

Guía de instalación y despliegue de Miradore

Contenido

Guía de instalación y despliegue de Miradore	1
Primeros pasos y registro del primer usuario y dispositivo.	2
Creación de perfiles de configuración.....	5
Añadiendo un dispositivo Apple	7
Informes	10
Perfil de configuración para iOS – Lista negra	11
Perfil de configuración para Android – Activar Localización.....	13
Añadir aplicación - Android.....	15
Despliegue de aplicación – Android	17
Monitorización de ubicación.....	18
Bloqueo remoto del dispositivo	19

Primeros pasos y registro del primer usuario y dispositivo.

Una vez nos hemos creado la cuenta de usuario, comenzaremos con un asistente bastante sencillo:

Primer paso: añadir el primer dispositivo. Para ello seleccionamos el sistema operativo, en este caso seleccionamos Android:

Welcome to Miradore Online!

Add your first device to get started with securing and managing your company's devices.

Select device type:



Android

Miradore Online supports Android devices from version 2.3.3 onwards.



iOS

Miradore Online supports iOS devices from version 4 onwards.



Windows Phone

Miradore Online supports Windows Phone devices from version 8.0 onwards.

Enviamos el correo de invitación al que será nuestro primer usuario. Hay que tener en cuenta que el primer usuario que definamos será el administrador del sitio.

1. Add device

2. Invite device user

3. Complete enrollment

4. Get started with MDM

Invite device owner

Select who'll receive device enrollment invitation. You can invite new people and customize invitation text.

Email:

Send enrollment by SMS: ☐

[Back](#) [Send enrollment invitation](#)

[Skip](#)

Se nos provee de una contraseña y usuarios temporales para añadir el dispositivo. Tal y como podemos ver en la captura, basta con descargar la app cliente desde Play Store e introducir los datos:

1. Add device


2. Invite device user

3. Complete enrollment

4. Get started with MDM

Complete enrolling your first device

Here's how you can enroll your Android device to Miradore Online. We'll continue once you've enrolled.



- 1 Install [Miradore Online Client](#) from Google Play
- 2 Open Miradore Online Client
- 3 Enter username: **pvk1@online.miradore.com**
- 4 Enter password: **6963**
- 5 Click "Enroll device"

Enrollment credentials have also been sent to you by email.

[Back](#) [Next](#)

[Skip](#)

Una vez el dispositivo ha sido reconocido, se nos confirma el modelo y versión de SO:

1. Add device


2. Invite device user

3. Complete enrollment

4. Get started with MDM

Complete enrolling your first device

Here's how you can enroll your Android device to Miradore Online. We'll continue once you've enrolled.



Congratulations, you've enrolled your first device!

