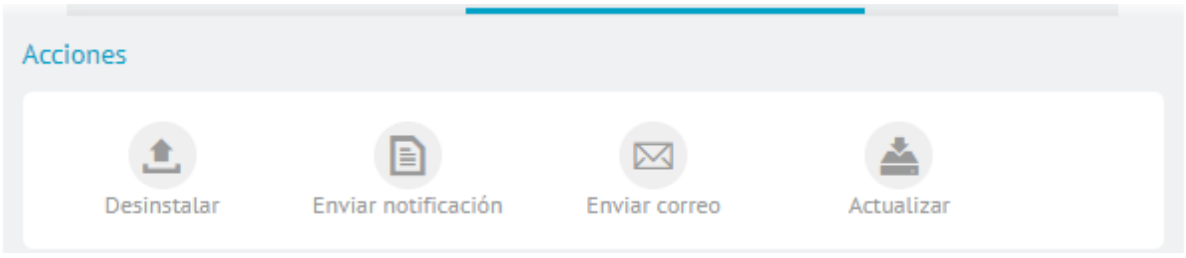
Pestaña Dispositivos



En la pestaña dispositivos se listan y se presentan opciones diversas para los móviles que han reportado la apliación como instalada en los inventarios reportados.

En un principio se muestra la cantidad de dispositivos que han reportado la aplicación como instalada, las versiones instaladas y conteo de tales versiones en los dispositivos, asi como el listado de los dispositivos incluidos.

Además se presentan las siguientes acciones posibles a realizar en los dispositivos, con respecto a la aplicación:

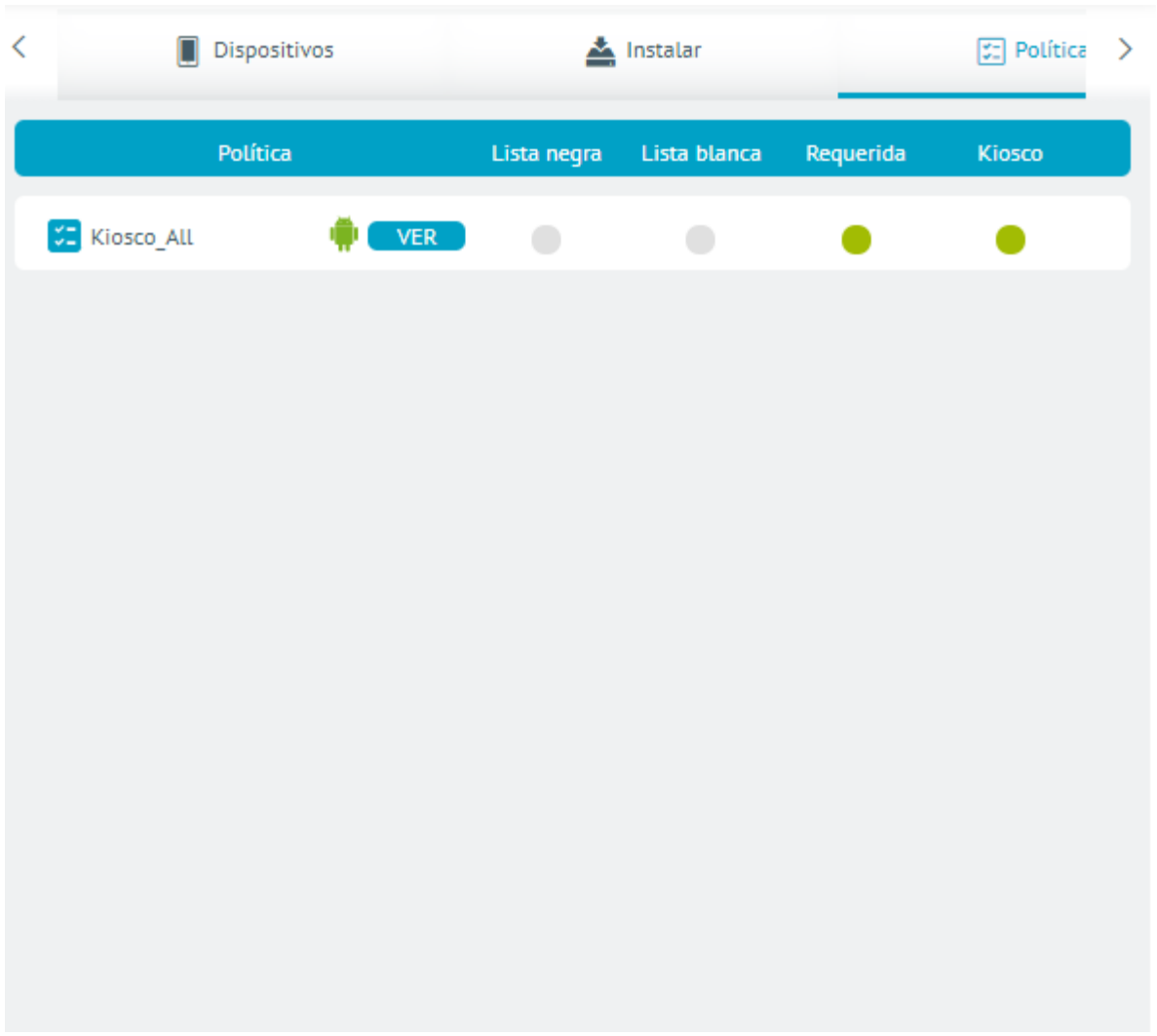


Acciones	Descripción
Desinstalar:	Envía comando de desinstalación a los dispositivos seleccionados.
Enviar Notificación:	Envía un mensaje al agente de los dispositivos seleccionados.
Enviar Correo:	Envía un correo electrónico a los usuarios responsables de cada uno de los dispositivos seleccionados.
Actualizar:	Envia un comando de instalación a los dispositivos que tengan una versión inferior de la aplicacion con respecto a la que aparece en el catálogo.

Pestaña Instalar

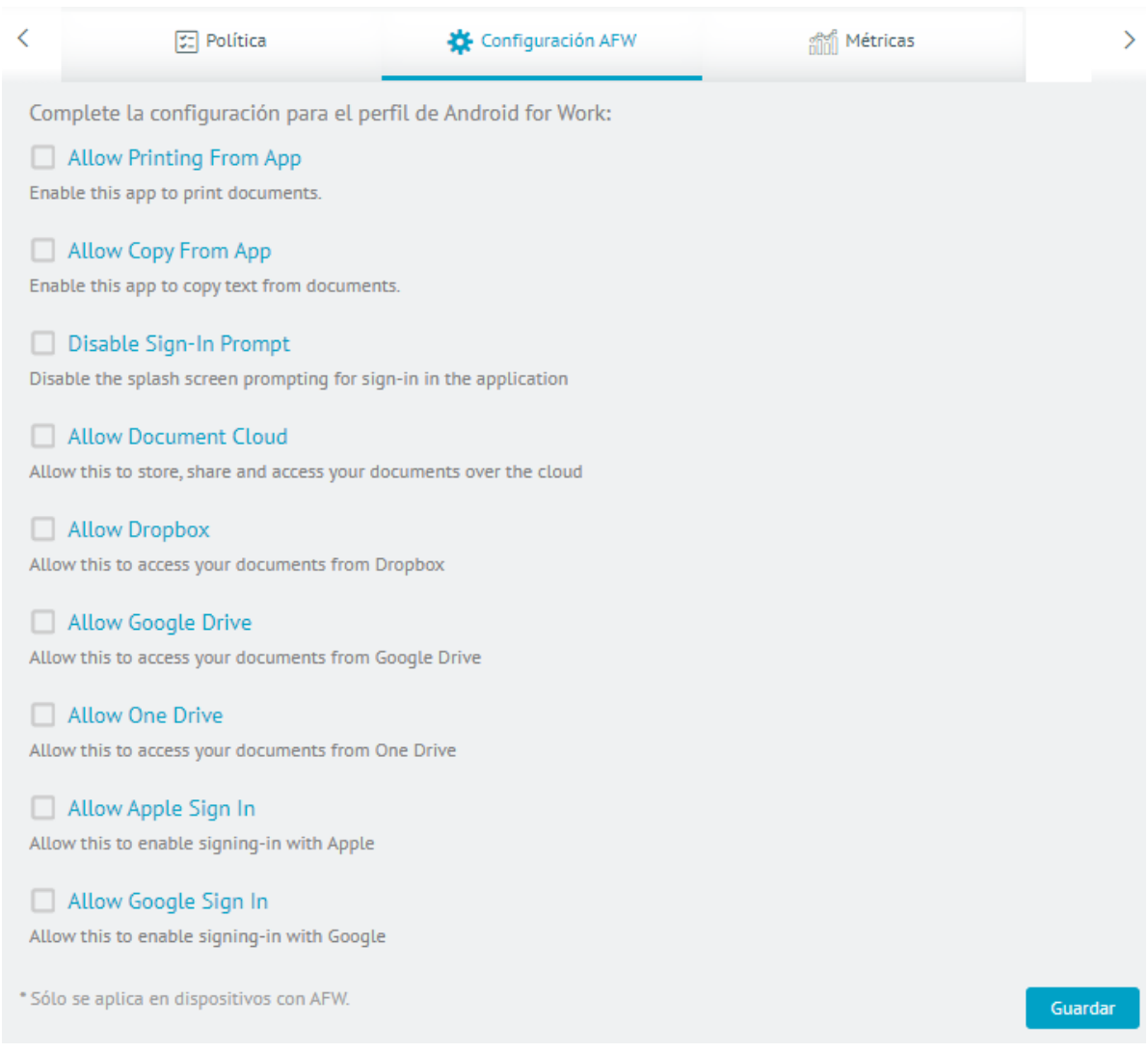
Esta pestaña presenta la opción de envío de comando de instalación de la aplicación a un número limitado de disopsitivos (50 como máximo). Seleccione la opción Buscar Dispositivos, escoger los dispositivos y finalmente la opción Instalar para enviar los comandos.

Pestaña Política



En esta pestaña se presentan las políticas en las que la aplicación esta siendo referenciada y en los items de politica en cuestión donde se usa.

Pestaña Configuracion AFW (Sólo Aplicaciones para Android)



En esta pestaña se presentan las configuraciones manejadas que la aplicacion ha implementado para su funcionamiento en el modo de trabajo para Android For Work. Estas configuraciones son cargadas directamente desde la tienda de Google Play y no son controladas por Aranda ENTERPRISE MOBILE MANAGEMENT AEMM. Cualquier modificación a estas configuraciones, afectará a todos los dispositivos que tengan la aplicación instalada y los dispositivos estén vinculados bajo cualquier modo de AFW (DO o PO). Algunas aplicaciones que son aprobadas por Android For Work pueden ser determinadas mediante las configuraciones manejadas, estas dependen de la naturaleza de las aplicaciones. A continuación, se detallarán algunas de estas:

1. Navegue hasta la opción Aplicaciones y por medio del browser ingrese la aplicación a parametrizar (asegúrese que la app se encuentra importada y marcada como aprobada en AFW desde la consola AEMM)
2. Dar click sobre esta aplicación y al lado derecho se visualizará un formulario con la información correspondiente.
3. Ir a la Opción de Configuración AFW, para estas tenga en cuenta algunas indicaciones o formas de uso.

Configuraciones Manejadas para aplicaciones aprobadas en Android For Work

Las configuraciones generales para aplicaciones, se pueden efectuar sin intervención del cliente, a continuación se describen algunas de estas:

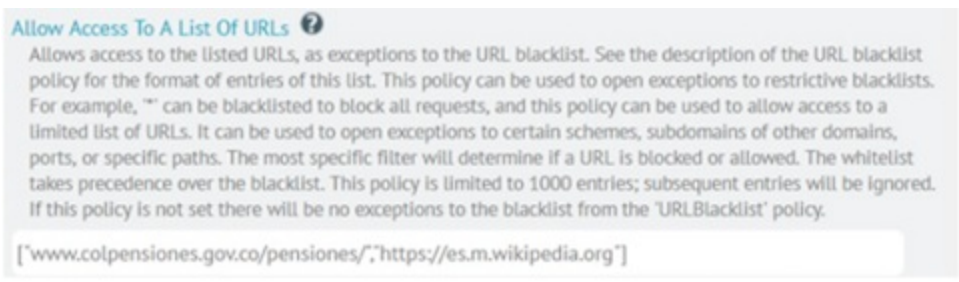
Google Chrome:

En esta aplicación nos encontramos con diferentes opciones de configuración, a continuación, se especificarán algunas de ellas:

Listas Blancas (Permitir el acceso a una lista de URL)

Por medio de esta opción se ingresan las URL autorizadas, convirtiéndose en excepciones a páginas restringidas o URL restringidas (La lista blanca tendrá prioridad sobre las listas negras configuradas). Para realizar la configuración de las listas de URL permitidas o listas blancas, tenga en cuenta las siguientes parametrizaciones o estructuras de ingreso de las URL´s requeridas.

Si una empresa necesita acceder a algunas páginas ingrese con el siguiente formato; ejemplo de lista de URL permitidas:

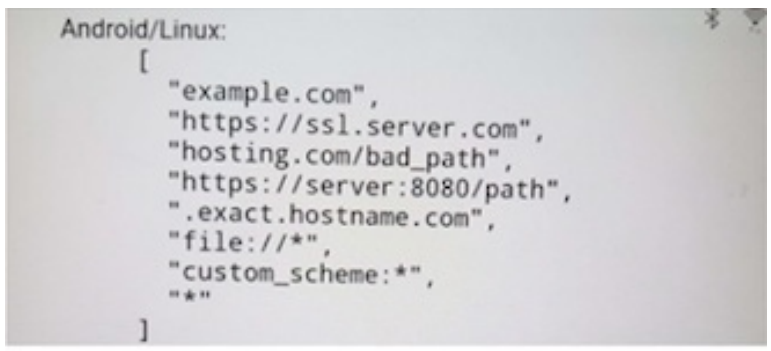


Listas Negras (Bloquear el acceso a una lista de URL)

Por medio de esta opción se restringe URL, convirtiéndolas en listas negras. Para realizar esta configuración tenga en cuenta las siguientes parametrizaciones o estructuras de ingreso en las URL´s requeridas.

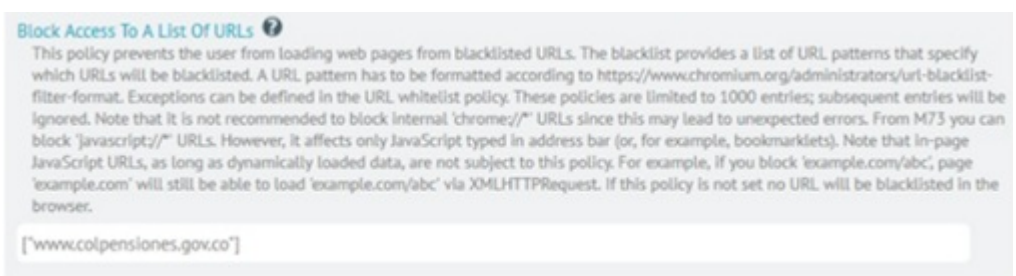
Si una empresa necesita restringir todas las páginas, ingrese el siguiente patrón [{"*"}] en lista negra para que bloquee todo.

Ejemplo restricción de todas las páginas:



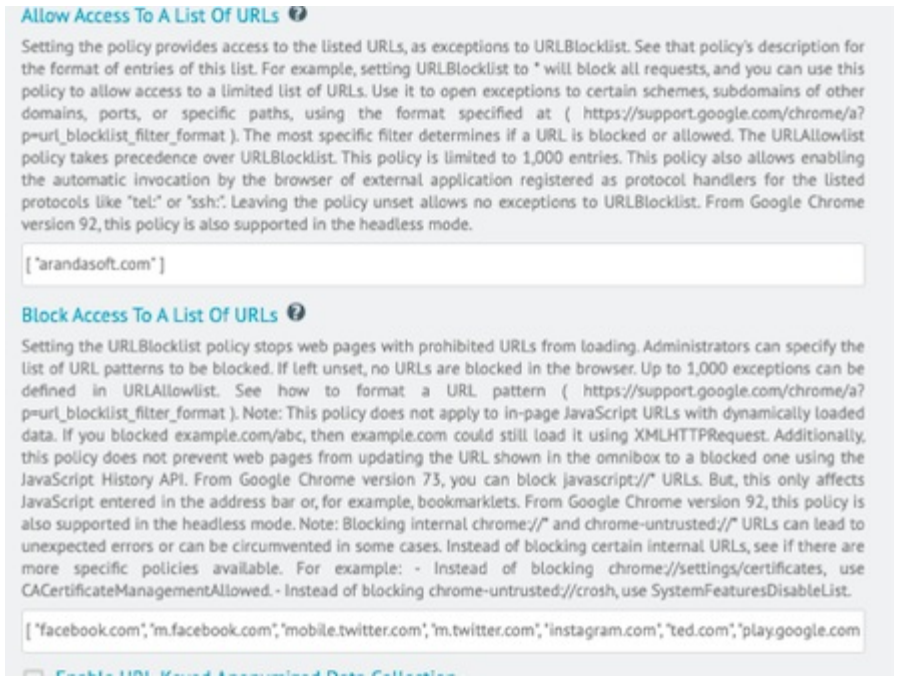
Si una empresa necesita restringir algunas páginas ingresar las URL's correspondientes.

Ejemplo restricción de todas las páginas:



Configuración Mixtas listas Blancas y Negras

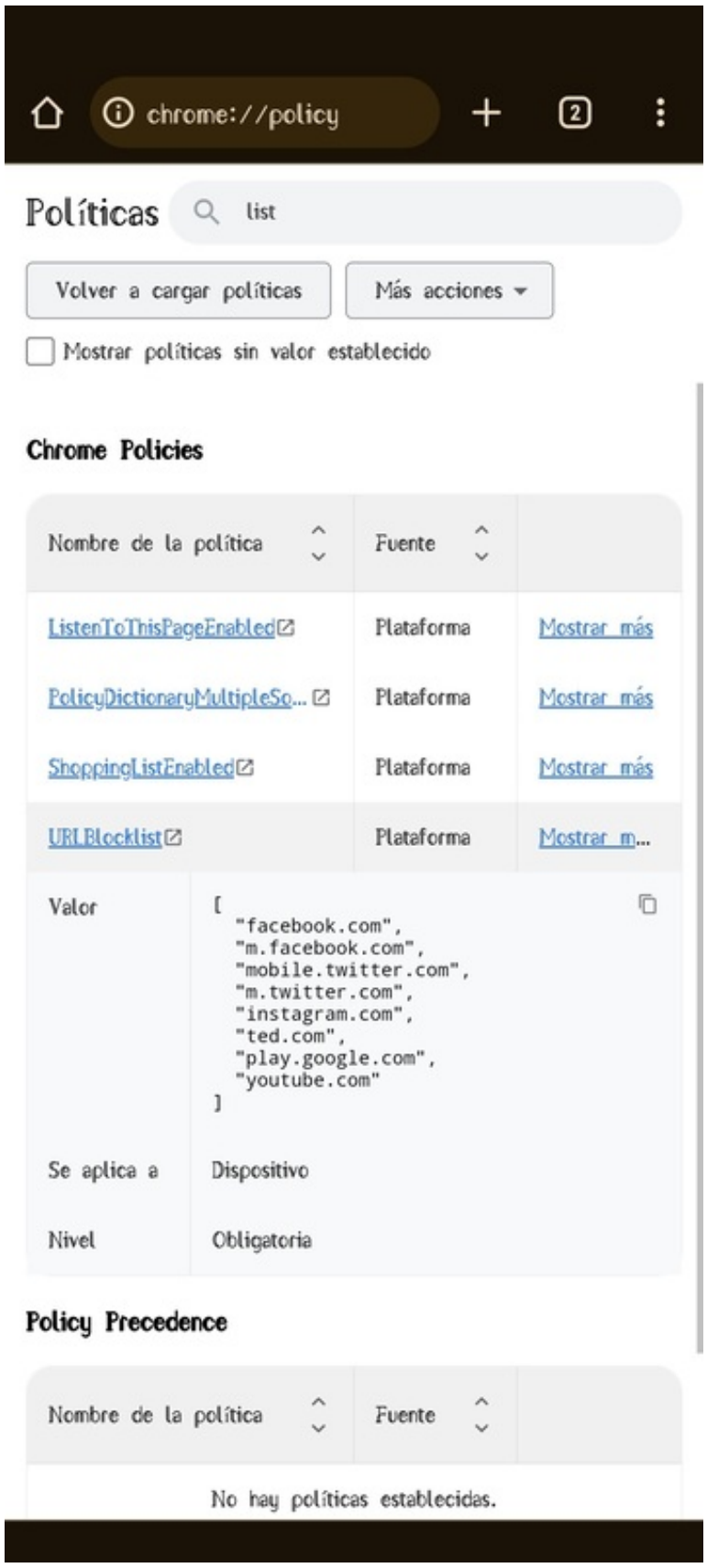
A continuación se presenta la combinación de políticas de listas blancas y negras; en el primer recuadro se observa la restricción de dominio y en el segundo recuadro podrá visualizar una lista de páginas con excepción de bloqueo y una de estas hace parte del dominio restringido; es decir dar permisos al subdominio.



¿Cómo consultar las configuraciones manejadas AFW desde su dispositivo?

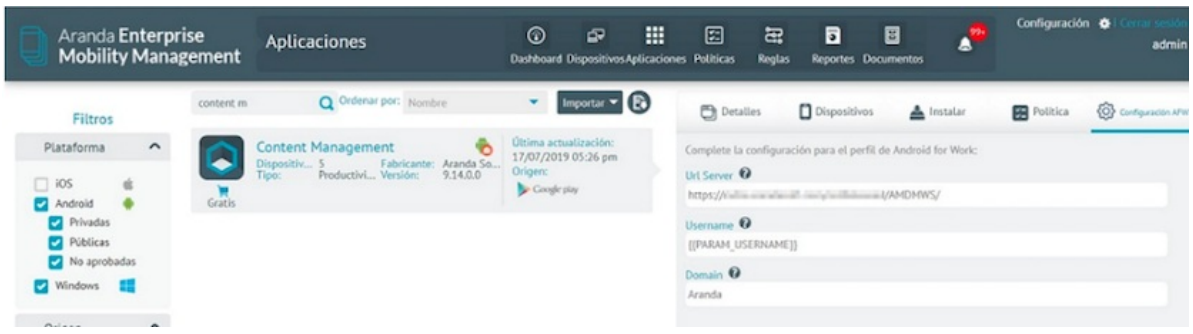
Desde su dispositivo podrá consultar las políticas configuradas desde consola; ingrese la URL en el buscador de Chrome y registre la siguiente línea:

Chrome://policy Se visualizará los nombres de las políticas aplicadas



Aranda Content Manager

Url de Servidor Dominio Usuario



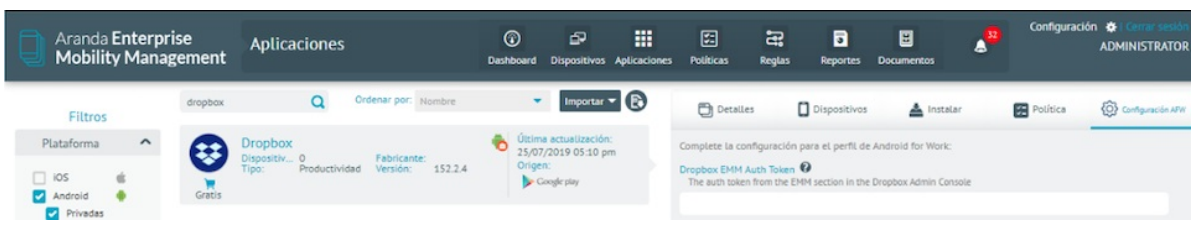
Dropbox

A través de las configuraciones manejadas, esta aplicación permite configurar su uso sólo a dispositivos administrados, a través del token de autenticación generado en la consola de configuración de su cuenta Dropbox Business con plan Enterprise.

A través de la consola de configuración de Dropbox, puede agregar excepciones a la regla EMM correspondiente, de tal manera que sólo los usuarios agregados en dichas excepciones puedan iniciar sesión desde la aplicación Dropbox aprobada en AFW en AEMM, e instalada en los dispositivos.

Para mayor información acerca de la configuración de excepciones a la regla EMM en la consola de configuración de Dropbox, visite el siguiente enlace:

https://help.dropbox.com/es-la/teams-admins/admin/enterprise-mobility-management



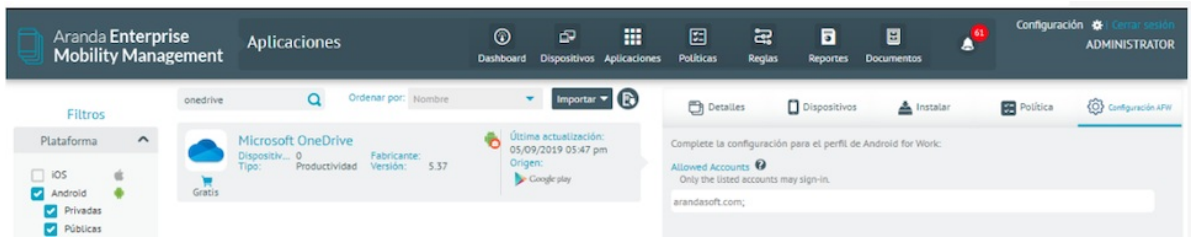
Microsoft OneDrive

Las configuraciones manejadas de Microsoft OneDrive permiten agregar cuentas permitidas, garantizando que solo podrá iniciar sesión en la aplicación aprobada en AFW desde AEMM, e instalada en los dispositivos, con dichas cuentas.

Para hacer efectiva la funcionalidad, agregue las directivas de configuración de aplicaciones para dispositivos Android administrados, a través del portal Azure de su directorio activo. Para acceder, debe ingresar su cuenta de correo empresarial.

Para mayor información acerca de la configuración de aplicaciones para dispositivos Android administrados en el portal Azure, visite el siguiente enlace:

https://docs.microsoft.com/es-mx/intune/app-configuration-policies-use-android

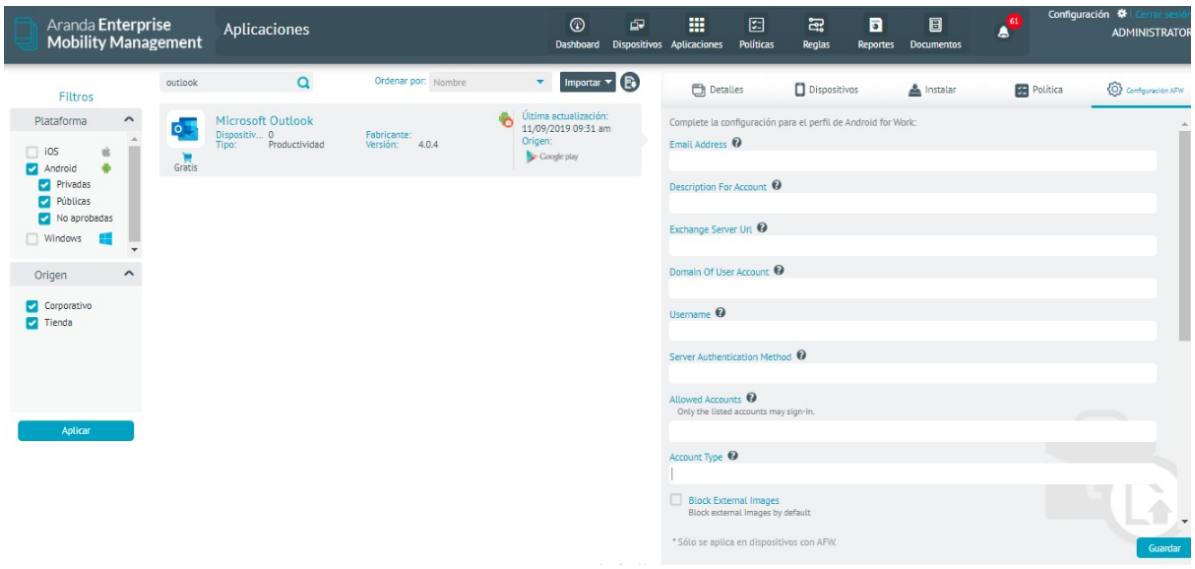


Microsoft Outlook

Esta aplicación admite configuraciones manejadas, las cuales permiten personalizar su comportamiento tanto al servicio de Office 365 como a los MDM.

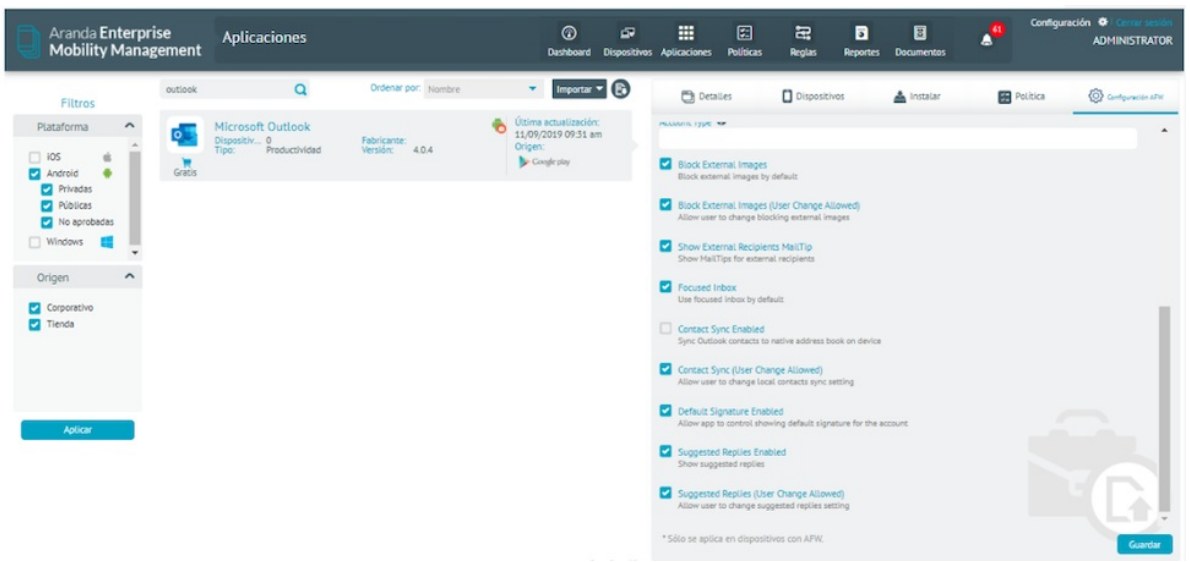
Existen dos secciones de configuración disponibles se clasifican en Configuración de la cuenta y Configuración general de la aplicación.

La configuración de la cuenta se realiza a través de los siguientes campos:



Campos	Descripción
Email Address:	Dirección de correo electrónico que se va a usar para enviar y recibir correos. Los valores aceptados son direcciones de correo electrónico con formato tradicional; ejemplo user@companyname.com.
Descripiotn For Account:	Descripción de la cuenta para poder identificarla.
Exchange Server Url:	Dirección URL del servidor Exchange asociado a su directorio activo. Generalmente para correos empresariales bajo de Office 365, la dirección URL es outlook.office365.com.
Domain Of User Account:	Especifica el dominio de la cuenta de usuario, generalmente es el nombre de la compañía y es exactamente el que se encuentra en el dominio de su correo. Para el caso ejemplo, será companyname.
Username:	Especifica el nombre de usuario asociado a la cuenta de correo que se está configurando.
Server Authentication Method:	Determina el método de autenticación del usuario. Para una autenticación básica, el método será por usuario y contraseña, y se debe ingresar el valor Username and Password.
Allowed Accounts:	Listado de cuentas habilitadas para iniciar sesión, separadas por punto y coma (;).
Account Type:	Determina el tipo de cuenta que se está configurando, de acuerdo al modelo de autenticación, para el caso ejemplo será BasicAuth ya que se está realizando una autenticación básica.

Para la configuración general de la aplicación, se utilizan los siguientes campos:



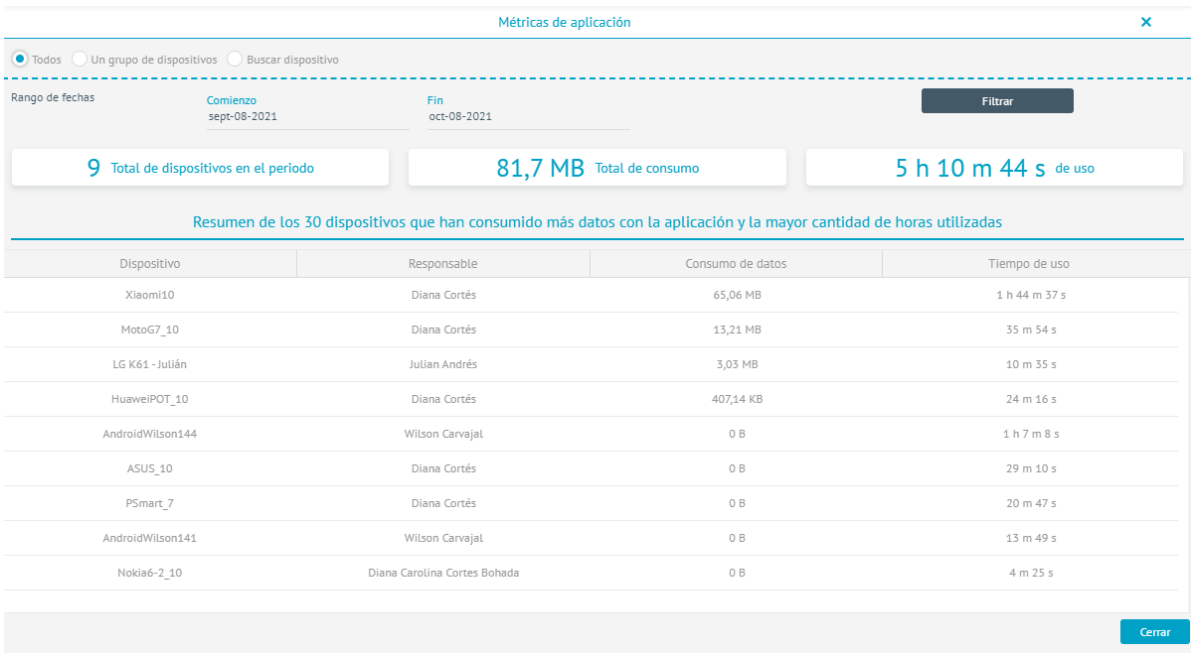
Campos	Descripción
Block External Images:	Determina si se bloquea la visualización de imágenes externas.
Block External Images (User Change Allowed):	Determina si el usuario puede cambiar la configuración de bloqueo de visualización de imágenes externas.
Show External Recipients MailTip:	Determina si se muestran sugerencias de correos de destinatarios externos.
Focused Inbox:	Determina si está habilitada la bandeja de entrada “Prioritarios”.
Contact Sync Enabled:	Determina si se habilita la sincronización de contactos de Outlook con la aplicación de contactos nativa.
Contact Sync (User Change Allowed):	Determina si el usuario puede cambiar la configuración de sincronización de contactos de Outlook con la aplicación de contactos nativa.
Default Signature Enabled:	Determina si la aplicación usa la firma predeterminada.
Suggested Replies Enabled:	Determina si se habilita las respuestas sugeridas a correos entrantes.
Suggested Replies (User Change Allowed):	Determina si el usuario puede cambiar la configuración de las respuestas sugeridas a correos entrantes.

Pestaña Métricas

Esta pestaña presenta información acerca de las métricas recolectadas desde los dispositivos con relación a los datos consumidos y uso de la aplicación en los dispositivos que la tienen o tuvieron instalada.

Como primer dato se mueestra el conteo de dispositivos que tienen instalada la aplicación y han reportado métricas de dicha aplicación.

Para detallar las métricas seleccione la opción Conocer Métricas.



En esta pantalla de pueden ver consolidados los reportes que los dispoisitivos han realizado sobre el consumo de datos y uso de la aplicación.

Se pueden filtrar los datos por:

- Todos los dispositivos, grupos de dispositivos, un dispositivo en cuestión
- Rango de fechas

Instalación usando URI Externa

AEMM provee un mecanismo para usar URIs externas para almacenar archivos de instalación y asi proveer una mayor velocidad y disponibilidad en la descarga para los dispositivos móviles.

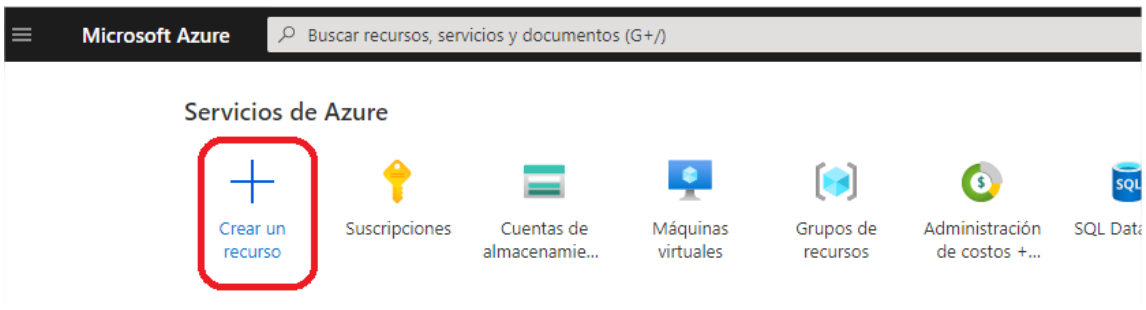
A continuación se presenta un ejemplo de creación y utilización de una URI externa usando como almacen una cuenta de almacenamiento de Microsoft Azure.

Precondiciones:

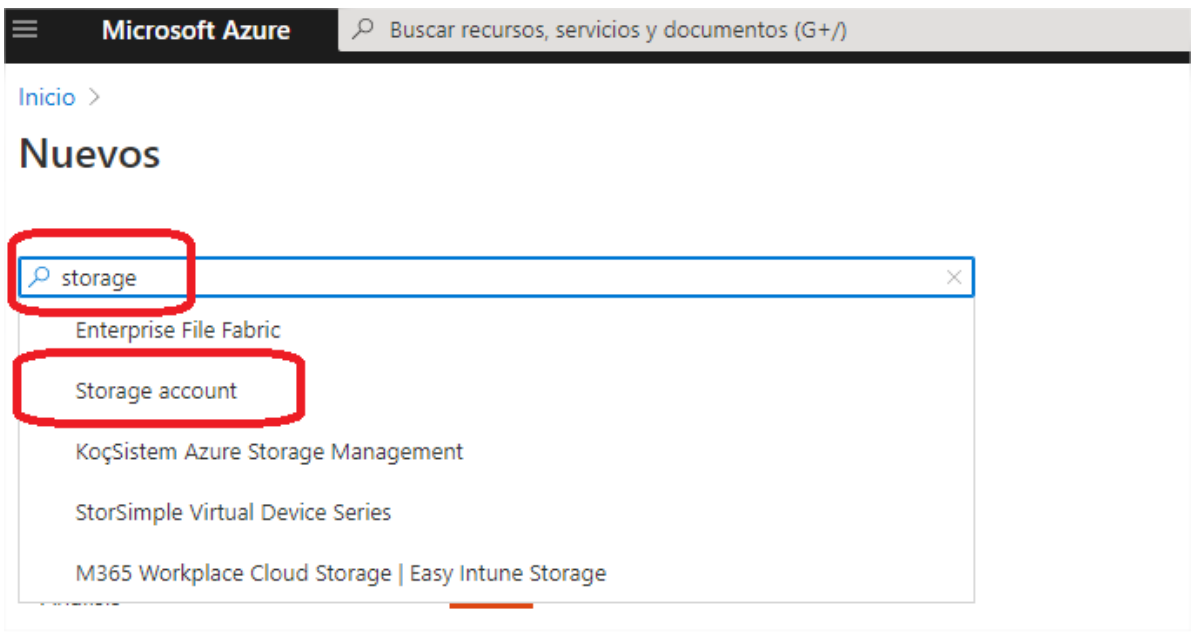
- Una cuenta activa y con saldo disponible en Microsoft Azure
- Archivo APK de la aplicación en cuestión
- Nombre del paquete de la aplicación

Proceso De Carga Y Publicación De Archivo En Microsoft Azure

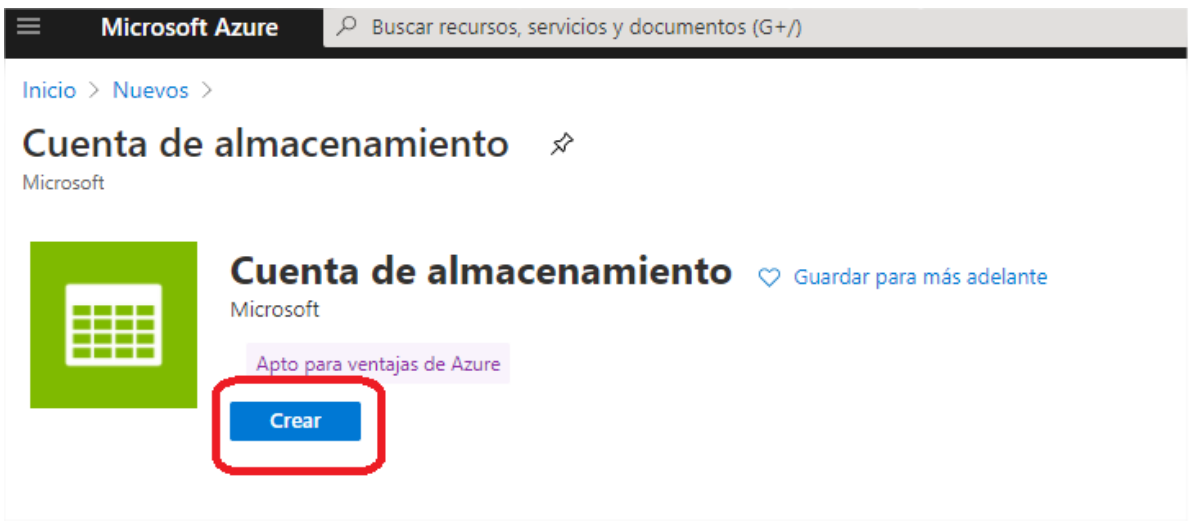
1. Ingrese a Microsoft Azure (https://portal.azure.com/#home)
2. Clic en la opción crear un recurso.



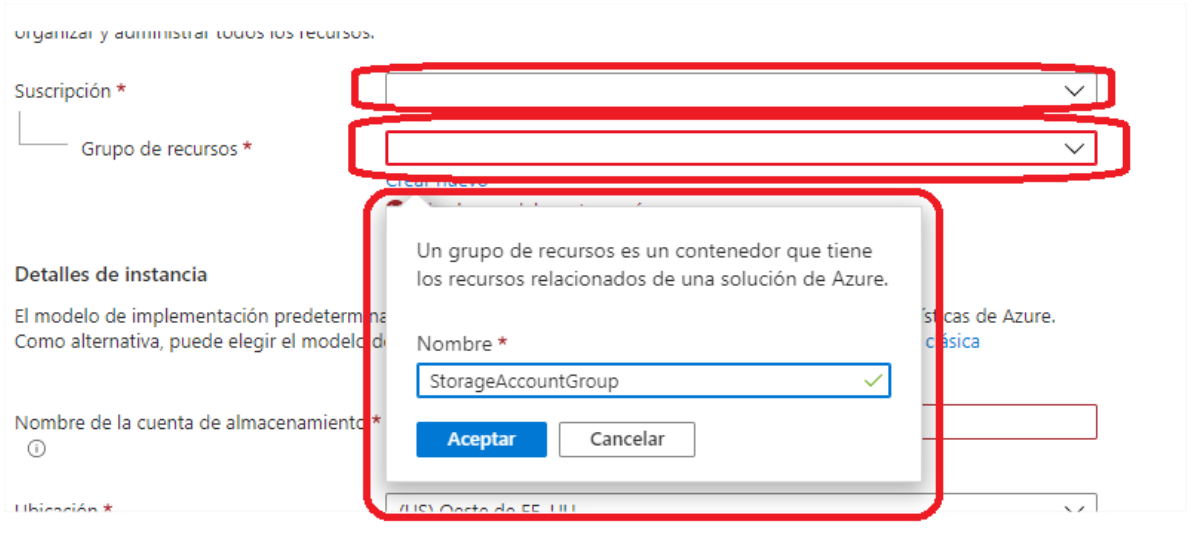
1. Escriba en la barra de búsqueda de recursos la palabra “storage” y luego clic en “Storage Account” o en español “Cuenta de almacenamiento”.



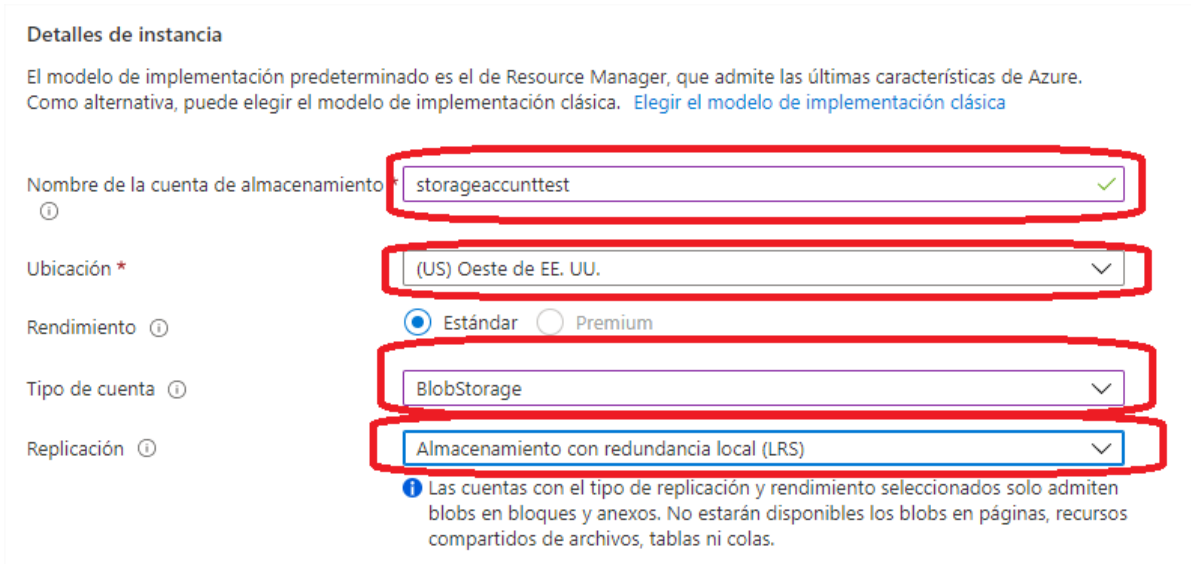
1. Clic en “Crear”.



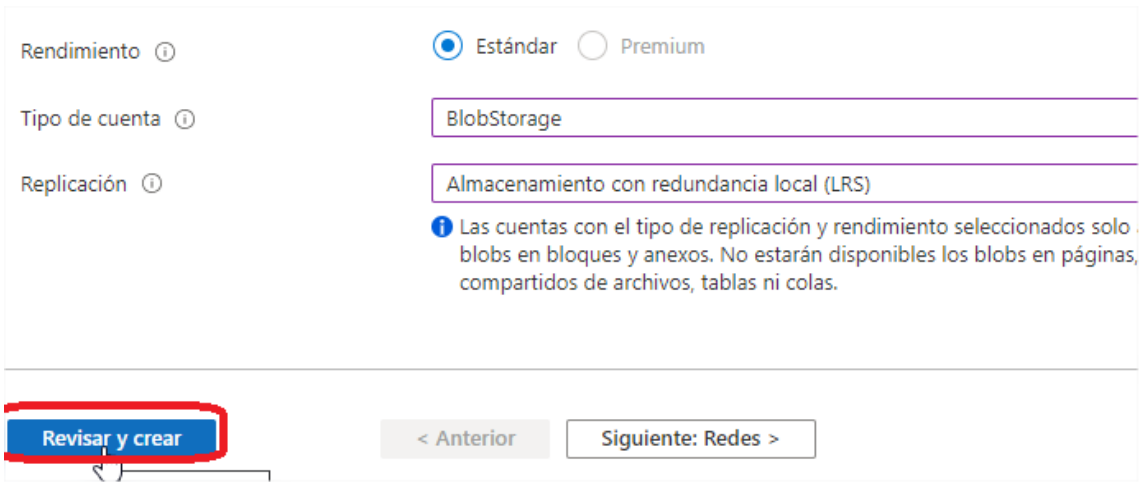
1. Escoja la suscripción y escoja o cree un grupo de recursos.



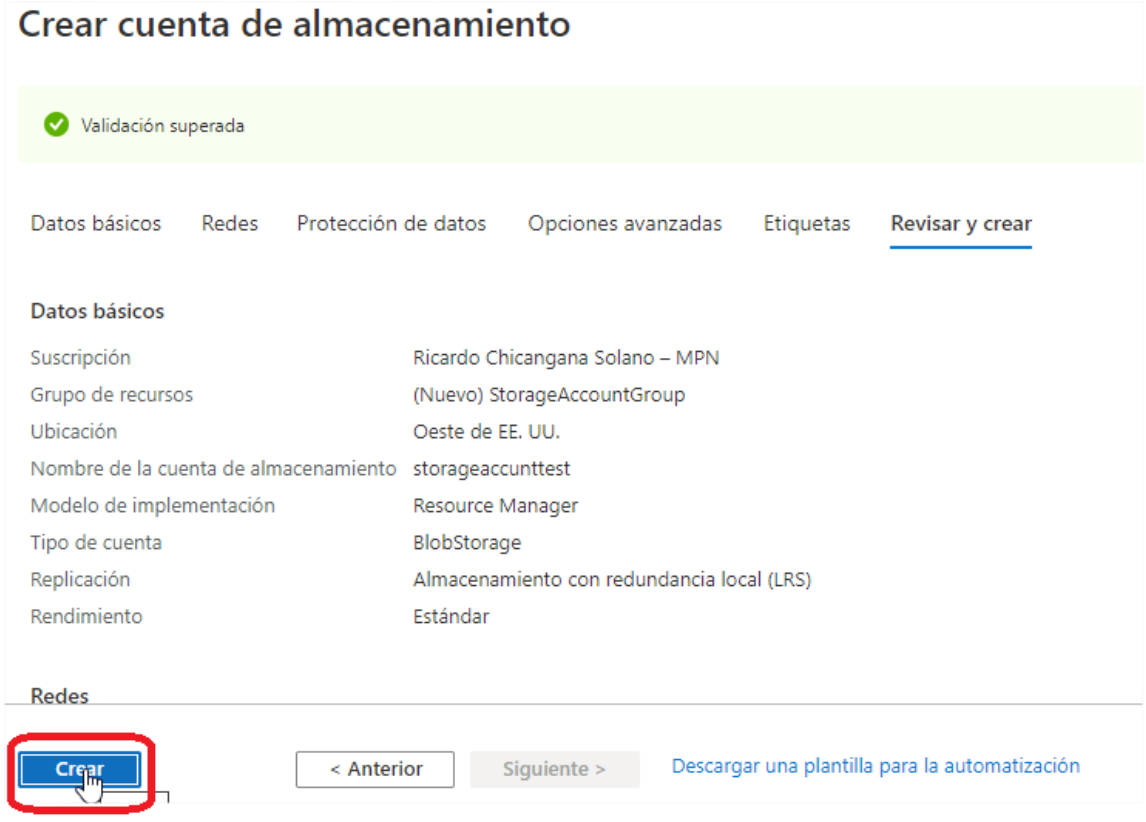
1. Escriba el nombre de la cuenta de almacenamiento, escoja la ubicación o simplemente déjela en la predeterminada, en el tipo de cuenta escoja “BlobStorage”, y por ultimo escoja la replicación con redundancia local (opción más económica), o escoja el tipo de replicación a su conveniencia.



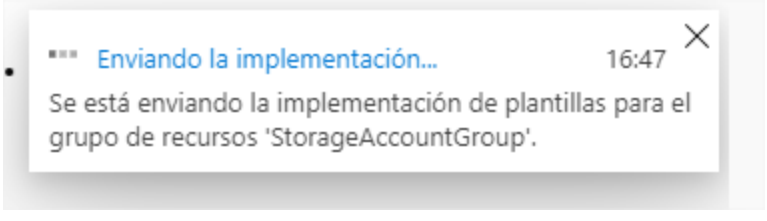
1. Haga clic en “Revisar y crear”.



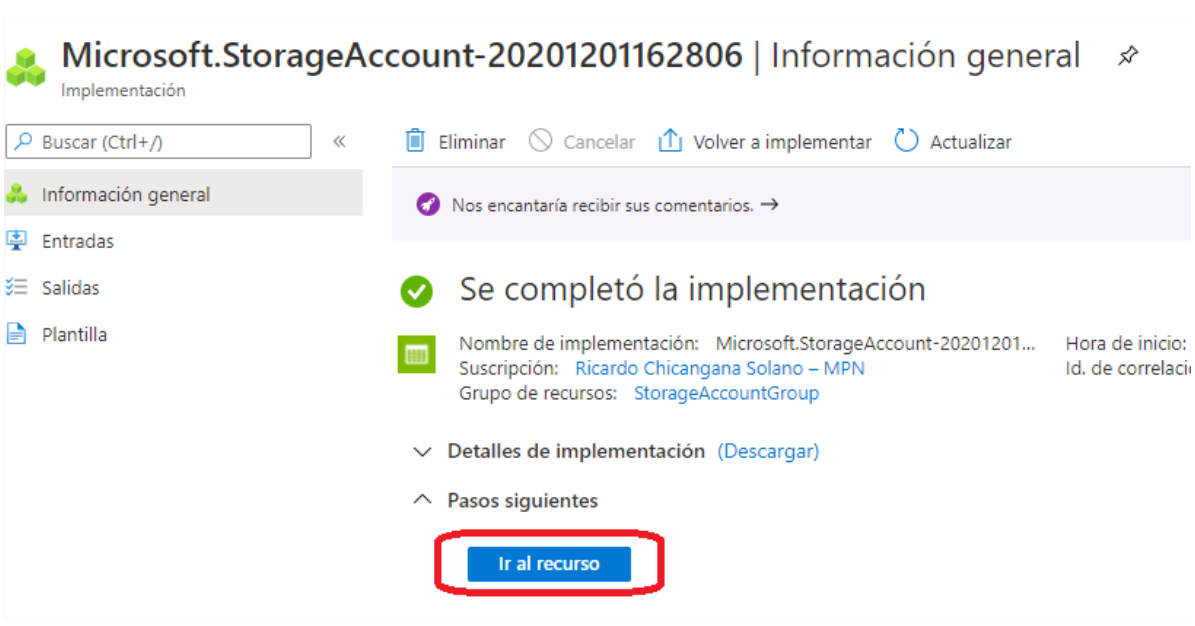
1. Haga clic en “Crear”.



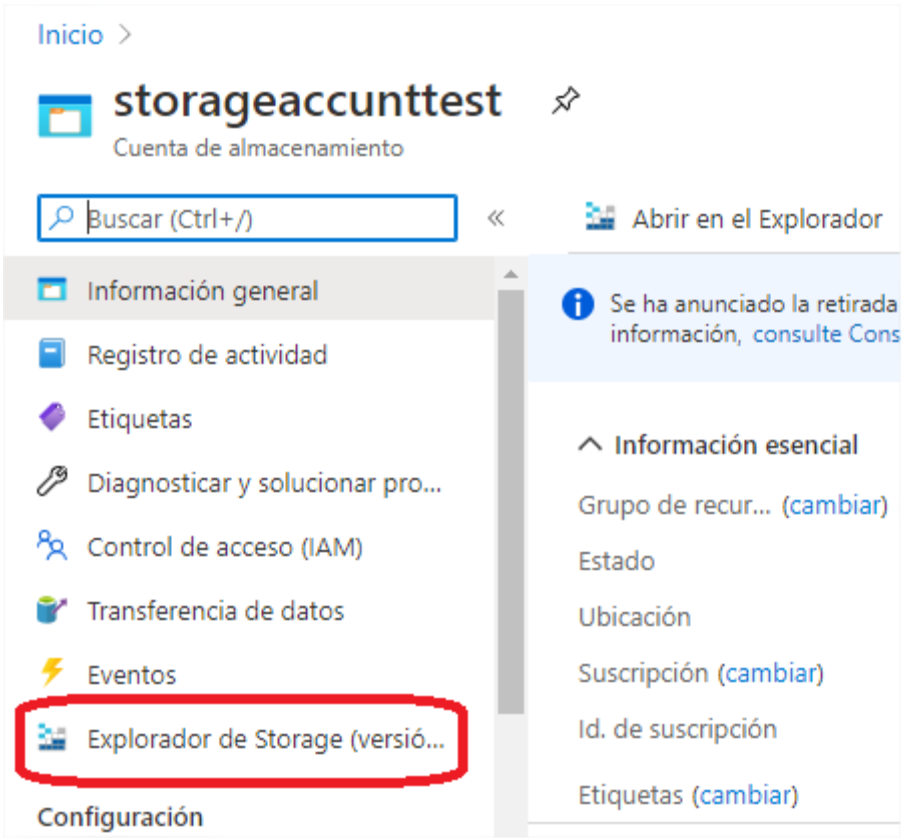
1. Espere a que el recurso sea creado.



1. Una vez creado el recurso haga clic en “Ir al recurso”.

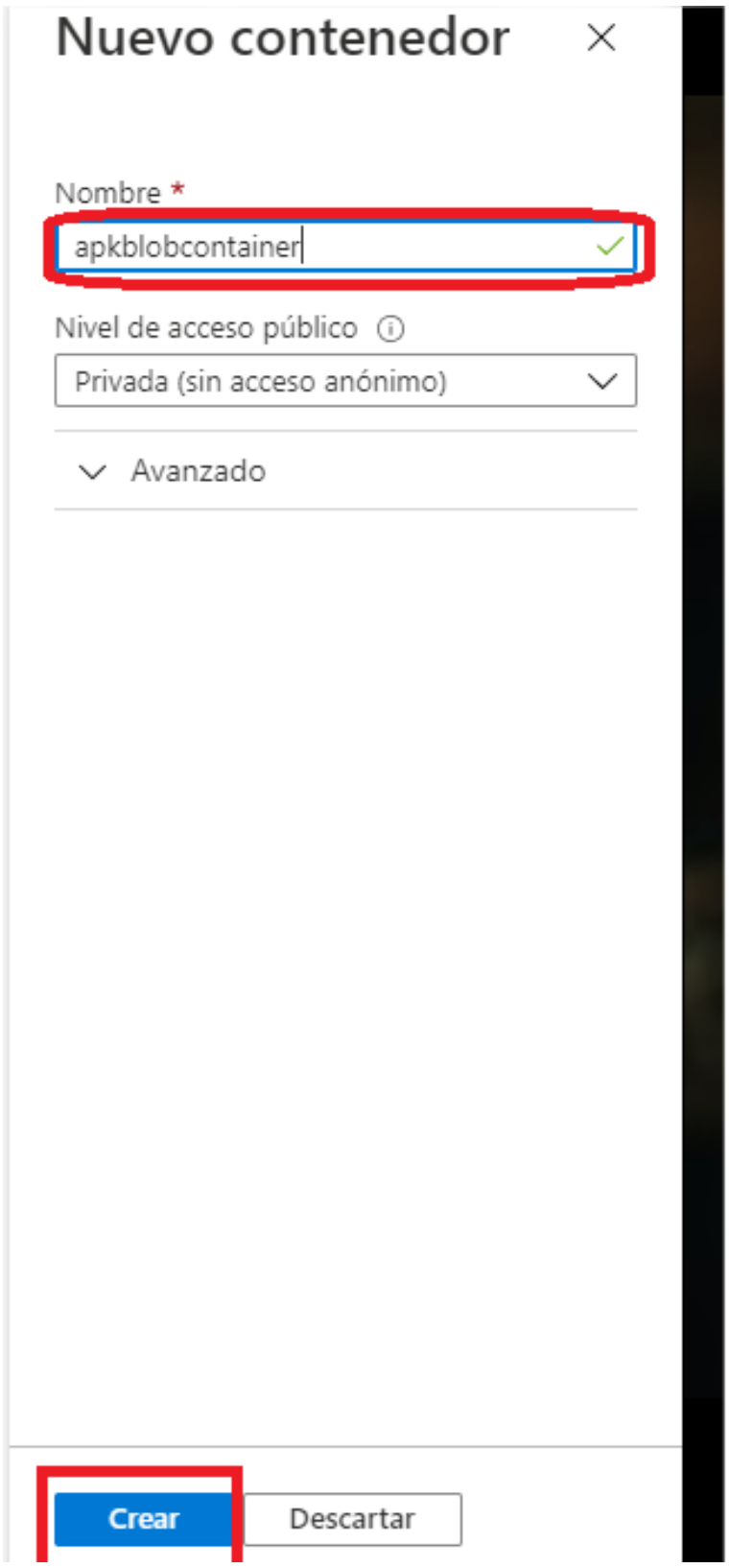


1. En la interfaz del recurso haga clic en “Explorador de Storage”.

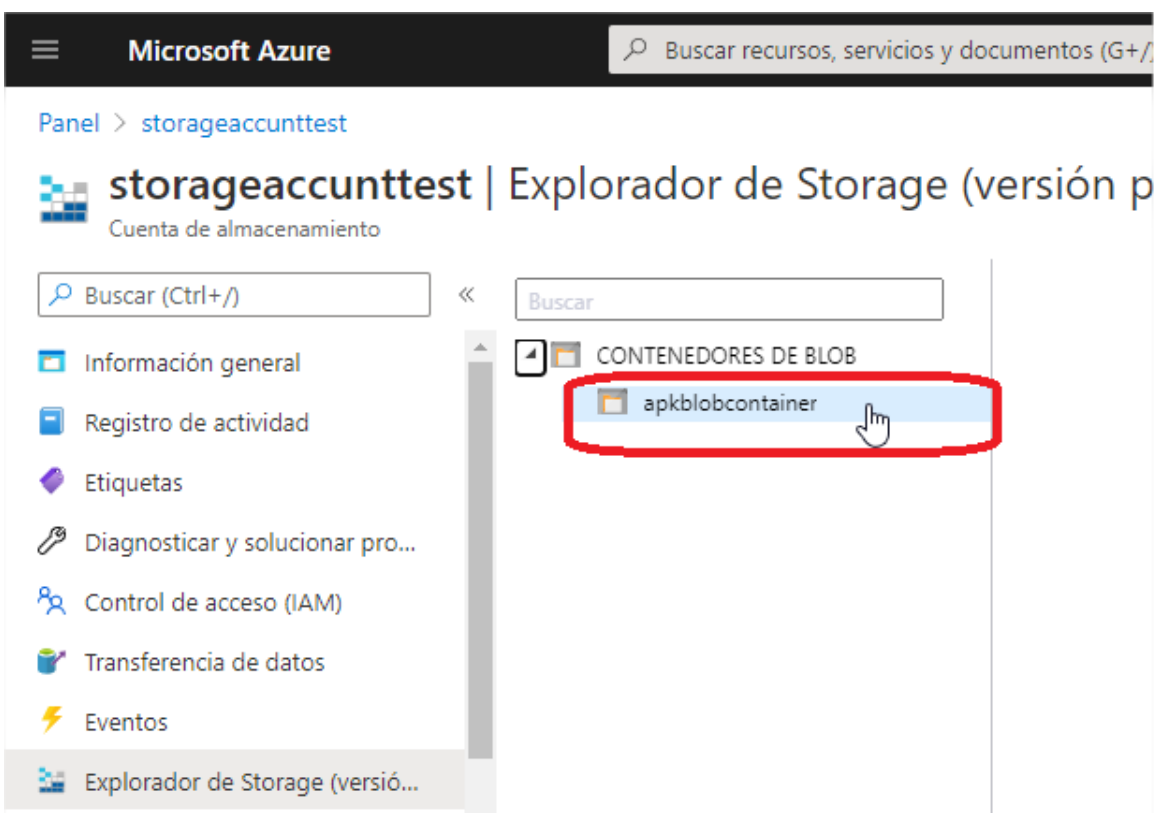


1. Ya en el explorador, haga clic derecho sobre “CONTENEDORES DE BLOB”, luego en el menú emergente haga clic sobre “Crear contenedor de blobs”.

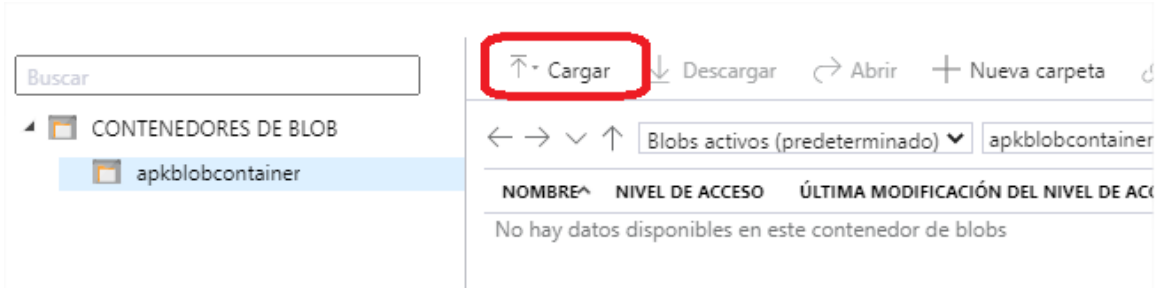
Ingrese el nombre del nuevo contenedor y luego haga clic en “Crear”



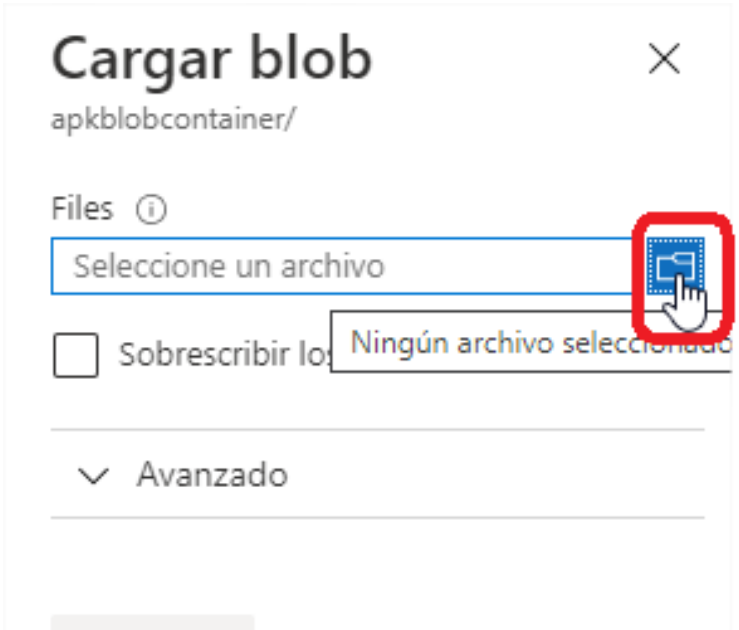
1. De ser necesario refresque la página para que aparezca el nuevo contenedor creado. Luego expanda el árbol de contenedores y haga clic sobre el que se acaba de crear.



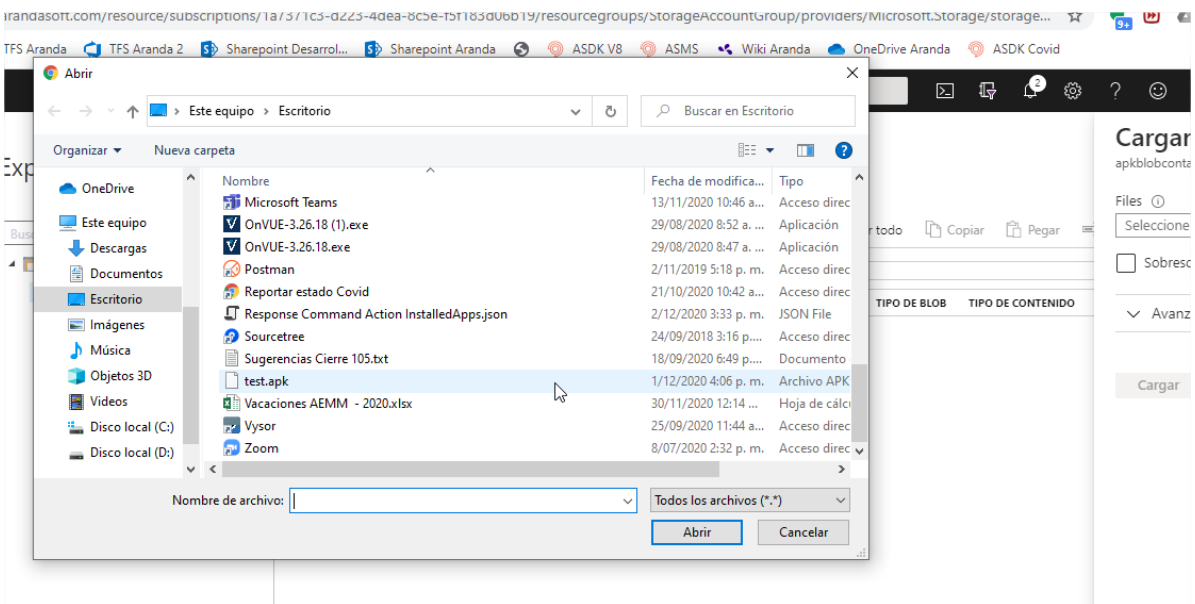
1. Haga clic en “Cargar”.



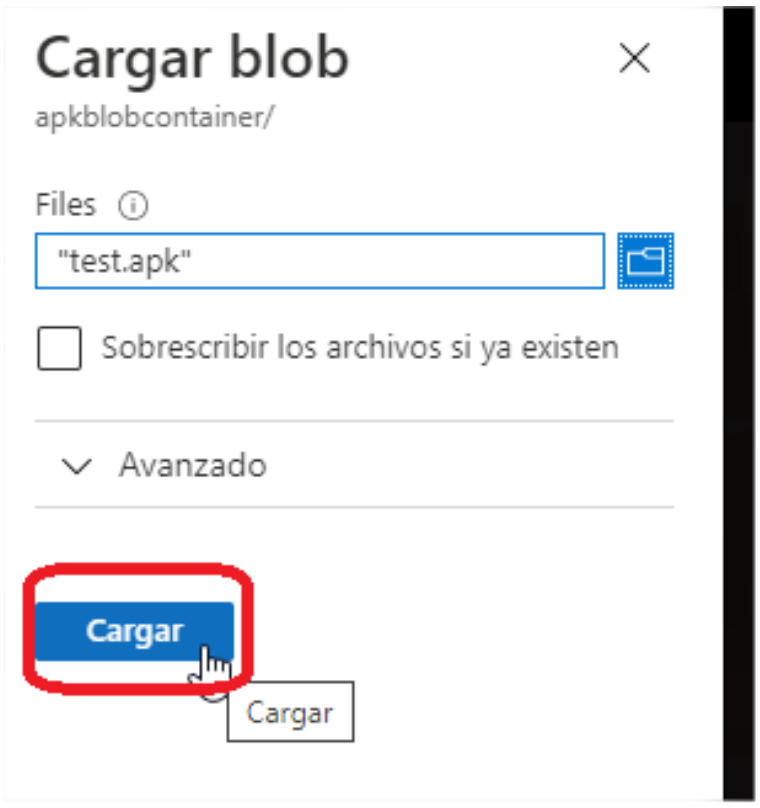
1. Haga clic en el ícono de archivo.



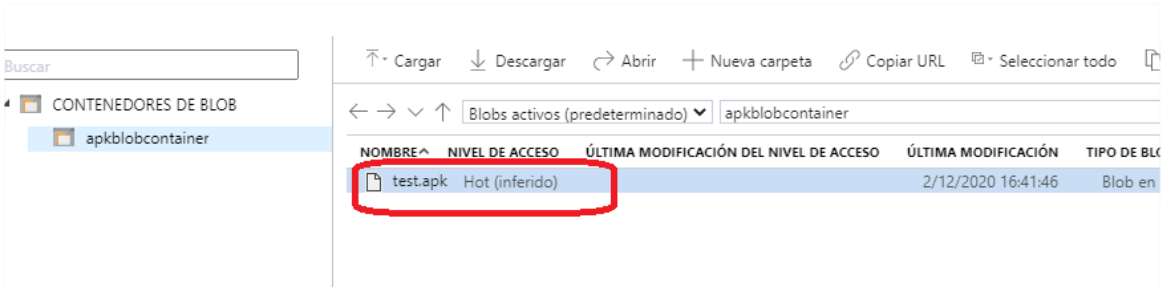
1. Ubique y escoja el archivo APK o IPA específico.



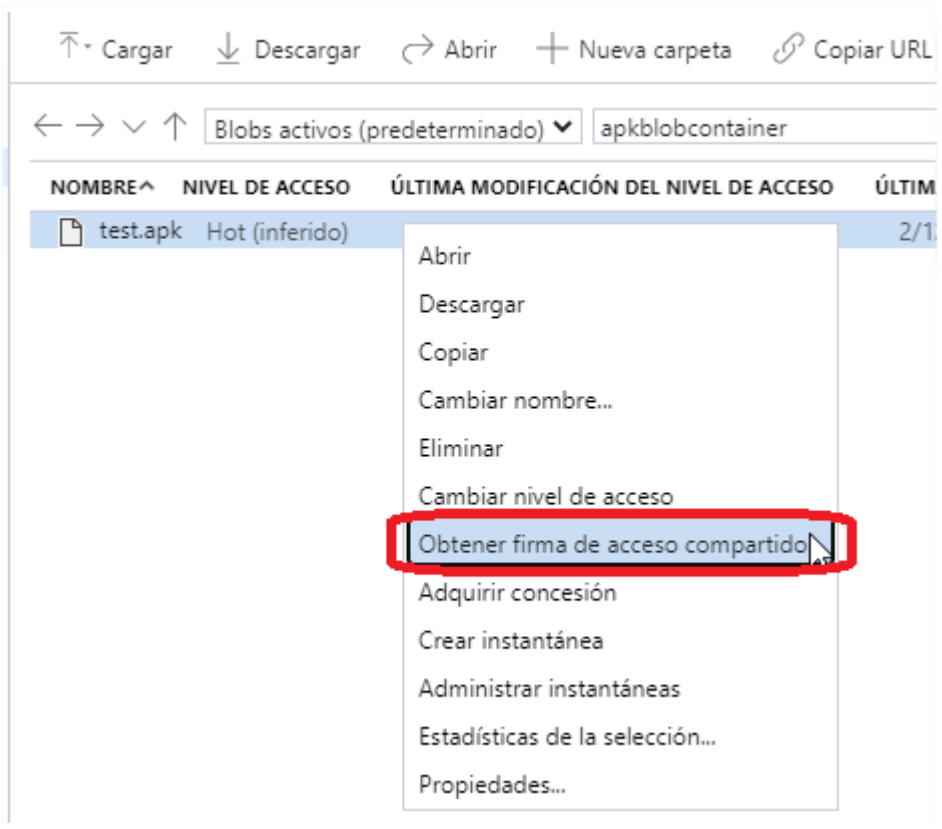
1. Haga clic en “Cargar”.



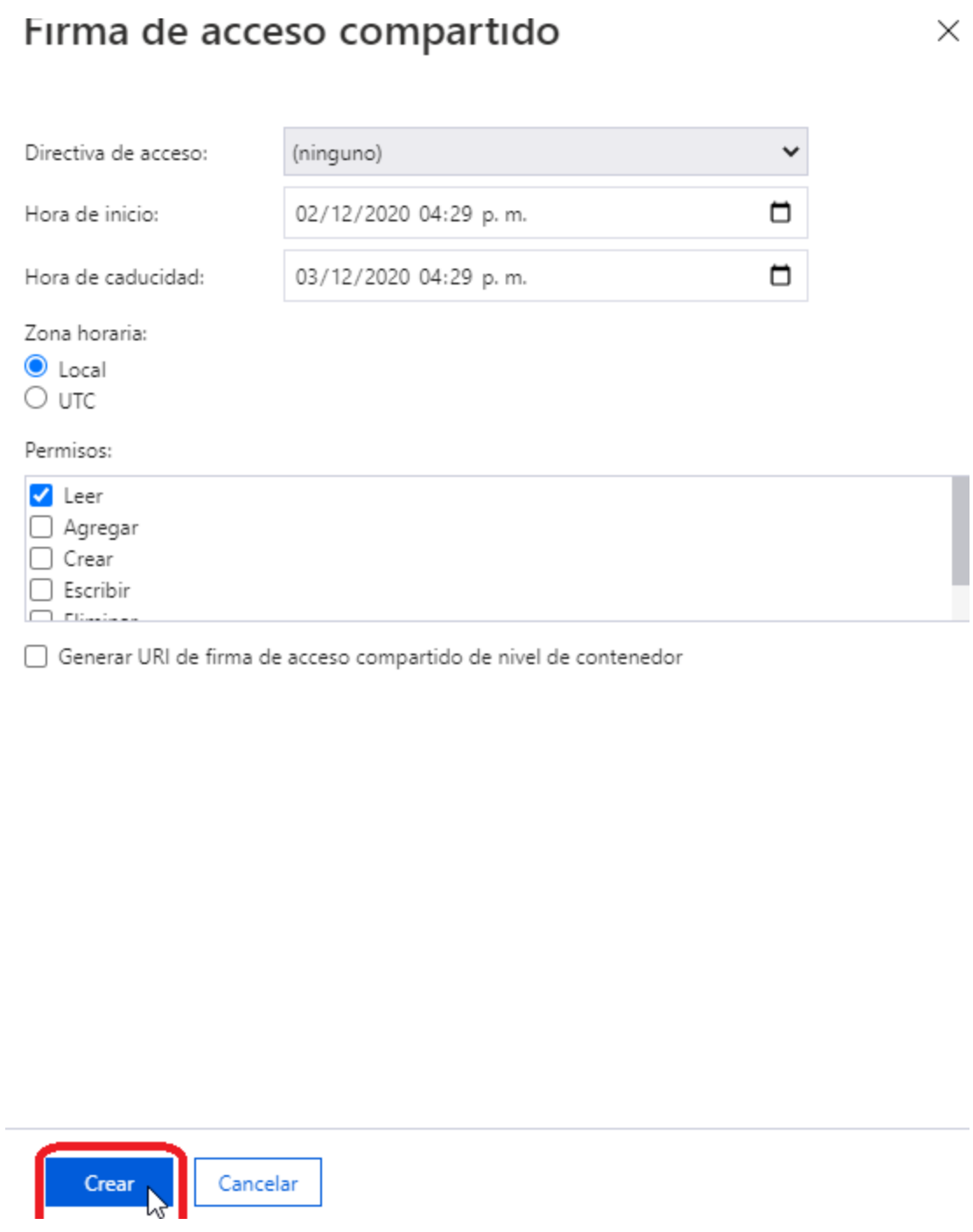
1. Una vez completada la carga del archivo aparecerá en el explorador.



1. Haga clic derecho sobre el archivo cargado y luego clic en “Obtener firma de acceso compartido”.

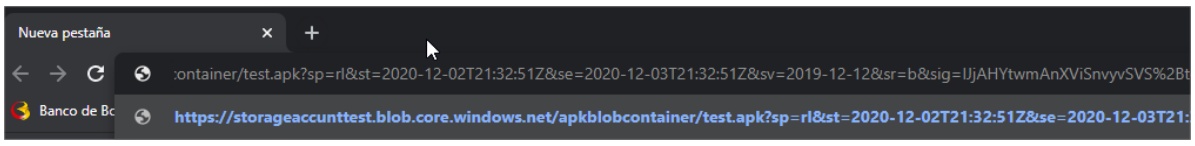


1. Haga clic en “Crear”, teniendo en cuenta la caducidad del enlace, dado que cuando dicho enlace caduque será necesario la creación de un nuevo enlace.



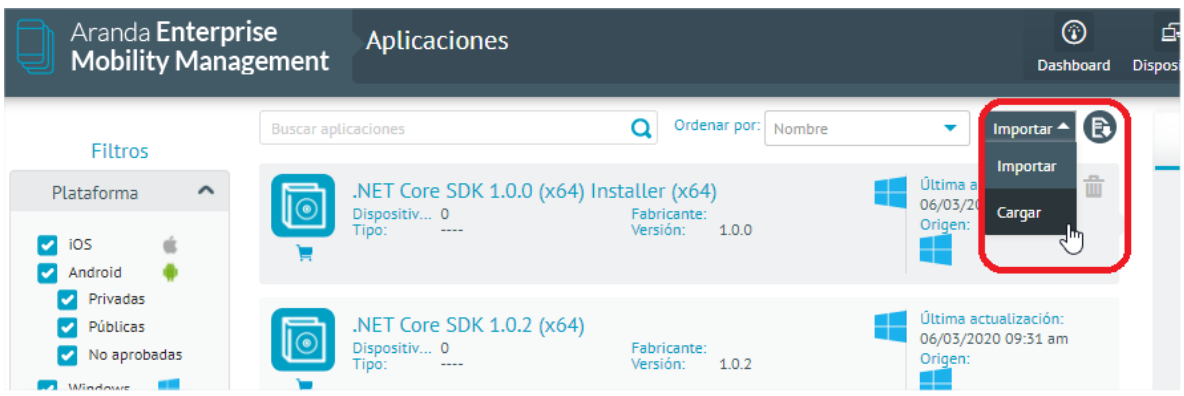
1. Haga clic en copiar de la sección URI.

1. Abra un navegador y pegue la URI copiada en la parte de direcciones y compruebe que la descarga del archivo se hace correctamente.

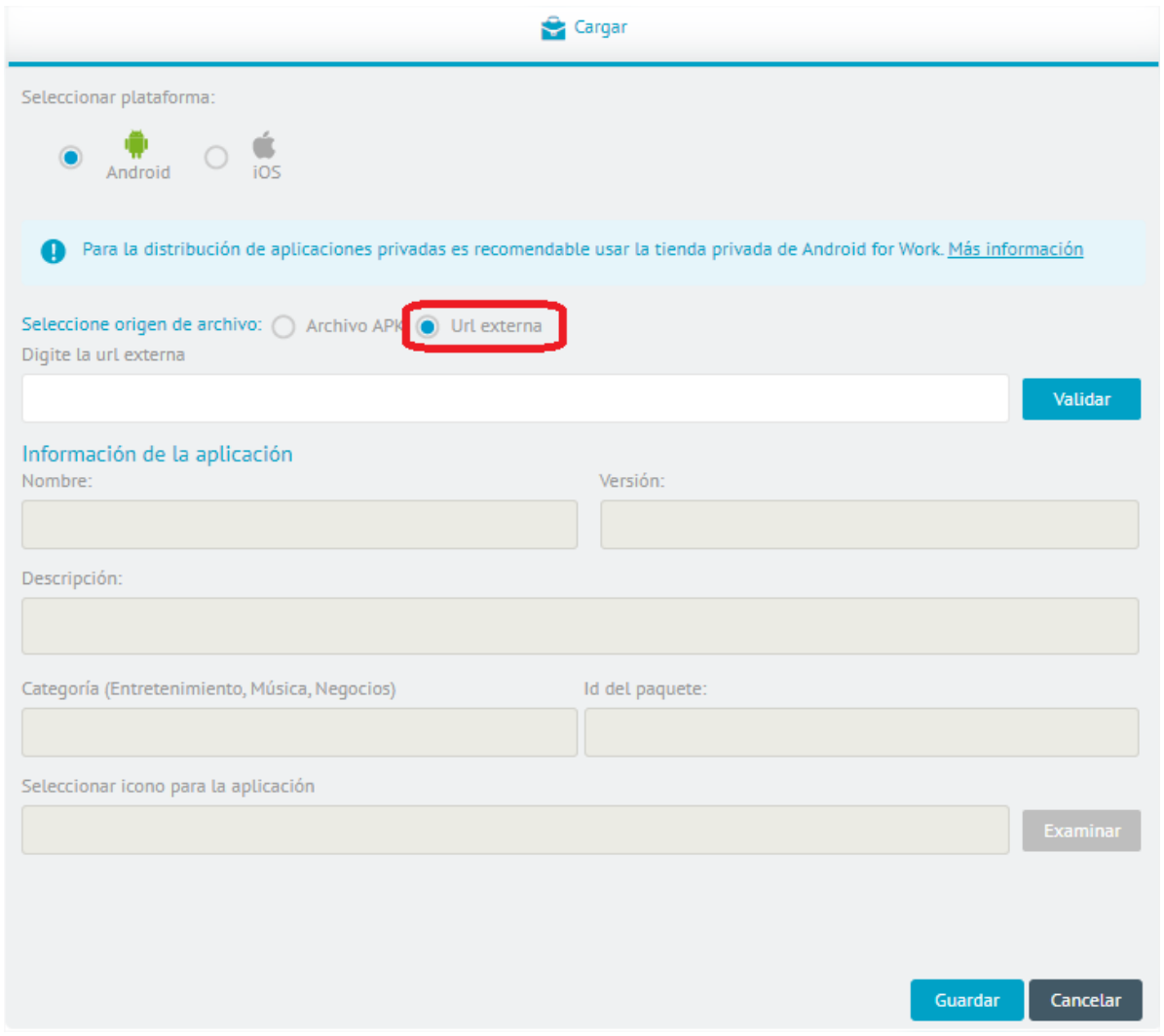


Utilización De La Uri Creada En Microsoft Azure Como Url Externa de Aplicación

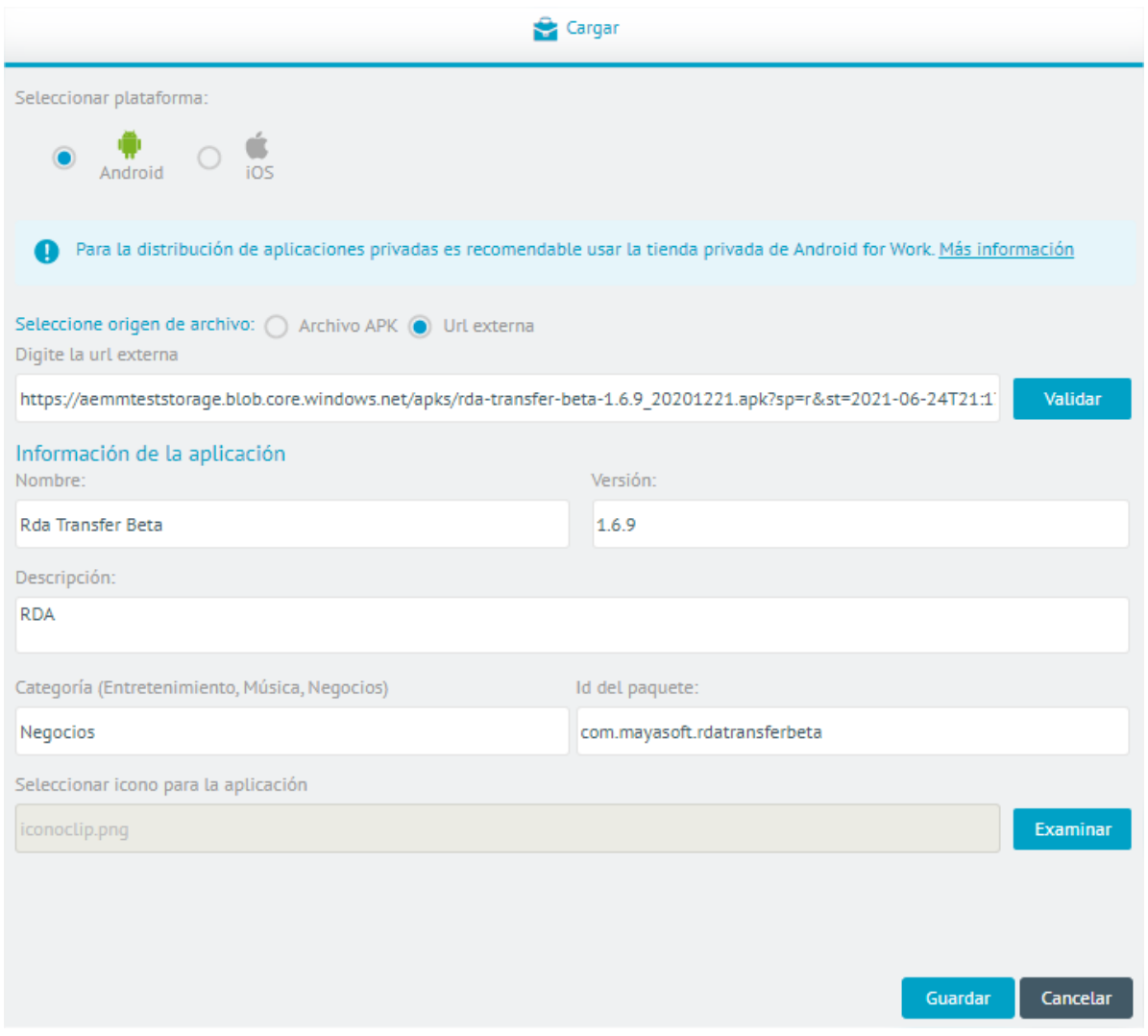
1. Ingrese a la consola AEMM y vaya a la sección aplicaciones, luego haga clic en la opción “Cargar” del menú “Importar”.



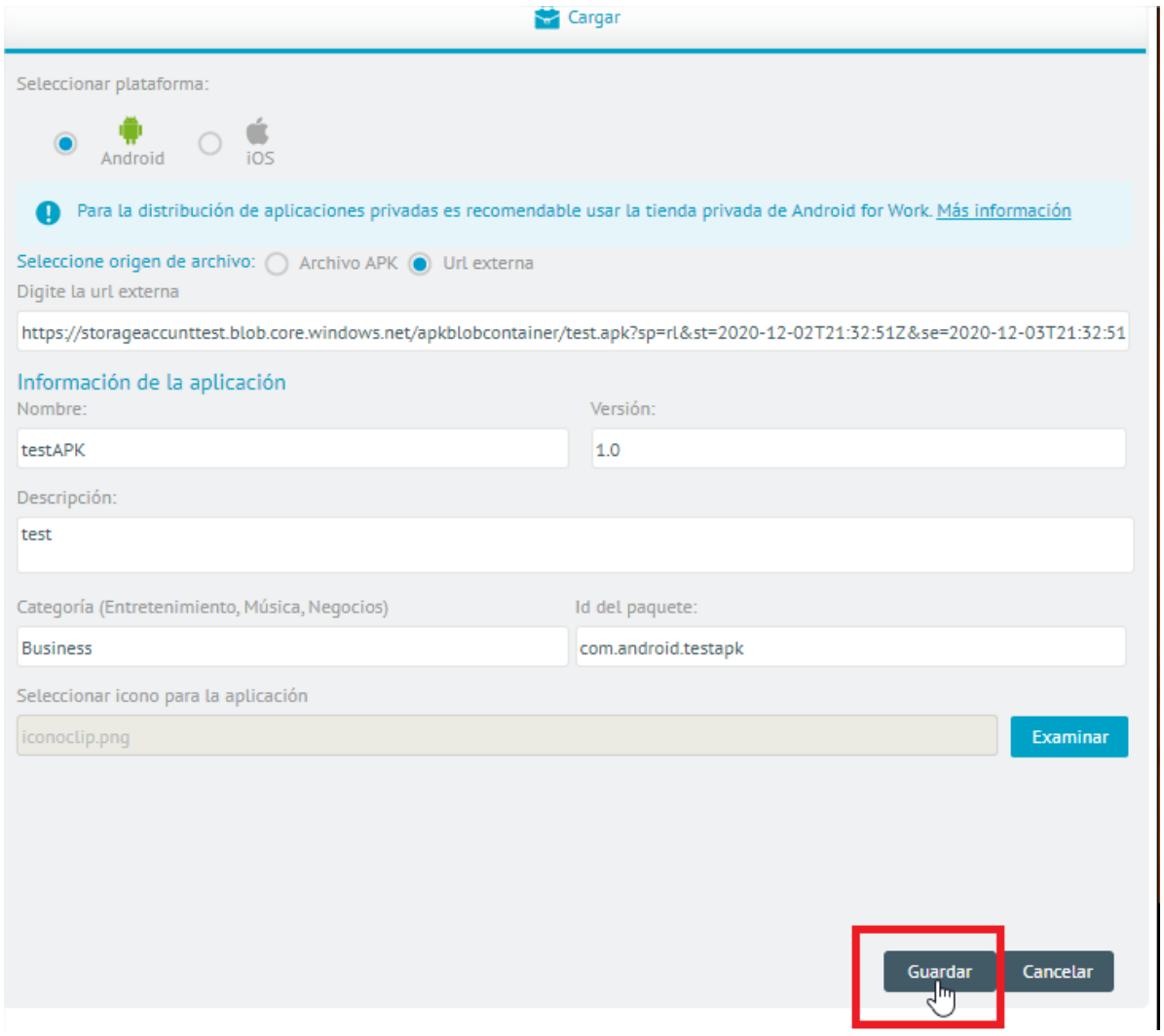
1. Una vez en la sección de detalles escoja el origen del archivo como “Url Externa”.

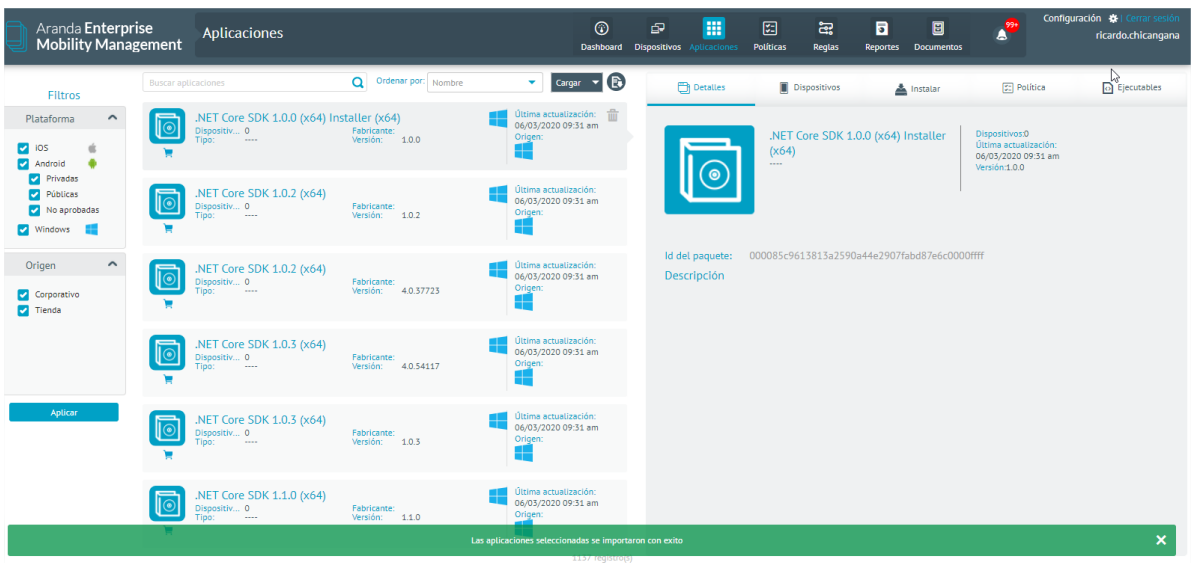


1. Posteriormente pegue la URI obtenida en Azure, luego haga clic en el botón “Validar” para proceder a la respectiva validación de la url ingresada y la carga de los datos que se puedan extraer del archivo cargado en la url.

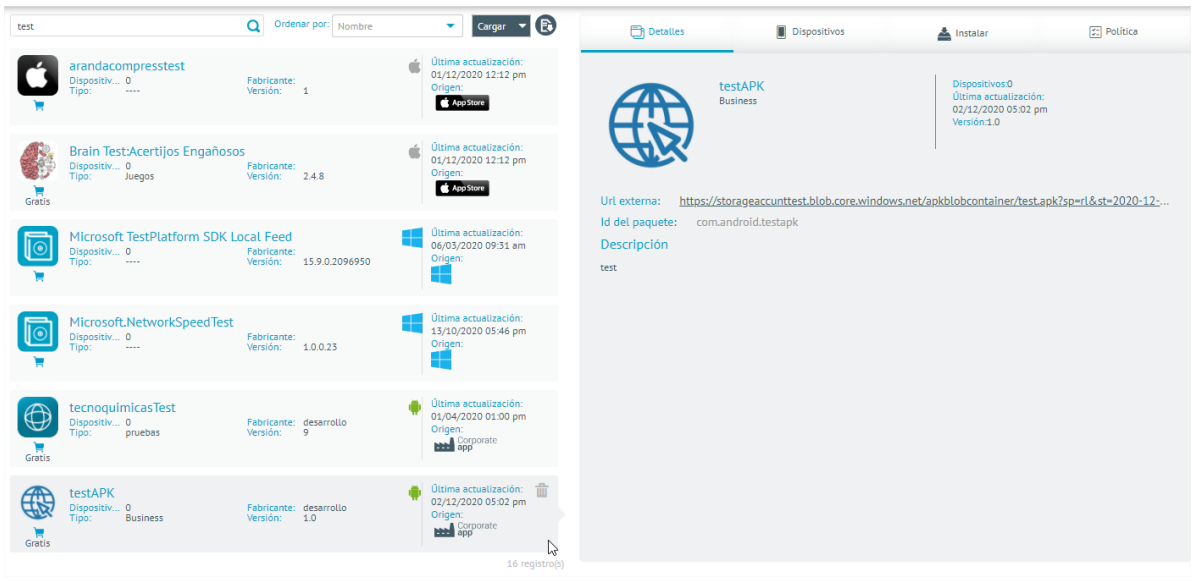


1. Una vez validada correctamente la url se cargarán los datos de nombre, versión e id del paquete. Proceda a completar los datos de descripción, categoría y seleccione un ícono para la aplicación. Finalmente haga clic en “Guardar” para agregar la aplicación al catálogo.





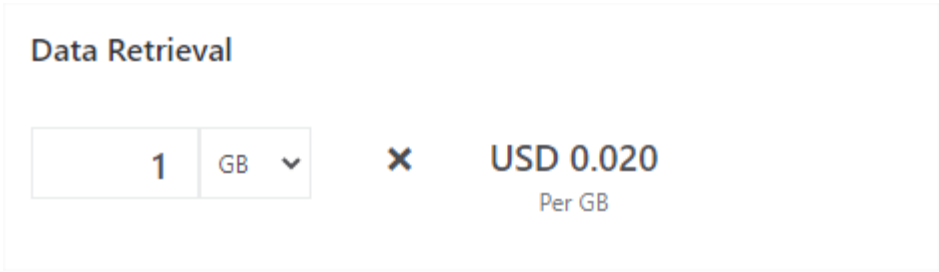
1. Luego de hecho este proceso se puede encontrar la aplicación creada e iniciar su instalación en la misma sección de aplicaciones o ser agregada como aplicación requerida en una política.