Device
asus Nexus 7

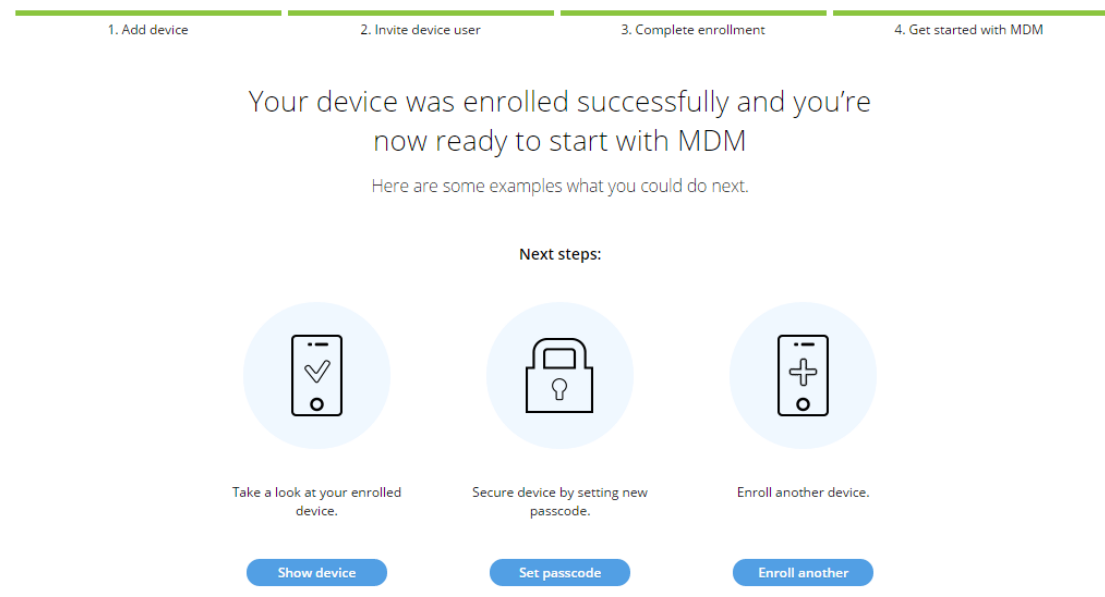
Software
Android 5.1.1

Operator network
-

[Back](#) [Next](#)

[Skip](#)

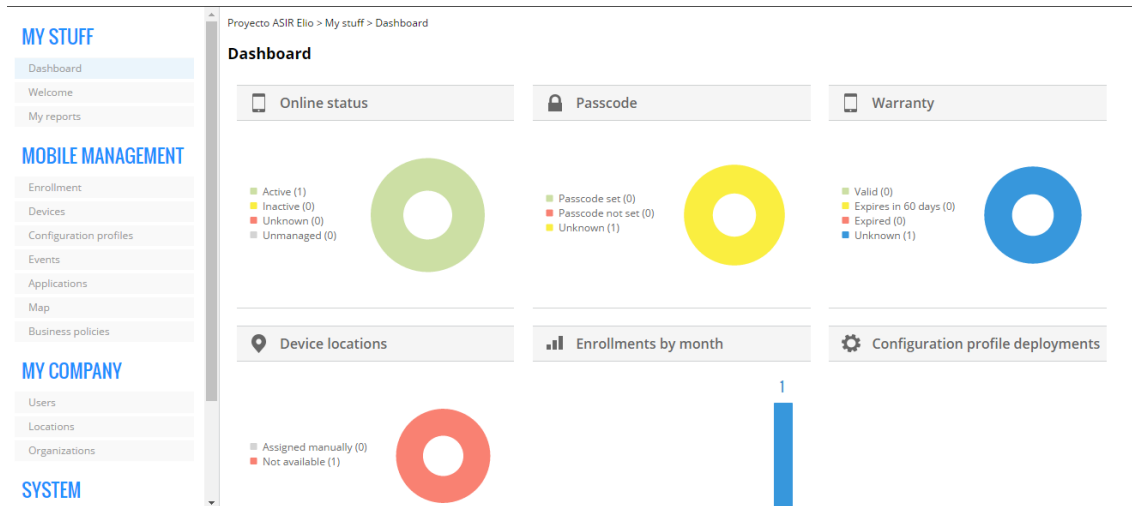
La siguiente pantalla nos informa de que el primer dispositivo ha sido añadido, y se nos da la opción de ver el dispositivo desde el panel de control, establecer una contraseña o añadir otro dispositivo:



Seleccionamos “ver el dispositivo” y comprobamos los parámetros que podemos observar:

The screenshot shows the MDM console interface for a device named "asus Nexus 7". The top bar includes "Contact us", a user icon, and a help icon. The main content area has a sidebar with "Main", "Settings", "Applications", "Events", and "Inventory". The "Main" tab is active, showing device details: "Device: asus Nexus 7", "Software: Android 5.1.1", "User", "Last reported: 2 minutes ago", "Tags: Add tags...", "Free storage: 26,6GB", "Total: 27,6GB", "Storage name: Internal", "Encrypted: No", "Warranty starts", "Warranty ends", "Days left", and "Warranty status". A map shows the device location with a tooltip: "Location not set", "Assign location", and "Enable location tracking". A "Less" link is also visible. The bottom section shows "Configuration profiles" with columns for "Deployment time", "Configuration type", and "Name". The right sidebar contains "Actions" such as "Unenroll device", "Lock device", "Wipe device", "Reset passcode", "Sync now", "Send message", "Deploy configuration profile", "Remove configuration profile", "Deploy application", "Remove application", and "Delete".

Ahora en el menú lateral seleccionamos dashboard y se nos muestra un panel de control en el que podemos observar los dispositivos asociados y su estado actual, así como si tienen establecida contraseña y si están en garantía (para ello necesitamos introducir su fecha de compra)



Creación de perfiles de configuración

Ahora vamos a proceder a establecer la primera configuración común a todos los dispositivos (Configuration profile)

The screenshot shows the 'Deploy configuration profile' screen in Miradore. The top section is titled 'Step 1 of 3: Select devices to deploy the selected configuration'. Below this is a table of devices:

<input checked="" type="checkbox"/>	Product name	Software version	User	Last reported	Online status	IMEI	MAC address	Tags
<input checked="" type="checkbox"/>	asus Nexus 7	Android 5.1.1		17/05/2016 17...	Active		08:60:6e:ab:b2...	

Below the table are 'Cancel' and 'Next' buttons. The bottom section is titled 'Configuration profiles' and shows a table of profiles:

<input checked="" type="checkbox"/>	Name	Description	Platform	Configuration ty
<input checked="" type="checkbox"/>	4 number passcode	Require minimum 4 number passcode	Android	Android Passcod
<input type="checkbox"/>	4 number passcode	Require minimum 4 number passcode	Windows Phone	Windows Phone

On the right side, there is an 'Actions' panel with options: 'Create configuration profile', 'Deploy configuration profile', and 'Delete'.

Como se puede ver, podemos seleccionar el/los dispositivo(s) sobre los que aplicar la configuración, así como elegir un perfil predefinido o crear uno personalizado. En este caso seleccionamos la opción predefinida "Contraseña de 4 números".

Una vez seleccionados los parámetros, confirmamos con el botón deploy:

The screenshot shows the 'Deploy configuration profile' screen in the Miradore interface. The left sidebar contains navigation menus for 'MY STUFF', 'MOBILE MANAGEMENT', 'MY COMPANY', and 'SYSTEM'. The main content area is titled 'Deploy configuration profile' and shows 'Step 2 of 3: Confirm'. It displays the configuration details: '4 number passcode' and 'Require minimum 4 number passcode'. At the bottom, there are three buttons: 'Cancel', 'Previous', and 'Deploy'. Below the deployment section, a breadcrumb trail reads 'Proyecto ASIR Elio > Mobile management > Configuration profiles'. A table titled 'Configuration profiles' lists two entries, both with the name '4 number passcode' and description 'Require minimum 4 number passcode'. The first entry is for 'Android' and the second for 'Windows Phone'. The right sidebar contains an 'Actions' menu with options: 'Create configuration profile', 'Deploy configuration profile', and 'Delete'.

Deploy configuration profile

Step 2 of 3: Confirm

Deploy configuration
Description

4 number passcode
Require minimum 4 number passcode

Cancel Previous Deploy

Proyecto ASIR Elio > Mobile management > Configuration profiles

Configuration profiles

Name	Description	Platform	Configuration ty
4 number passcode	Require minimum 4 number passcode	Android	Android Passcod
4 number passcode	Require minimum 4 number passcode	Windows Phone	Windows Phone

Actions

- Create configuration profile
- Deploy configuration profile
- Delete

Pantalla de confirmación de cambios aplicados:

The screenshot shows the 'Deploy configuration profile' screen in the Miradore interface, now at 'Step 3 of 3: Done'. The main content area displays a green checkmark icon and the message 'Configuration added to deployment queue successfully'. A 'Close' button is visible. The breadcrumb trail remains 'Proyecto ASIR Elio > Mobile management > Configuration profiles'. The 'Configuration profiles' table is identical to the previous screen, showing two entries for '4 number passcode' on 'Android' and 'Windows Phone' platforms. The right sidebar 'Actions' menu is also identical.