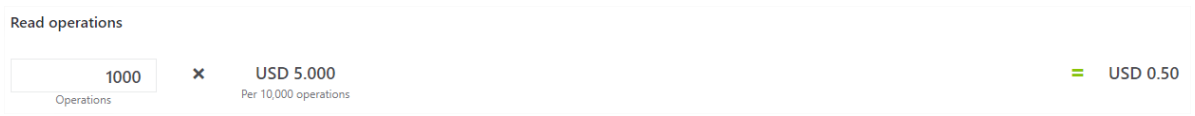
Costos

Tomando como referencia la calculadora de precios de Microsoft Azure (https://azure.microsoft.com/es-mx/pricing/ alculator) los costos aproximados por cada 1 GB de descargas acumuladas sobre el (los) archivo(s) es de

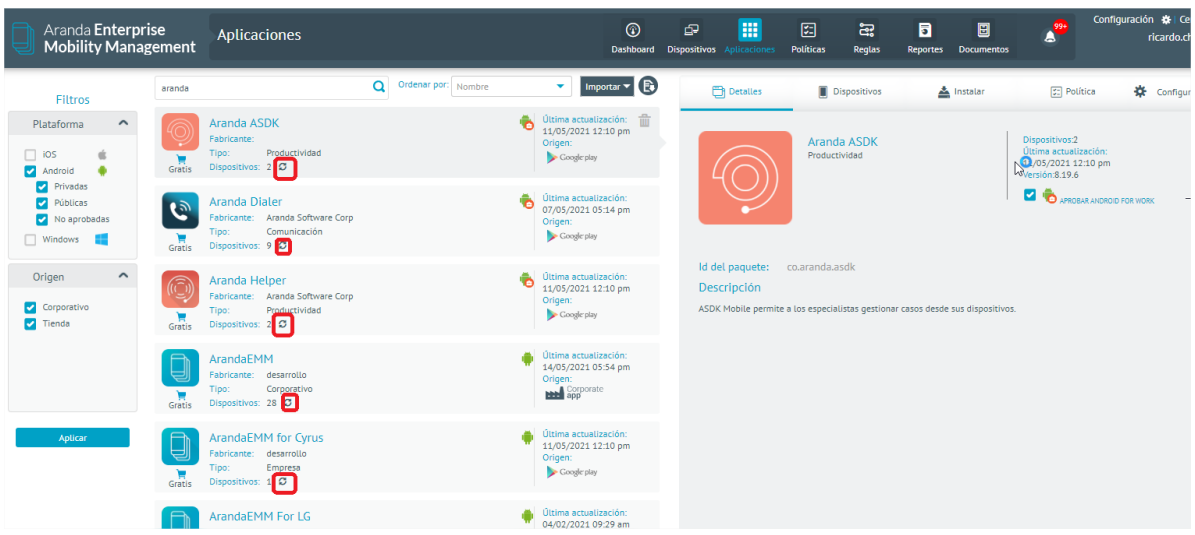
US $ 0.02



Adicional a lo anterior se calcula el costo aproximado por cada 1000 operaciones de lectura a US $ 0.5

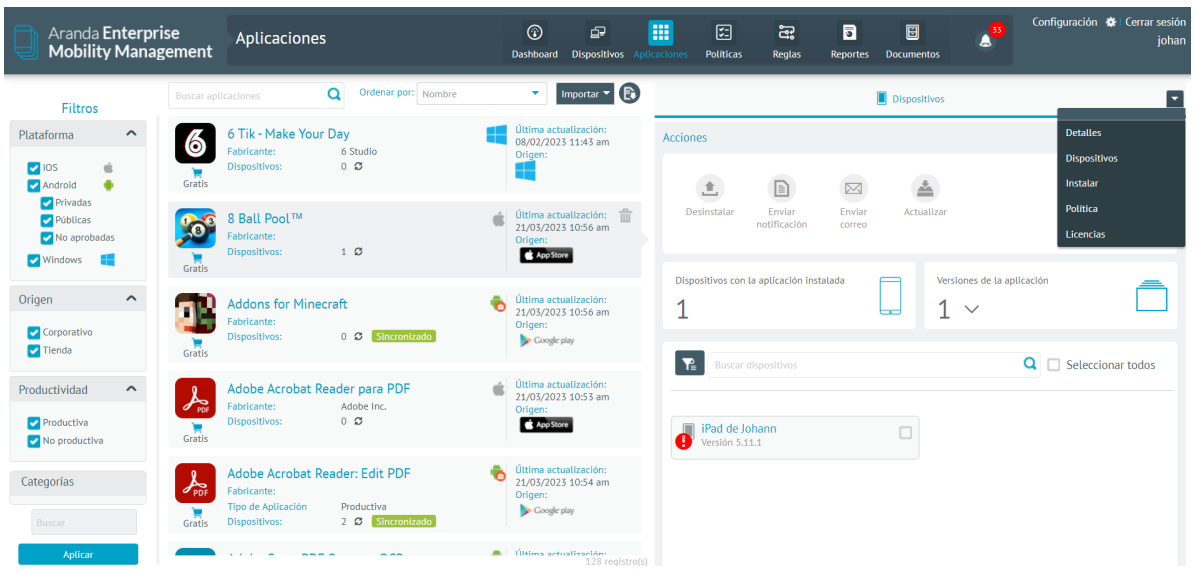


Conteo de Dispositivos por Aplicación

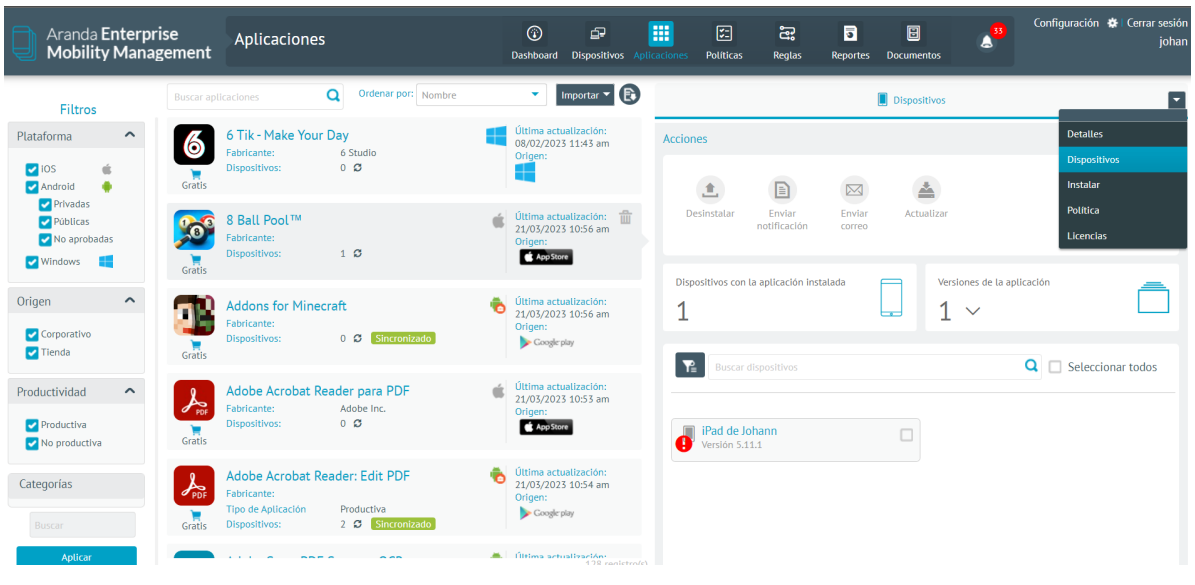


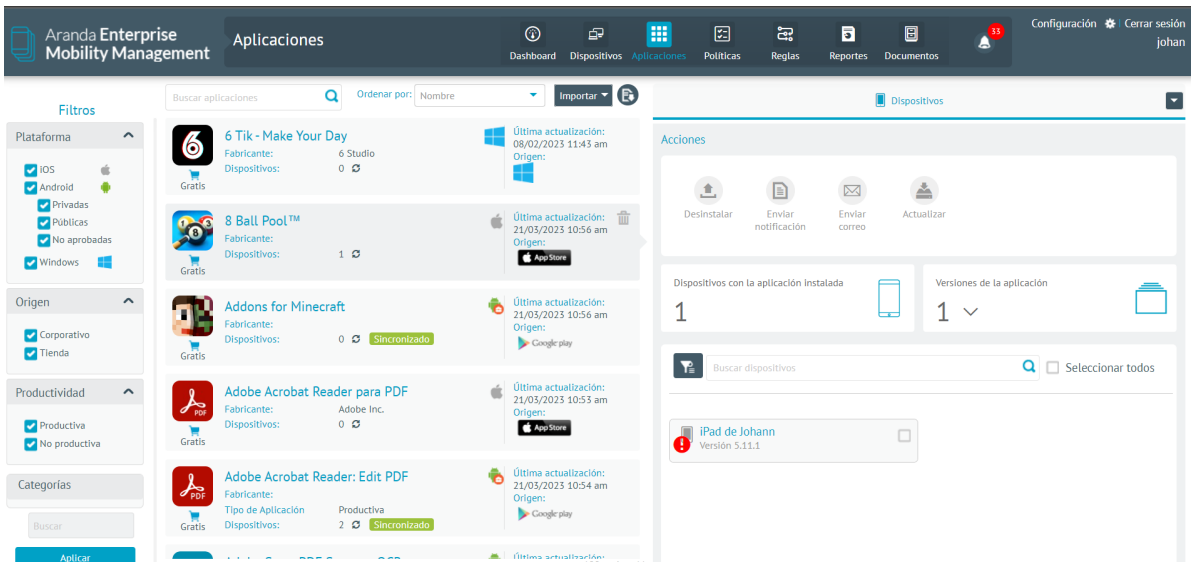
Haga clic sobre el ícono para actualizar y visualizar el conteo de dispositivos con la aplicación instalada.

Al dar clic sobre el ícono, se actualiza el conteo de dispositivos con la aplicación instalada. El conteo se visualiza a la izquierda del botón.

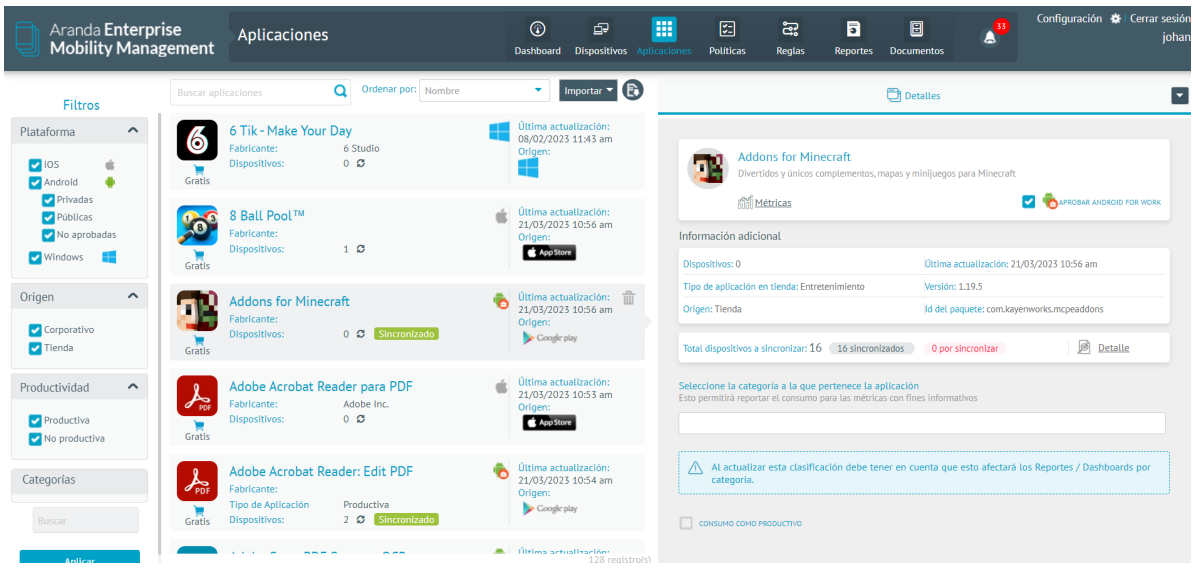


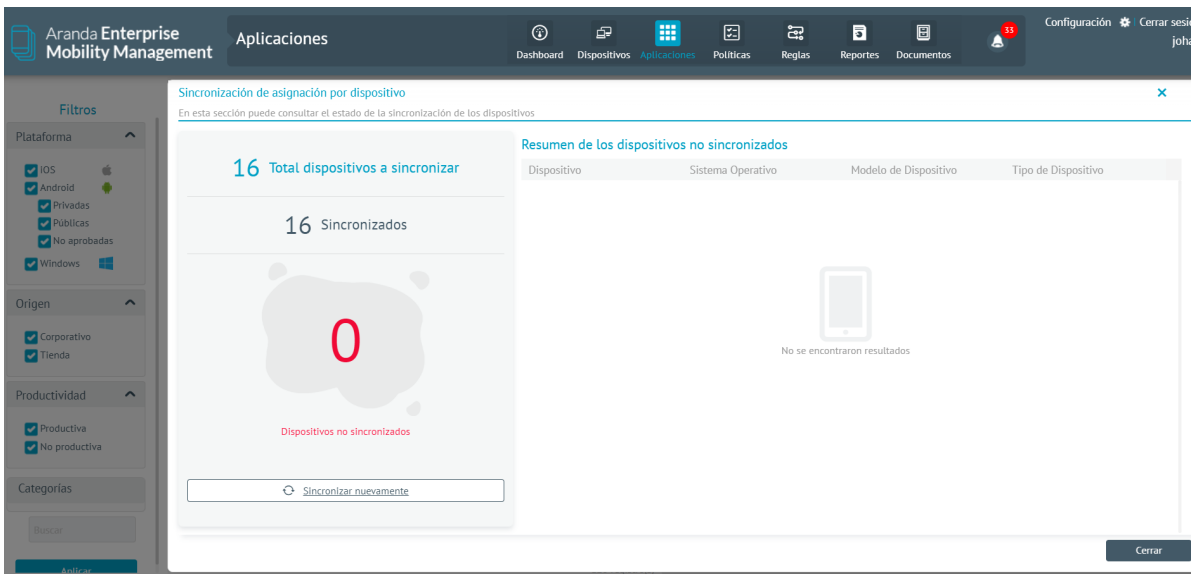
La manera de poder ver el detalle de la sincronizacion de la aplicacion con los dispositivos se muestra en segundo lugar en el menú desplegado anteriormente.





Tambien se implementa la vista mas detalla a nivel general que especifica que dispositivos tienen una aplicacion especifica instalada, que dispositivo esta pendiente por sincronizar.





Políticas

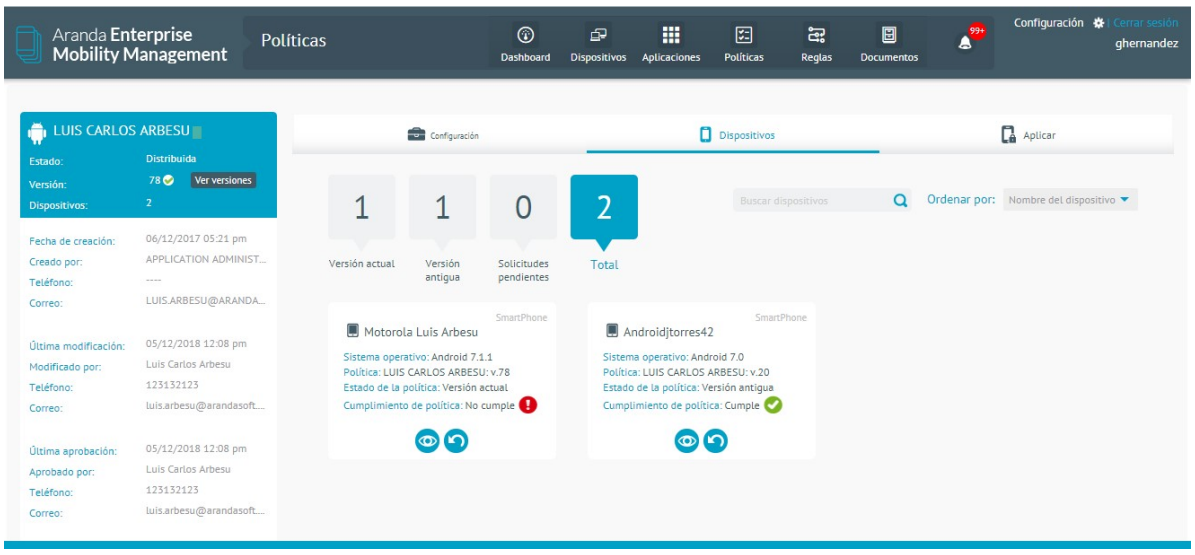
Módulo Políticas

Las políticas son parámetros que se asignan a los dispositivos móviles para su funcionamiento, es decir, establecer un contexto de operación en el que el dispositivo tendrá la posiblidad de funcionar.

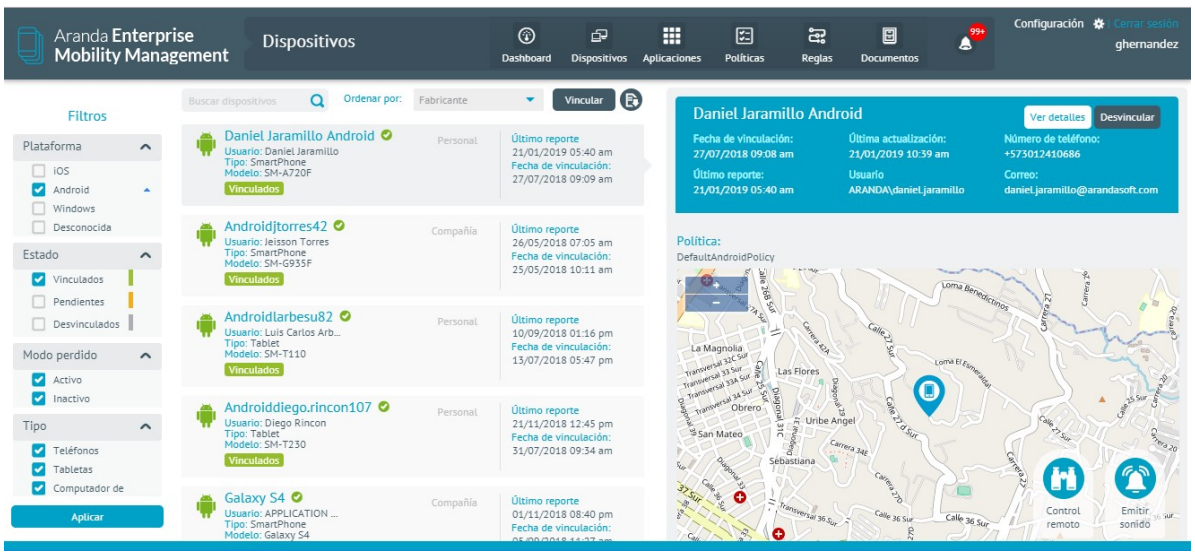
Cumplimiento de una Política asignada

Si al dispositivo se le asigna una política y este cumple con la condición, se visualiza un Check de color verde. Esto se puede evidenciar en diferentes secciones de la consola:

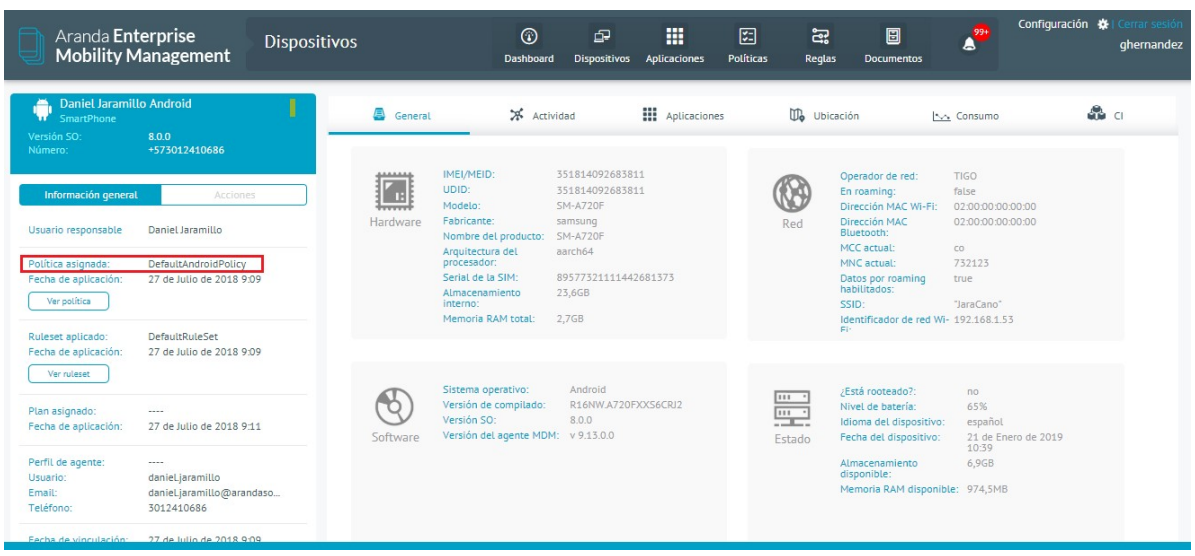
La pestaña de dispositivo



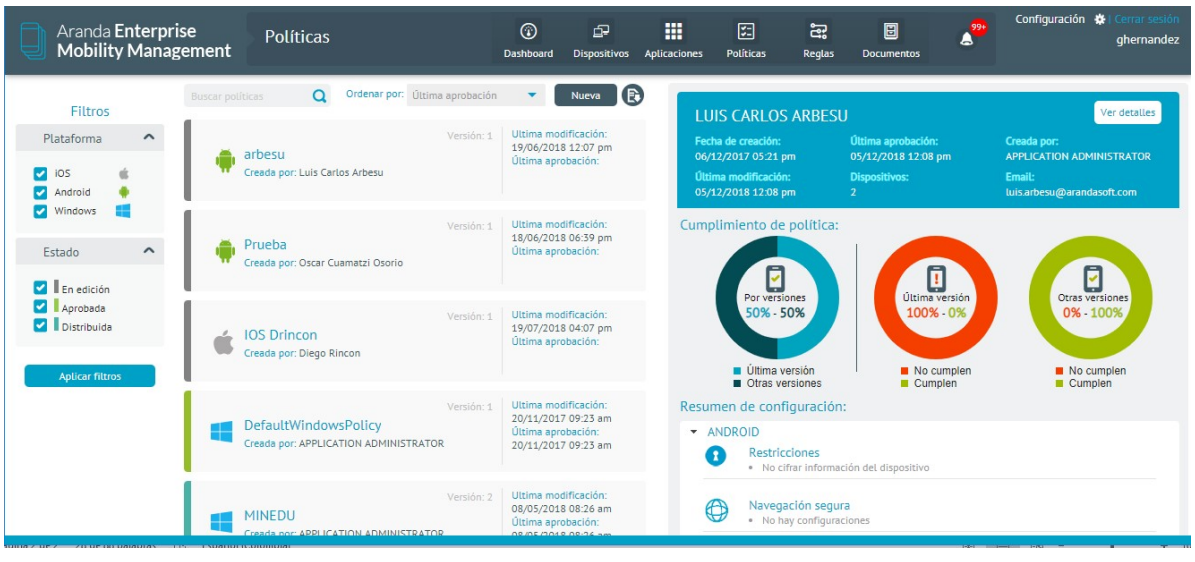
Listado de dispositivos



Hoja de vida del dispositivo



Listado y pre visualización



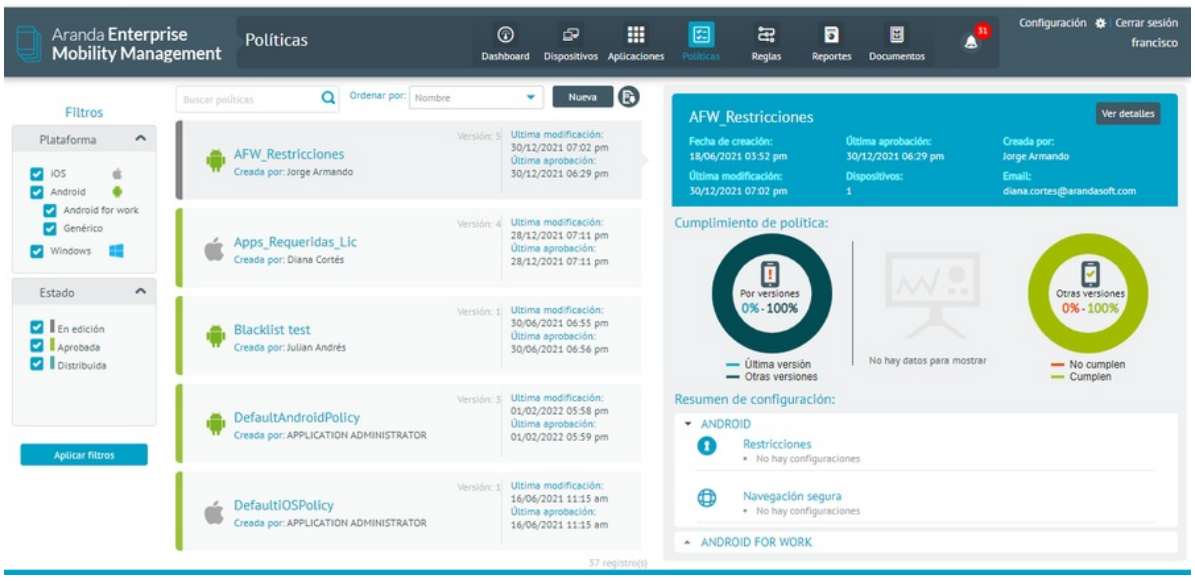
- Se visualiza el filtro para la información, esto se puede realizar por plataforma y/o estado.
- Es el resumen de política, donde se almacena el nombre, fecha de modificación y fecha de aprobación.
- Es la tarjeta donde se consigna fecha de creación, última modificación, ultima aprobación, dispositivos asociados y creado por.
- Son las gráficas que registran la cantidad de dispositivos asociados y su cumplimiento.

- Es el resumen de configuración por tipo de política.

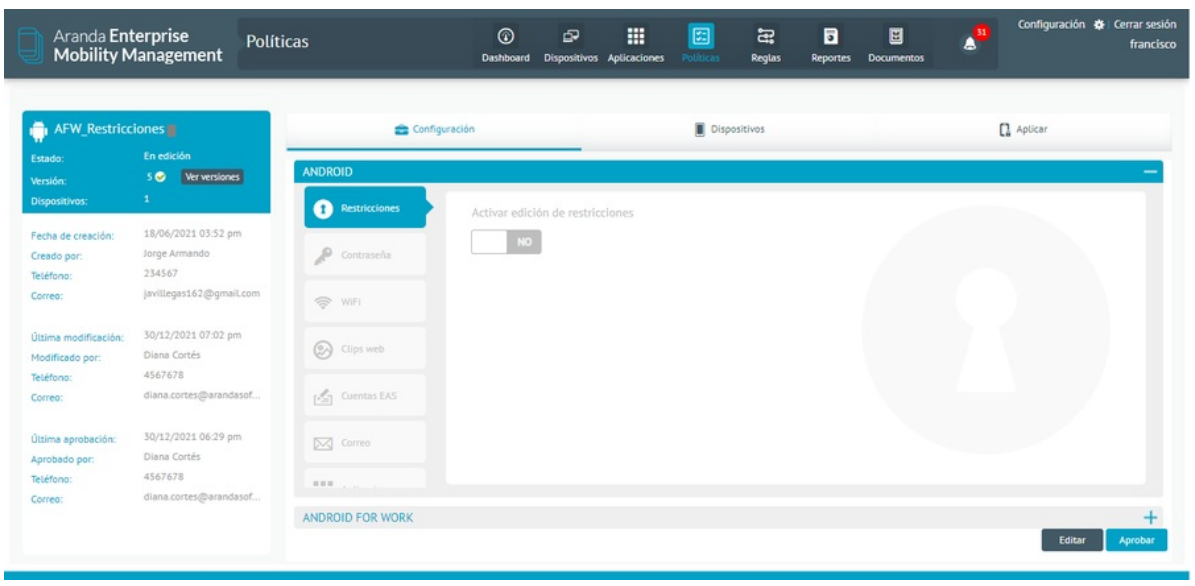
Configuración de Políticas

Configuración de Políticas en Dispositivos

1. En la vista de información de la consola de inicio de AEMM ,podrá visualizar los dispositivos encontrados para los criterios definidos. Seleccione un dispositivo y en la vista detalle podrá visualizar la hoja de vida del dispositivo



2. Seleccione la opción **Ver Detalles** para editar o aprobar las políticas asociadas a la hoja de vida del dispositivo.

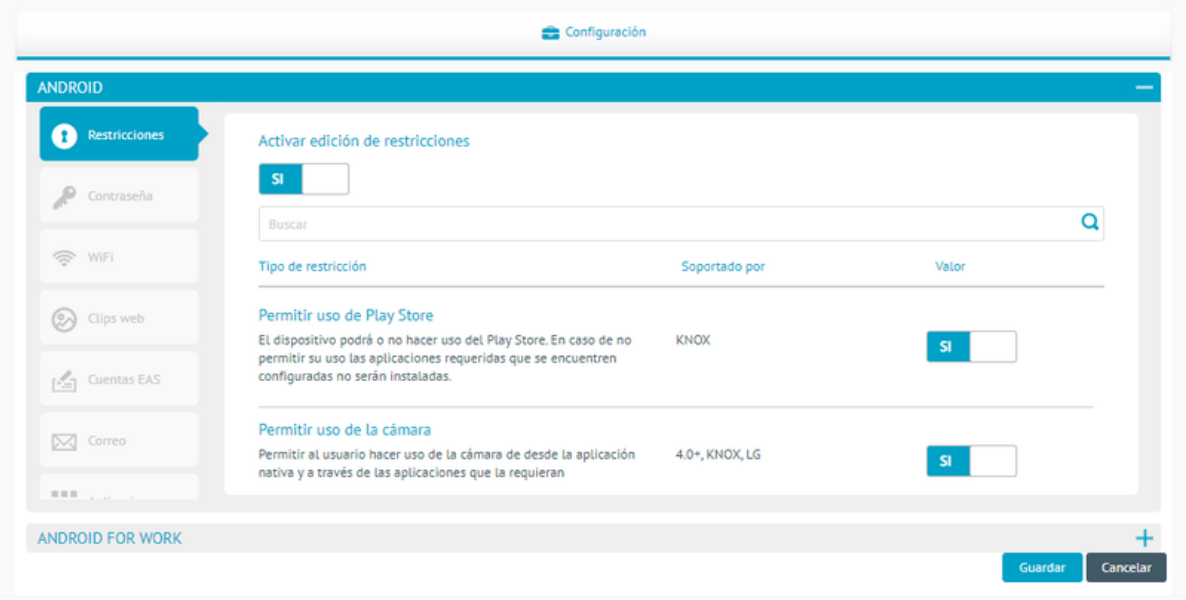


3. En la pestaña **Configuración** de la hoja de vida del dispositivo, seleccione el botón **Editar**, defina una política (restricciones, contraseña, wifi, clips web, correo, cuentas EAS, aplicaciones, kiosko) y active la edición de la política.

Restricciones

Restricccciones en Android

Son los parámetros que se restringen a dispositivos móviles Android, luego de aplicar una política.

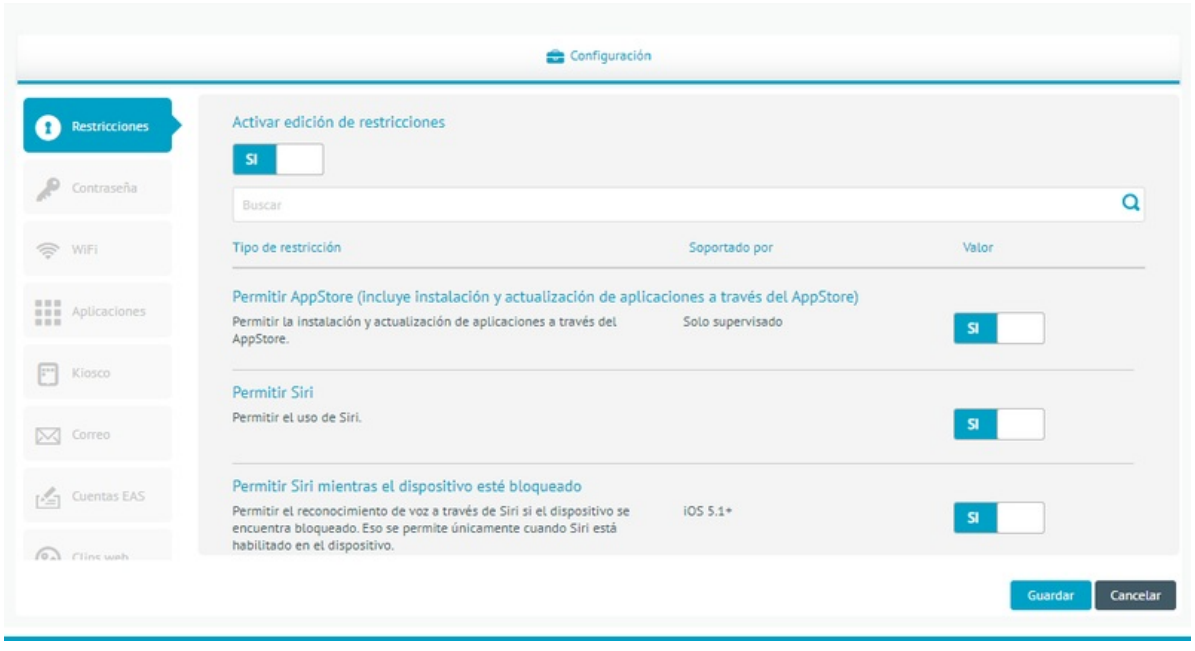


Nombre	Descripción
Permitir uso de la cámara	Si esta opción no está seleccionada, el dispositivo no puede hacer uso de la cámara ni a través de aplicaciones que la requieran (Solo aplica para Android versión superior a 4.0 o Knox)
Permitir pop-ups en el navegador de Android	Si se habilita esta política el navegador del dispositivo no permite pop up. (Solo aplica para Android Knox).
Permitir backup en servicios de la nube	Si este parámetro está activo el dispositivo. (Solo aplica para Android Knox).
Cifrar dispositivo Android	Esta opción por defecto viene deshabilitada, pero si se decide aplicar al dispositivo este permite fusionar todos los datos con una contraseña o clave. (Solo aplica para Android Knox)
Permitir roaming	Si se habilita esta política el dispositivo no permite el servicio de rooming. (Solo aplica para Android Knox)
Permitir tethering USB	Si se aplica esta política el dispositivo no permite compartir la conexión con cualquier otro ordenador (Solo aplica para Android Knox).
Permitir Reproductor de Multimedia USB (Kies)	Si esta opción no está seleccionada, el dispositivo Android no permite sincronizarse con Kies de Samsung (Solo aplica para Android Knox).
Permitir Bluetooth	Si este parámetro está activo no permite la conexión por medio de Bluetooth en el dispositivo móvil. (Solo aplica para Android Knox)
Habilitar Javascript en el navegador de Android	Si se habilita esta política el navegador de Android no habilita el JavaScript. (Solo aplica para Android Knox).
Permitir cookies en el navegador de Android	Este parámetro se activa y el móvil no habilita las cookies para el navegador. (Solo aplica para Android Knox).
Habilitar WiFi en un	Esta restricción si se aplica al dispositivo Android no permite que este se conecte a la Wifi.

Nombre	Descripción
dispositivo Android	(Solo aplica para Android Knox)
Permitir marcación por voz	Si este parámetro está activo no es posible realizar marcación por voz a través del dispositivo. (Solo aplica para Android Knox)
Permitir roaming de datos	Si se habilita esta política el dispositivo no permite el servicio de rooming de datos. (Solo aplica para Android Knox).
Permitir depuración USB	Si esta opción no está seleccionada no es posible realizar depuración USB con el dispositivo móvil (Solo aplica para Android Knox).
Permitir uso de SMS	Si esta política se aplica no es posible enviar o recibir SMS al móvil. (Solo aplica para Android Knox).
Permitir manipulación del GPS	Se este parámetro está activo no se tiene acceso al GPS (Solo aplica para Android Knox).
Permitir actualización de sistema operativo	Si esta opción esta inactiva no se permitirá descargar ni instalar actualizaciones de sistema operativo, tanto manualmente como automáticamente (Solo aplica para vinculaciones en AFW con agente samsung knox).
Permitir activar el servicio de copia de seguridad	Permite que el propietario del dispositivo o del perfil active o desactive el servicio de copia de seguridad. Deshabilitar el servicio de copia de seguridad evitará que se realice una copia de seguridad o restauración de los datos. De forma predeterminada, el servicio de copia de seguridad esta deshabilitado. PO, DO, API 26.
Permitir añadir cuentas en la tienda google play	Permite que el usuario añada cuentas adicionales en la tienda de google play. PO, DO, Para versiones de la aplicación de Google Play mayor a 80970100.

Restricciones en iOS

Son los parámetros que se restringen a dispositivos móviles iOS, luego de aplicar una política.



Detalles

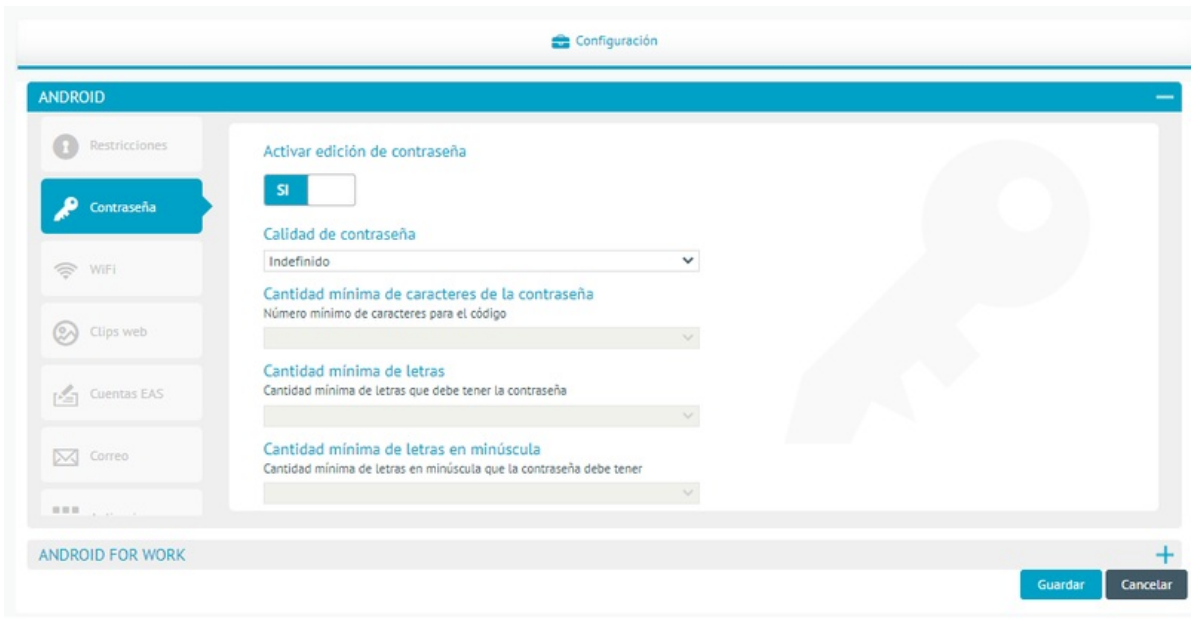
Nombre	Descripción
Permitir App Store (incluye instalación y actualización de aplicaciones a través del App Store)	Si se aplica estaconfiguración el dispositivo iOS no tendrá acceso al App Store.
Permitir Siri mientras el dispositivo esté bloqueado	Esta política no activa el reconocimiento de voz a través de SIRI si el dispositivo se encuentra bloqueado (Solo aplica para dispositivos iOS versión superior a 5.1).
Permitir informes automáticos de diagnóstico	Este parámetro activo deshabilita la opción de enviar informes automáticos de diagnóstico (Solo aplica para dispositivos iOS versión superior a 6.0)
Permitir Game Center	Si esta opción no es seleccionada el dispositivo no tiene acceso al Game Center. (Solo aplica para dispositivos iOS versión superior a 6.0).
Permitir uso del iTunes Store	Esta política no permite el acceso a la tienda en línea de contenido digital a través de iTunes Store.
Permitir Safari	Este parámetro activo no permite el acceso al navegador Safari.
Permitir backup en servicios de la nube	Si se aplica esta configuración no se le permite al dispositivo realizar backup en la nube de servicios de Apple (Solo aplica para dispositivos iOS versión superior a 5.0)
Permitir Photo Stream	Este parámetro no permite la sincronización de fotos a través del PhotoStream (Solo aplica para dispositivos iOS versión superior a 5.0)
Permitir Shared Photo Stream	Si se aplica esta política el dispositivo no puede compartir las fotos que tienen sincronizada. El shared Photo Stream se deshabilita (Solo aplica para dispositivos iOS versión superior a 6.0)
Permitir cookies en Safari	Esta política puede configurar las Cookies de safari para que se permitan nunca, siempre o solo de los sitios visitados.
Permitir Siri	Esta política no activa el reconocimiento de voz a través de SIRI.
Permitir uso de la cámara	Si esta opción no está seleccionada, el dispositivo no puede hacer uso de la cámara ni a través de aplicaciones que la requieran.
Permitir contenido explícito	Este parámetro no permite el acceso a contenido explícito.
Permitir capturas de pantalla	Cuando se aplica esta política en el dispositivo no es posible realizar capturas de pantalla en el dispositivo móvil.
Forzar ingreso de contraseña de iTunes para cada transacción	Si este parámetro está activo, siempre que se realice alguna transacción con el iTunes solicitara la clave de acceso (Solo aplica para dispositivos iOS versión superior a 5.0)
Advertir al usuario sobre certificados HTTPS no confiables en vez de rechazarlos automáticamente	Si esta política se aplica al móvil siempre se le advierte al usuario cuando el certificado HTTPS no es confiable (Solo aplica para dispositivos iOS versión superior a 5.0)
Permitir sincronización de documentos en iCloud	Esta política no permite el almacenamiento en cloud computing de Apple (Solo aplica para dispositivos iOS versión superior a 5.0).
Permitir BookStore	Si se aplica esta política el dispositivo no tienen acceso al BookStore de Apple. (Solo aplica para dispositivos iOS versión superior a 6.0).
Permitir Javascript en Safari	Este parámetro no permite el uso de Javascript en safari.

Nombre	Descripción
Permitir habilitar teclados predictivos	Si esta opción no está seleccionada, el dispositivo no hará uso de la opción de teclados predictivos.
Permitir habilitar la función de AirDrop	Si esta opción no está seleccionada, el dispositivo no hará uso de la opción de AirDrop.
Permitir el modo restringido USB	Permite que el dispositivo se conecte accesorios USB mientras está bloqueado, en caso de estar inactivo restringe la conexión.
Permitir autocompletar contraseñas	Permite ativar/desativar la función de autocompletar contraseñas. Esta restricción también desactiva las contraseñas seguras automáticas y ya no se sugieren contraseñas seguras a los usuarios.
Permitir huella digital y/o face ID para desbloquear	Permite activar/desactivar el dispositivo a través de huella digital o face ID. En caso de estar inactiva la restricción, no se podrá desbloquear el dispositivo a través de los mecanismos anteriormente mencionados.
Permitir la modificación de huellas dactilares y/o face ID	Permite al usuario modificar tanto las huellas dactilares como el face ID configurado.
Permitir encontrar mi dispositivo	Permite activar/desactivar la opción buscar el dispositivo.

Contraseña

Android

Son los parámetros que se aplican a un dispositivo Android para configurar en el móvil.



Nombre	Descripción
Calidad de contraseña	Existen 5 tipos de configuración de contraseña, estos son: - **Indefinido**: Es necesario ingresar una contraseña con mínimo 4 caracteres. - **Alfabética:** La contraseña debe contener por lo menos 4 caracteres alfabéticos. - **Alfanumérica:** La contraseña debe contener por lo menos 4 caracteres alfanuméricos. - **Compleja**: La contraseña debe contener por lo menos 4 caracteres de los cuales mínimo uno es letra, una letra en minúscula, una letra en mayúscula, un carácter especial y un número. - **Cualquiera:** La contraseña puede ser un patrón, un pin o una contraseña.
Longitud mínima del código	Es la cantidad de caracteres que mínimo debe tener la contraseña que va desde 4 hasta 16.
Cantidad mínima de letras	Es la cantidad de letras que mínimo debe tener la contraseña que va desde 1 hasta 16.
Cantidad mínima de letras en minúscula	Es la cantidad de letras minúsculas que mínimo debe tener la contraseña que va desde 1 hasta 16.
Cantidad mínima de letras en mayúscula	Es la cantidad de letras mayúsculas que mínimo debe tener la contraseña que va desde 1 hasta 16.
Cantidad mínima de caracteres que no sean letras	Es la cantidad de caracteres especiales que mínimo debe tener la contraseña que va desde 1 hasta 16.
Cantidad mínima de números	Es la cantidad de números que mínimo debe tener la contraseña que va desde 1 hasta 16.
Cantidad mínima de símbolos	Es la cantidad de símbolos que mínimo debe tener la contraseña que va desde 1 hasta 16.

iOS

Son los parámetros que se aplican a un dispositivo iOS para configurar en el móvil

Nombre	Descripción
Permitir valor simple	Permite el uso de secuencias de caracteres repetitivas, ascendentes y descendentes
Requerir valor alfanumérico	Exige que los códigos contengan al menos una letra.
Longitud mínima del código	Es la cantidad mínima de caracteres que debe contener la contraseña que va desde 1 hasta 16.
Número mínimo de caracteres complejos	Es la cantidad mínima de caracteres complejos que debe contener la contraseña que va desde 1 hasta 4.
Periodo máximo de validez del código	Número de días (1-730) tras el cual se deberá cambiar la contraseña.
Bloqueo automático máximo:	El dispositivo se bloquea tras el tiempo establecido se encuentra entre 1 a 15 minutos
Historial de contraseñas	Número de contraseñas únicas (1-50) antes de poder repetirlas.
Periodo de gracia máximo para el bloqueo de dispositivo	Cantidad máxima de tiempo que el dispositivo puede permanecer bloqueado sin solicitar el código de desbloqueo. Las opciones son: De inmediato, 1 minuto, 5 minutos, 15 minutos, 1 hora o 4 horas.
Número máximo de intentos fallidos	Número máximo de intentos permitidos de introducir la contraseña antes de que se borren todos los datos del dispositivo o este se bloquee hasta que se conecte con el iTunes designado. Se encuentra entre 2 a 11.

Wifi

Es la política que configura la red WIFI en el dispositivo móvil.

Android

Nombre	Descripción
Identificador de conjunto de servicios (SSID)	Es el nombre de la red inalámbrica a la que se conectará
Tipo de seguridad	Cifrado de la red inalámbrica que se utilizará para la conexión. Existe WEP, WPA/WPA2, WPA2 Enterprise. Para el caso de tipo de seguridad WPA2 Enterprise adicionalmente se deberá proporcionar un nombre de usuario que se usará para autenticarse ante el servidor radius asociado a la red inalámbrica. La contraseña en este caso será la asociada al usuario ingresado.
Contraseña	Es la contraseña para la autenticación en la red inalámbrica.

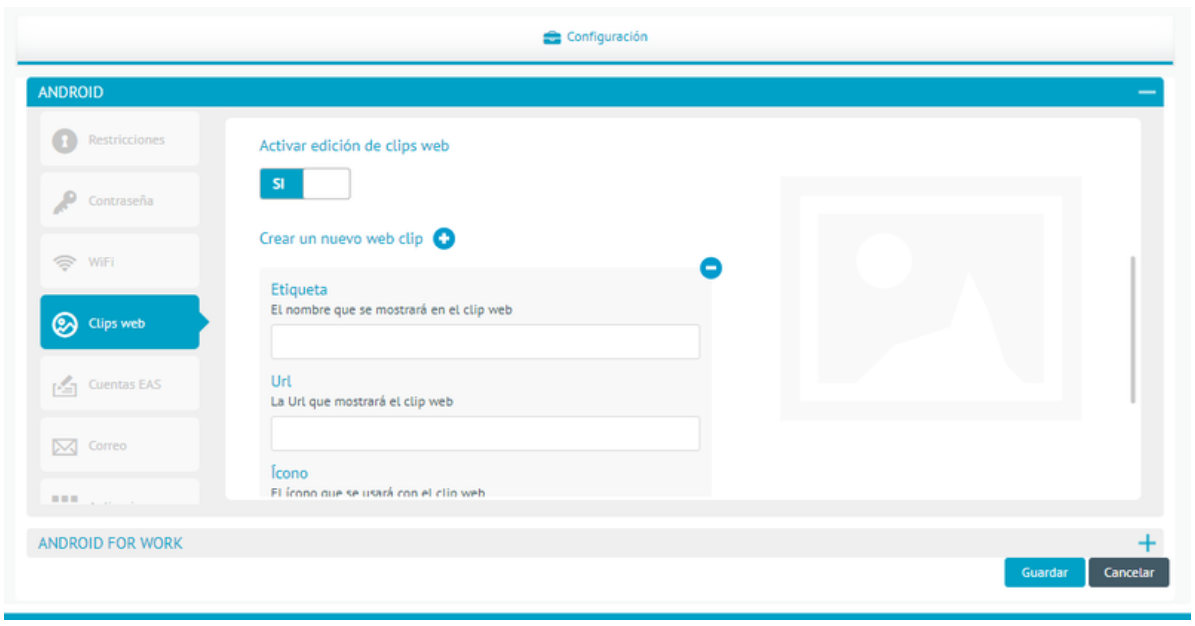
iOS

Nombre	Descripción
Identificador de conjunto de servicios (SSID)	Es el nombre de la red inalámbrica a la que se conectará
Conexión automática:	Se selecciona si desea conectarse automáticamente a la red de destino.
Red oculta	Se selecciona si la red de destino está abierta o no.
Tipo de seguridad	Cifrado de la red inalámbrica que se utilizará para la conexión. Existe WEP o WPA/WPA2.
Contraseña	La contraseña para la autenticación en la red inalámbrica.
Proxy	Se seleccionada si el ajuste para la red inalámbrica del proxy es ninguno, automático o manual. De acuerdo a la selección hecha se cargaran distintos campos adicionales a saber: **Automático**: - ProxyPACFallback permitido: Permite conectarse directamente al destino si el archivo PAC no es accesible. - URL del servidor proxy: Servidor desde el cual se obtienen los ajustes de proxy. **Manual**: - Servidor y Puerto: La dirección completa y el puerto del servidor proxy - Autenticación: Nombre de usuario usado para conectarse al proxy - Contraseña: Contraseña utilizada para conectarse al proxy

Clips Web

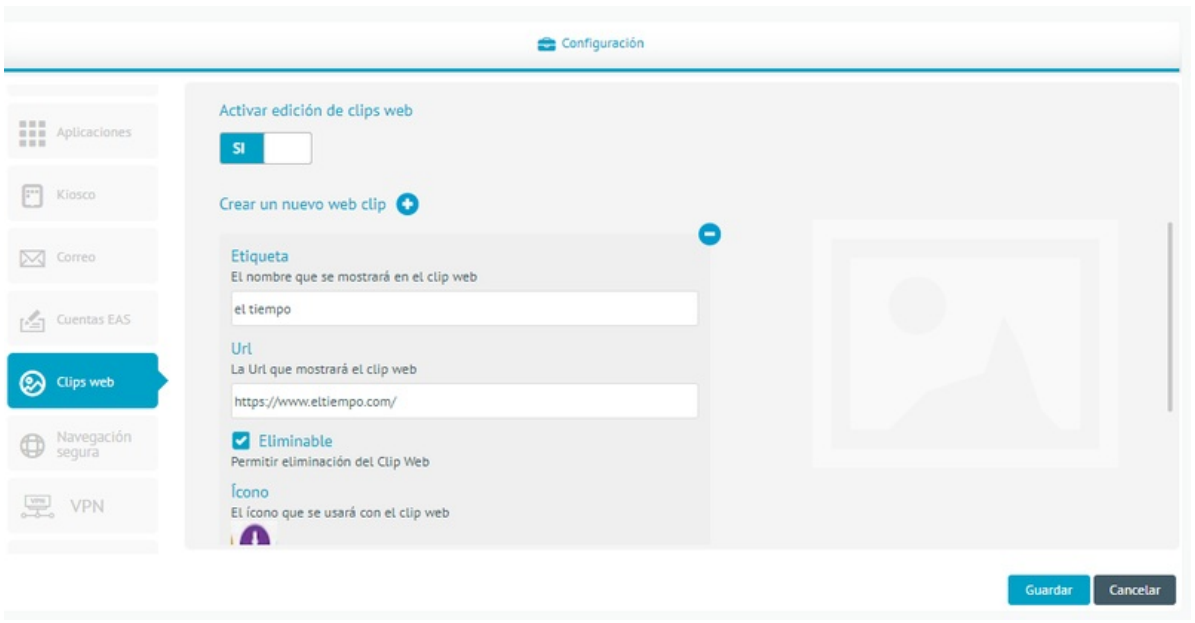
Esta política crea un acceso directo en el dispositivo móvil, el cual dirige a una URL.