Deploy configuration profile

Step 3 of 3: Done

Configuration added to deployment queue successfully

Close

Proyecto ASIR Elio > Mobile management > Configuration profiles

Configuration profiles

Name	Description	Platform	Configuration ty
4 number passcode	Require minimum 4 number passcode	Android	Android Passcod
4 number passcode	Require minimum 4 number passcode	Windows Phone	Windows Phone

Actions

- Create configuration profile
- Deploy configuration profile
- Delete

Añadiendo un dispositivo Apple

Para añadir un dispositivo Apple, necesitaremos también generar un certificado firmado por Apple para que Miradore pueda enviar notificaciones Push a través del Servicio de notificaciones Push de Apple.

El proceso sería:

- Crear una solicitud de certificado .csr (Certificate Signing Request)
- Enviar dicha solicitud a Apple.
- Descargar el certificado firmado.
- Subirlo a los servidores de Miradore para vincularlo a nuestro dominio.

Descarga del csr:

Create Apple Push certificate

Create the Apple Push certificate to be able to manage iOS devices. Don't worry, you only need to do this once.

- 1.** First download the Certificate Signing Request file [Download csr.txt](#)
- 2.** Sign in to Apple Push Certificates Portal [Open Apple Portal](#)
 - Sign in with an Apple ID, preferably a corporate ID.
 - Then upload CSR file downloaded in step 1.
 - Finally create the Apple Push Certificate file (MDM*.PEM).
- 3.** Return to Miradore Online and upload Apple certificate (MDM*.PEM) here [Upload certificate](#)
- 4.** Done! You can move forward

[Back](#) [Next](#)

Asistente de firmado de certificados de Apple:

Apple Push Certificates Portal

elioacpinar@gmail.com [Sign out](#)


Get Started

Create a push certificate that enables your third-party server to work with the Apple Push Notification Service and your Apple devices.

[Create a Certificate](#)

FAQ

[Learn more about Mobile Device Management](#)
[What about OS X Server?](#)



Shop the [Apple Online Store](#) (1-800-MY-APPLE), visit an [Apple Retail Store](#), or find a [reseller](#).

[Apple Info](#) | [Site Map](#) | [Hot News](#) | [RSS Feeds](#) | [Contact Us](#) | 

Copyright © 2014 Apple Inc. All rights reserved. [Terms of Use](#) | [Privacy Policy](#)

Subida del .csr a los servidores de Apple:

Apple Push Certificates Portal

elioacpinar@gmail.com [Sign out](#)

Create a New Push Certificate

Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.


Notes

Vendor-Signed Certificate Signing Request

Seleccionar archivo

 Ningún archivo seleccionado

[Cancel](#) [Upload](#)



Certificado creado y listo para su descarga:

Apple Push Certificates Portal

elioacpinar@gmail.com [Sign out](#)

Confirmation

You have successfully created a new push certificate with the following information:

Service	Mobile Device Management
Vendor	Miradore Oy
Expiration Date	May 17, 2017

[Manage Certificates](#) [Download](#)



Subida del certificado firmado a Miradore:

Create Apple Push certificate

Create the Apple Push certificate to be able to manage iOS devices. Don't worry, you only need to do this once.



First download the Certificate Signing Request file

[Download csr.txt](#)



Sign in to Apple Push Certificates Portal

[Open Apple Portal](#)

- Sign in with an Apple ID, preferably a corporate ID.
- Then upload CSR file downloaded in step 1.
- Finally create the Apple Push Certificate file (MDM*.PEM).



Return to Miradore Online and upload Apple certificate (MDM*.PEM) here

[Upload certificate](#)



4. Done! You can move forward

[Back](#)

[Next](#)

Completamos el registro de nuestro dispositivo Apple:

1. Add device

2. Create Certificate

3. Invite device user

4. Complete enrollment

5. Get started with MDM

Complete enrolling your first device

Here's how you can enroll your iOS device to Miradore Online. We'll continue once you've enrolled.



Congratulations, you've enrolled your first device!

Device
Apple iPad2,5
Software
iOS 9.2.1

Operator network
-

[Back](#)

[Next](#)

[Close](#)

Informes

En este apartado vamos a crear un informe personalizado, para ello definimos una query a la que añadiremos condiciones:

Create new report

Step 1 of 4: Define a search query (optional). Leave empty if you want to include all devices in your report.

Start by defining conditions for searching your devices from Miradore Online. All devices matching the conditions will be included in the report. The search query may include multiple conditions.

AND [icon] x

OnlineStatus EqualTo Active x

OnlineStatus eq Unavailable

Cancel Next

Por ejemplo, vamos a hacer un SELECT de todos los dispositivos que cumplan la CONDICIÓN de ser ANDROID y estar en estado ACTIVO:

Create new report

Step 1 of 4: Define a search query (optional). Leave empty if you want to include all devices in your report.

Start by defining conditions for searching your devices from Miradore Online. All devices matching the conditions will be included in the report. The search query may include multiple conditions.

AND [icon] Add condition

OnlineStatus EqualTo Active x

Platform EqualTo Android x

OnlineStatus eq Active and Platform eq Unknown

Cancel Next

Ahora seleccionamos las columnas que se mostrarán en nuestro informe, como podemos ver estos campos son totalmente personalizables. Esto sería equivalente a elegir las columnas en una sentencia SELECT de SQL:

Create new report

Step 2 of 4: Define columns shown in report

Drag and drop to select and reorder columns in your report. You can select up to 10 columns for your report.

Available:

- User.Email
- User.Firstname
- User.Lastname
- User.Middle
- User.PhoneNumber
- User.Source
- Location.FullName

Selected:

- Online status (icon)
- User.Name
- InvDevice.Model
- InvDevice.SoftwareVersion

Cancel Previous Next

Proyecto ASIR Elio > My stuff > My reports

Una vez configurado, podemos almacenarlo para volver a ejecutarlo bajo demanda:

Create new report

Step 3 of 4: Name the report

Name: Informe de prueba

Description: Muestra dispositivos Android Activos

Cancel Previous Create

Proyecto ASIR Elio > My stuff > My reports

Como se puede ver, podemos consultarlo y ejecutarlo bajo la pestaña My Reports:

Proyecto ASIR Elio > My stuff > My reports

My reports

 [Informe de prueba](#)
Muestra dispositivos Android Activos

Resultado del informe:

Proyecto ASIR Elio > My stuff > My reports

Informe de prueba

Export Page 1 of 1 1 - 1 of 1 Page size: 100

	User.Name	InvDevice.Model	InvDevice.SoftwareVersion
		asus Nexus 7	Android 5.1.1

Perfil de configuración para iOS – Lista negra

Creación de un perfil de configuración para iOS. Como se ha explicado más detalladamente a lo largo del proyecto, iOS es más restrictivo que Android a la hora de establecer ciertas políticas a sus dispositivos. En esta lista podemos ver qué opciones dependen de que el dispositivo esté en modo supervisado.

Create configuration profile

Step 1 of 5: Select the platform for the configuration profile.