Android



Nombre	Descripción
Etiqueta	Es el nombre que se asigna al clip web
URL	Dirección que dirige el Web Clip
Icono	Imagen que se va visualizar en el WebClip. Esta imagen debe tener un tamaño máximo de 200 pixeles de alto y 200 pixeles de ancho. Es posible adicionar más de un web clip con la opción “Crear un nuevo web clip”.

iOS



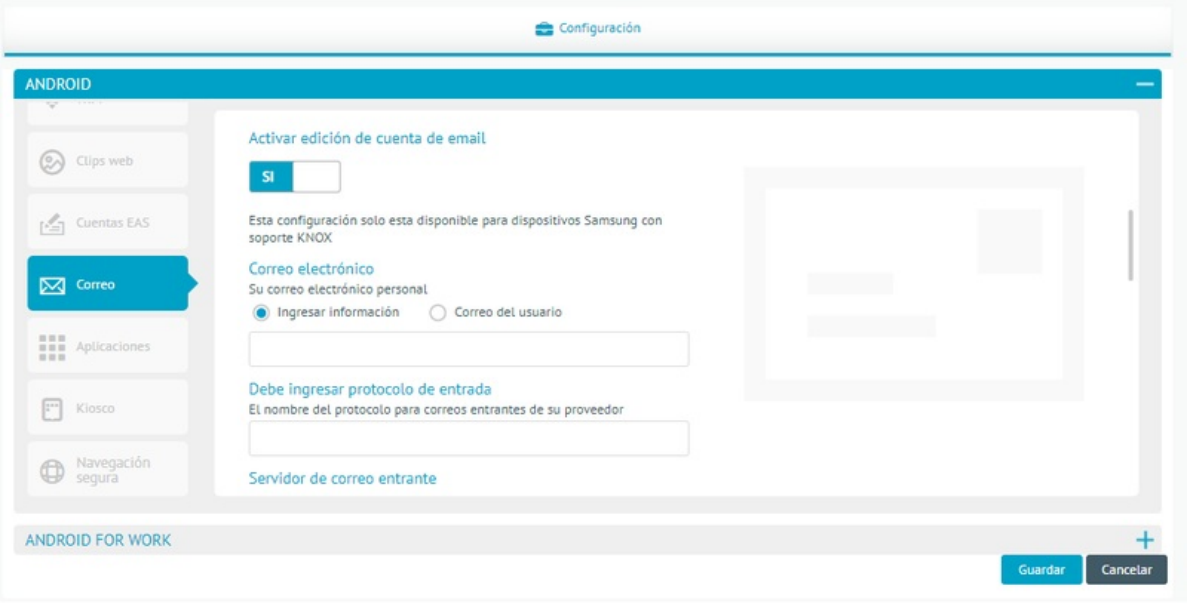
Nombre	Descripción
Etiqueta	Es el nombre que se asigna al clip web
URL	Dirección que dirige el Web Clip
Eliminable	Permitir eliminación del Clip Web.
Icono	Imagen que se va visualizar en el Web Clip. Esta imagen debe tener un tamaño máximo de 200 pixeles de alto y 200 pixeles de ancho.
Icono pre compuesto	El icono se mostrará sin efectos visuales añadidos.
Pantalla completa	Presentar el clip web como una aplicación de pantalla completa. Es posible adicionar más de un web clip con la opción “Crear un nuevo web clip”.
URL	Dirección que dirige el Web Clip

Correo

Es la configuración de una cuenta de correo que se aplica a un dispositivo móvil.

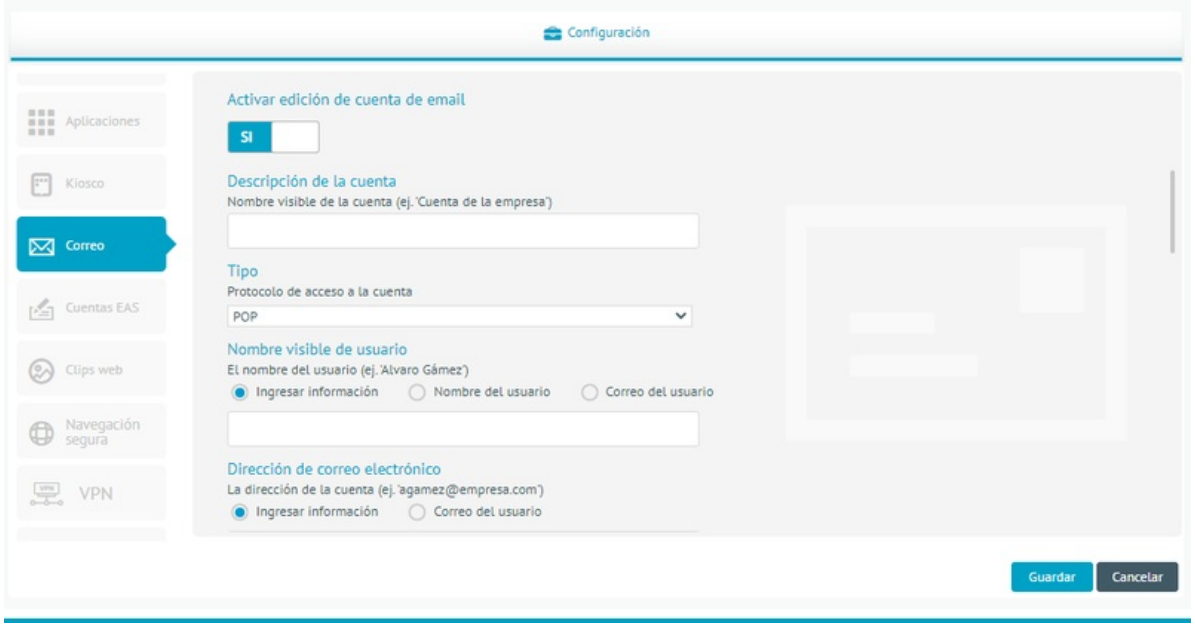
Android

Esta configuración solo está disponible para dispositivos Samsung con soporte KNOX.



Nombre	Descripción
Correo electrónico	Es el correo electrónico que se va configurar. El administrador tiene la opción de ingresarlo o el usuario del móvil.
Protocolo de entrada	El nombre del protocolo para correos entrantes de su proveedor.
Servidor de correo entrante	La dirección del servidor de correo entrante.
Puerto del servidor de correo entrante	El puerto utilizado por el servidor de correo entrante.
Login del servidor de correo entrante	Login utilizado en el servidor de correo entrante. El administrador tiene la posibilidad de ingresar el usuario o solicitarle al usuario el ingreso del Nombre de usuario o Correo.
Contraseña del servidor de correo entrante	Contraseña utilizada en el servidor de correo entrante. Este campo solo se habilita si se ingresa la información de la casilla anterior.
Protocolo de salida	El nombre del protocolo para correos salientes de su Proveedor.
Servidor de correo saliente	La dirección del servidor de correo saliente
Puerto del servidor de correo saliente	El puerto utilizado por el servidor de correo saliente
Login del servidor de correo saliente	Login utilizado en el servidor de correo saliente. El administrador tiene la posibilidad de ingresar al usuario o solicitarle al mismo el ingreso de Nombre de usuario o correo.
Contraseña del servidor de correo saliente	Contraseña utilizada en el servidor de correo saliente. Este campo solo se habilita si se ingresa la información de la casilla anterior

iOS


Configuración
Aplicaciones
Kiosco
Correo
Cuentas EAS
Clips web
Navegación segura
VPN
Activar edición de cuenta de email
SI
Descripción de la cuenta
Nombre visible de la cuenta (ej. 'Cuenta de la empresa')
Tipo
Protocolo de acceso a la cuenta
POP
Nombre visible de usuario
El nombre del usuario (ej. 'Alvaro Gámez')
Ingresar información
Nombre del usuario
Correo del usuario
Dirección de correo electrónico
La dirección de la cuenta (ej. 'agamez@empresa.com')
Ingresar información
Correo del usuario
Guardar
Cancelar

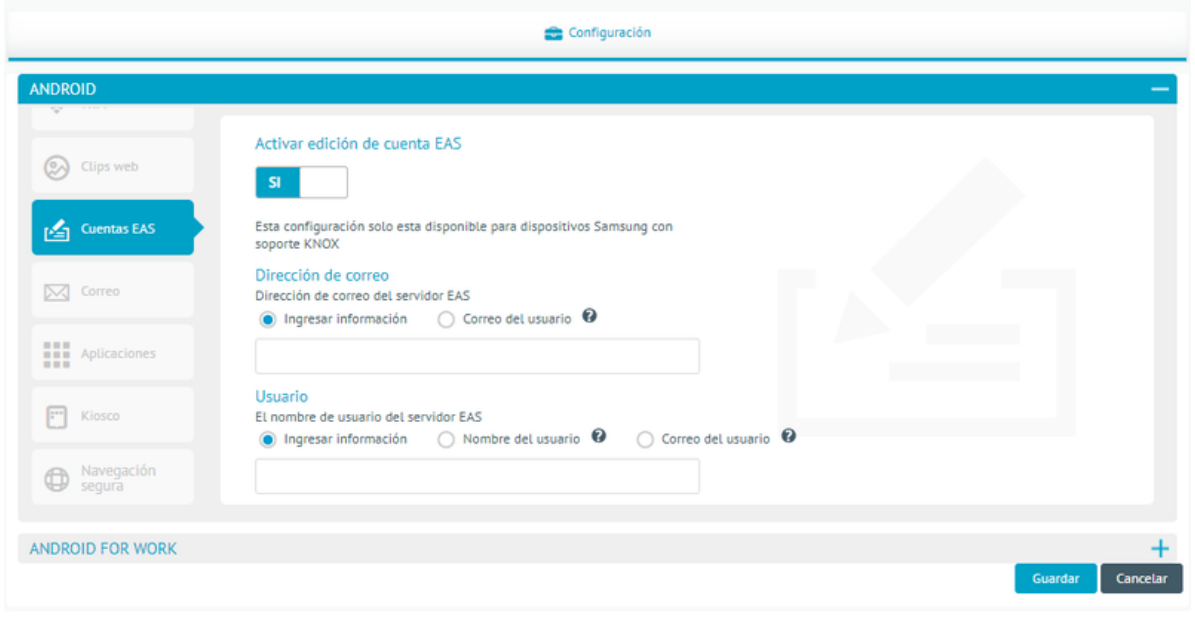
Nombre	Descripción
Descripción de la cuenta	Nombre visible de la cuenta.
Tipo	Protocolo de acceso a la cuenta. Existen dos protocolos: - **Pop:** Se utiliza en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. - **Imap:** Con este protocolo se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet.
Nombre visible de usuario	Es el nombre del usuario. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Nombre de usuario o Correo.
Dirección de correo electrónico	La dirección de la cuenta. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Correo.
Servidor (Correo entrante)	Url del servidor o IP.
Puerto (Correo entrante)	Número del puerto para conexión.
Nombre de usuario (Correo entrante)	El nombre usado para conectarse al servidor de correo entrante. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Nombre de usuario o Correo.
Tipo de autenticación (correo entrante)	El método de autenticación del servidor de correo entrante.
Contraseña (Correo entrante)	La contraseña del servidor de correo entrante.
Usar SSL (correo entrante)	Recuperar correo entrante a través de SSL.
Servidor (Correo saliente)	Url del servidor o IP.
Puerto (Correo saliente)	Número del puerto para conexión
Nombre de usuario (Correo saliente)	El nombre usado para conectarse al servidor de correo saliente. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Nombre de usuario o Correo.
Tipo de autenticación (correo saliente)	El método de autenticación del servidor de correo saliente
Contraseña (Correo saliente)	La contraseña del servidor de correo saliente.

Cuentas EAS (Exchange Active Sync)

Es la configuración de una cuenta de correo que se aplica a un dispositivo móvil.

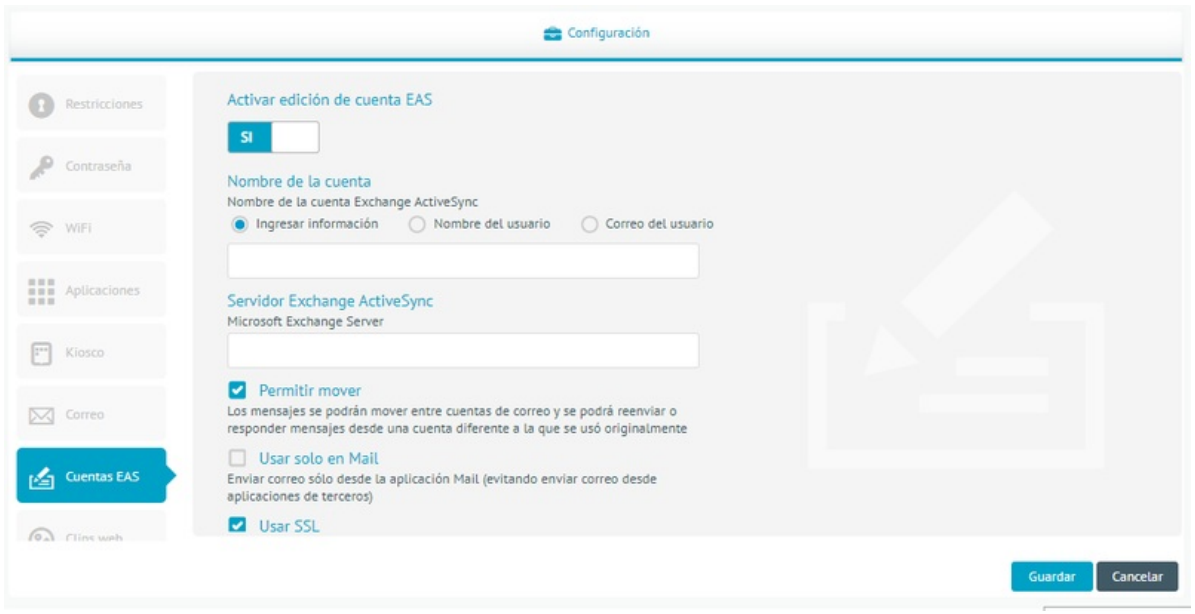
Android

Esta configuración solo está disponible para dispositivos Samsung con soporte KNOX



Nombre	Descripción
Correo electrónico	Su correo electrónico personal. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Correo.
Protocolo de entrada	El nombre del protocolo para correos entrantes de su proveedor
Servidor de correo entrante	La dirección del servidor de correo entrante
Puerto del servidor de correo entrante	El puerto utilizado por el servidor de correo entrante.
Login del servidor de correo entrante	Login utilizado en el servidor de correo entrante. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Nombre de usuario o Correo.
Contraseña del servidor de correo entrante	Contraseña utilizada en el servidor de correo entrante.
Protocolo de salida	El nombr La dirección del servidor de correo saliente
Puerto del servidor de correo saliente	El puerto utilizado por el servidor de correo saliente.
Login del servidor de correo saliente	Login utilizado en el servidor de correo saliente. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Nombre de usuario o Correo.
Contraseña del servidor de correo saliente	Contraseña utilizada en el servidor de correo saliente.

iOS



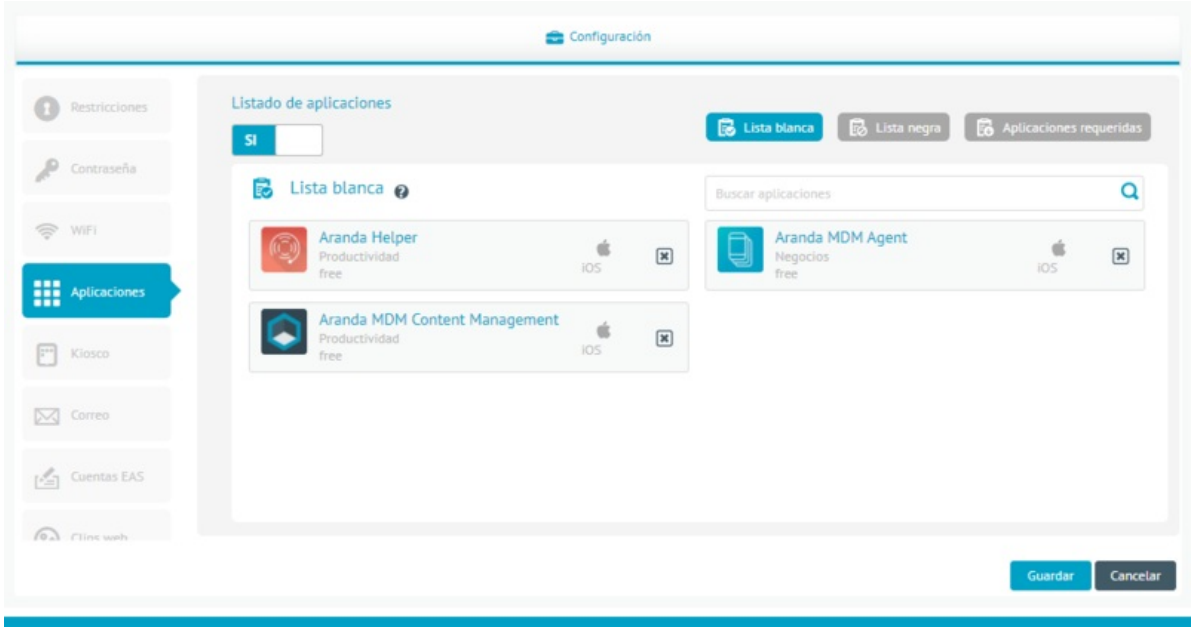
Nombre	Descripción
Nombre de la cuenta Exchange ActiveSync:	Nombre de la cuenta Exchange ActiveSync. El administrador tiene la osibilidad de ingresar la información o solicitarle al usuario el Nombre de usuario o Correo.
Microsoft Exchange Server	Microsoft Exchange Server.
Permitir mover	Los mensajes se podrán mover entre cuentas de correo y se podrá reenviar o responder mensajes desde una cuenta diferente a la que se usó originalmente.
Usar solo en Mail	Enviar correo sólo desde la aplicación Mail (evitando enviar correo desde aplicaciones de terceros).
Usar SSL	Enviar todas las comunicaciones a través de SSL.
Dominio	Dominio de la cuenta (si deja este campo vacío el dispositivo se lo solicitará al usuario). El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Correo.
Usuario	Usuario de la cuenta (si deja este campo vacío el dispositivo se lo solicitará al usuario). El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Nombre de usuario o Correo.
Dirección de correo electrónico	La dirección de la cuenta. El administrador tiene la posibilidad de ingresar la información o solicitarle al usuario el Correo.
Contraseña	La contraseña de la cuenta.
Días pasados de correo incluidos en la sincronización	El número de días pasados de correo que se incluirán en la sincronización. Tiene la opción de seleccionar: Sin límite, un día, tres días, una semana, dos semanas o un mes.

Aplicaciones

Es una política que se aplica a los dispositivos móviles, para auditar las aplicaciones que tienen instaladas. Existen tres tipos de listas que clasifican el estado que deben tener las aplicaciones.

Lista Blanca

Listado de aplicaciones que tendrá permitido instalar el dispositivo asociado a esta política. Para dispositivos KNOX es posible desinstalar las aplicaciones que no se encuentran en la lista.

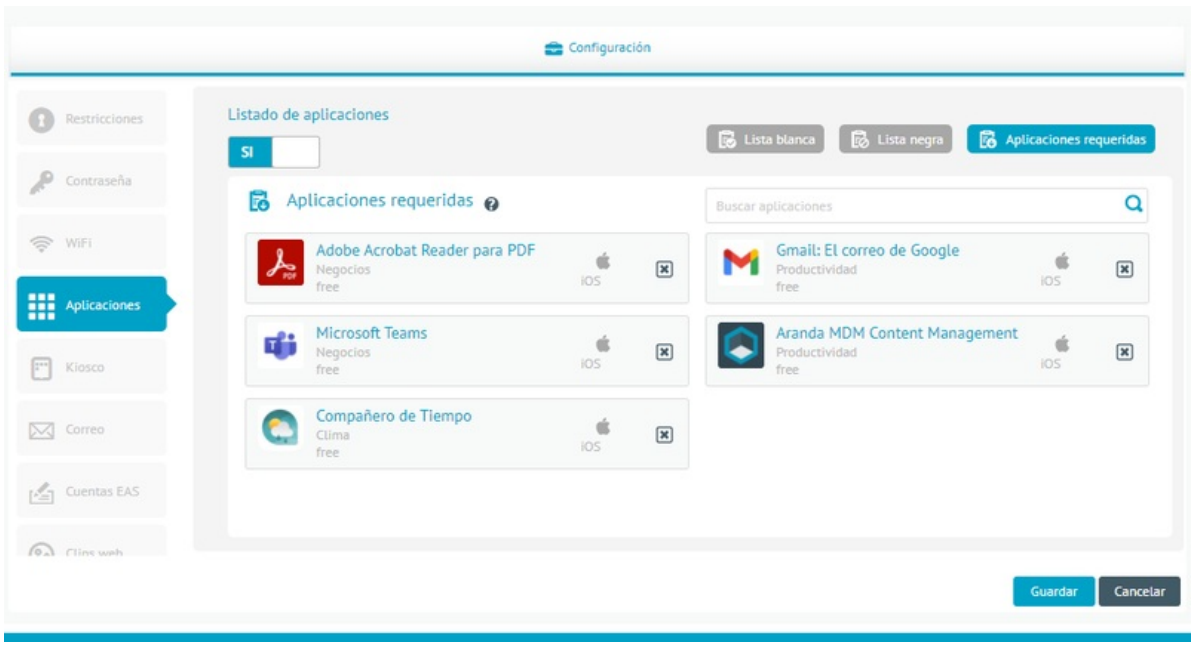


Lista Negra

Listado de aplicaciones que tendrá prohibido instalar en los dispositivos asociados a esta política. Para dispositivos Knox de Android se puede forzar la desinstalación de estas aplicaciones.

Aplicaciones requeridas

Listado de aplicaciones que deben tener instaladas obligatoriamente el dispositivo asociada a esta política. Para dispositivos Knox de Android se tiene la posibilidad de evitar la desinstalación de estas aplicaciones.



Kiosco

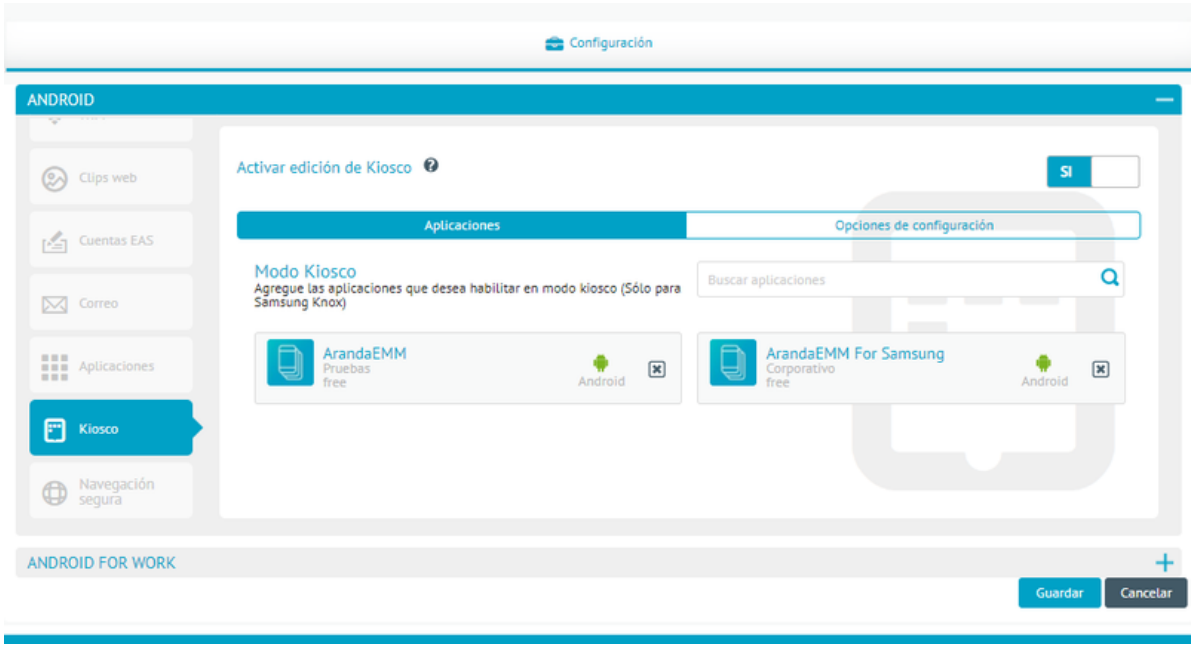
El módulo de Kiosco está destinado a que el dispositivo presente una interfaz por defecto con las aplicaciones y configuraciones aquí seleccionadas únicamente.

Android

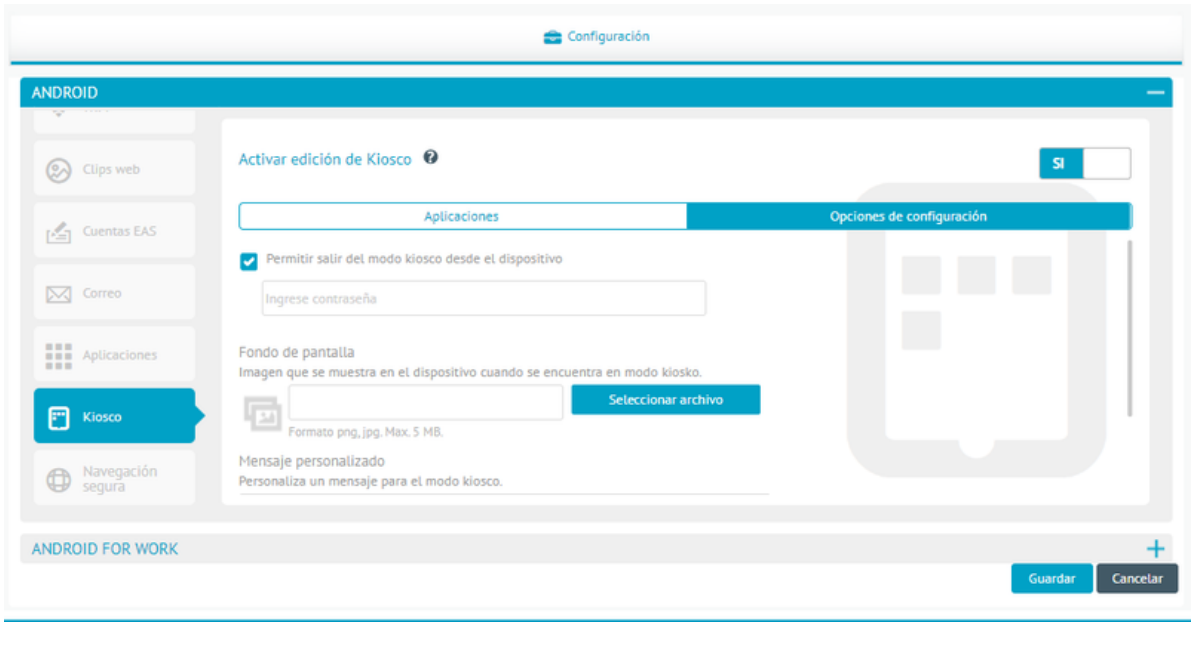
El modo Kiosco para Android genérico está disponible únicamente para vinculaciones con Agente Samsung Knox y Android superior a 4.0.

Para agregar aplicaciones al modo kiosco digite al menos 3 caracteres en la caja de texto para búsqueda y a continuación la consola presentará los resultados coincidentes en una lista desplegable tal y como se observa en la siguiente captura.

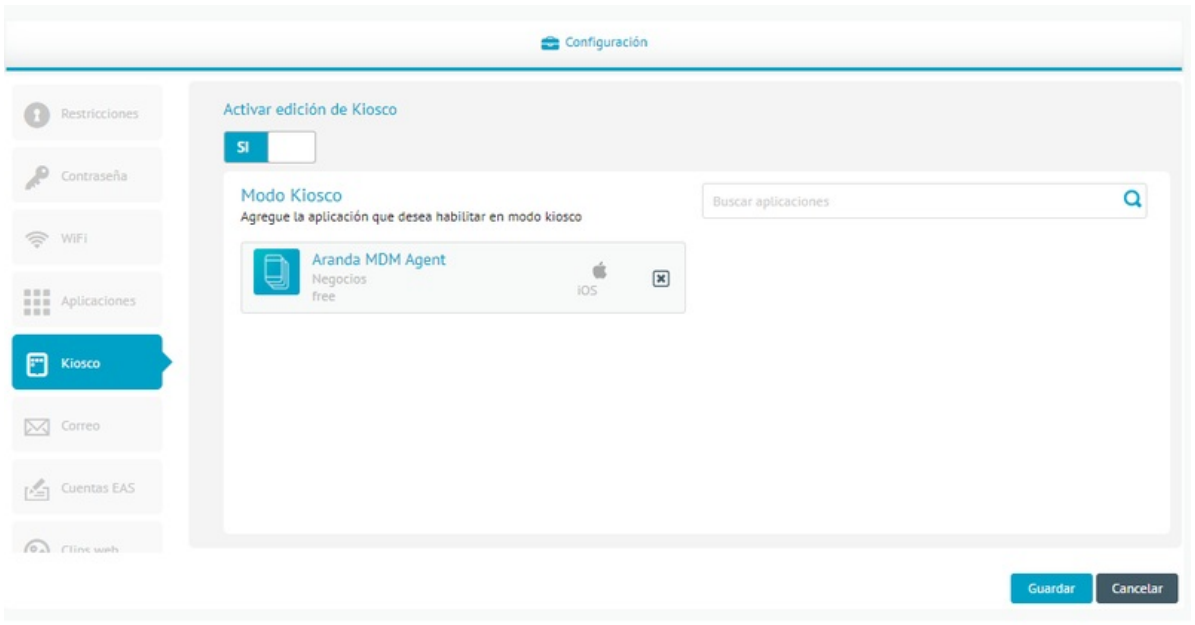
Luego haga clic en la aplicación para agregarla al listado.



Repita el proceso para cada aplicación



Para configurar opciones adicionales ingrese a la pestaña “opciones de configuración” y configure las opciones que se necesiten.



Las opciones de configuración disponibles son las siguientes:

- Contraseña de salida de kiosco: Al ingresar una contraseña, el usuario final del dispositivo tendrá la posibilidad de salir del modo kiosco, luego de ingresar dicha contraseña.
- Fondo de pantalla: El modo kiosco en el dispositivo mostrará la imagen que aquí de cargue. (5 Mb como máximo)
- Mensaje personalizado: La interfaz de modo kiosco presentará el mensaje que aquí se configure. (100 caracteres como máximo)

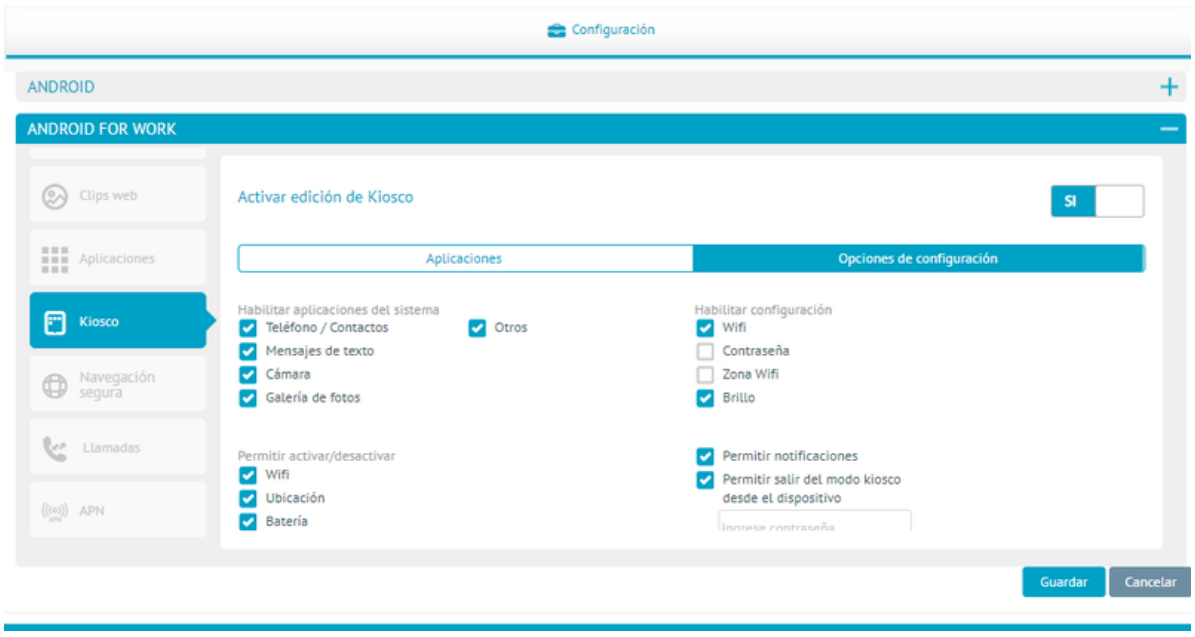
Android For Work

El modo kiosco para Android for Work está disponible únicamente para dispositivos vinculados en el modo AFW DO (Device Owner).

Para Android for Work, unicamente se podrán agregar aplicaciones que con anticipación hayan sido aprobadas para AFW.

Para agregarlas a kiosco se procede de igual forma que en la seccion anterior.

En el caso de las opciones de configuración se presentan los siguientes grupos adicionales a las de la anterior sección



En este grupo se pueden activar/desactivar aplicaciones de sistema cuyos paquetes hayan sido agregados con anterior en la sección de configuración de Aplicaciones del Sistema Android. Al marcar cada casilla aparecerán en el kiosco las aplicaciones seleccionadas.

En este grupo se pueden activar/desactivar pantallas de configuración en modo kiosco para cada una de las opciones presentadas.

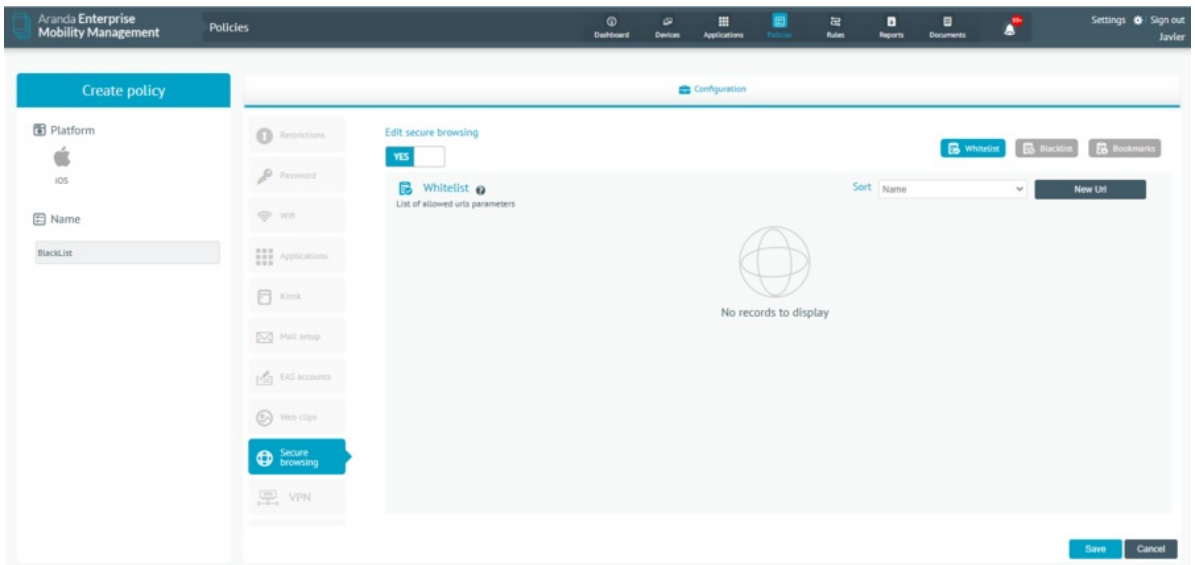
Para este grupo se pueden activar/desactivar interruptores de encendido en modo kiosco para apagar o prender cada una de las opciones presentadas.

⚐ **Nota:** En la configuración de kiosco se debe tener presente:

- La funcionalidad de bluetooth para los dispositivos menores de la versión del sistema operativo 9 no pueden ver las notificaciones para otorgar el permiso de transmisión de archivos por medio de bluetooth.

Navegación segura (iOS, Android y Android For Work)

En el módulo de navegación segura, podrá configurar los sitios web para acceder o restringir el acceso desde la aplicación Aranda Secure Browser. Esta aplicación permite el acceso a sitios web de internet y sirve como navegador web del dispositivo.

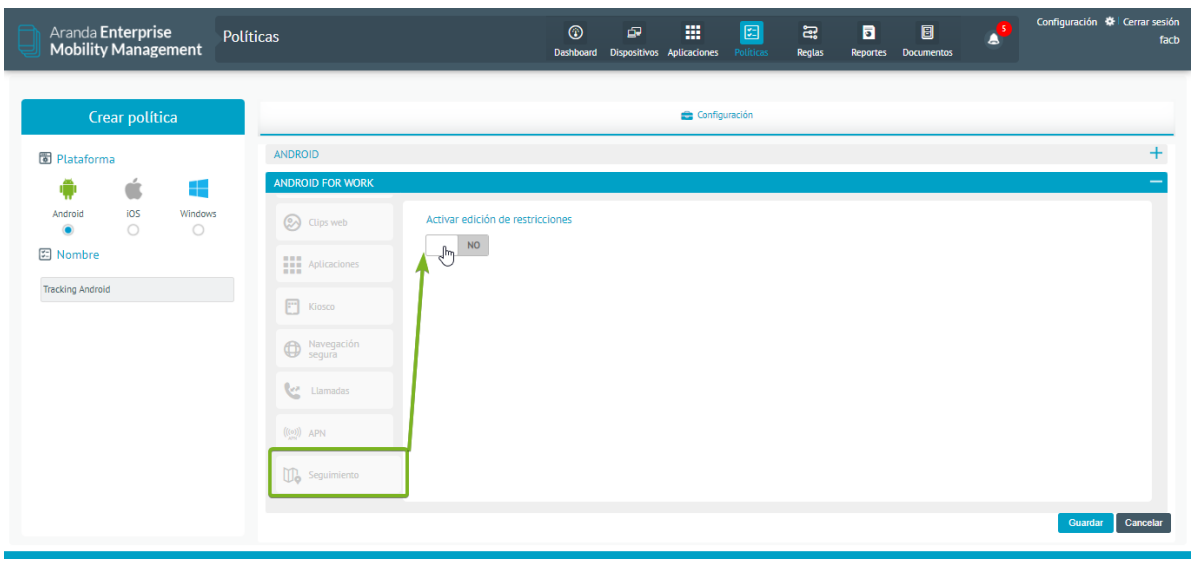


⚐ **Nota:** - Actualmente esta funcionalidad se usa con la aplicación Aranda Secure Browser, la cual, no está habilitada en tienda ya que será retirada de la suite.

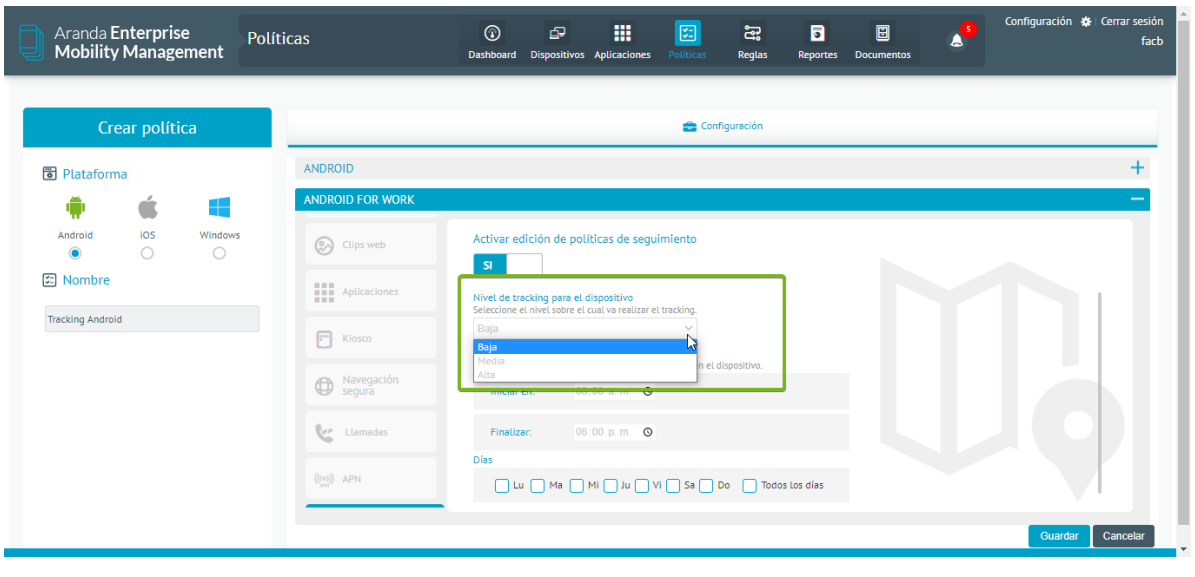
Podrá realizar la configuración en la política, pero no acceder a la aplicación Aranda Secure Browser.

Configuración política de seguimiento

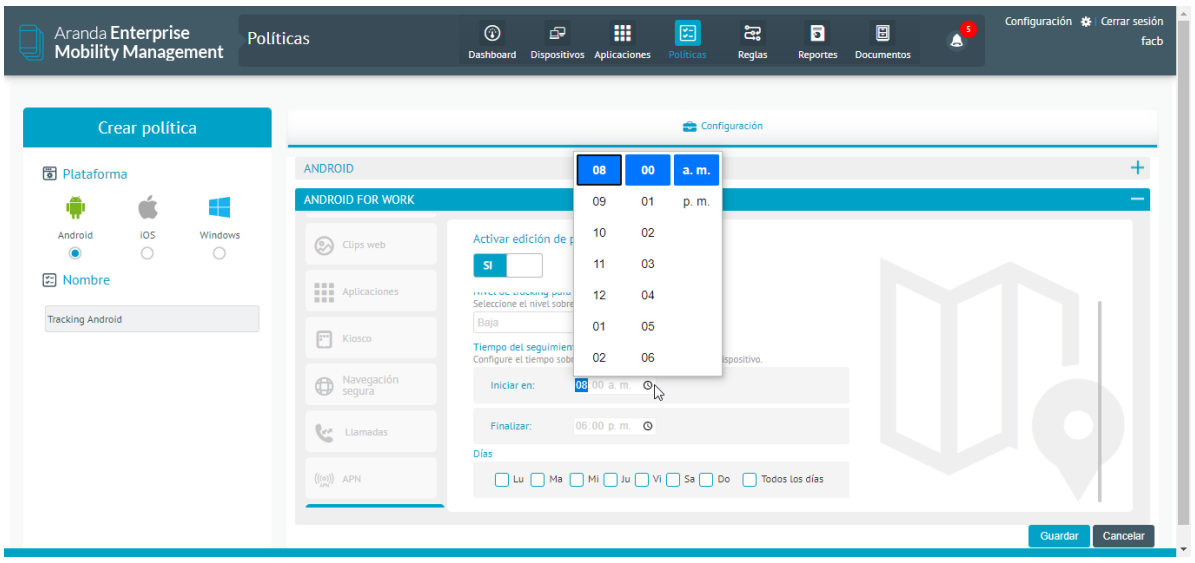
En el módulo de políticas, luego de seleccionar la plataforma y de asignarle un nombre a la política, se visualizará la sección que permite realizar la parametrización de seguimiento.



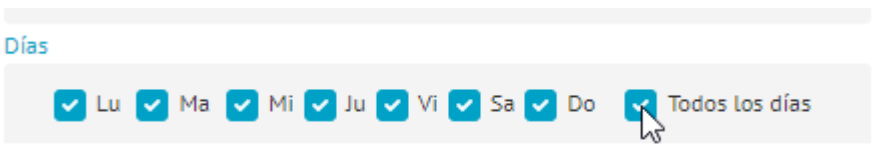
Al hacer clic en la opción “Activar edición de políticas de seguimiento”, se presentan las opciones para seleccionar el nivel de seguimiento a con los valores de: baja, media y alta.



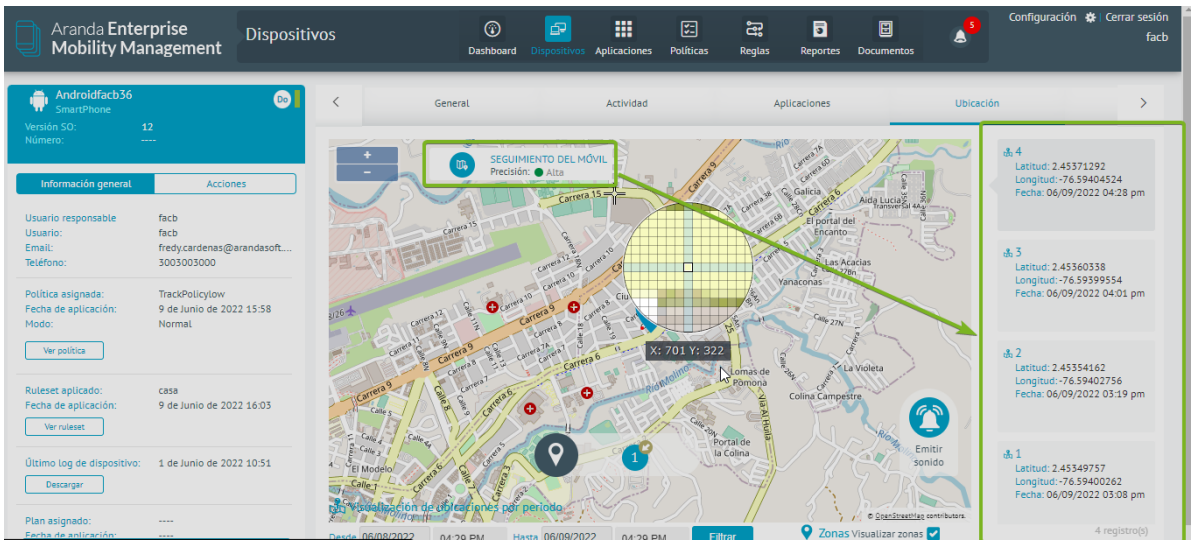
Una vez se ha seleccionado la frecuencia de seguimiento, se dispone de la sección en la cual se puede configurar el tiempo del seguimiento. Al dar clic en el ícono del reloj , aparece la sección que permite seleccionar las horas, minutos y jornada (a.m./p.m.) en la cual se realizará el seguimiento.



Finalmente está la sección que permite configurar los días, la cual permite seleccionar de manera individual los días para aplicar la configuración o también está la opción que permite marcar todos los días.



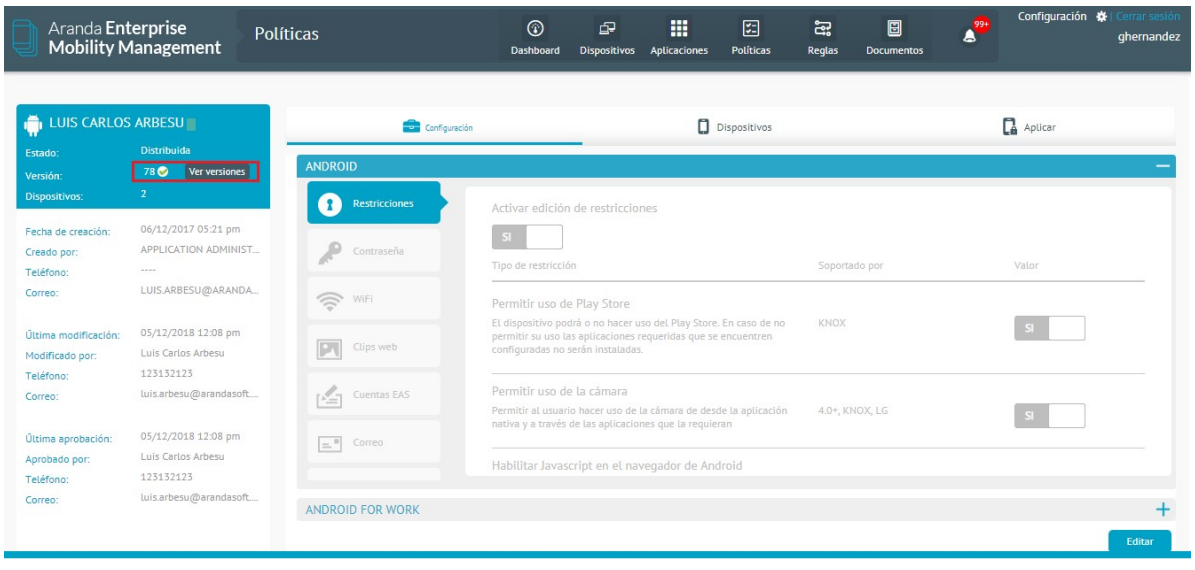
Una vez creada la política de seguimiento y asignada a un dispositivo, esta se podrá consultar en los detalles de localización del dispositivo



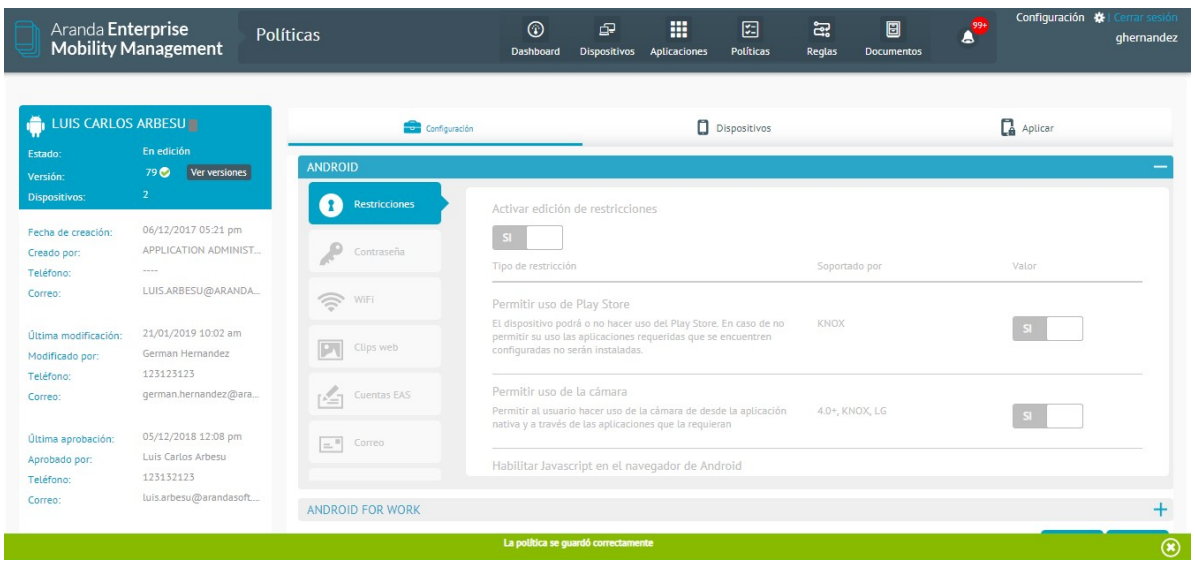
4. Después de configurar las políticas, seleccione la opción **Guardar**.