☐ Android

☒ iOS

☐ Windows Phone

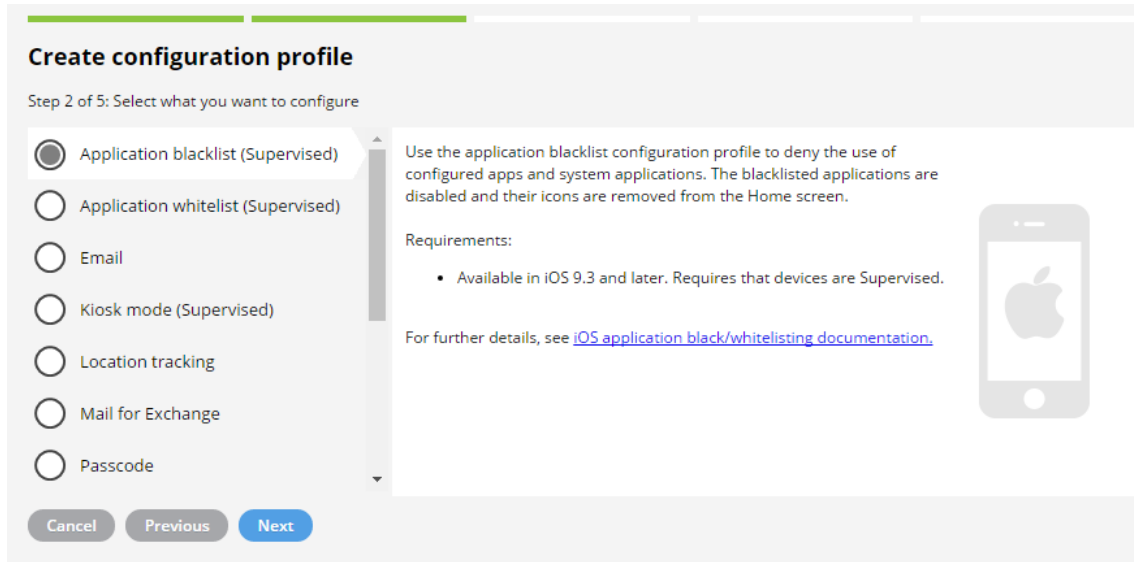
Configuration profiles can be used to manage and distribute configuration settings for mobile devices. As desired settings are stored as configuration profiles, it is quick and easy to implement policies and standardize device configurations by applying the configuration profiles for multiple devices. See [configuration profile video in product guide](#).

Configuration profile types available for iOS:

- Application blacklist (Supervised)
- Application whitelist (Supervised)
- Email
- Kiosk mode (Supervised)
- Location tracking
- Mail for Exchange
- Passcode
- Restrictions
- Roaming configuration
- VPN
- Wallpaper (Supervised)
- Web Clip
- Wi-Fi

Cancel Next

En este caso, crearemos una lista negra de aplicaciones (aunque no se haga efectiva, mostraremos el proceso igualmente):



Create configuration profile

Step 2 of 5: Select what you want to configure

☒ Application blacklist (Supervised)

☐ Application whitelist (Supervised)

☐ Email

☐ Kiosk mode (Supervised)

☐ Location tracking

☐ Mail for Exchange

☐ Passcode

Use the application blacklist configuration profile to deny the use of configured apps and system applications. The blacklisted applications are disabled and their icons are removed from the Home screen.

Requirements:

- Available in iOS 9.3 and later. Requires that devices are Supervised.

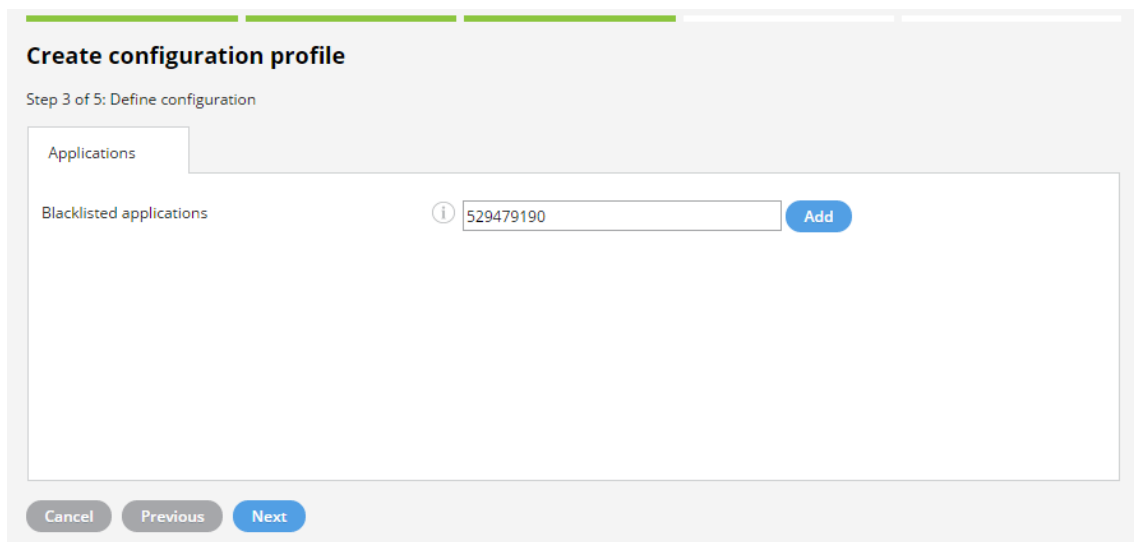
For further details, see [iOS application black/whitelisting documentation](#).