Aplicación de Políticas

Las políticas se pueden aplicar a usuario, grupos de usuarios o grupos de dispositivos en estado activo y pertenecer a la misma plataforma con la que se configuro la política.

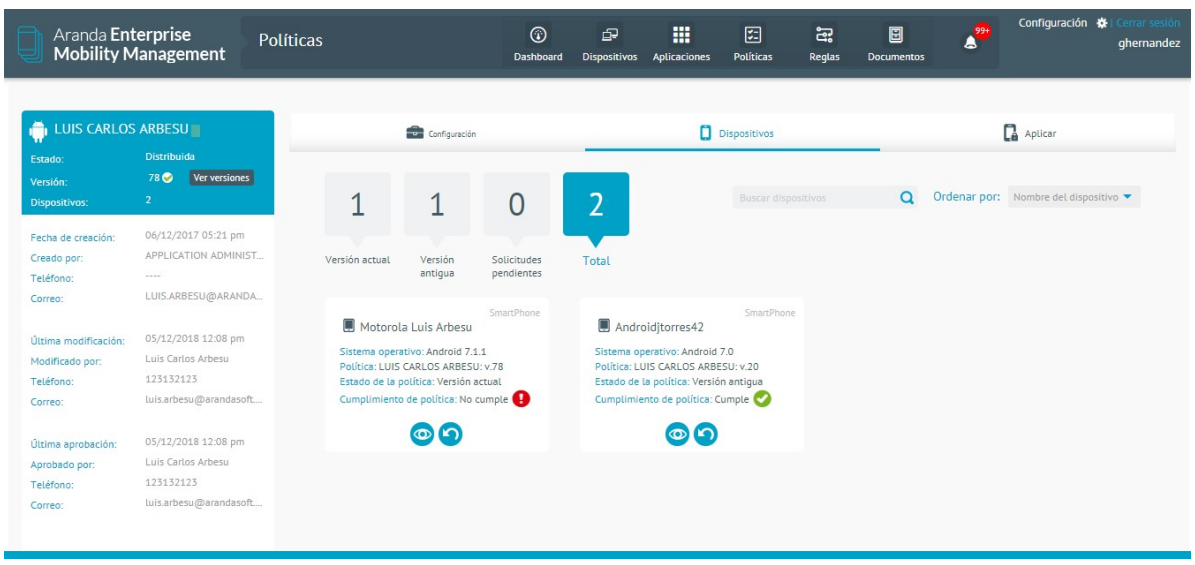


Para que la política se aplique correctamente es necesario aprobar la política.

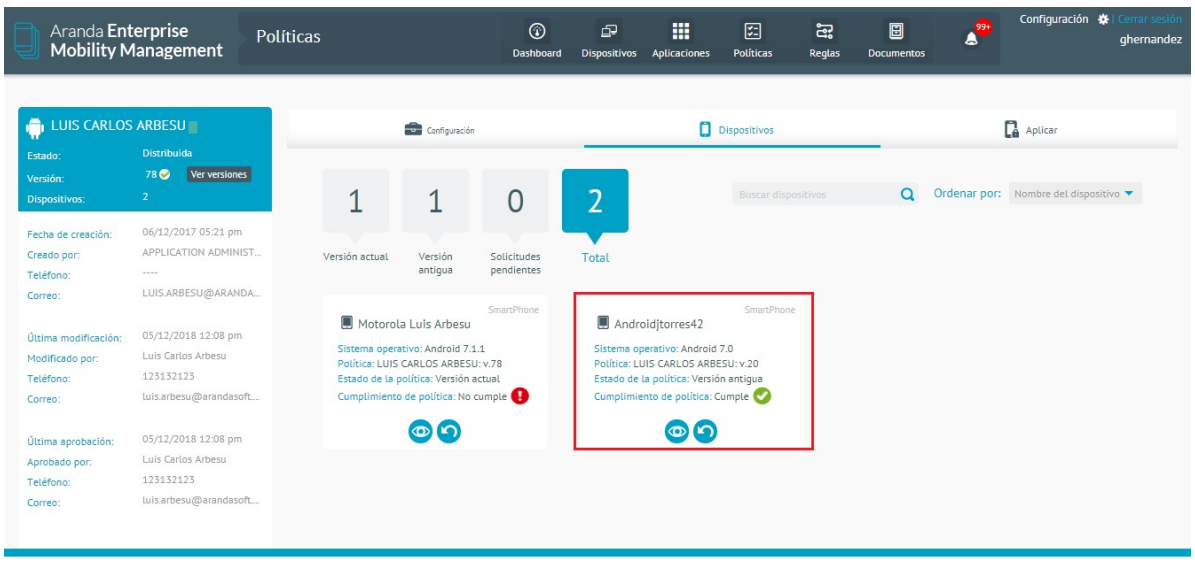


Dispositivos asociados

En la pestaña dispositivos se visualizan los móviles que tienen asociada la política. Siempre que se aplica una política la solicitud se encuentra inicialmente en estado pendiente y pasa a versión actual cuando el móvil la recibe y la aplica. Si se realizan cambios en la política y no se actualiza la versión a los dispositivos que la tienen aplicada esta pasa a versión antigua. Dentro del listado de dispositivos asociados es posible realizar ordenamiento y búsqueda.

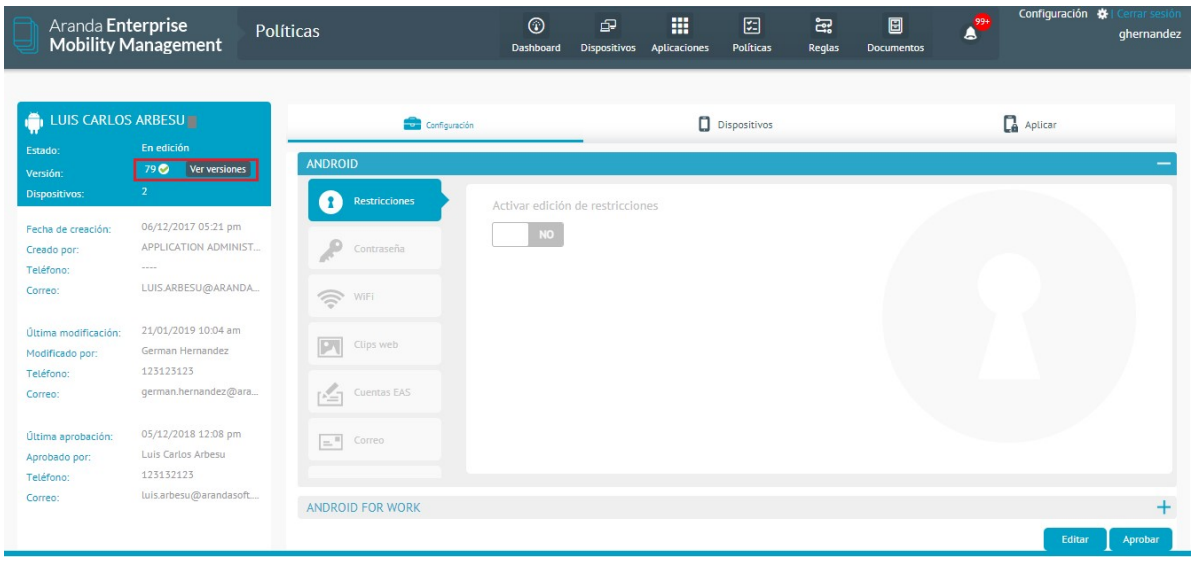


El dispositivo muestra un resumen de la política aplicada, indicando: el nombre de dispositivo, tipo, sistema operativo y versión, nombre de la política junto con su versión, estado de política y cumplimiento.

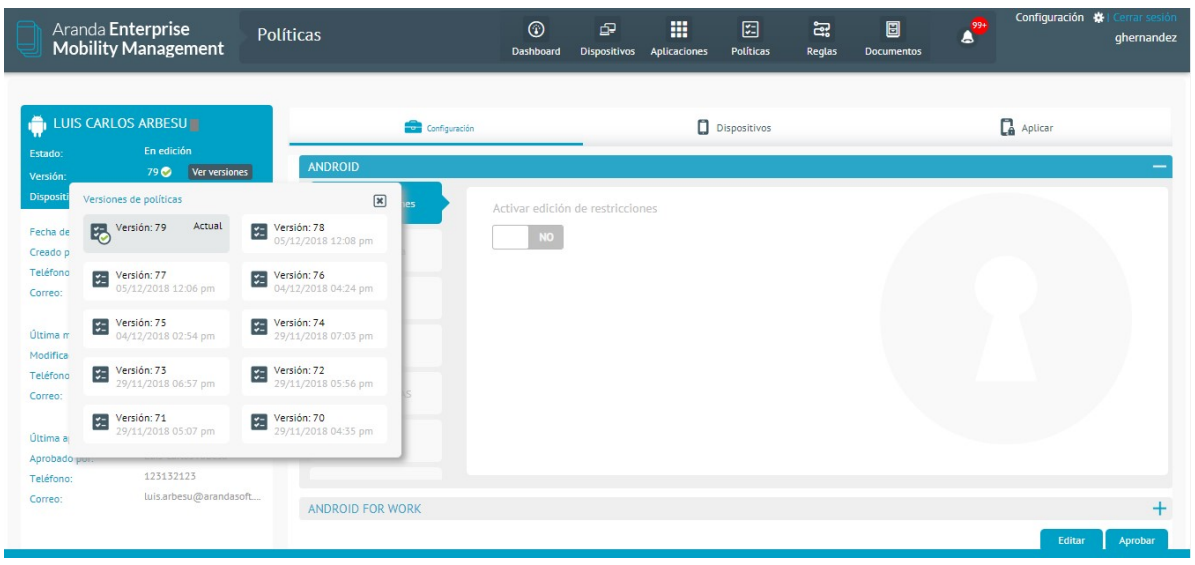


Versionamiento y Redistribución de Políticas

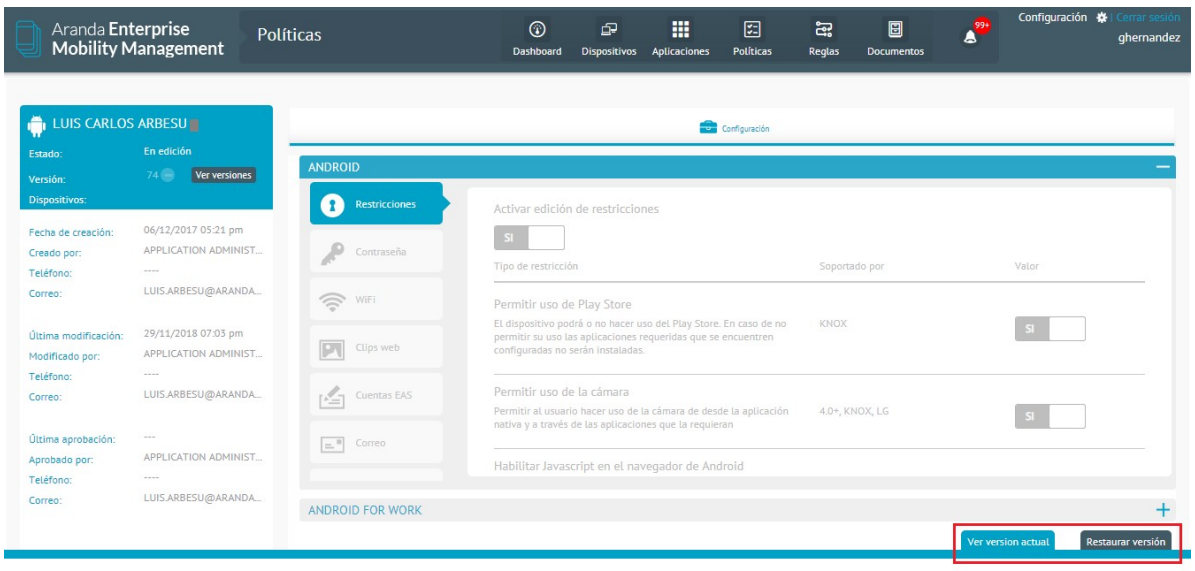
Por cada cambio que se realice sobre la política aumenta el número de versión. Cabe aclarar que si la política no se aprueba la versión que se aplica al dispositivo es la última aprobada.



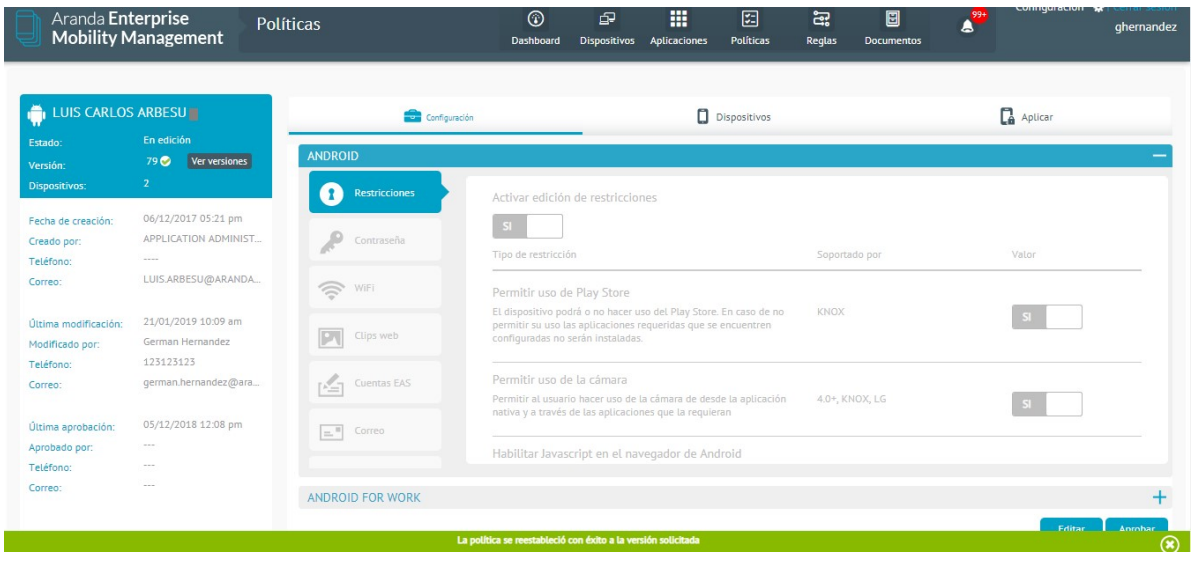
Las versiones almacenadas se pueden visualizar al dar clic en "**Ver versiones**"



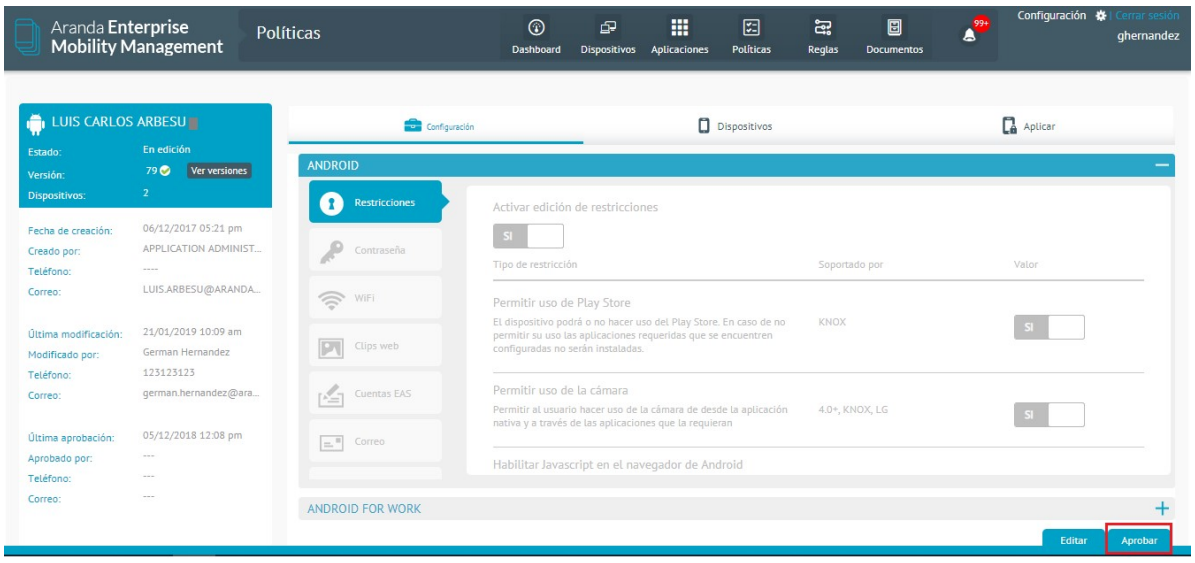
Se tiene la posibilidad de ver la versión actual o restaurar la versión



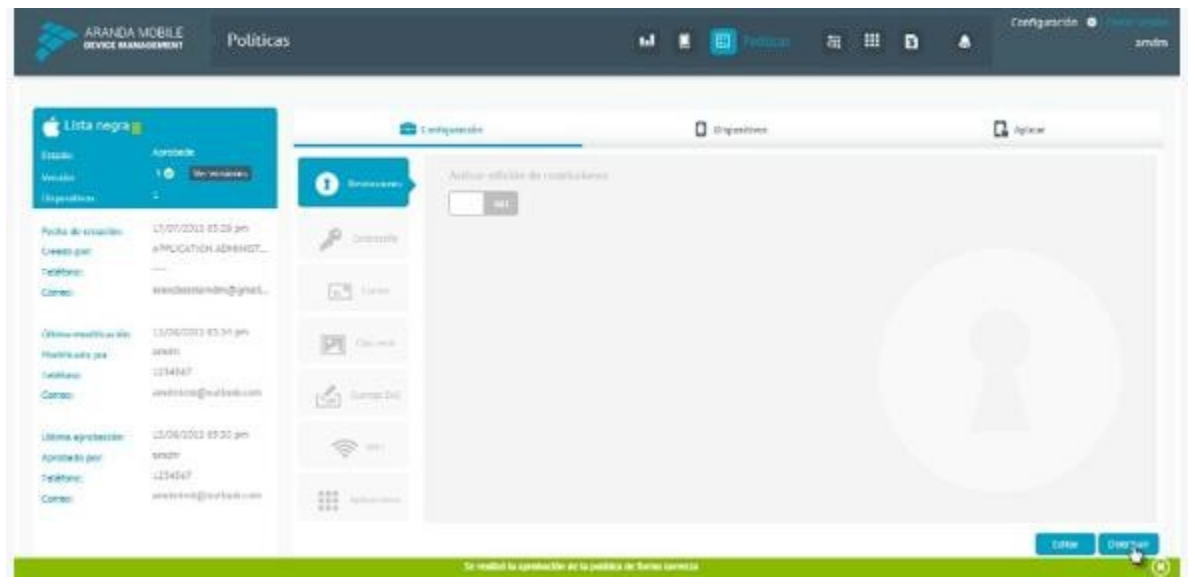
La política se restaura.



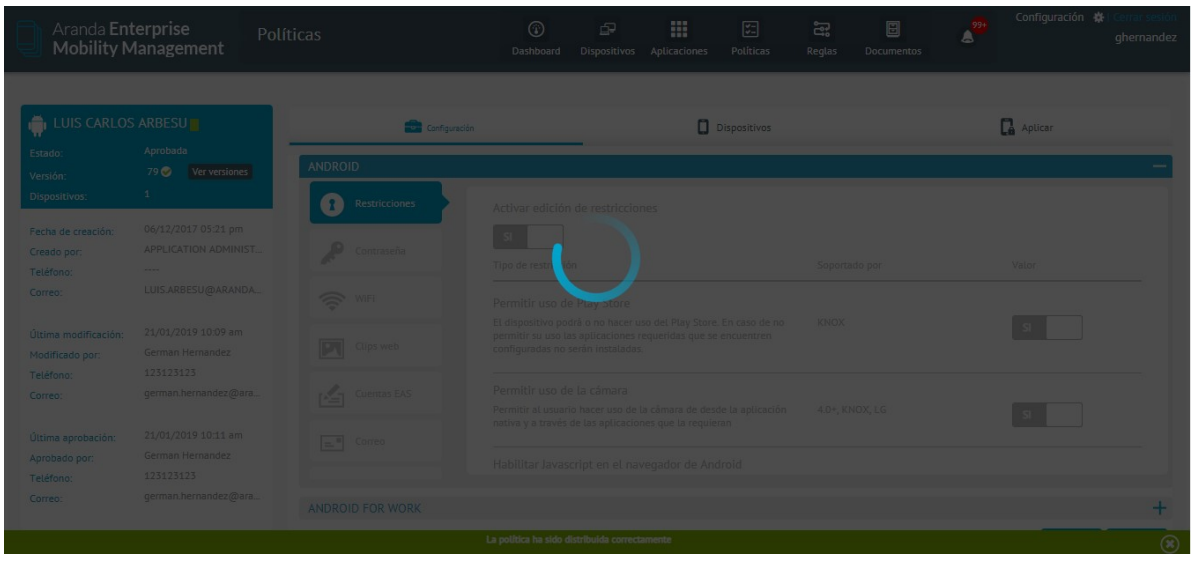
Esta se debe aprobar.



Y distribuir para aplicar todos los cambios a los dispositivos que tienen asociada la política.

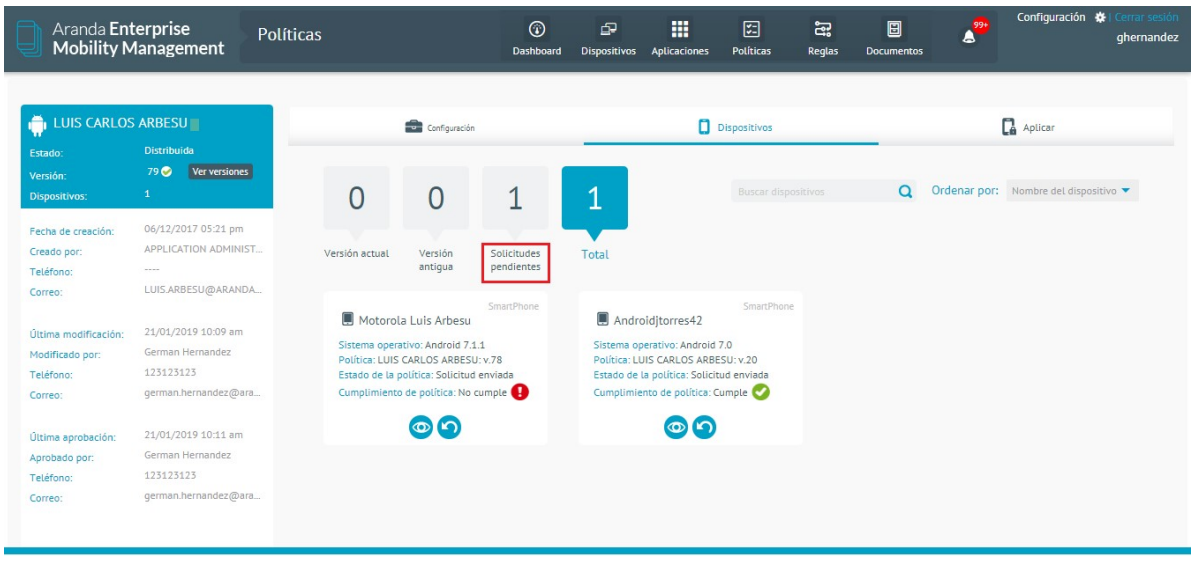


La política se distribuye exitosamente.



Problemas comunes en el manejo de políticas

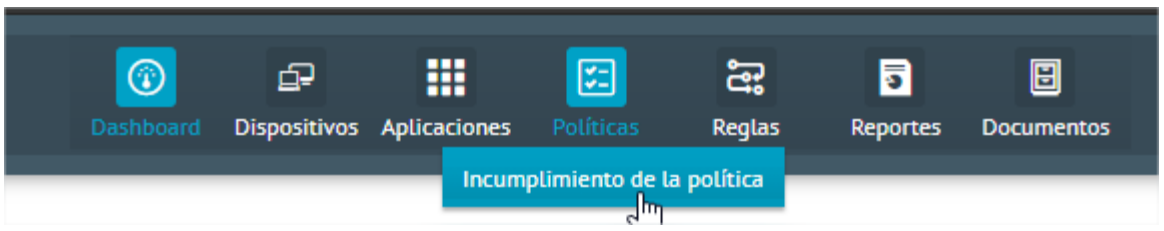
- Si la política se aplica y esta permanece como “Solicitudes pendientes” es necesario validar si el dispositivo móvil tiene problemas de conectividad.

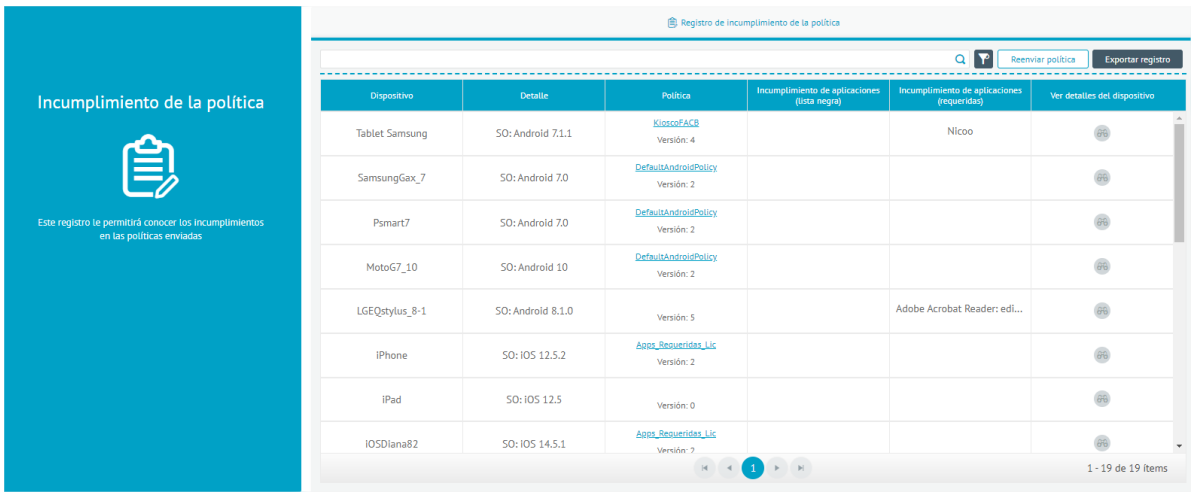


- Cuando aplique una política de cuenta EAS o correo a un dispositivo Android genérico, esta nunca la recibirá el

dispositivo móvil, ya que solo aplica para dispositivos Samsung Knox
- La única restricción que es posible aplicar a Android genérico es bloqueo de cámara.
- No es posible aplicar una política en estado Edición, está siempre debe estar aprobada, solo se aplica en edición si la política ya se encontraba en estado aprobada.

Módulo de Incumplimiento de Políticas





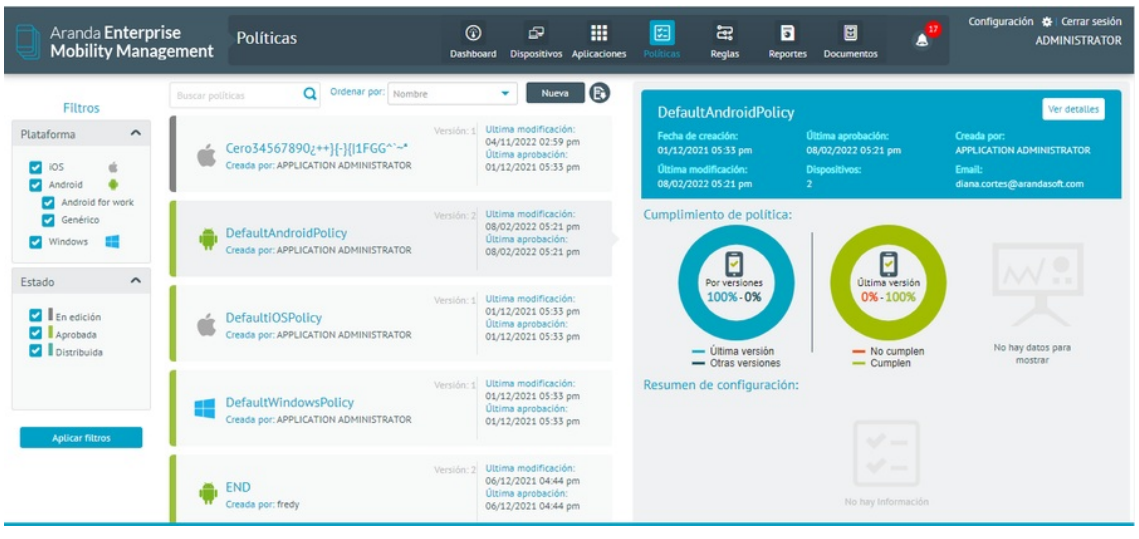
Esta sección está destinada a gestionar los incumplimientos de política que actualmente presentan los dispositivos a nivel de aplicaciones.

Presenta las siguientes subsecciones/funcionalidades

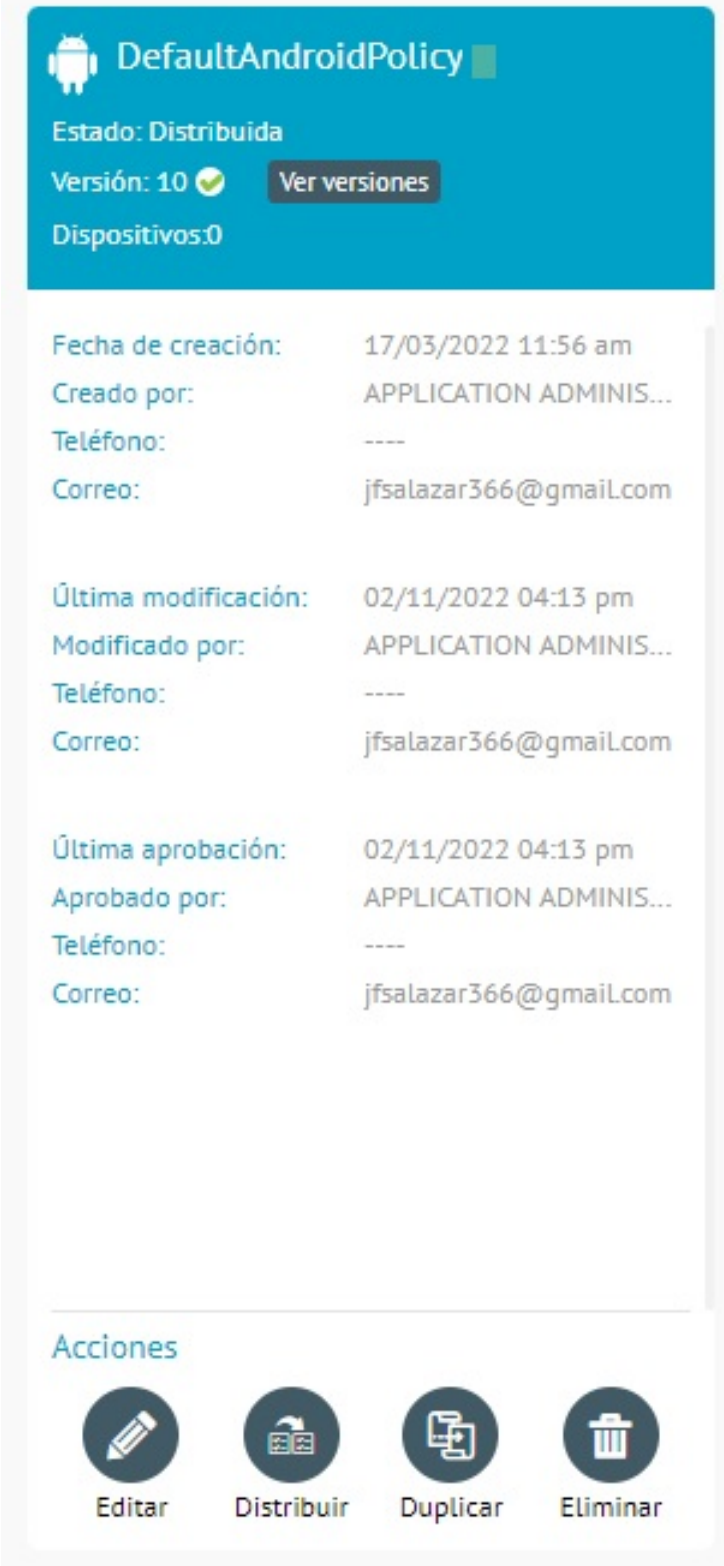
- Filtro por dispositivos: Permite filtrar por dispositivos específicos
- Filtro por sistema operativo y política: Filtro anidado que filtra el listado por plataforma y respectiva política aplicada al dispositivo.
- Reenviar política: Ejecuta en reenvío masivo a todos los dispositivos listados que incumplen su política actualmente asignada.
- Exportar registro: Exporta el listado a un archivo Excel.

Duplicar política

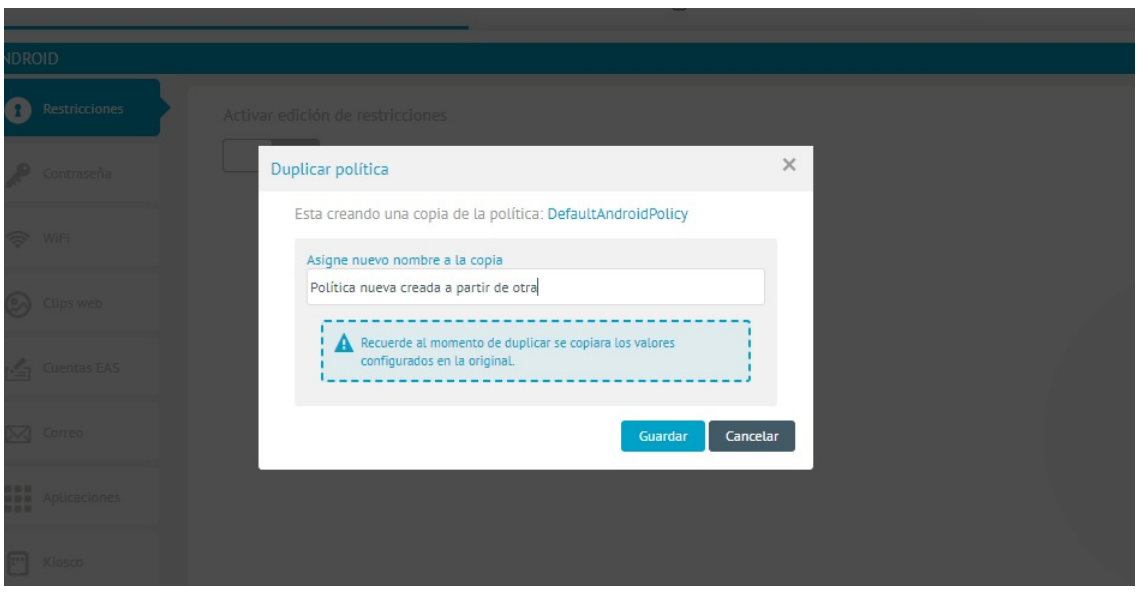
1. Para duplicar una política, ingrese a la consola de inicio de AEMM, seleccione la opción **Políticas** del menú encabezado. En la vista de información podrá visualizar el listado de políticas y buscar los registros por nombre y ordenar la información asociada. Seleccione una política y en la vista detalle acceda a la información configurada



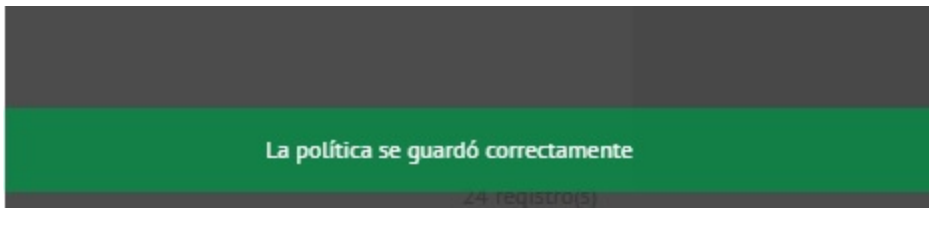
2. En el menú principal de la política tendrá disponible la sección de Acciones. Seleccione la opción **Duplicar** para crear una nueva política a partir de una existente.



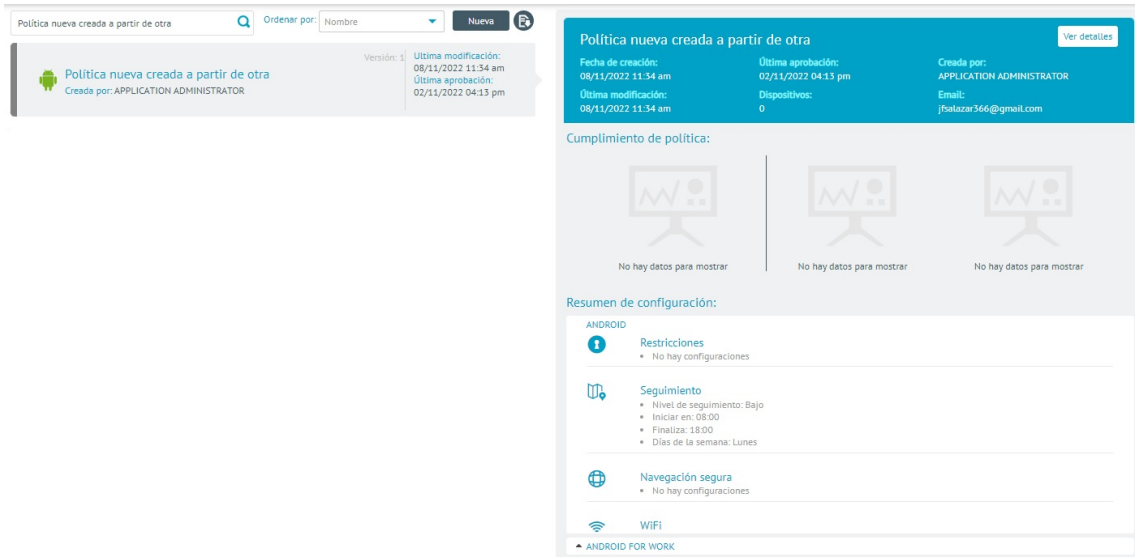
3. Se habilita la ventana **Duplicar Política**, donde podrá ingresar el nombre de la política y Guardar la información asociada.



4. Al guardar los cambios realizados podrá visualizar un mensaje de confirmación de éxito si no se presentan problemas en la configuración



5. Terminado el proceso podrá consultar dentro de nuestro listado de políticas, editar o distribuir la política según la necesidad.



Reglas

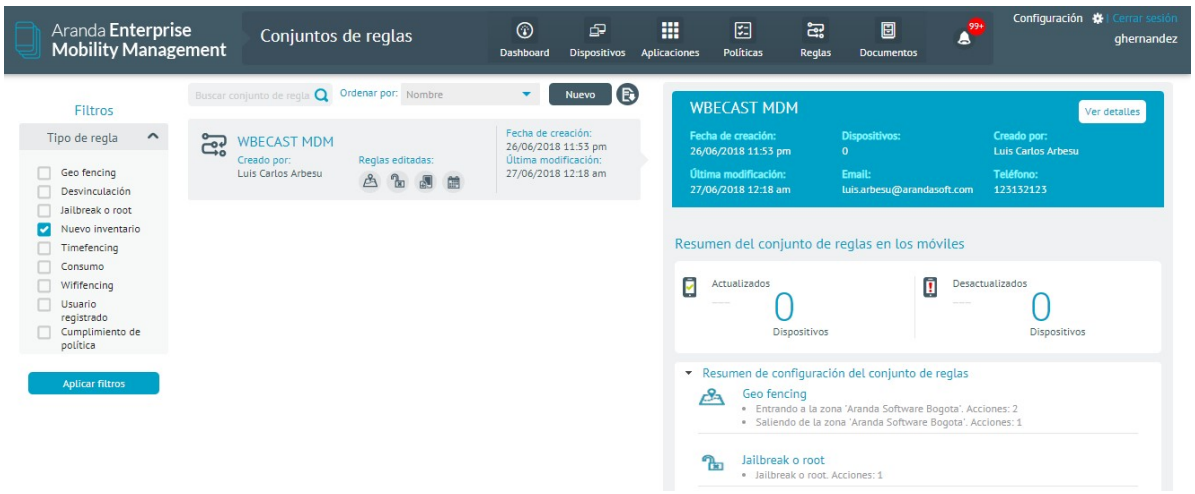
Módulo de Conjuntos de Reglas

Actualmente se manejan los siguientes tipos de reglas:

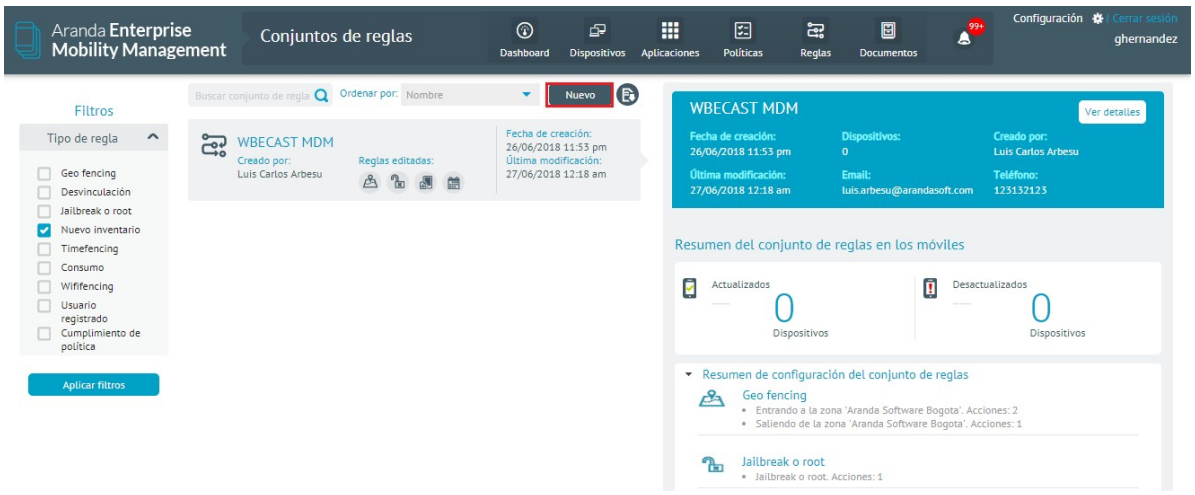
Reglas de negocio en AEMM	Descripción
Geofencing:	Se realiza seguimiento de la ubicación del dispositivo en determinada área geográfica, la configuración de la regla informa si el dispositivo entra o sale del área configurada. (Zonas geofencing)
Desvinculación:	Notificar al sistema cuando el dispositivo fue desvinculado, ya sea la acción desde la consola o desde el móvil.
Jailbreak o root:	Notificar al sistema si el dispositivo tiene Jailbreak o root.
Nuevo Inventario:	Siempre que se solicita nuevo inventario se genera un evento para que sea evaluado por las configuraciones de reglas.
Timefencing:	Seguimiento del horario configurado en el cual se encuentra un dispositivo, indicando si el dispositivo entra o sale del horarios establecido.
Consumo:	Seguimiento al consumo realizado de voz y/o datos tanto local como en roaming.
WifiFencing:	Seguimento para controlar las redes a las que se conecta el dispositivo en una lista de wifi para saber si el dispositivo se conecta o se desconecta a determinada red de wifi.
Usuario Registrado:	Indica qué hacer cuando hay un cambio de usuario logueado en el dispositivo.
Fallo de autenticación:	Se implementa una nueva regla para ejecutar una determinada acción ante el intento fallido de desbloqueo del móvil, se ejecutan las acciones de acuerdo al número de intentos fallidos que se definan (Tener en cuenta que se toman intentos fallidos, con el mismo número de caracteres de la contraseña).

Configuración de Conjuntos de Reglas

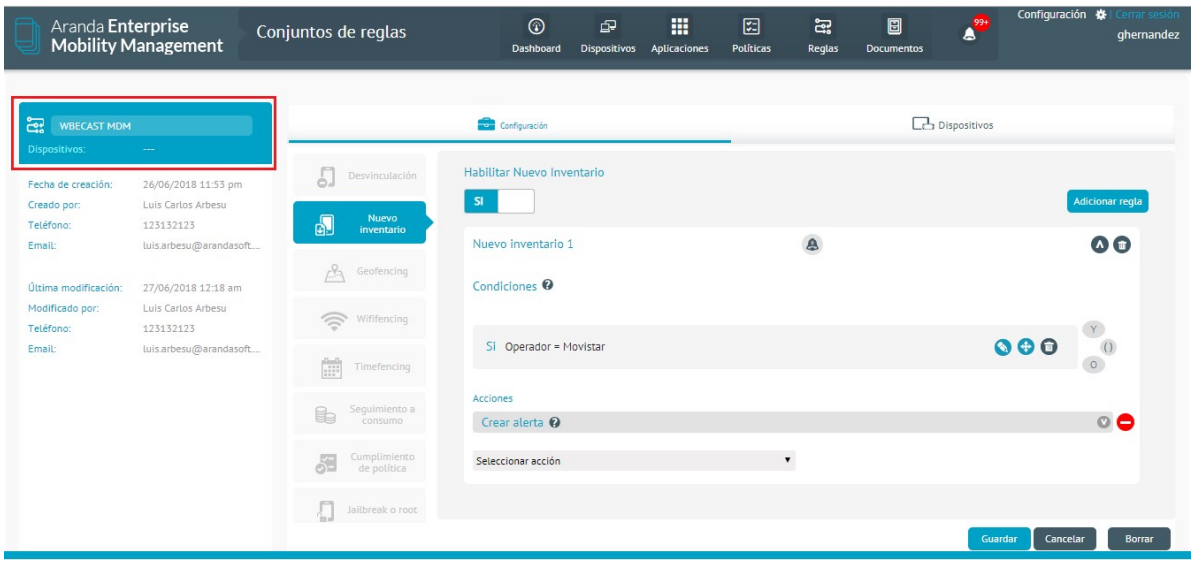
Para acceder a la sección del conjunto de reglas se debe seleccionar desde el menú superior de la consola web.



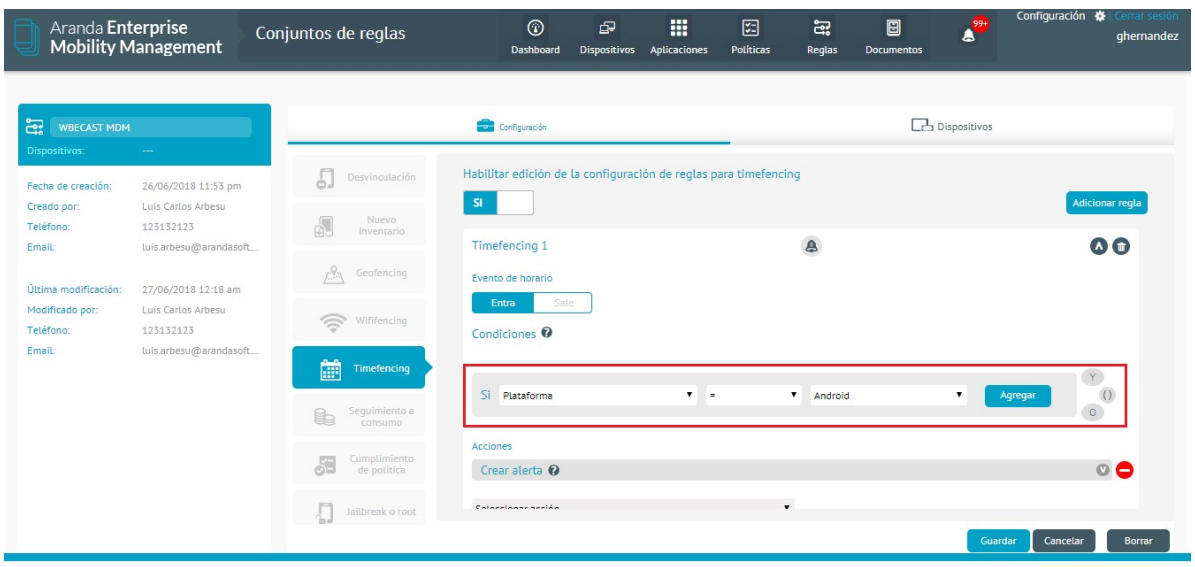
Para agregar una nueva regla presione de clic en **Nuevo**, ubicado en la parte superior del panel de listados de reglas.



En el formulario para agregar una nueva regla se debe ingresar el nombre de la regla, y luego se puede habilitar cualquiera de las disponibles, cuando se habilita cualquiera de estas se despliega un formulario para indicar la acción asociada a la regla.

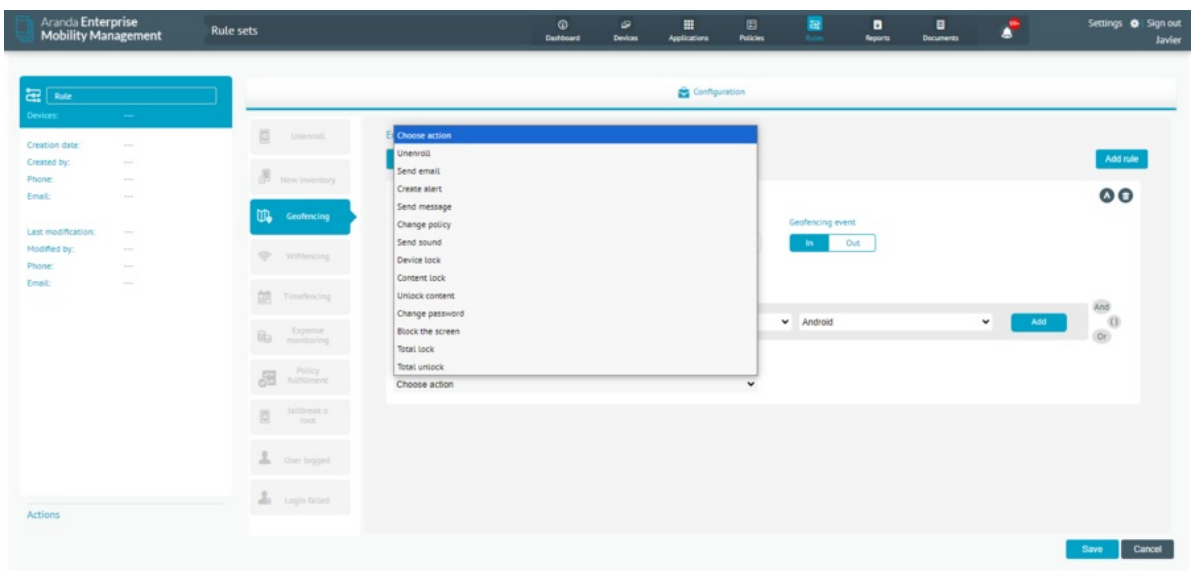


Dentro del formulario de acciones en cada una de las reglas se puede configurar una serie de condiciones y agregarlas según su configuración.



Después de esto en la parte inferior se puede configurar acciones a tomar dentro de las que encontramos las siguientes:

Acción	Descripción
Desvinculación	El dispositivo se desvinculará de la plataforma.
Enviar mail	Se envía un correo electrónico previamente configurado notificando el cumplimiento de la regla.
Crear alerta	Se crea una alerta en la plataforma cuando se cumpla la regla.
Enviar mensaje	Envía una notificación personalizada al dispositivo cuando se cumpla la regla.
Cambiar política	Se realiza un cambio de política en el dispositivo, esta se configura previamente y se realiza cuando se cumpla la regla.
Enviar sonido	Se envía un comando de sonido (aviso sonoro) al dispositivo cuando se cumpla la regla.
Bloquear dispositivo	Se bloquea la pantalla del dispositivo cuando se cumpla la regla.
Bloquear contenido	Bloquea todo el contenido del dispositivo cuando se cumpla la regla.
Desbloquear contenido	Desbloquea todo el contenido del dispositivo cuando se cumpla la regla.
Cambiar contraseña	Cambia la contraseña de acceso al dispositivo por una previamente configurada cuando se cumpla la regla.
Bloquear la pantalla	Bloquea la pantalla del dispositivo, el usuario puede desbloquear usando una contraseña
Restablecer dispositivo	Restablece el dispositivo a su estado de fábrica
Bloqueo total	Bloquea totalmente el uso del dispositivo
Desbloqueo total	Revierte el bloqueo total del dispositivo



Para almacenar los cambios realizados de clic en **Guardar** en la parte inferior derecha del formulario.

> ⚐ **Nota:** La totalidad de las acciones mencionadas previamente NO aplican en todas las reglas.

Listado y Previsualización de Conjuntos de Reglas

La lista de reglas almacenadas se visualiza desde la vista principal del menú de reglas. Los filtros permiten buscar

por:

- Regla de negocio
- Nombre

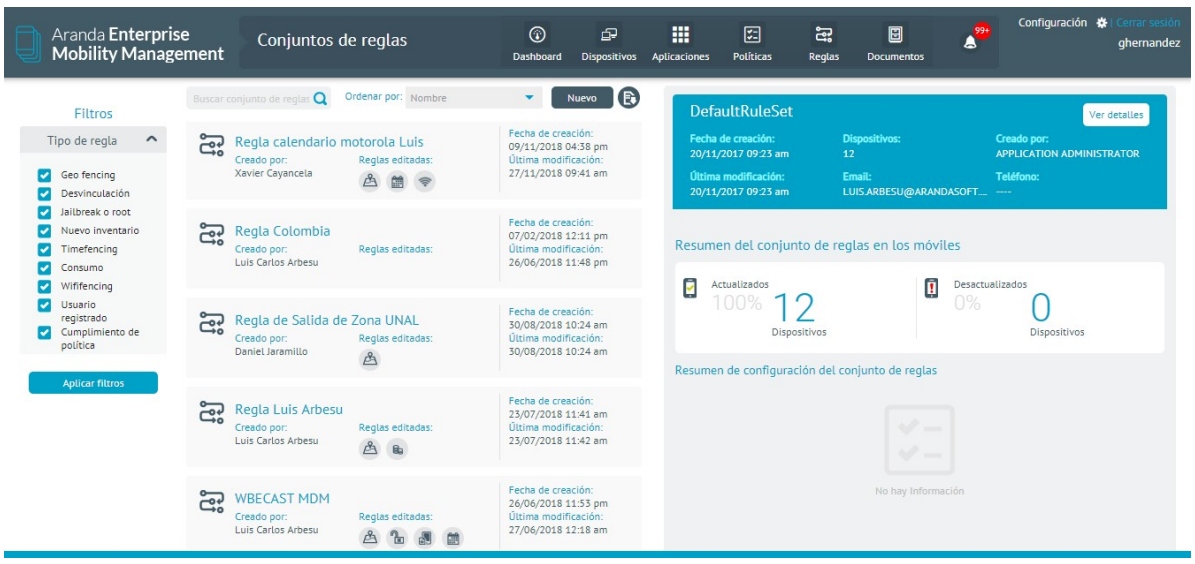
Además, estas se pueden ordenar por:

- Nombre
- Usuario creador
- Fecha de creación
- Fecha de modificación

En la parte derecha de la vista se presenta un resumen de la regla seleccionada, en la parte superior del resumen se presenta la siguiente información:

- Fecha de creación
- Última modificación
- Dispositivos
- Email
- Creado por
- Teléfono

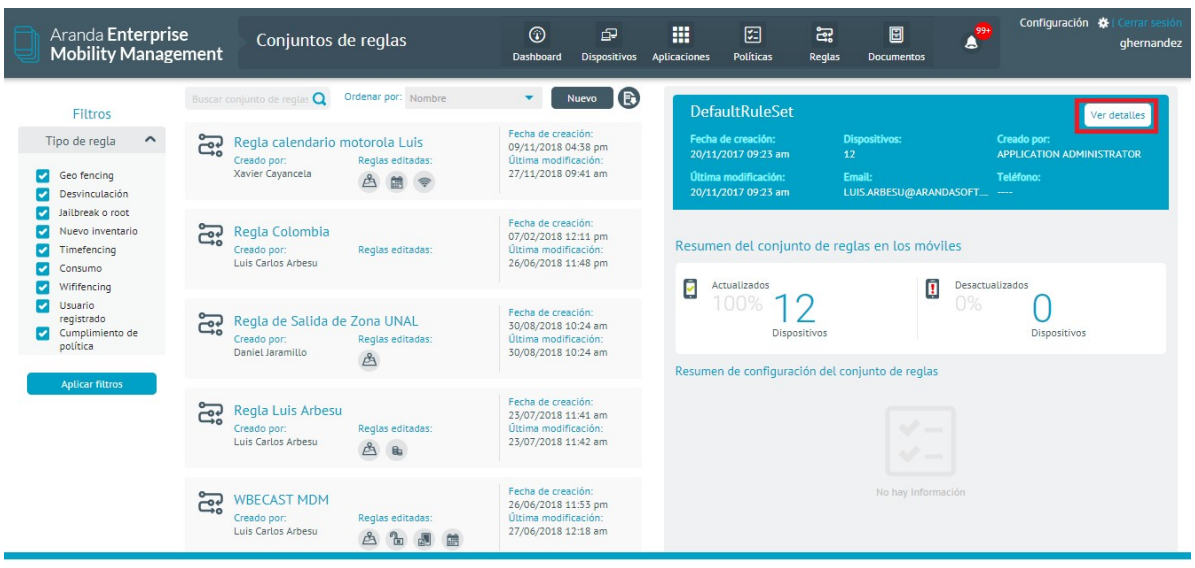
En la parte media del resumen se presenta el número de dispositivos que tienen aplicada la regla separada por los que están actualizados y los que no están actualizados. En la parte inferior del resumen se presentan las acciones asociadas a cada regla de negocio existente en EMM.



Dispositivos Asociados

Visualizar dispositivos

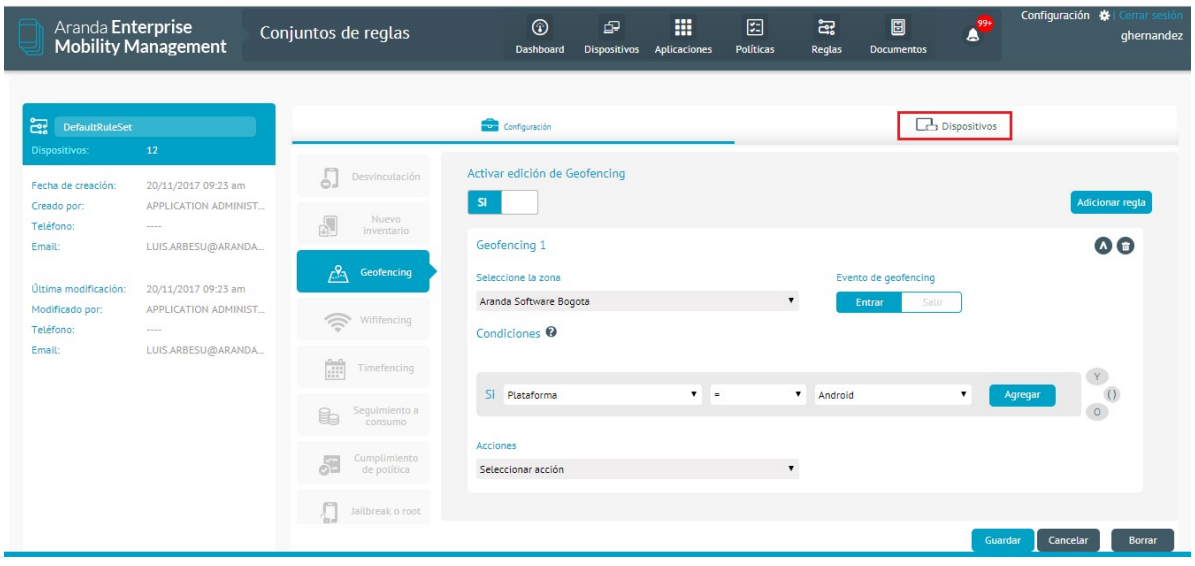
Para visualizar la lista de dispositivos a los cuales se le aplicó una regla, se debe seleccionar el botón Ver detalles ubicado en la parte superior derecha del resumen de la regla.



En el detalle de la regla seleccione la pestaña **Dispositivos**. En esta vista se puede visualizar la lista de dispositivos asociados a la regla, mostrando el tipo de dispositivos (teléfono o tableta), el nombre del dispositivo, su dueño y si la regla está actualizada, además presenta opciones para actualizar la regla y ver la información detallada del dispositivo.

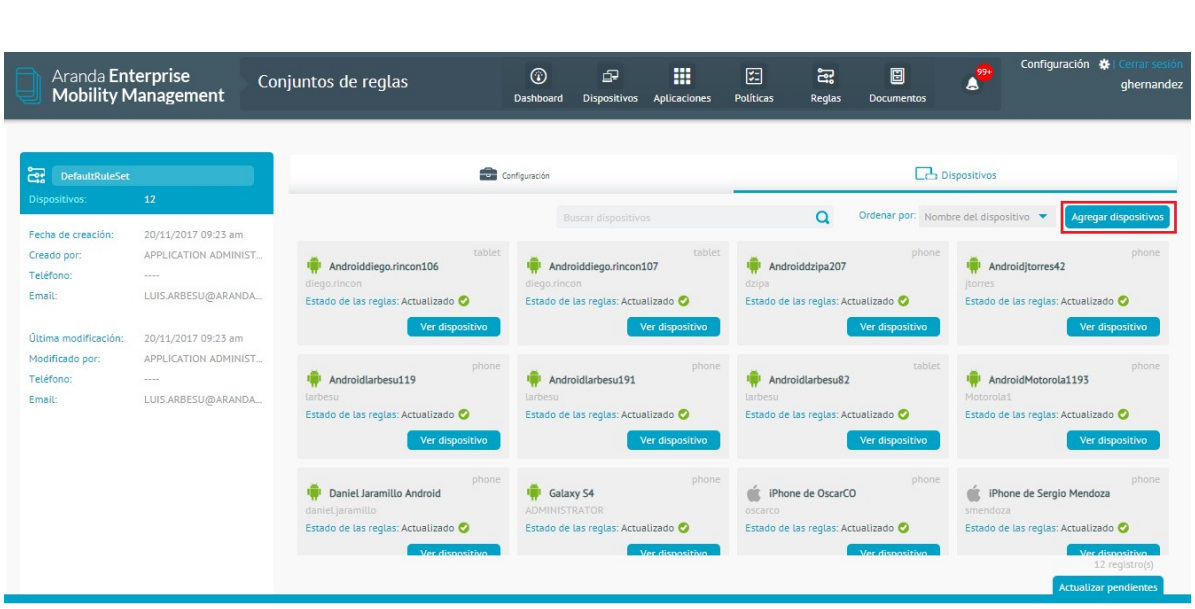
En la parte inferior de la vista está el botón **Actualizar pendientes** para hacer una actualización masiva de la regla a los

dispositivos asociados.

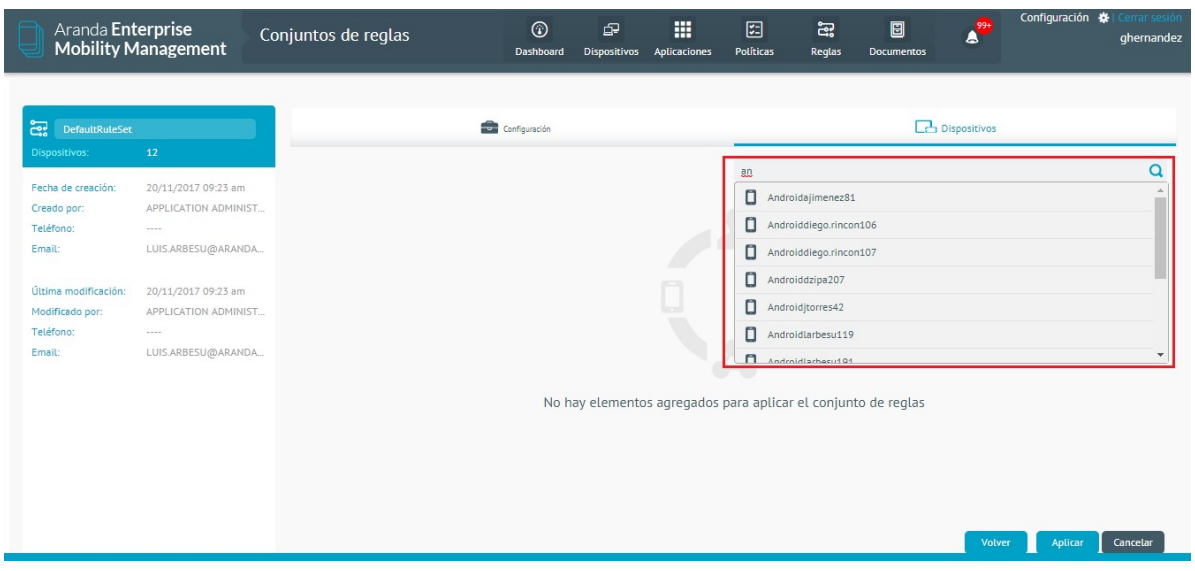


Agregar dispositivos

Para agregar dispositivos a una regla determinada se debe ver el detalle de la regla y dar clic en la pestaña **Dispositivos**, al seleccionar la pestaña, en la parte derecha se debe seleccionar el botón **Agregar dispositivos.**



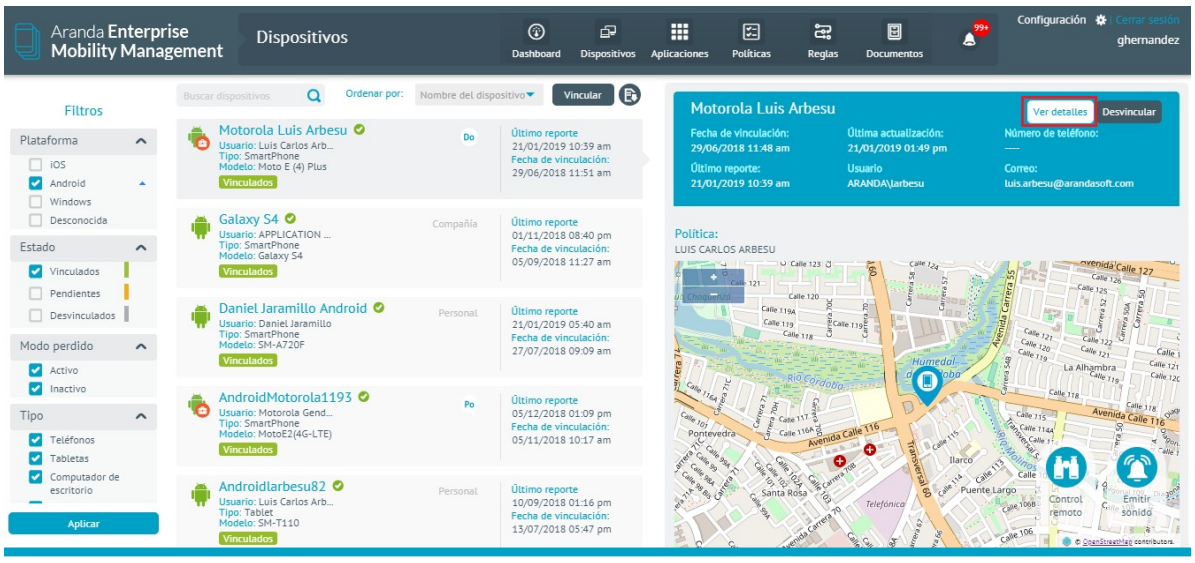
En el campo de búsqueda se filtran y agregan los dispositivos, grupos de dispositivos, usuarios y grupos de usuarios que se quieren agregar para aplicarles la regla.



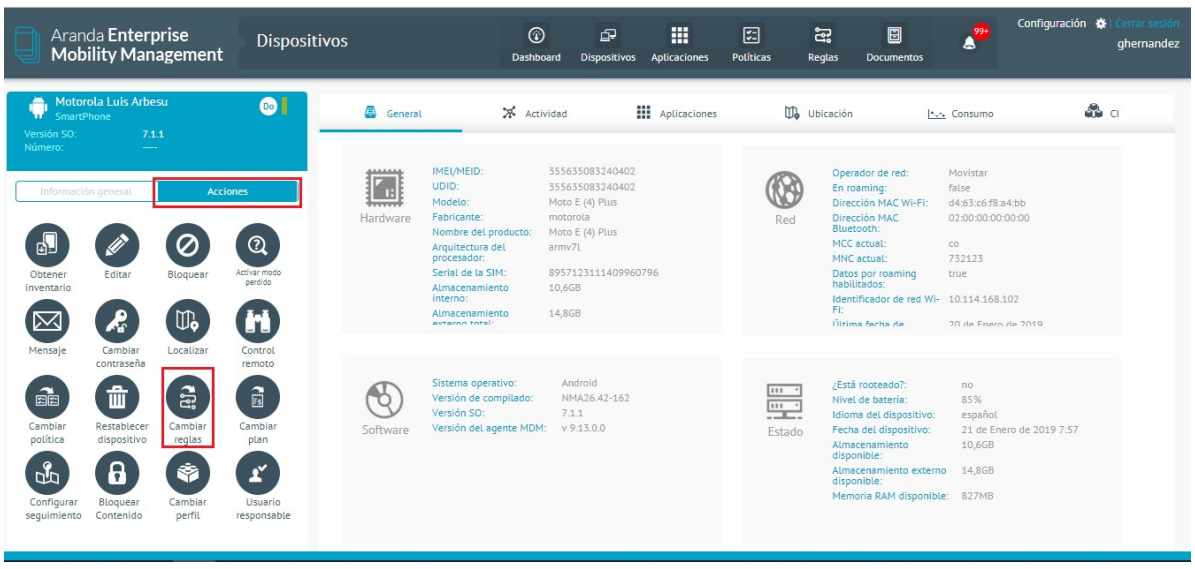
Aplicación de Conjuntos de Reglas

Las reglas pueden ser aplicadas para todos los dispositivos a los que aplican o de forma individual. Para aplicar un conjunto de reglas desde la sección de Reglas del menú principal se deben seguir los pasos explicados en la sección **Dispositivos asociados**.

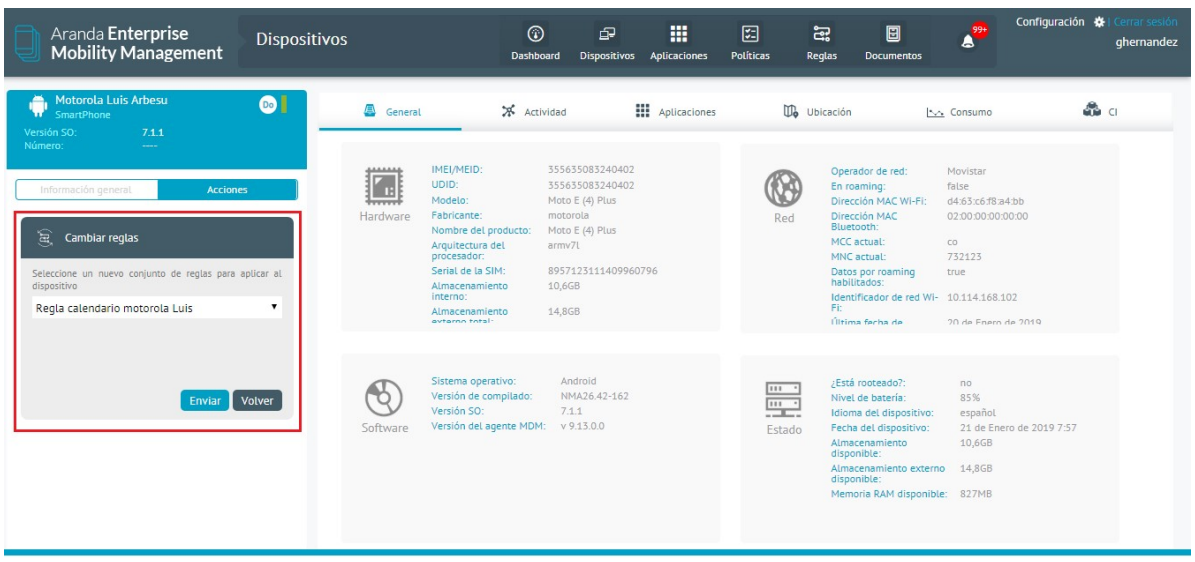
También se pueden aplicar un conjunto de reglas desde la hoja de vida del dispositivo, para esto se debe seleccionar la sección **Dispositivos** del menú principal, seleccionar un dispositivo de la lista y presionar el botón **Ver detalles** del panel ubicado a la derecha



Al presionar el botón de **ver detalles**, aparece la hoja de vida del dispositivo, en la parte inferior izquierda se presenta un menú con una lista de acciones para realizar con ese dispositivo, entre las cuales se encuentra la opción **Cambiar conjunto de reglas.**

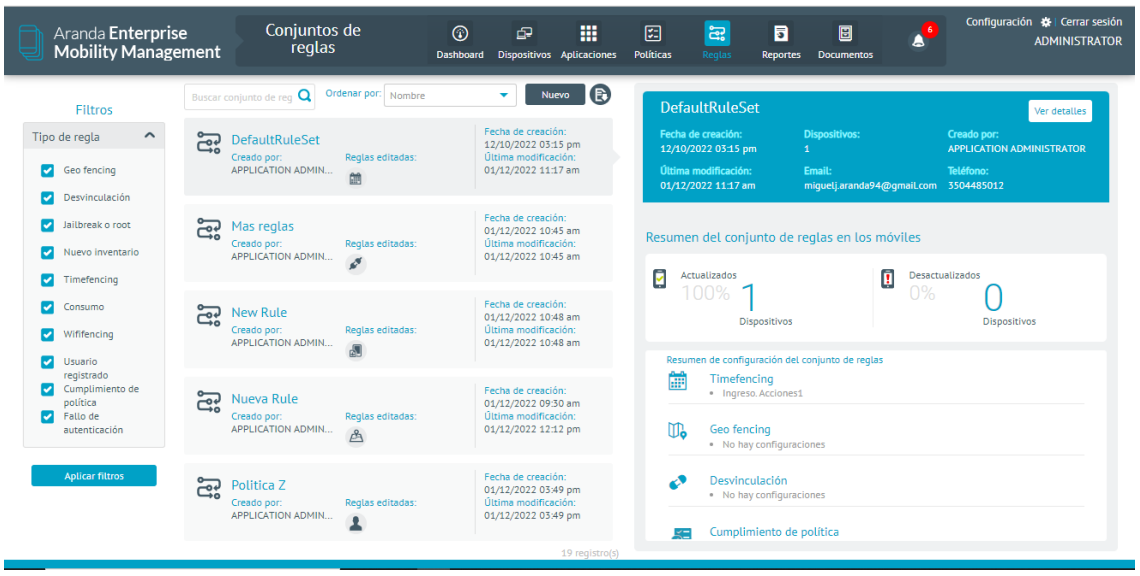


Al seleccionar la opción aparece un cuadro con una lista desplegable que contiene la lista de reglas existentes, se puede seleccionar una de las reglas y aplicarla al dispositivo.

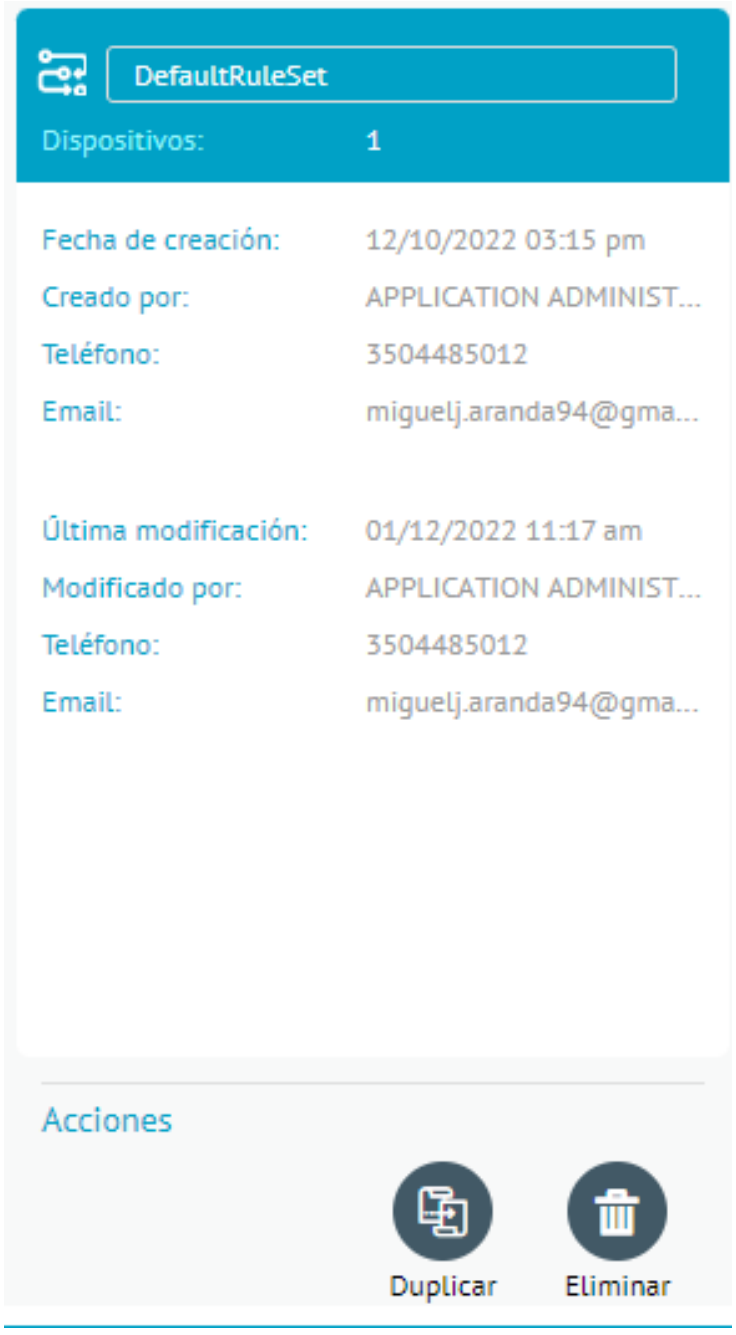


Duplicar reglas

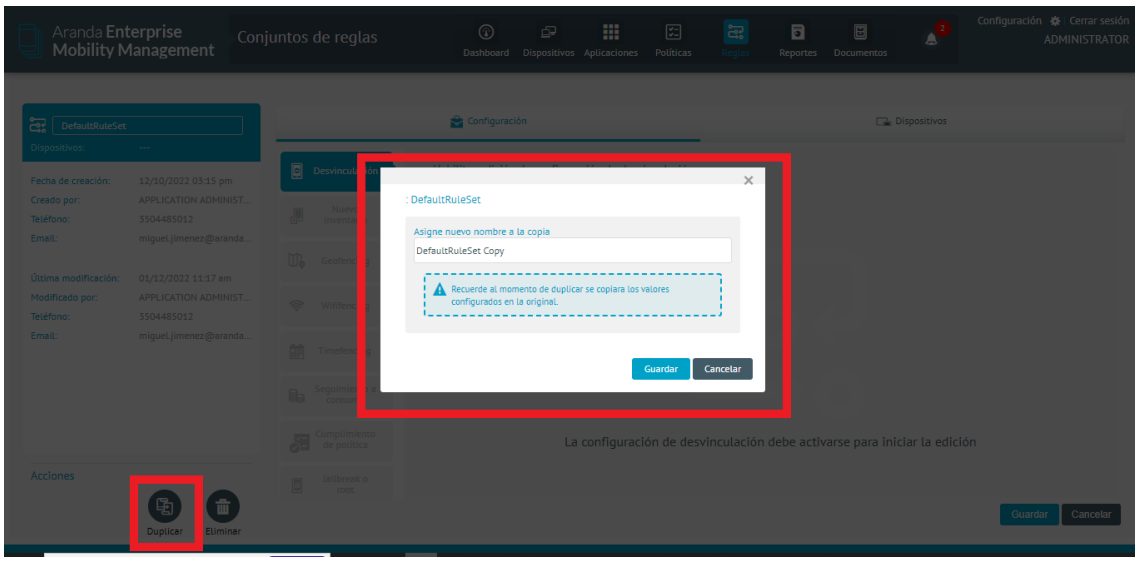
1. Para duplicar una regla, ingrese a la consola de inicio de AEMM, seleccione la opción **Reglas** del menú encabezado. En la vista de información podrá visualizar el listado de reglas y buscar los registros por nombre y ordenar la información asociada. Seleccione una regla y en la vista detalle acceda a la información configurada



2. En el menú principal de la regla tendrá disponible la sección de Acciones. Seleccione la opción **Duplicar** para crear una nueva regla a partir de una existente.

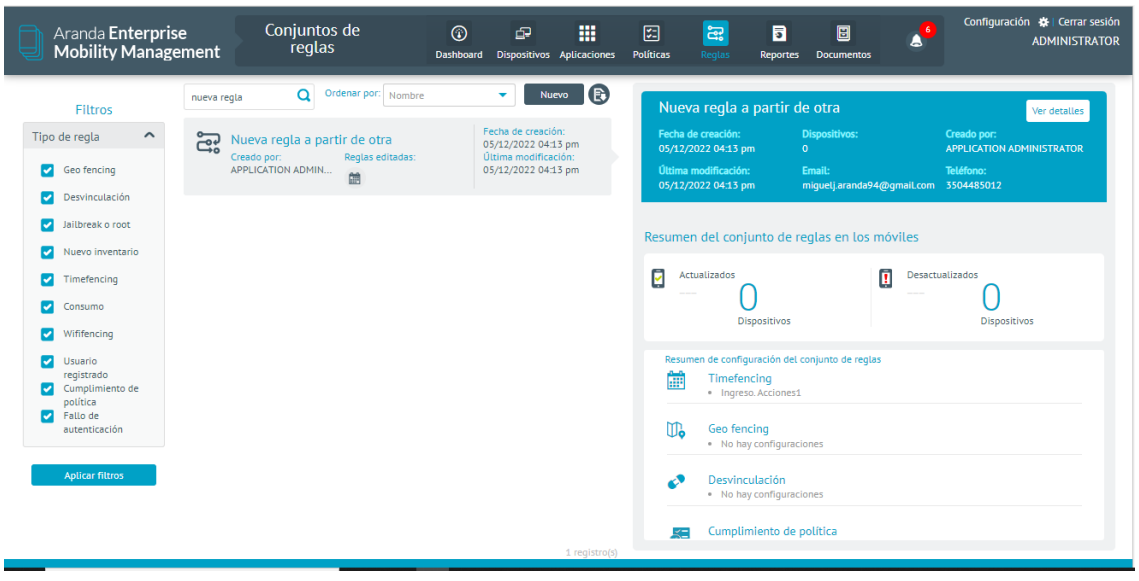


3. Se habilita la ventana **Duplicar regla**, donde podrá ingresar el nombre de la regla y Guardar la información asociada.



4. Al guardar los cambios realizados podrá visualizar un mensaje de confirmación de éxito si no se presentan problemas en la configuración. (El conjunto de Reglas se ha creado correctamente).

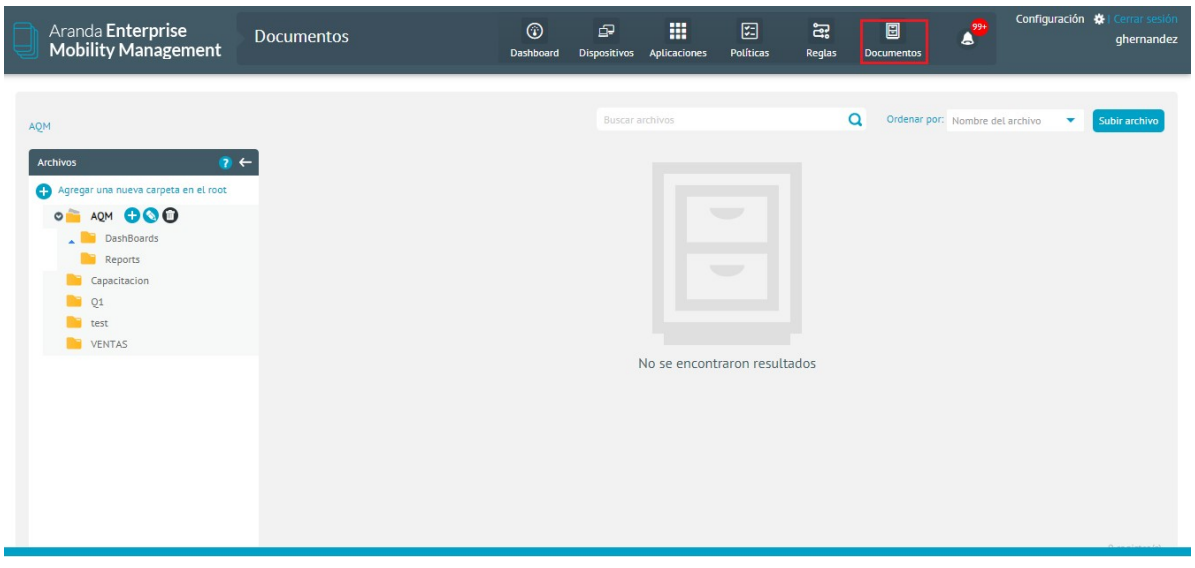
5. Terminado el proceso, en la vista de información podrá consular el listado de reglas; editar o distribuir la regla según la necesidad.



Documentos

Módulo de Documentos

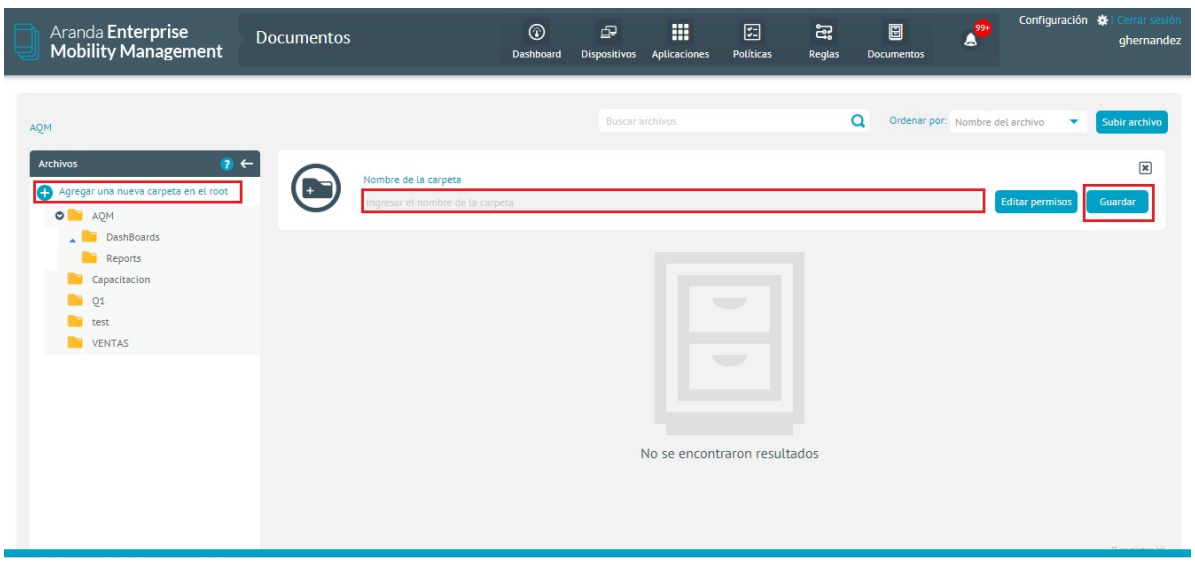
La sección de documentos permite la administración de contenido, ubicaciones y permisos sobre estas ubicaciones, para ingresar, debe seleccionar a la sección **Documentos** del menú principal. Para visualizar y administrar los contenidos desde los dispositivos móviles se cuenta con la aplicación (Content Manager).



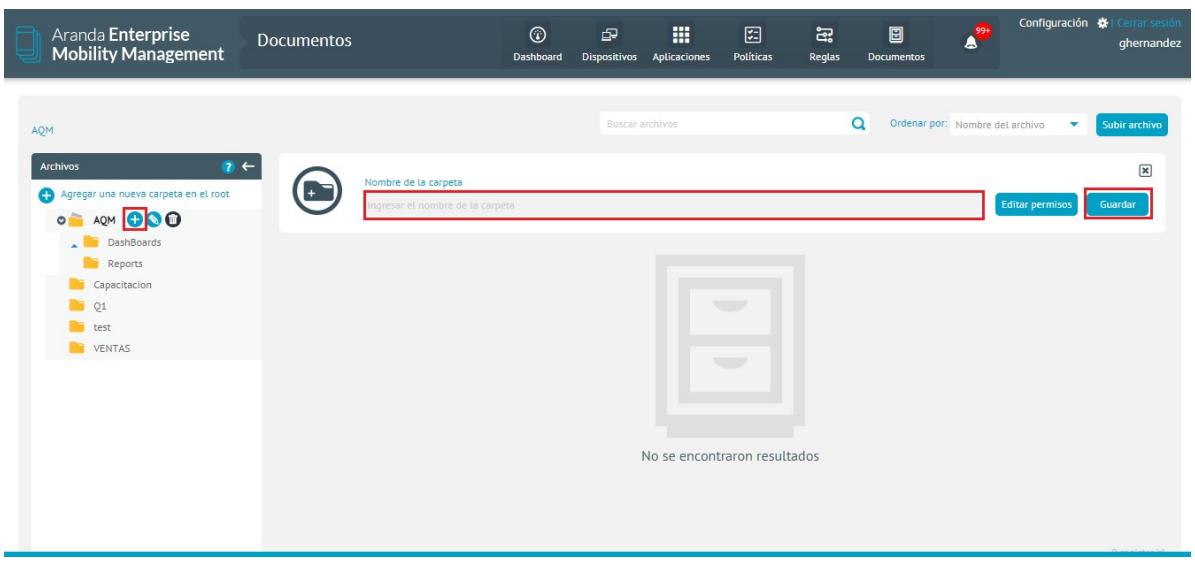
Carpetas

Administración de contenidos Creación de carpetas y Sub-carpetas

Para realizar la creación de una carpeta se dé clic en **Agregar una nueva carpeta** en el root, luego observará una pantalla en donde debe ingresar el nombre de la carpeta y posteriormente debe dar clic en **Guardar**.

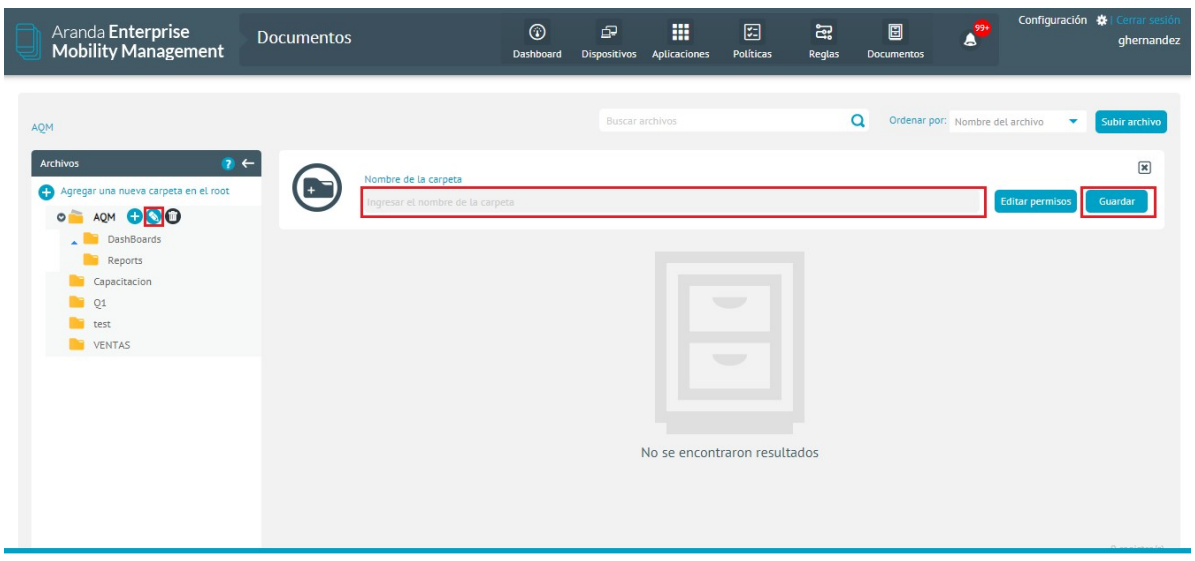


Para crear una sub- carpeta, diríjase hasta la carpeta contenedora y de clic en el icono **Agregar**, luego observará una pantalla en donde debe ingresar el nombre de la carpeta y posteriormente de clic en **Guardar.**

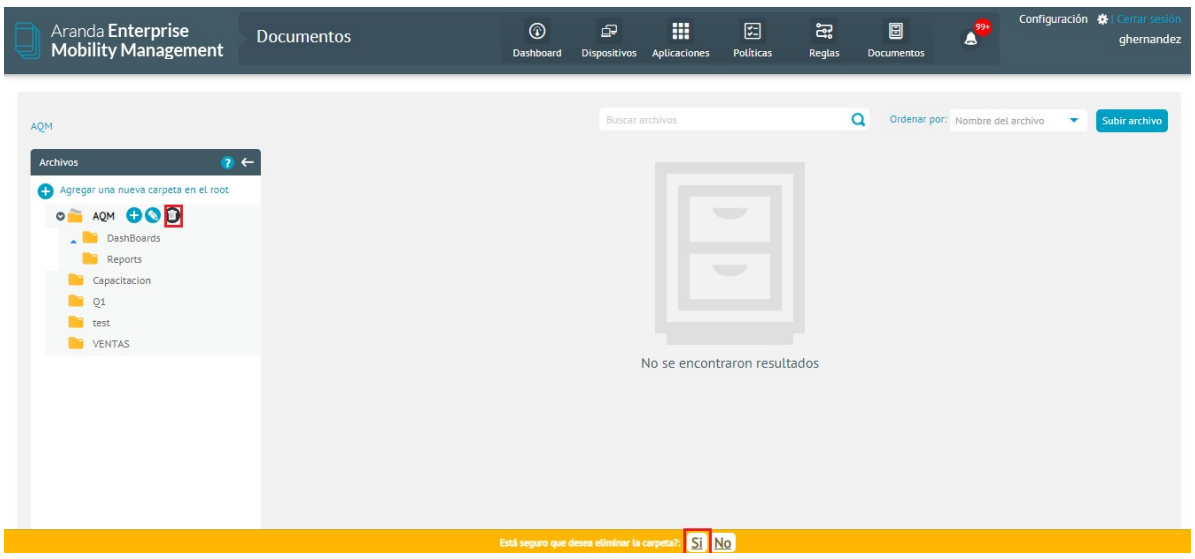


Edición y eliminación de carpetas

Para editar una carpeta de clic en el icono de **editar**, luego observará una pantalla en donde debe ingresar el nuevo nombre de la carpeta y posteriormente dar clic en **Guardar**.



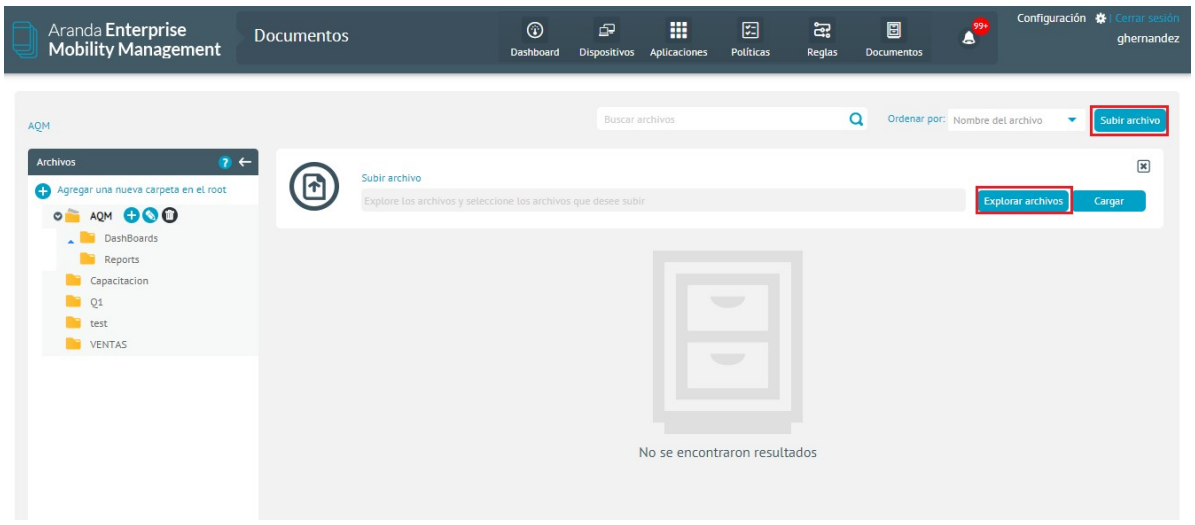
Para eliminar una carpeta de clic en el icono de **eliminar**, Luego aparecerá una ventana emergente en donde se solicita confirmar la eliminación, allí debe confirmar la eliminación de la carpeta que se eliminará siempre y cuando no contenga ni archivos ni sub-carpetas dentro de ella.



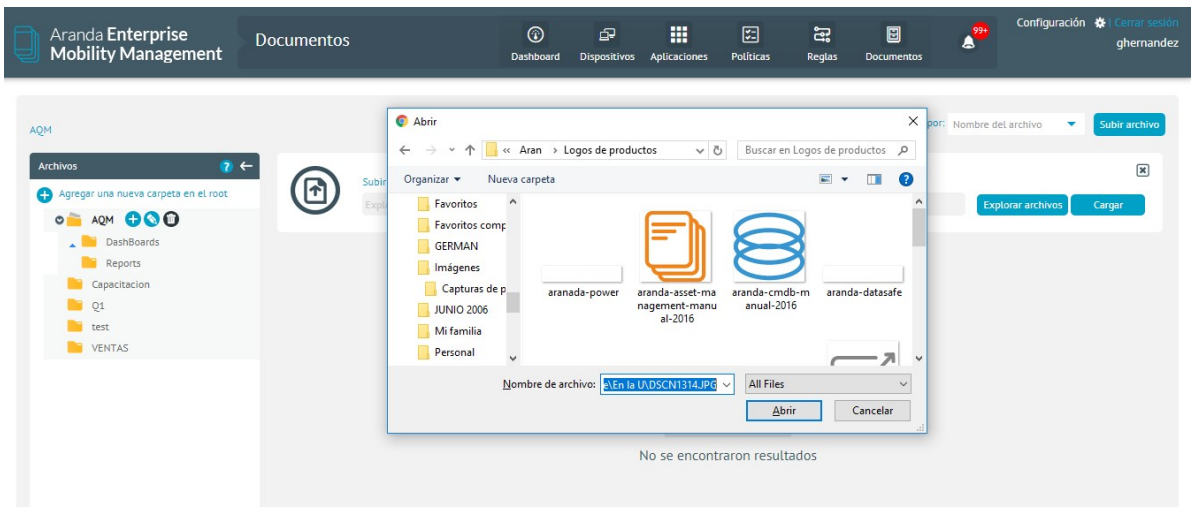
Archivos

Agregar Archivos

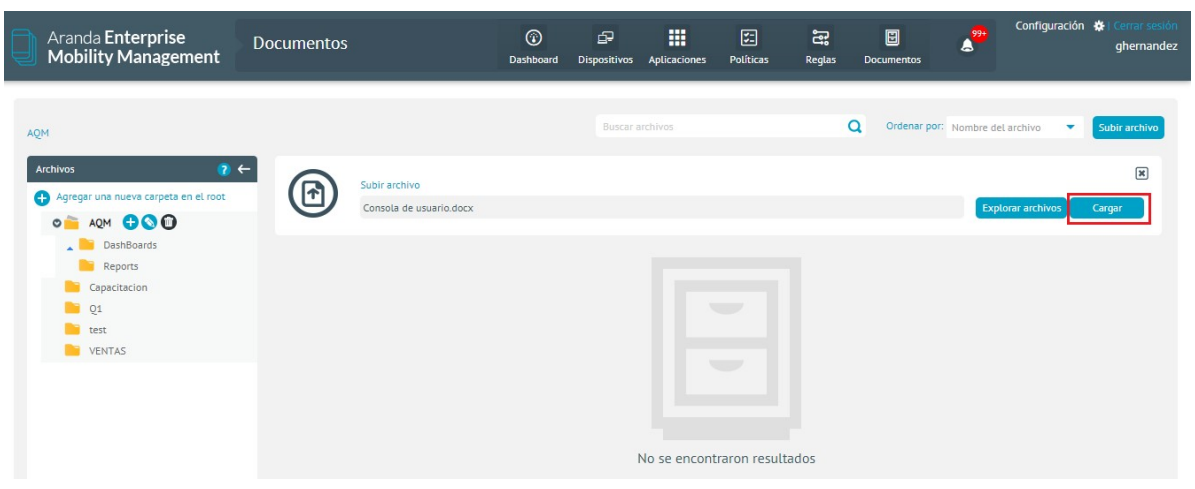
Para agregar archivos de clic en **subir archivo** y posteriormente en **Explorar archivos**.



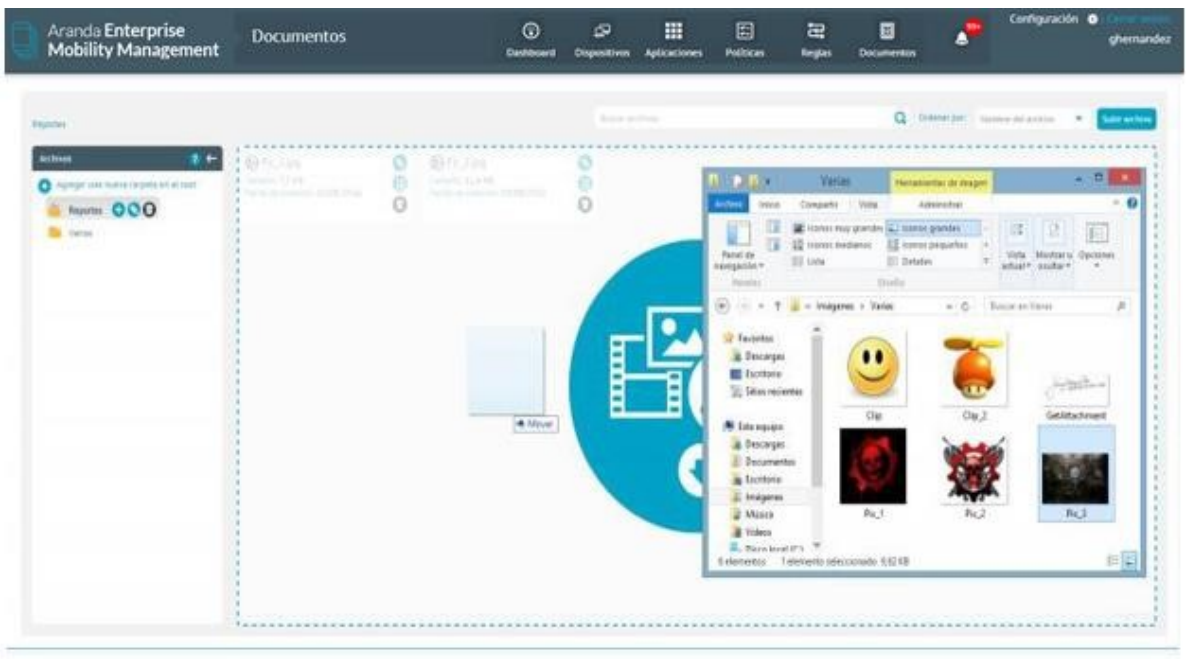
Se observa una ventana en la cual se debe buscar y seleccionar los archivos que desea subir, una vez seleccionados de clic en **Abrir**.



Visualizará la cantidad de archivos que se seleccionaron, y luego dar clic en cargar.

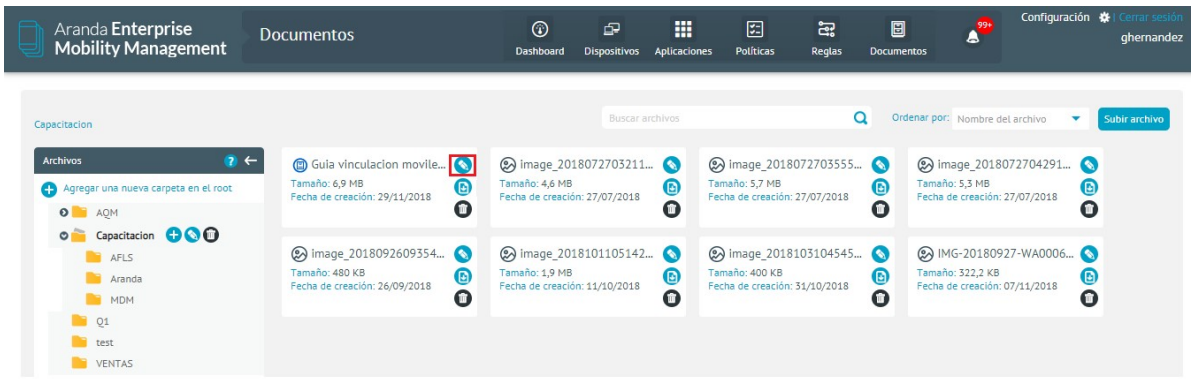


La subida de archivos a una carpeta especifica también se puede realizar por medio de drag and drop. En este caso se debe ubicar el archivo que desea subir y a través de un clic sostenido llevarlo hasta la carpeta en la cual se desea cargar.

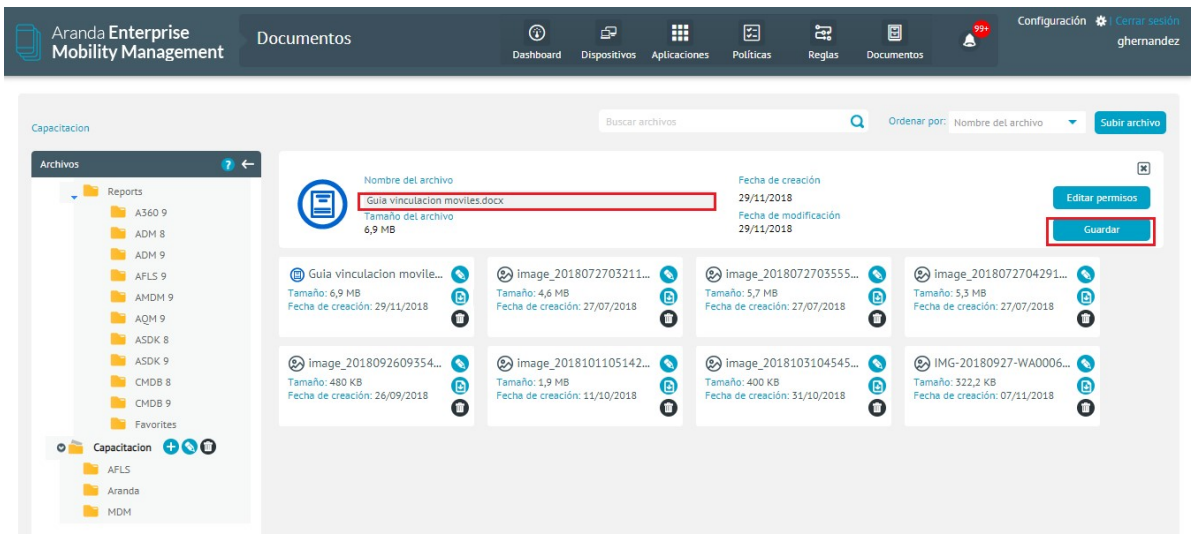


Editar, Descargar y Eliminar Archivos

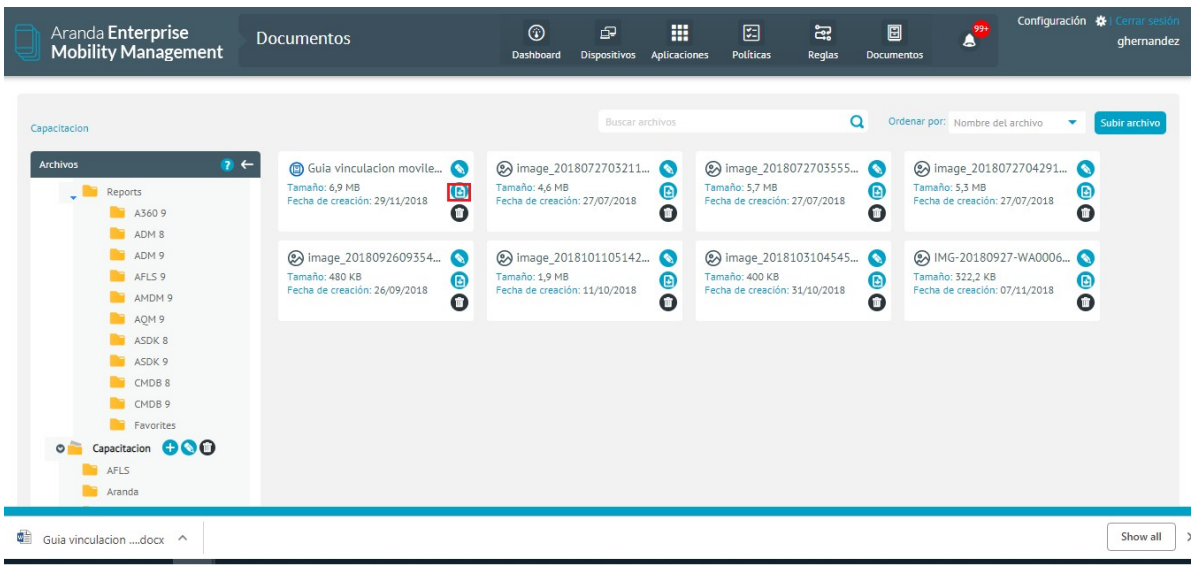
Para editar un archivo se debe seleccionar el icono **editar** en el archivo a modificar.



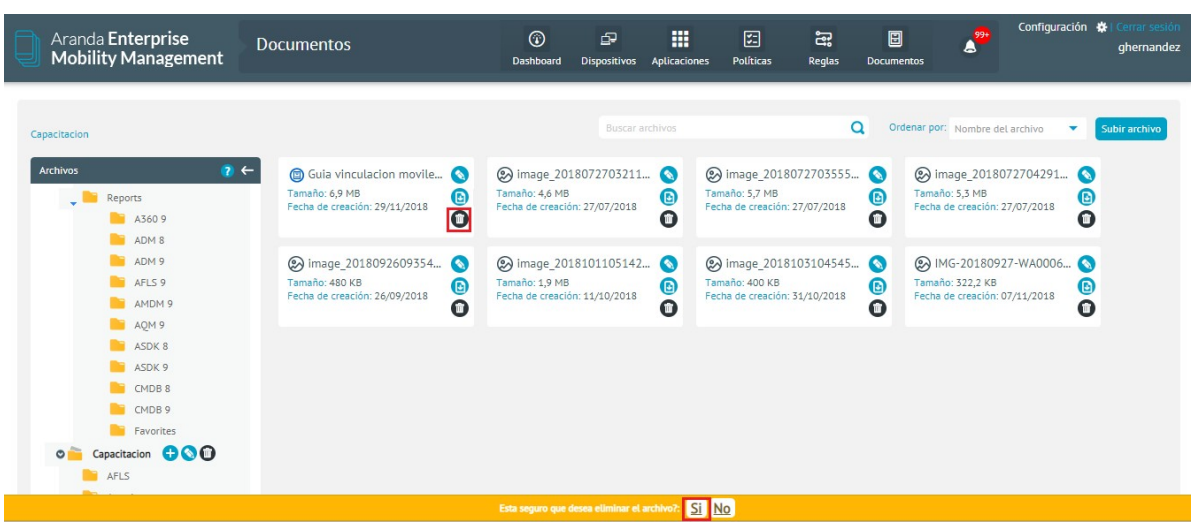
Ingrese el nuevo nombre del archivo y de clic en **Guardar**.



Para descargar un archivo seleccione el icono descargar sobre el archivo que desea visualizar.



Para eliminar un archivo de clic en el icono **eliminar**, Seguido de esto se muestra una ventana emergente en donde se solicita confirmar la eliminación, posterior a esto se debe confirmar la eliminación.



Administración de Roles y Permisos

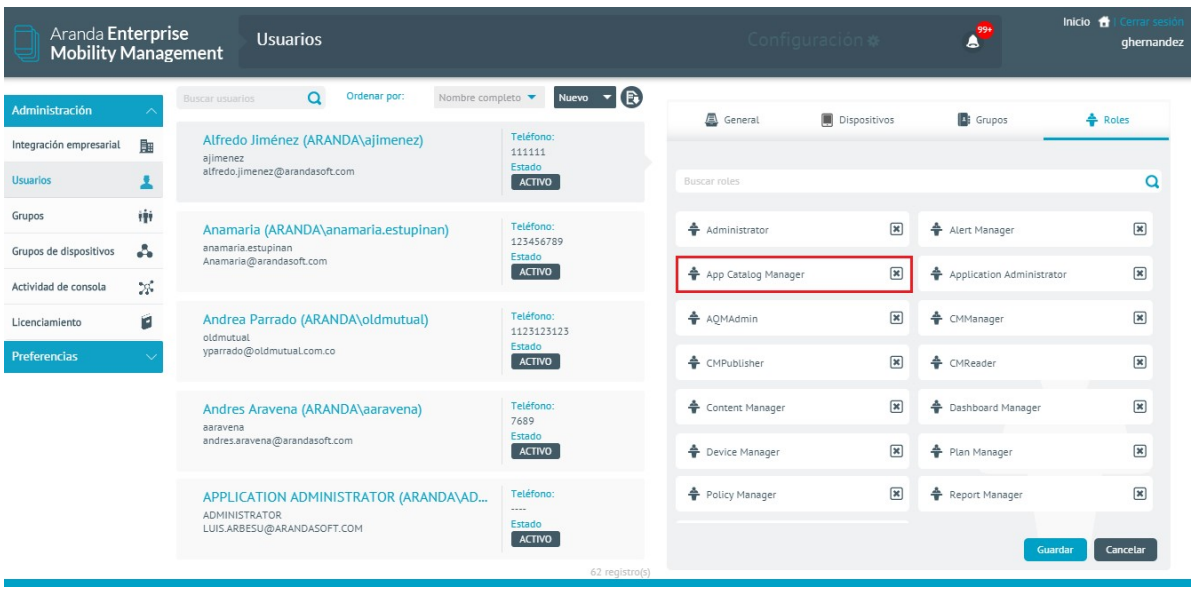
Roles

En la sección de documentos hay tres roles:

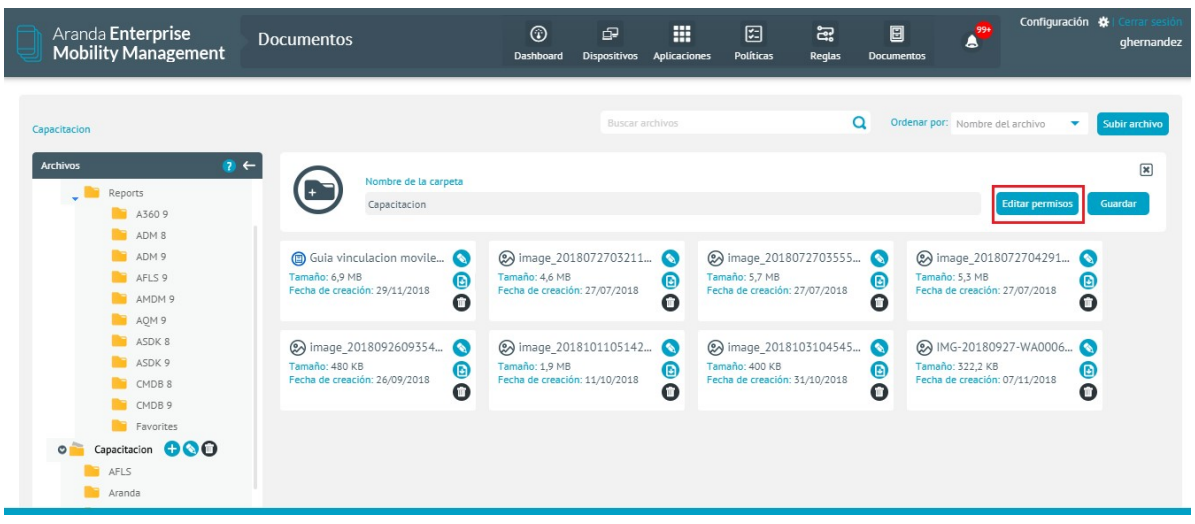
Roles	Descripción
CMReader:	Solo permite la lectura de contenido.
CMPublisher:	Permite lectura, edición y cargue de contenido, además de asignar permisos de Reader o Publisher sobre los contenidos a los que tenga acceso.
CMManager:	Permite lectura, edición, cargue y eliminación, además de la administración de permisos sobre los contenidos.

Se debe tener en cuenta que si se asignan roles sobre una carpeta específica dichos roles serán heredados por los archivos que se encuentren en ella mas no por las carpetas.

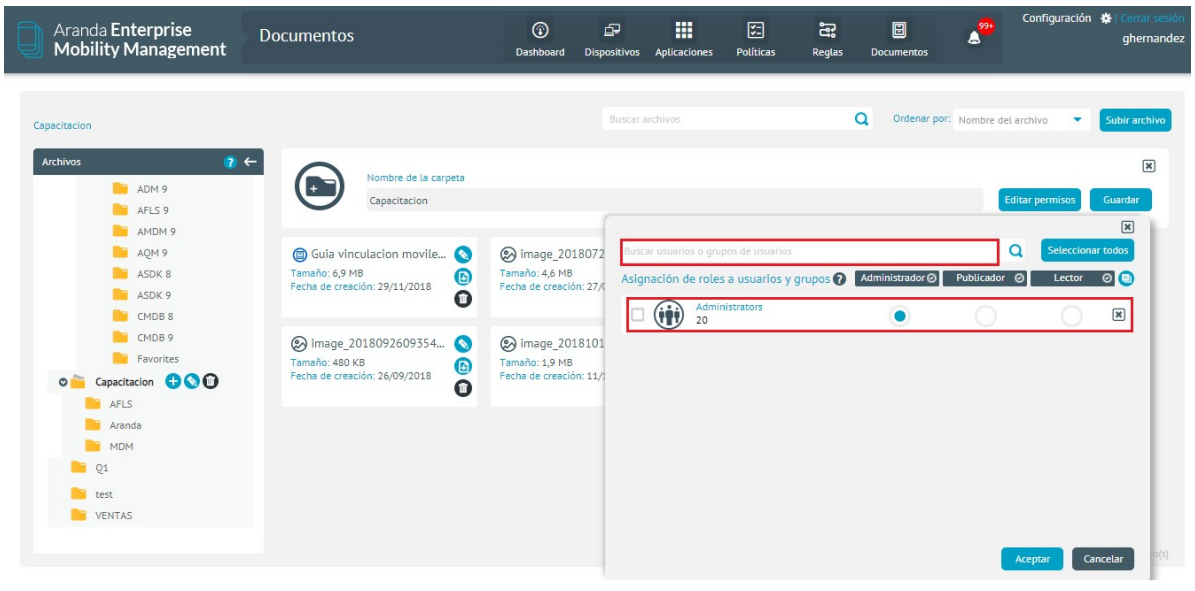
Permisos



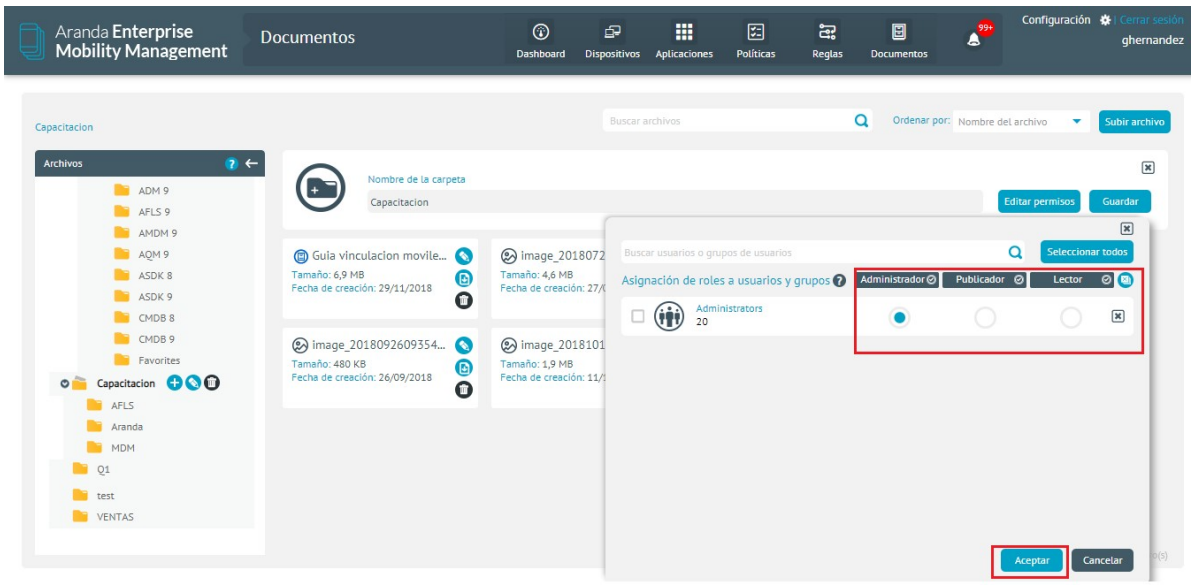
Para agregar un permiso sobre una carpeta especifica seleccione el icono **editar** y posteriormente de clic en **Editar permisos**.



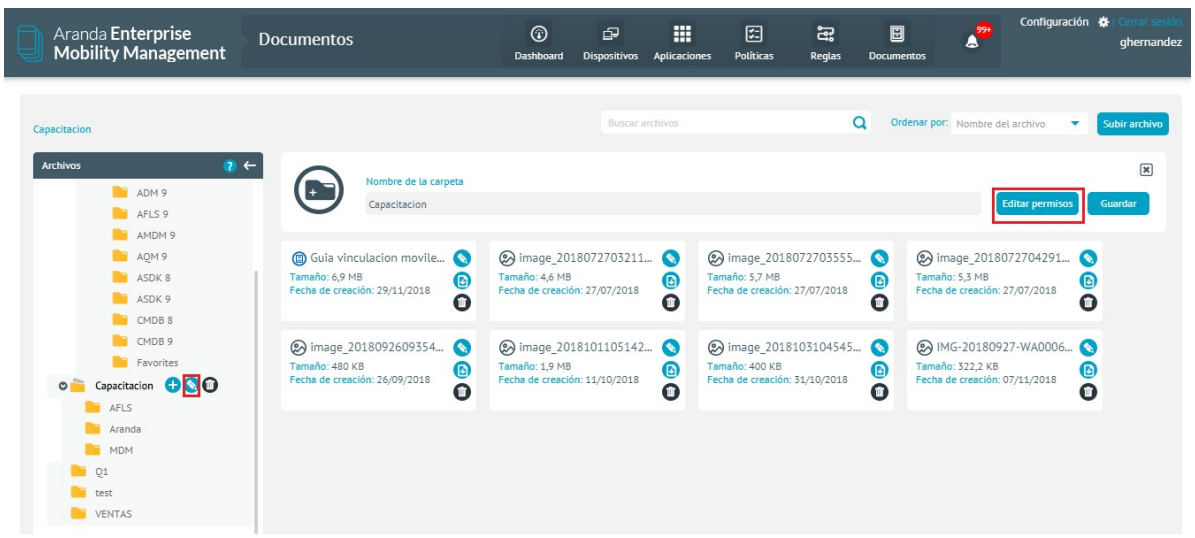
Realice la búsqueda del usuario y selecciónelo dentro de resultados según los criterios de búsqueda ingresados.



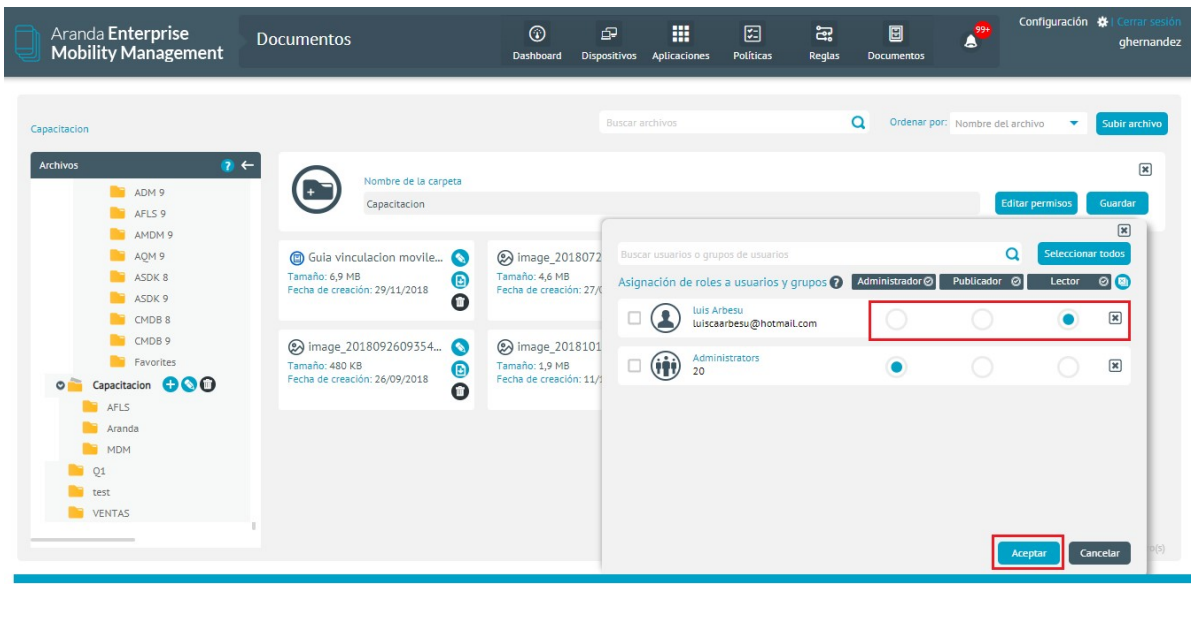
Seleccione el rol que se desea asignar al usuario, de clic en **Aceptar** y finalmente en **Guardar**.



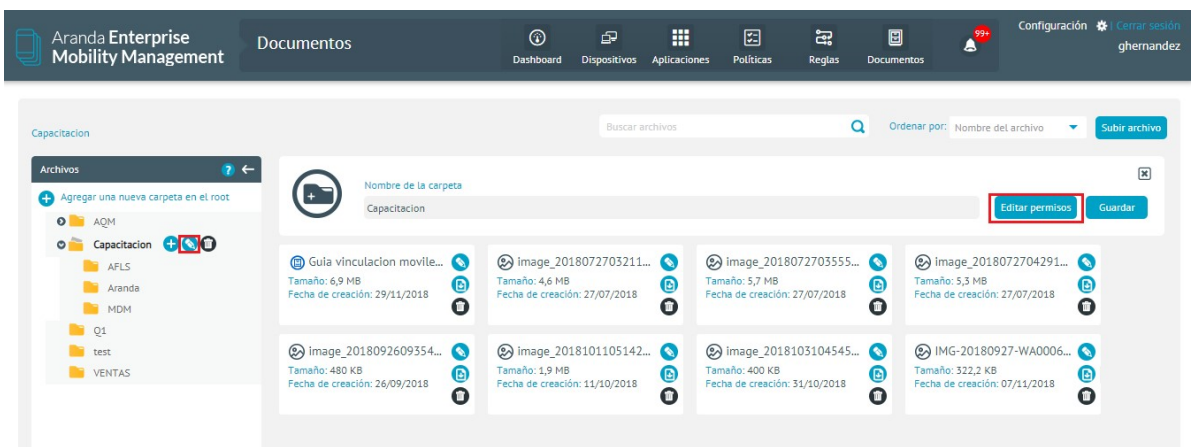
Para editar un permiso sobre una carpeta especifica seleccione el icono **editar** y posteriormente de clic en **Editar permisos**.



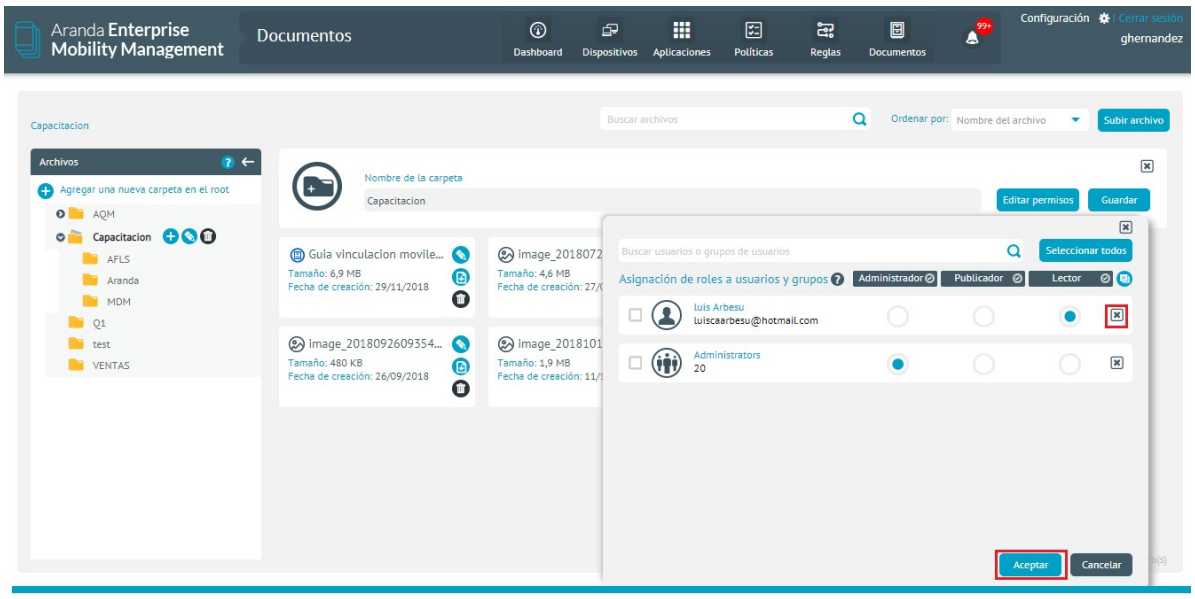
Seleccione el rol nuevo rol que se desea asignar al usuario, de clic en **Aceptar** y finalmente de clic en **Guardar**.



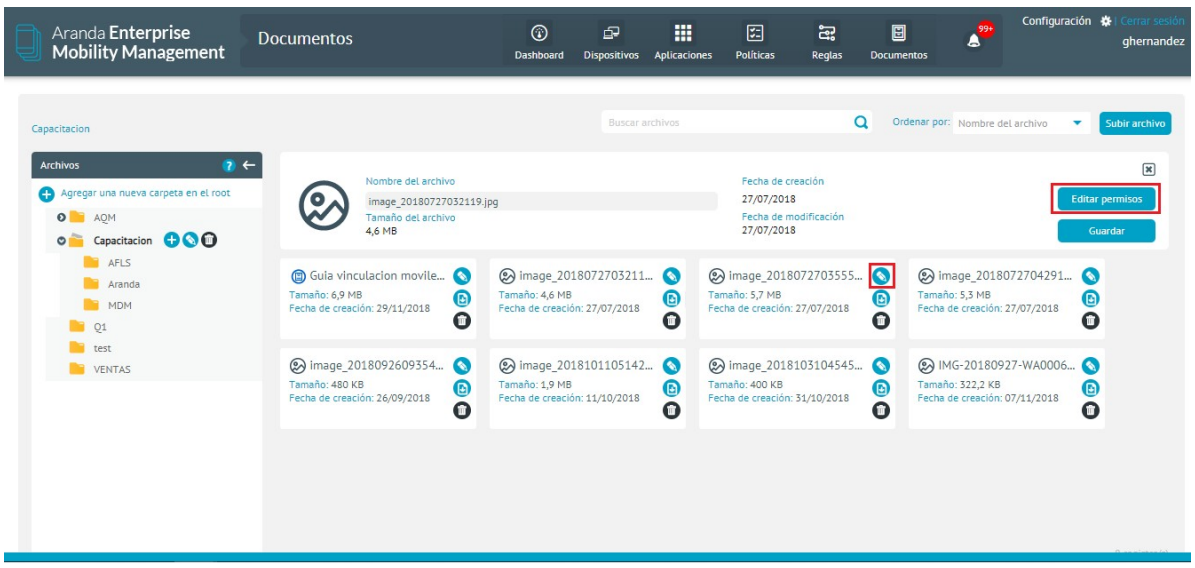
Para quitar un permiso sobre una carpeta especifica seleccione el icono **editar** y posteriormente de clic en **Editar permisos**.



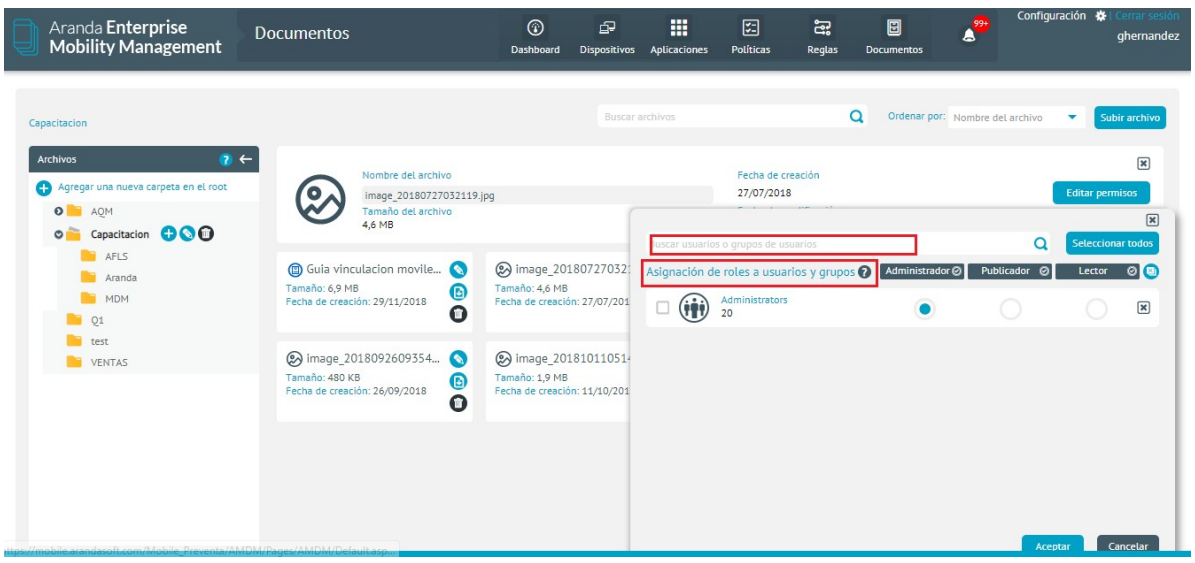
De clic en el icono **eliminar** al usuario que se desea retirar, luego de clic en **Aceptar** y finalmente en **Guardar**.



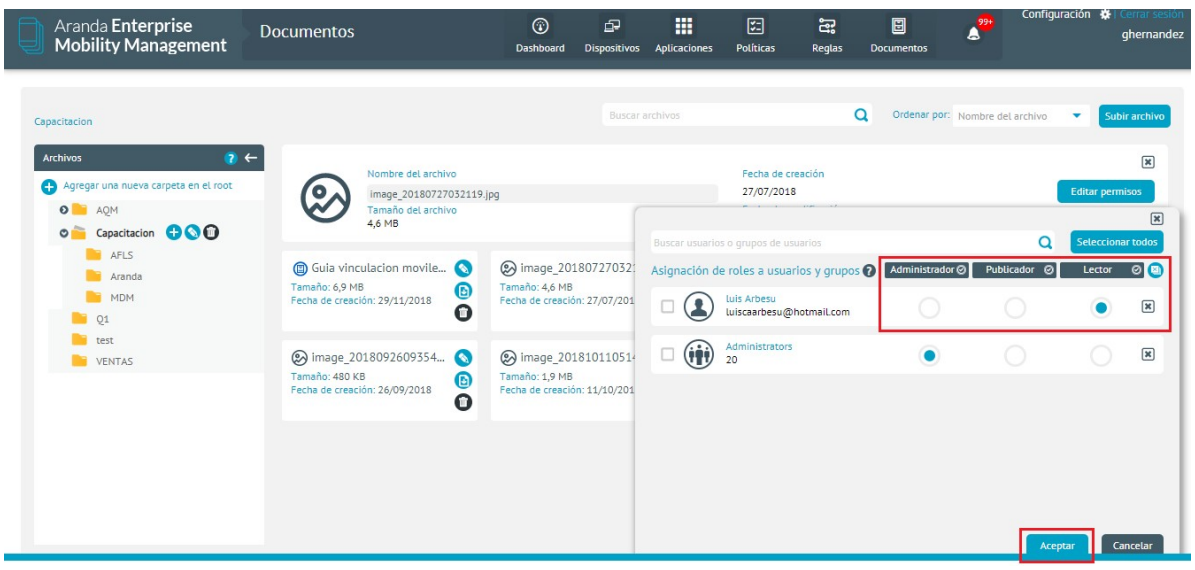
Para agregar un permiso sobre un archivo especifico debe seleccionar el icono **editar** y posteriormente hacer clic en Editar permisos.



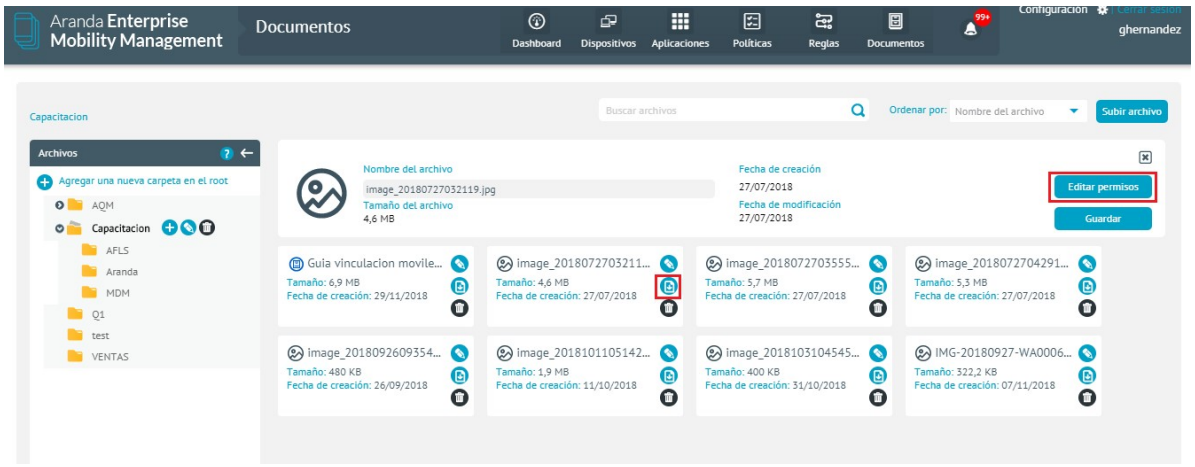
Realice la búsqueda del usuario y selecciónelo dentro de los resultados según los criterios de búsqueda ingresados.



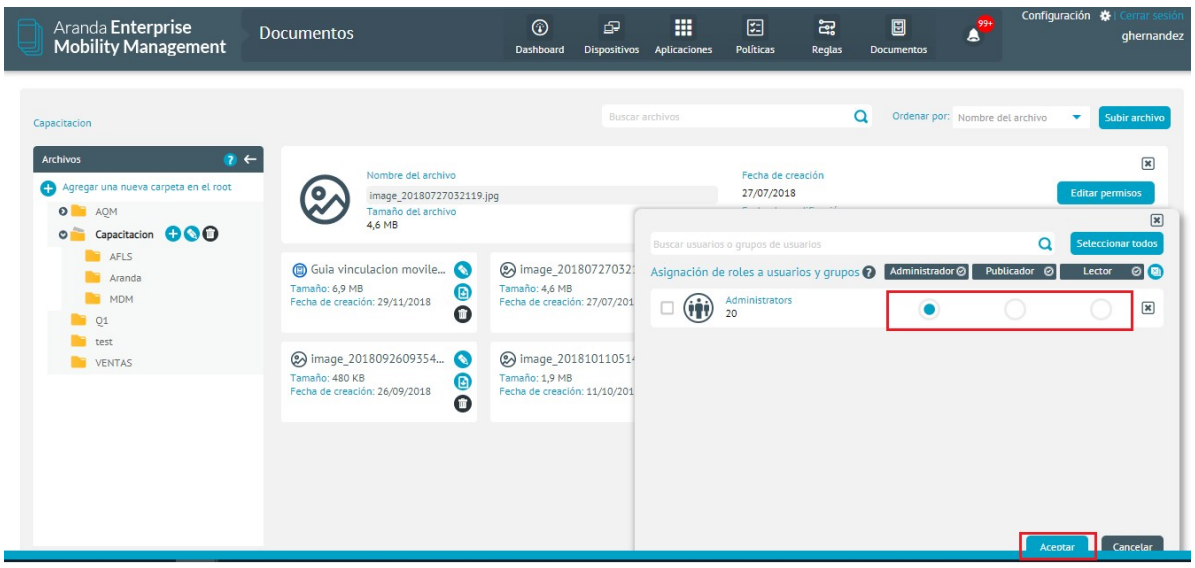
Seleccione el rol que se desea asignar al usuario, de clic en Aceptar y finalmente de clic en **Guardar**.



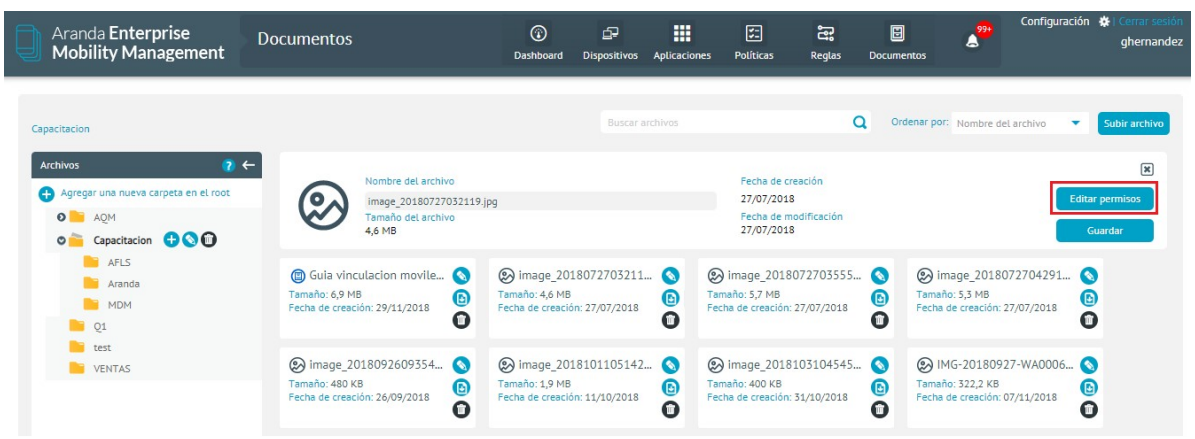
Para editar un permiso sobre un archivo especifico seleccione el icono **editar** y finalmente de clic en **Editar permisos**.



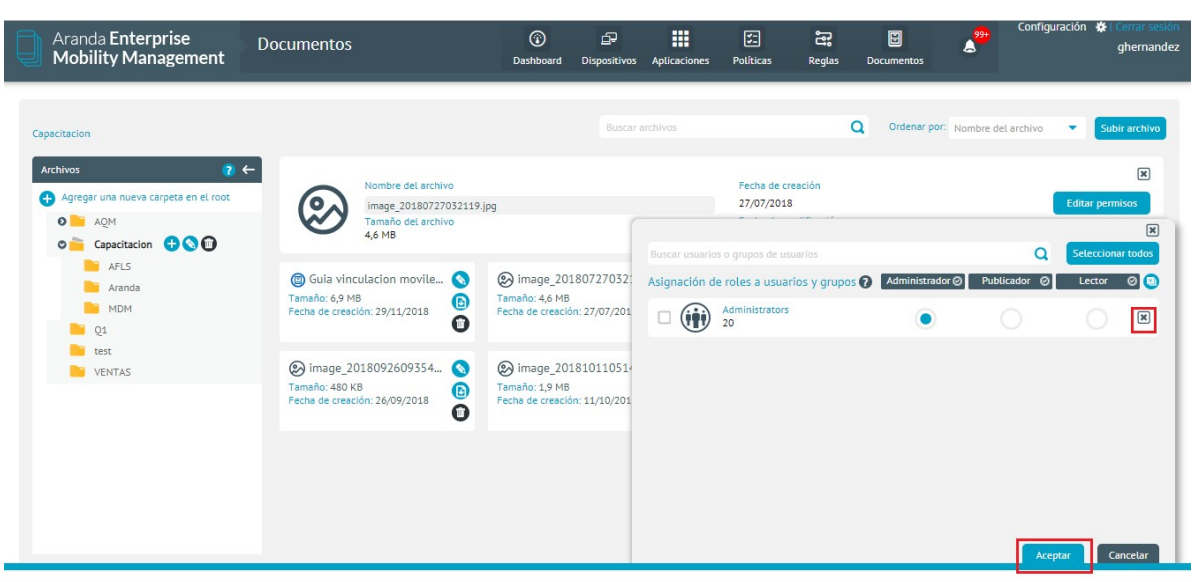
Seleccione el rol nuevo rol que se desea asignar al usuario, de clic en **Aceptar** y finalmente en **Guardar**.



Para quitar un permiso sobre un archivo especifico, seleccione el icono **editar** y posteriormente de clic en **Editar permisos**.



De clic en el icono eliminar en el usuario que se desea retirar, y luego de clic en **Aceptar** y finalmente en **Guardar**.

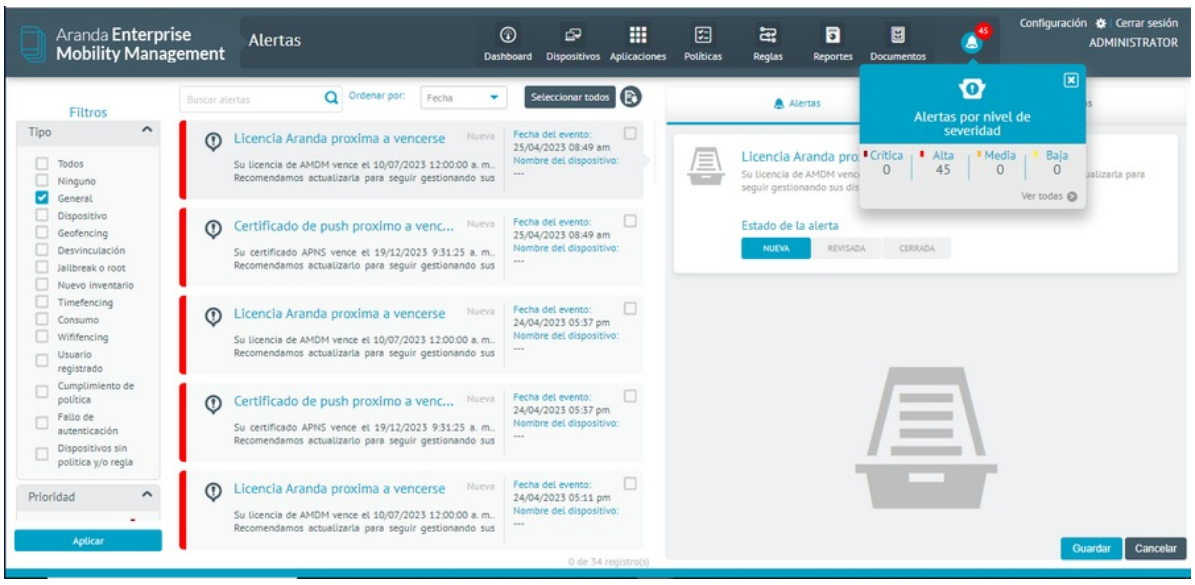


Alertas

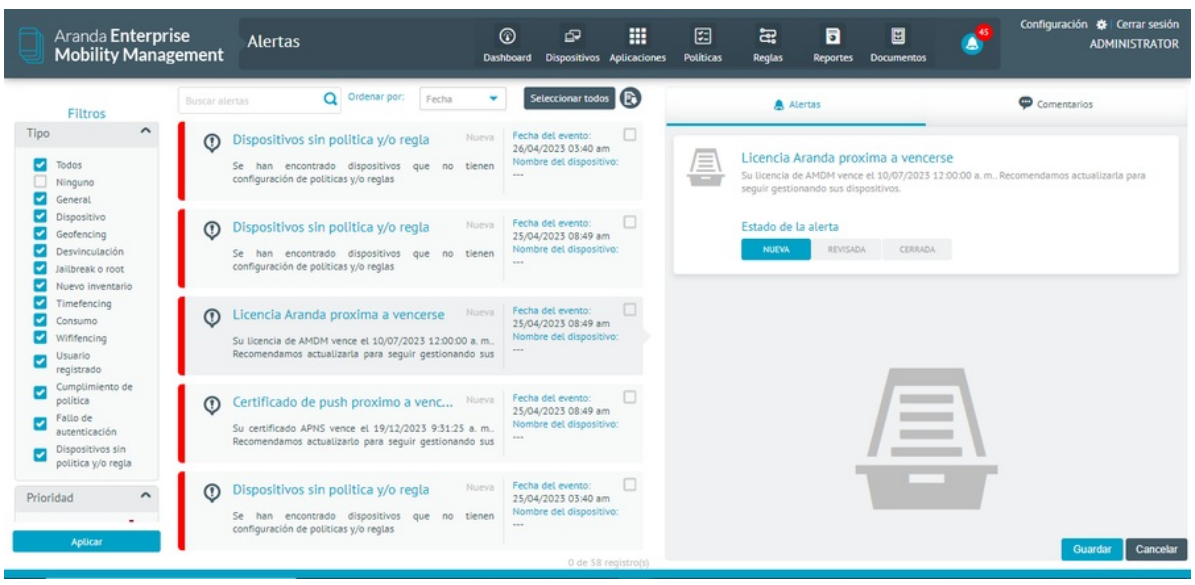
Módulo de Alertas

Las alertas son una lista de mensajes tipo notificación que se presentan en la consola. Listado y pre visualización. Para visualizar el resumen de las alertas en la consola, se debe poner el puntero de mouse sobre el icono de **alertas**

ubicado en la parte superior del menú.



Para visualizar las alertas de forma detallada, seleccione el ícono de alertas, o cualquiera de las opciones que presenta la vista emergente con el resumen de las alertas, de esta forma se puede ver el detalle de las alertas filtradas por su severidad o ver todas las alertas.



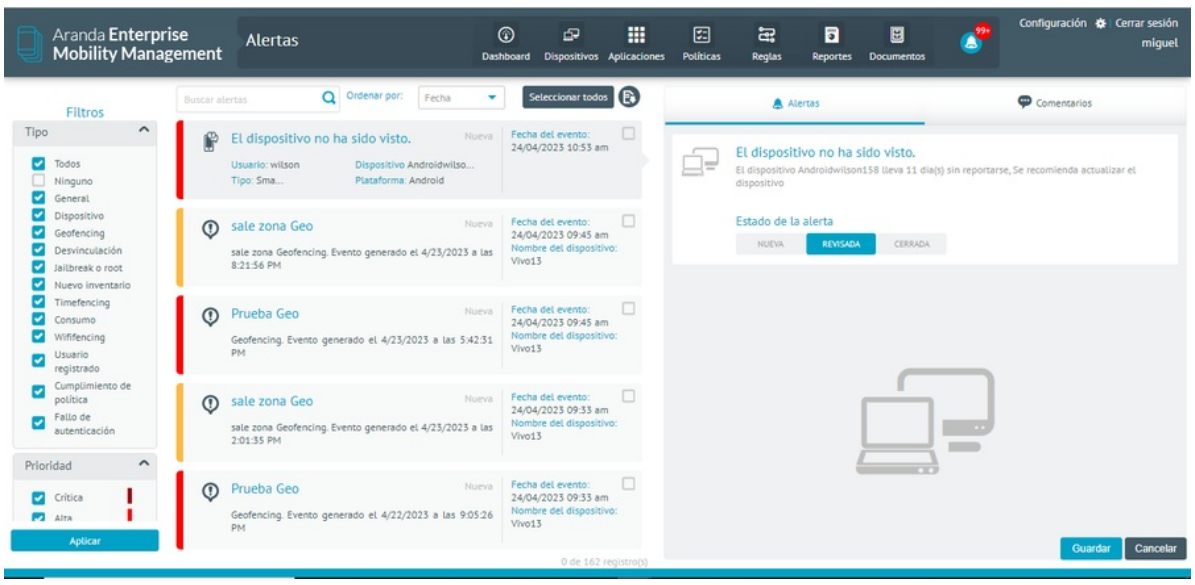
Generación y manejo de alertas

Las alertas son una de las acciones que se pueden definir para el cumplimiento de una regla, cuando se define un conjunto de reglas y esta(s) se cumple(n) el sistema dispara las acciones determinadas, en este caso generaría alertas que se visualizan en la consola.

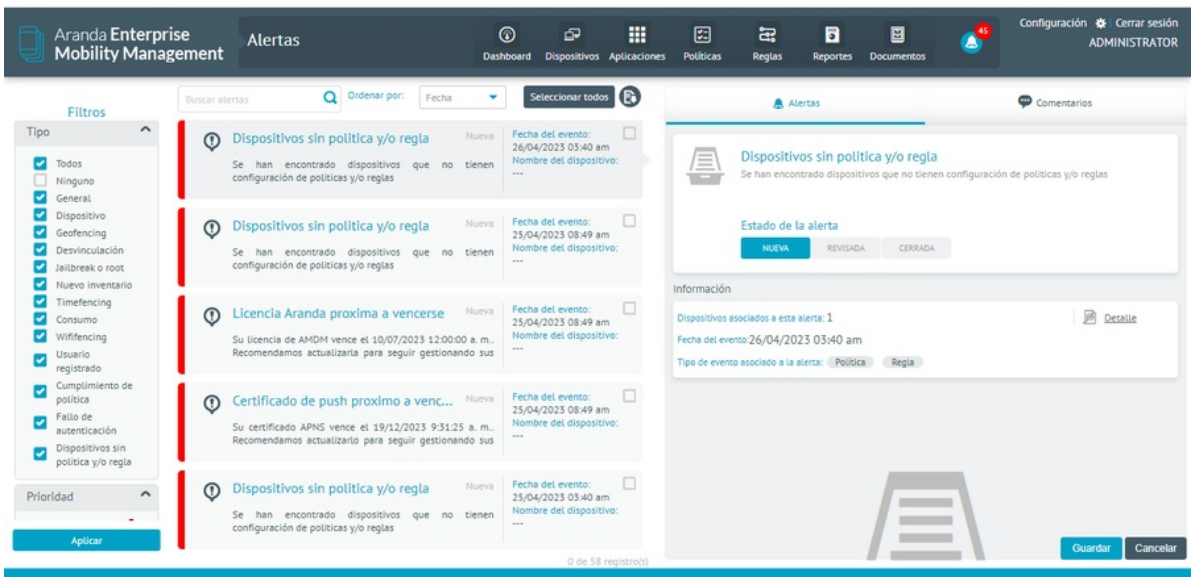
Al seleccionar una alerta de la lista, en el costado derecho se ve el detalle de esta con opciones para edición. Se manejan tipos de estado para la alerta:

- Nueva
- Revisada
- Cerrada

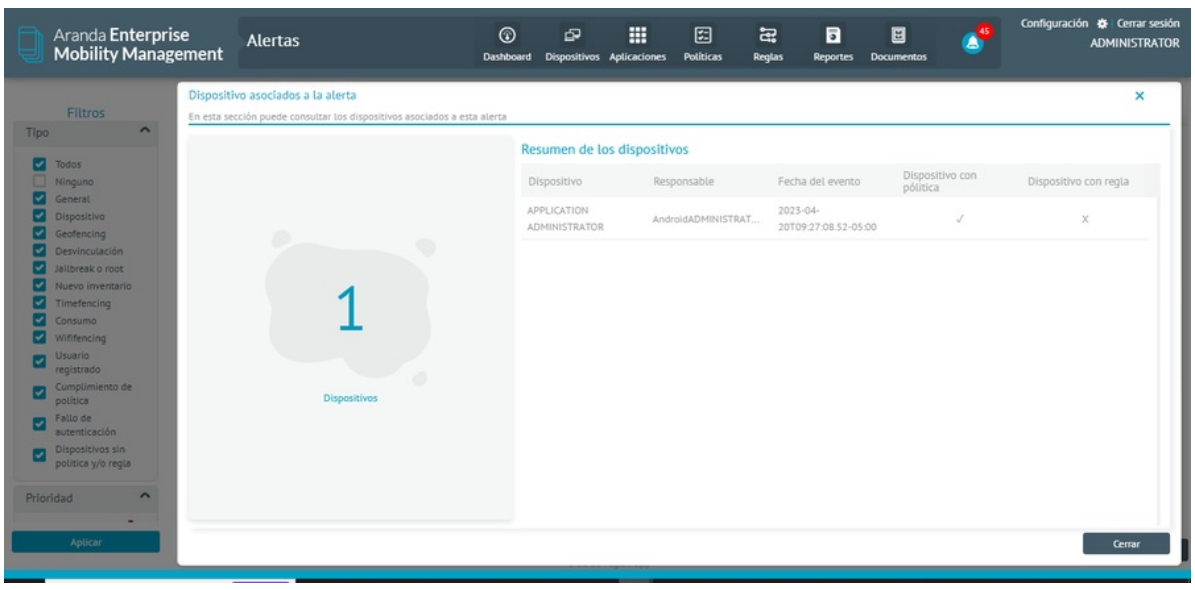
Además, se puede ver el detalle del dispositivo asociado a la alerta y agregar comentarios a esta.



Existen alertas que cuentan con información adicional, la cual puede ser consultada a través del detalle de la alerta. Dicha información se vera reflejada en un panel con el título de **información**.



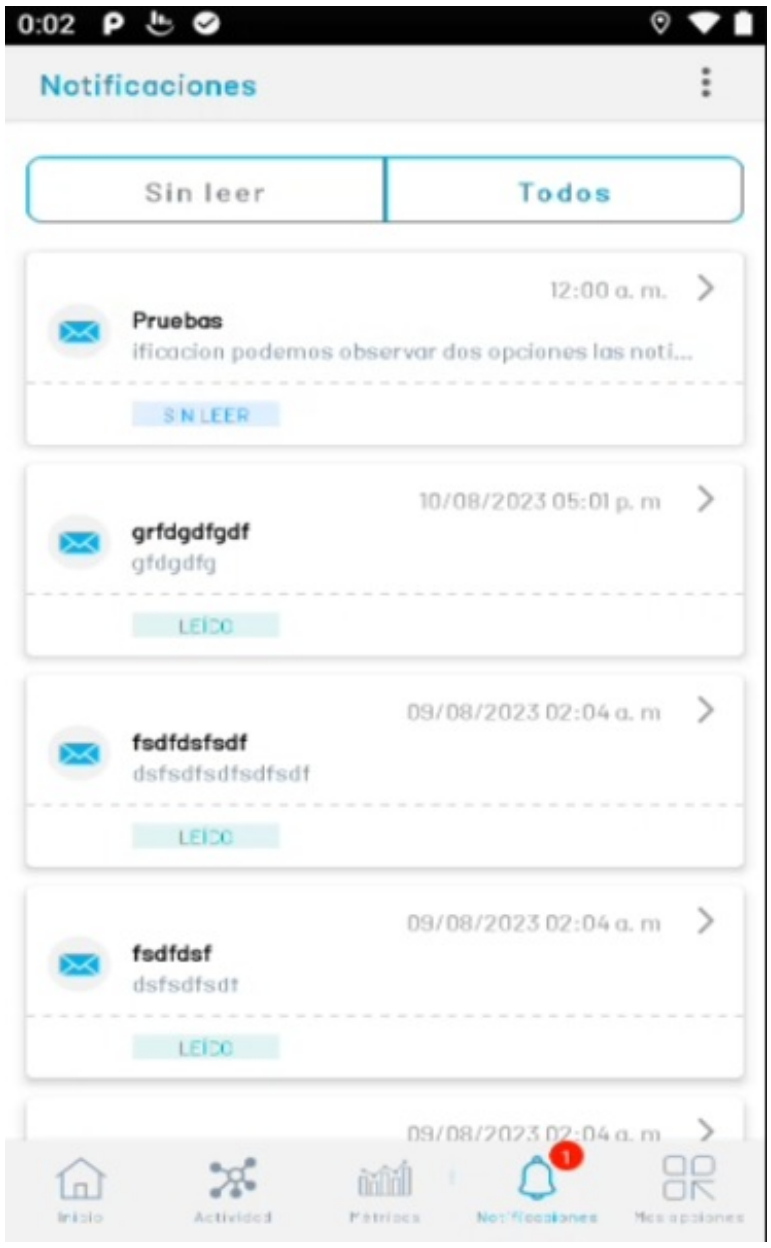
Al presionar el botón **detalle**, se desglosará mas información sobre la alerta generada.



Notificaciones en Dispositivos Móviles

Las notificaciones se generan por medio de eventos o acciones realizadas por la persona encargada del monitoreo del dispositivo. En el Agente (consola móvil AEMM) podrá acceder a estas notificaciones.

En la vista de notificación del Agente de AEMM podrá visualizar las notificaciones pendientes. Al ingresar a cada registro podrá identificar el título y contenido del mensaje y la hora en la que se envío.



contentmanagement

Aplicación Móvil Content Management

Aranda EMM Content Management provee una forma intuitiva de acceder y ver documentos almacenados por medio de la sección de documentos directamente desde el Content Management en dispositivos Móviles.

Ayuda a proteger su contenido sensible en un contenedor corporativo. Permite que usuarios con dispositivos móviles accedan de forma fácil y segura a los documentos requeridos para su trabajo, ellos pueden compartir de manera sencilla y segura contenido con sus compañeros de trabajo reduciendo el riesgo de comprometer información corporativa.

Content Management para Android

Ingreso a la aplicación

Se puede ingresar el servidor de conexión a través de un código QR el cual se escanea de la consola web o se puede ingresar manualmente la dirección web del servidor.

Si selecciona la opción ingresar servidor se muestra el campo para digitarlo, si ha ingresado anteriormente al servidor en la parte superior al campo se muestran los servidores a los que ha ingresado con anterioridad para que no sea necesario ingresarlos nuevamente.

Posteriormente se debe ingresar el usuario y la contraseña de inicio de sesión (Aranda para un usuario local o si tiene integrada la consola a un dominio puede seleccionarlo e ingresar con un usuario y contraseña de red)

Luego acepte los términos y condiciones y presione en **continuar**.

Se muestra a nivel información de la aplicación, pulse **saltar**.

Visualización general

Ingrese al menú en los tres puntos de la barra de opciones ubicados en la parte superior derecha, allí observará los archivos en dos formas de visualización.

En modo lista

Visualización de grilla.

Realizando Swipe hacia la izquierda sobre un archivo, visualizará las opciones: Información, renombrar, Eliminar y Marcar como favorito (Descargar archivo para consultarlo sin conexión).

Información del archivo, para salir pulse fuera del cuadro de información.

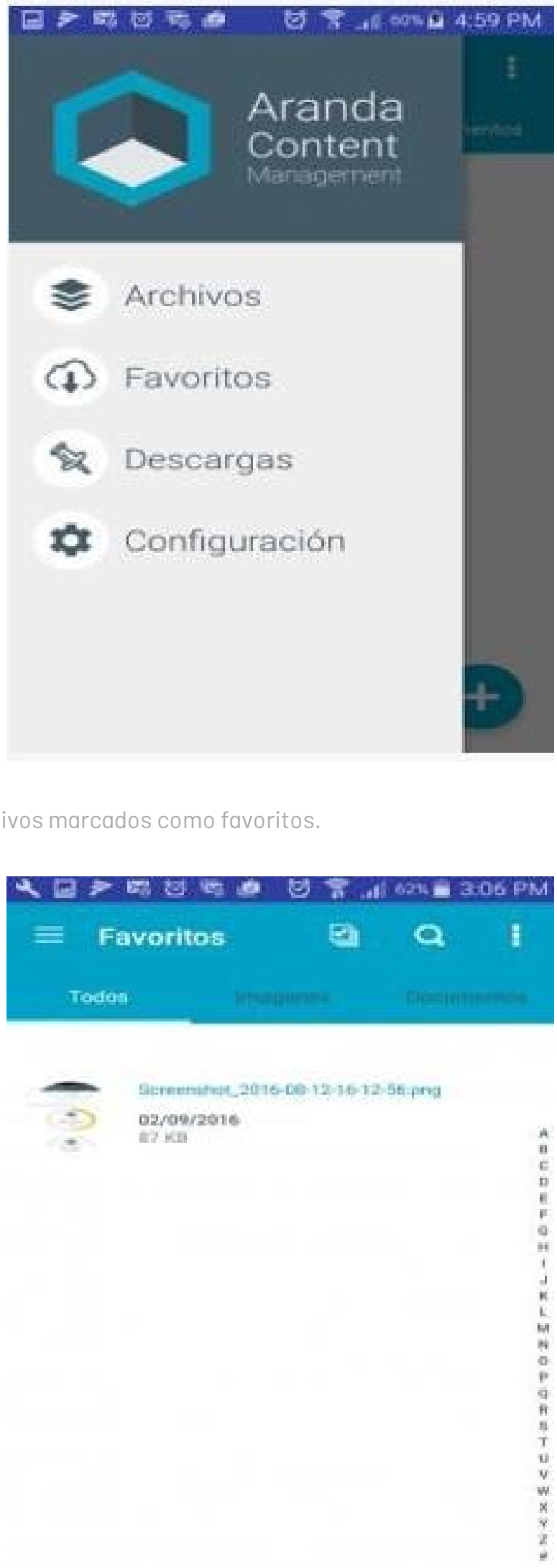
Para renombrar el archivo ingrese el nuevo nombre y presione en **guardar**.

Para borrar el archivo presione en **Aceptar.**

En vista de grilla puede acceder a las opciones de los archivos pulsando sobre los puntos ubicados en la parte inferior del archivo.

Menú de vistas

Cuenta con las vistas de Archivos (Visualización de todos los archivos y carpetas), Favoritos, Descargas, Configuración. Se puede ingresar a este menú realizando un Swipe al hacia la derecha o pulsando el icono de tres líneas en la parte superior izquierda.



Favoritos, Visualización de archivos marcados como favoritos.

Descargas, Visualización de descargas realizadas.

Configuración, Se puede seleccionar si desea la visualización de archivos conectado a los datos móviles o solo cuando se encuentra conectado a una red Wifi.

Desplace el selector según la configuración deseada.

Subir archivos

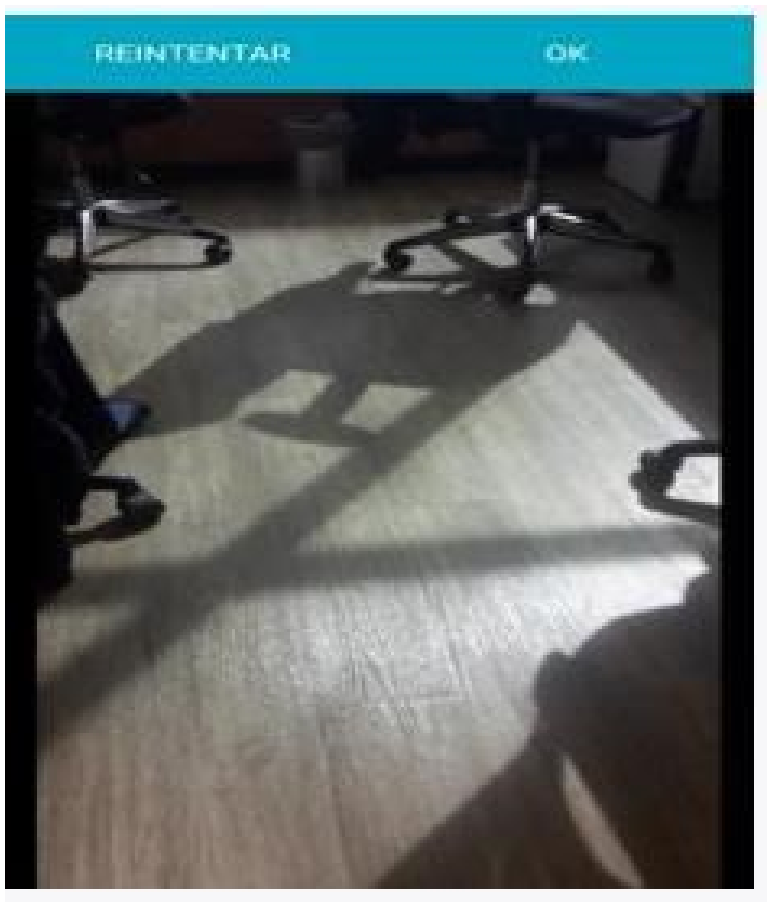
Para subir un archivo pulse en el icono “+”

Posteriormente seleccione el tipo de archivo que desea subir.

Para subir una imagen debe seleccionar el origen

Al seleccionar la imagen se muestra un mensaje informando el inicio y final del cargue.

Para subir foto y/o vídeo debe realizar la captura y pulsar en **Ok** (según el móvil se puede tardar uno o dos segundos mientras carga la imagen).



Para subir un audio debe pulsar en el icono de micrófono para iniciar la grabación

Posteriormente debe pulsar en el icono stop para finalizarla.

Se visualiza un control para reproducir el audio, adelantarlo, atrasarlo, subirlo (Icono de nube) o descartarlo (Icono de caneca).

Controles de la barra de opciones

Puede realizar búsquedas de archivos pulsando el icono de lupa en la barra de opciones de la aplicación y posteriormente ingresando el criterio de búsqueda.

Con base en el criterio ingresado se visualizarán los archivos existentes en todas las carpetas.

Puede realizar una selección múltiple de archivos para eliminar o descargar en forma masiva con los controles habilitados en la barra de opciones.

Filtros

Puede refinar la visualización de archivos por medio de las opciones de las pestañas ubicadas debajo de la barra de opciones, pulsando imágenes.

Pulsando documentos se visualizan los archivos en formato Word, Excel, PowerPoint y Pdf.

Content Management para iOS

Ingreso a la Aplicación

Para iniciar, se puede ingresar el servidor de conexión a través de un código QR el cual se escanea de la consola web o se puede ingresar manualmente la dirección del servidor.

Si selecciona la opción ingresar servidor se muestra el campo para digitarlo, si ha ingresado anteriormente al servidor en la parte superior al campo se muestran los servidores a los que ha ingresado con anterioridad para que no sea necesario ingresarlos nuevamente.

Posteriormente se debe ingresar el usuario y la contraseña de inicio de sesión (Aranda para un usuario local o si tiene integrada la consola a un dominio puede seleccionarlo e ingresar con un usuario y contraseña de red).

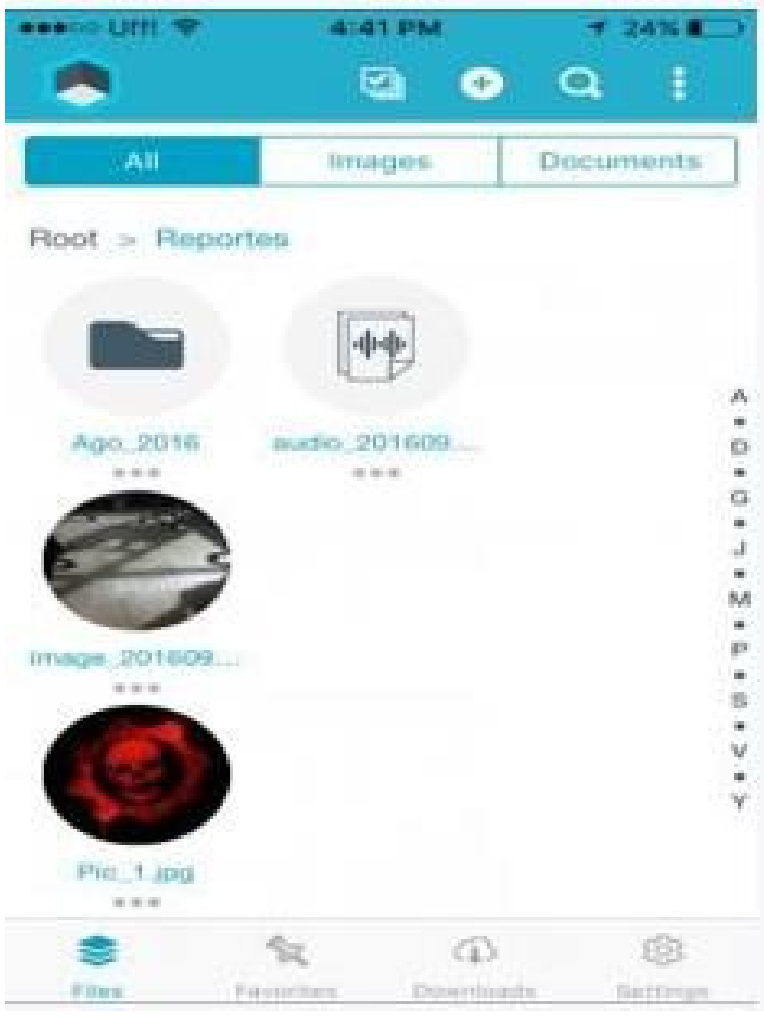
Luego acepte los términos y condiciones y pulse en **continuar**.

Se muestra a nivel información de la aplicación, pulse en saltar.

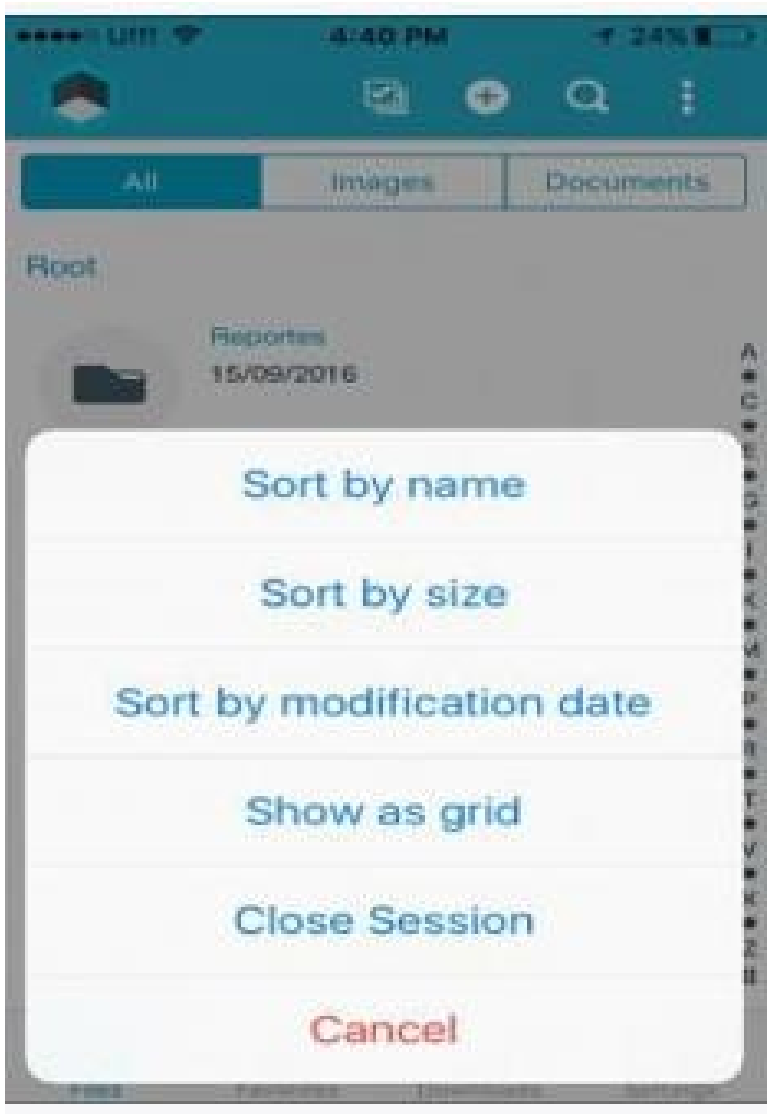
Visualización general

Puede visualizar los archivos en dos formas de visualización, en modo lista.

O en visualización de grilla.



Seleccione las visualizaciones ingresando al menú con los tres puntos de la barra de opciones en la parte superior derecha.

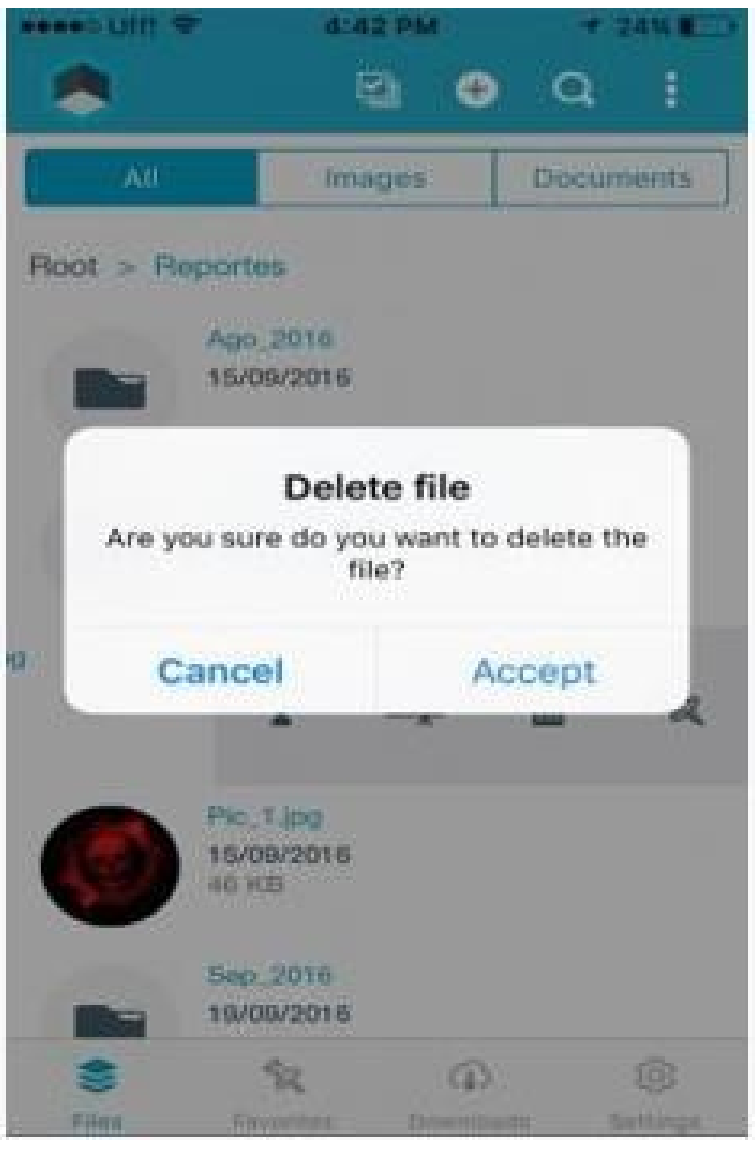


Realizando Swipe hacia la izquierda sobre un archivo visualice las opciones Información, renombrar, Eliminar y Marcar como favorito (Descargar archivo para consultarlo sin conexión).

Información del archivo, para salir puede pulsar fuera del cuadro de información.

Para renombrar archivo ingrese el nuevo nombre y pulse **guardar**.

Para borrar el archivo pulse **aceptar**.



Para marcar un archivo como favorito debe pulsar en el icono de pin y se mostrara un mensaje indicando el proceso de inicio y fin de descarga de dicho archivo.

En vista de grilla puede acceder a las opciones de los archivos pulsando sobre los puntos ubicados en la parte inferior del archivo.

Menú de vistas

Cuenta con las vistas Archivos (Visualización de todos los archivos y carpetas), Favoritos, Descargas, Configuración. Este menú se encuentra visible en la barra de opciones ubicada en la parte inferior de la pantalla.

Favoritos, Visualización de archivos marcados como favoritos.

Descargas, Visualización de descargas realizadas.

Configuración

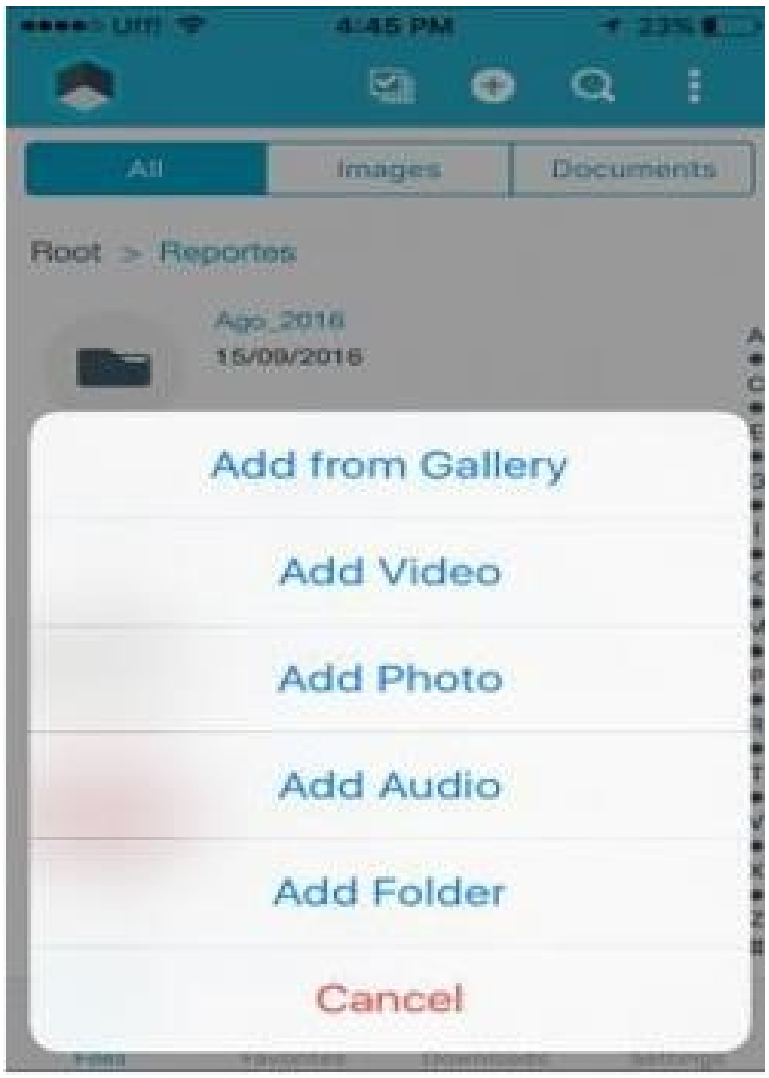
Es posbile seleccionar si se desea la visualización de archivos con datos móviles o solo cuando se encuentra conectado a una red Wifi.

Desplazar el selector según la configuración deseada.

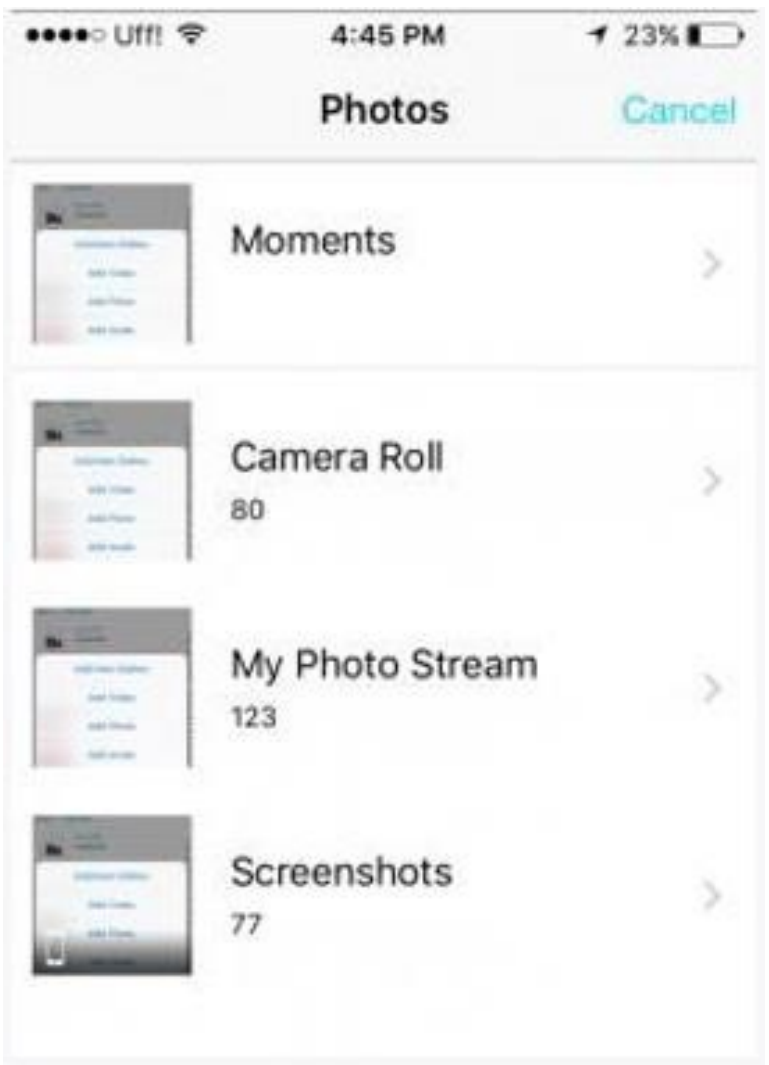
Subir archivos

Para subir un archivo debe pulsar en el icono "+" ubicado en la barra de opciones.

Posteriormente seleccione el tipo de archivo que desea subir.



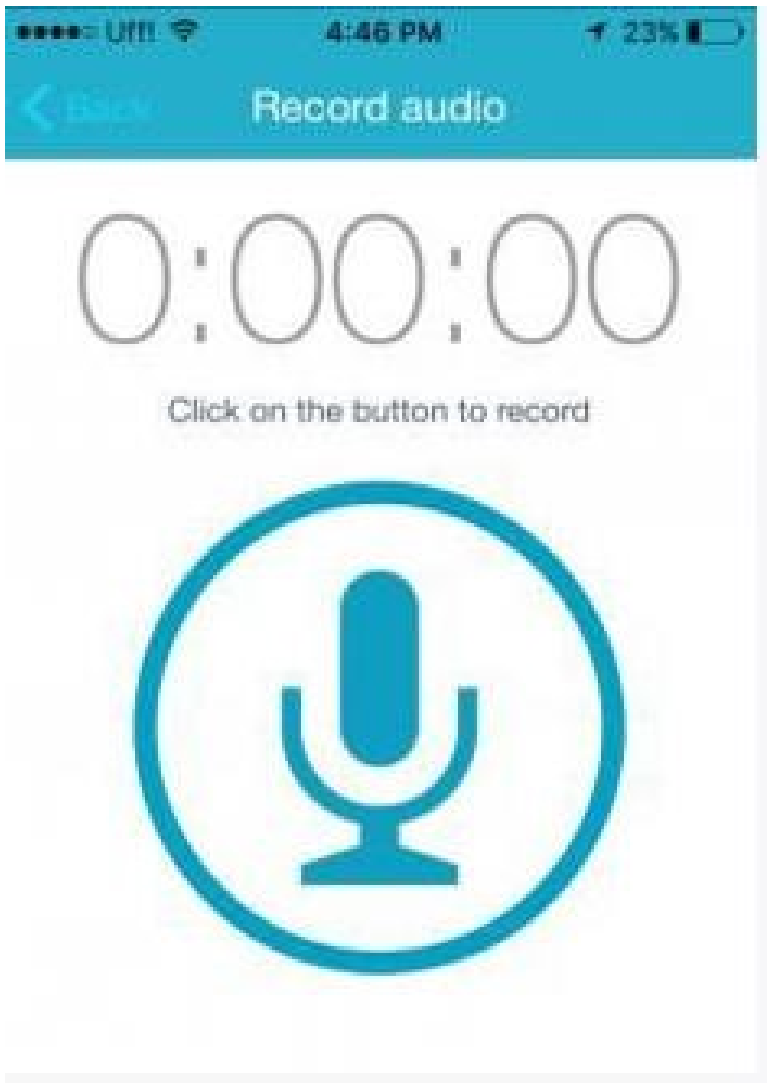
Para subir una imagen debe seleccionar el origen.



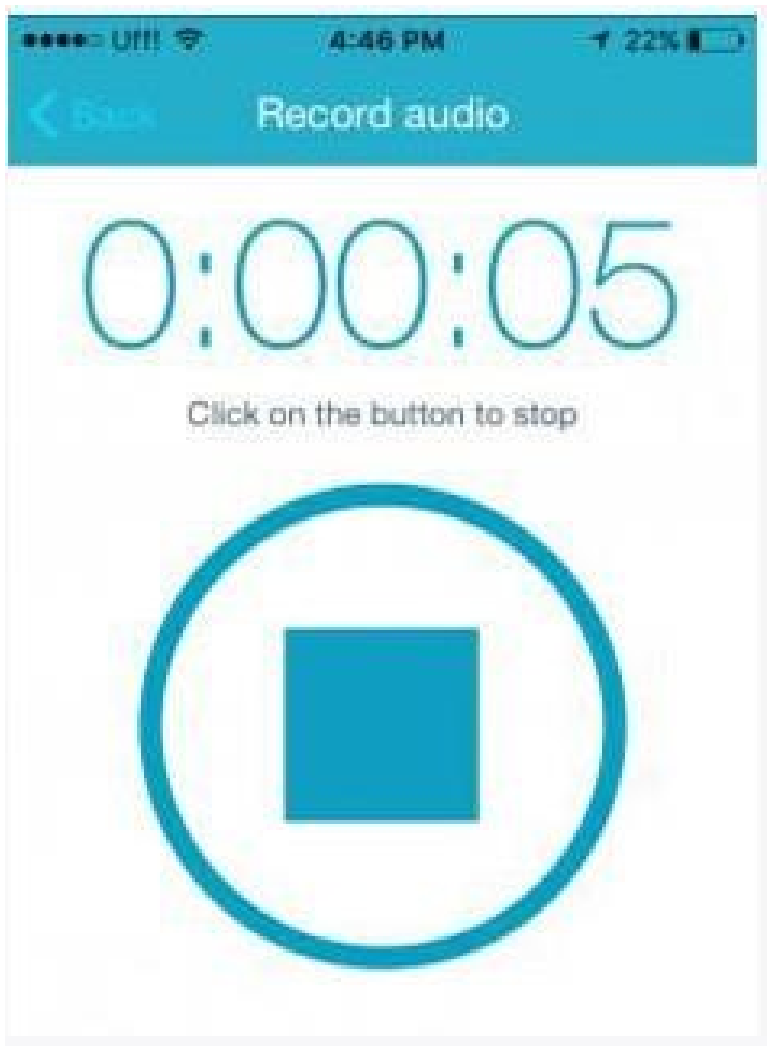
Al seleccionar la imagen se muestra un mensaje informado el inicio y final del cargue.

Para subir una foto y/o vídeo debe realizar la captura y pulsar en **Ok**.

Para subir un audio debe pulsar en el icono de micrófono para iniciar la grabación.



Posteriormente debe pulsar en el icono stop para finalizarla.



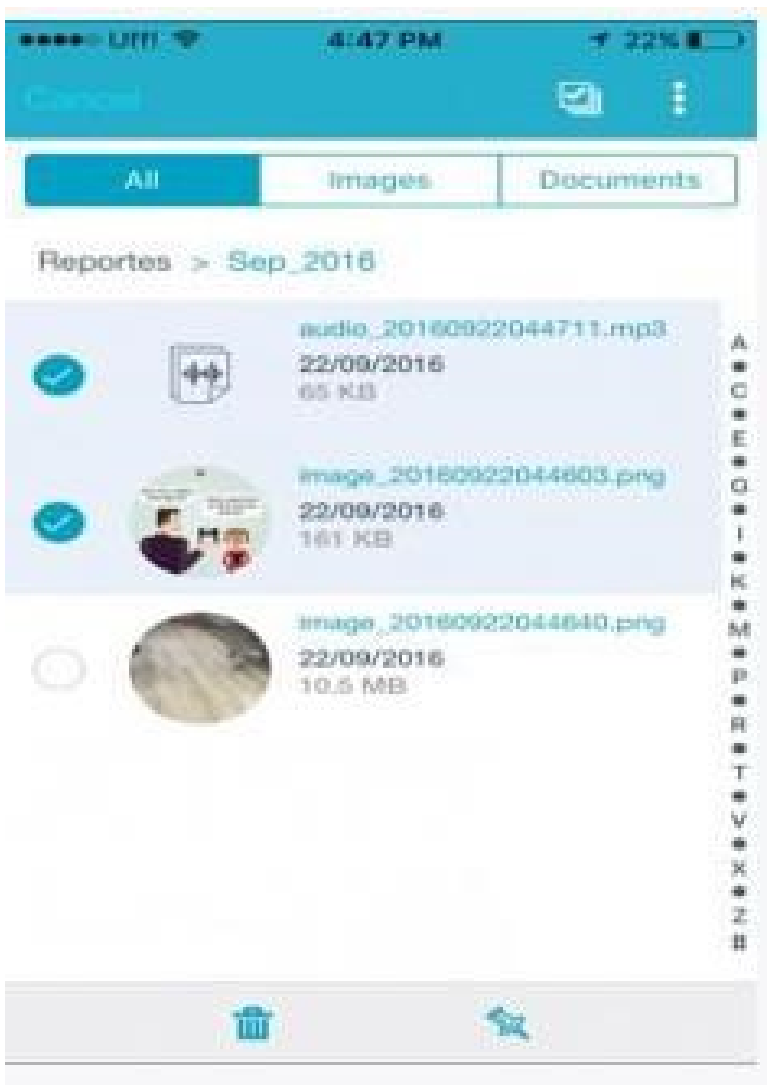
Se visualiza un control para reproducir el audio, adelantarlo, atrasarlo, subirlo (Icono de nube) o descartarlo (Icono de caneca).

Controles de la barra de opciones

Puede realizar búsquedas de archivos pulsando el icono de lupa en la barra de opciones de la aplicación y posteriormente ingresando el criterio de búsqueda.

Con base en el criterio ingresado visualizará los archivos existentes en todas las carpetas.

Puede realizar una selección múltiple de archivos para eliminar o descargar en forma masiva con los controles habilitados en la barra de opciones.



Filtros

Puede refinar la visualización de archivos por medio de las opciones de la barra segmentada ubicada debajo de la barra de opciones, pulsando imágenes.

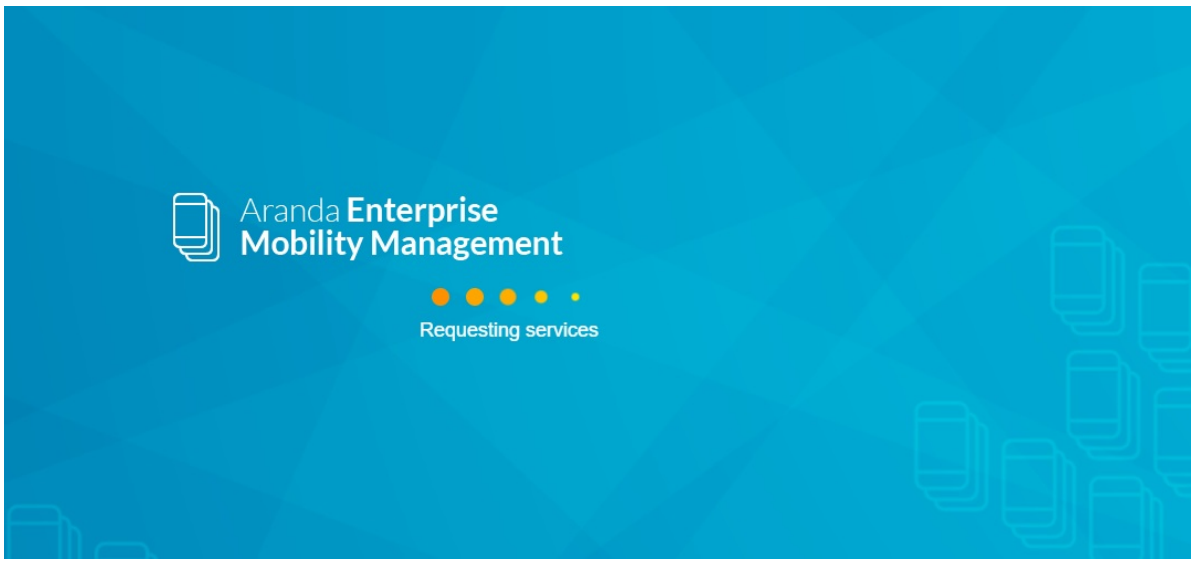
Pulsando documentos se visualizarán los archivos en formato Word, Excel, PowerPoint y PDF.

Estado del server

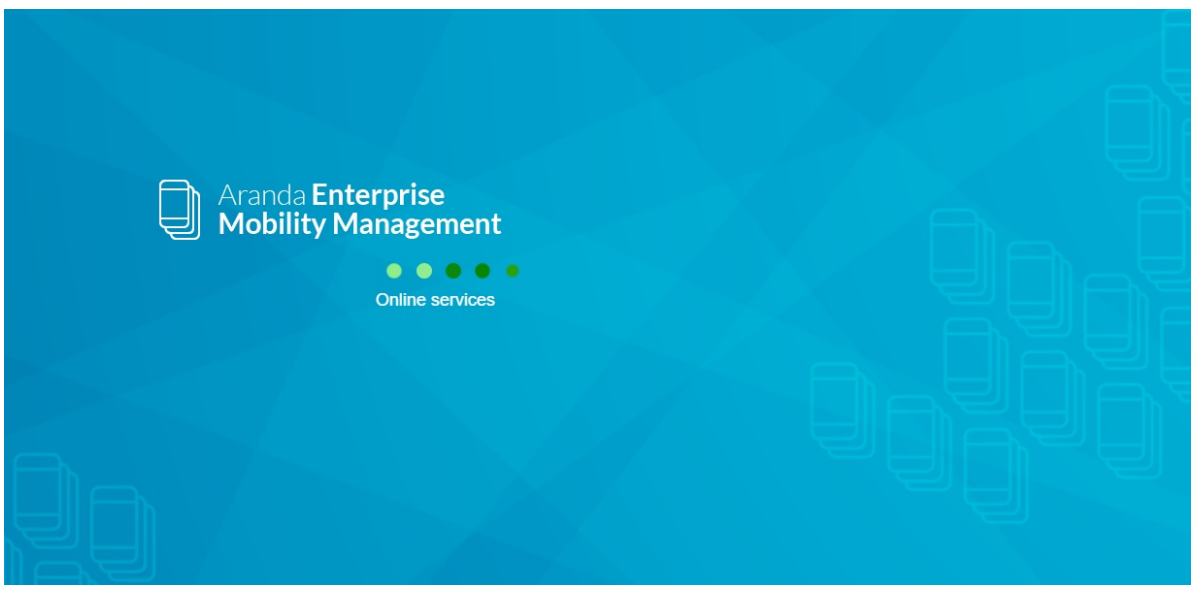
Visualización del estado del servidor

Aranda EMM provee una forma de visualizar el estado del servidor, para esto debemos dirigirnos a la url de nuestro servidor y añadir '/AMDMWS/' después de la url, de esta forma: 'https://{url_dominio}/AMDMWS/'.
En esta pantalla a nivel visual se mostrará 3 estados respecto a las peticiones que se le pueden realizar al servidor.

Solicitando estado



Estado en linea



Fallo llamando a servicio