Cancel Previous Next

Debemos obtener el id de la aplicación que vamos a incluir en la lista negra, para ello nos fijamos en su link a iTunes:

<https://itunes.apple.com/es/app/clash-of-clans/id529479190?mt=8>

De ahí obtenemos el número que va justo detrás de id y lo introducimos:



Create configuration profile

Step 3 of 5: Define configuration

Applications

Blacklisted applications

529479190 Add

Cancel Previous Next


Elegimos un nombre y descripción para el perfil de configuración:

Create configuration profile

Step 4 of 5: Define a name for the configuration

Name (i) Bloqueo de juego

Description (i) No se permite jugar en clase



Cancel Previous Create

Perfil de configuración para Android – Activar Localización

Ahora mostramos un ejemplo de perfil de configuración para activar la localización de forma remota:


Create configuration profile

Step 2 of 5: Select what you want to configure

- ☐ Kiosk mode (Samsung)
- ☒ Location tracking
- ☐ Mail for Exchange (Samsung)
- ☐ Passcode
- ☐ Restrictions (Samsung)
- ☐ Web shortcut
- ☐ Wi-Fi

Use the location tracking profile to enable location tracking in target devices.

For further details, see [location tracking documentation](#)



Cancel Previous Next

Configuramos si queremos notificar al usuario del cambio de configuración, el intervalo de actualización de la ubicación y la distancia mínima de desplazamiento para actualizar la ubicación, en este caso la dejamos desactivada para que se actualice cada minuto independientemente del cambio de ubicación del dispositivo:

Create configuration profile

Step 3 of 5: Define configuration

Settings

End user notification ☐

Minimum data update interval

Minimum distance change

End-user notification defines if the user is notified when location tracking is enabled.
Minimum data update interval defines how often location updates are reported to the server.
Minimum distance change defines a threshold of how many meters the location of the device has to change before it receives location updates.
Please note that when using small values the device receives location updates more frequently and this shortens the battery life. For further details, see [location tracking documentation](#)

Cancel Previous Next

Almacenamos el perfil de configuración:

Create configuration profile

Step 4 of 5: Define a name for the configuration

Name

Description

Android phone icon

Cancel Previous Create

Añadir aplicación - Android

Miradore nos permite añadir aplicaciones que luego podremos enviar a los dispositivos seleccionados para su instalación:

Add application

Step 1 of 4: Select platform for the application

☒ Android


☐ iOS

☐ Windows Phone

Application management allows to remotely install applications from Google Play store or by downloading and installing application packages (APK) directly from the web, or by uploading the application packages to Miradore Online.

In order to be able to remotely install an application from Google Play store, the user of the device must be signed in to Google Play with his/her account. Installing paid applications from Google Play store is supported, but the user must purchase the application prior to installation.

Installing APK packages downloaded from the web requires permissions to install applications from unknown sources on the device. APK packages can be installed silently, without user confirmation, to Samsung Android devices if the Samsung for Enterprise (SAFE) / KNOX is enabled on the device.



CancelNext

Podemos seleccionar su origen, ya sea Play Store o un archivo .apk. Hay que tener en cuenta que el usuario tendrá que confirmar la instalación:

Add application

Step 2 of 4: Select application type


☒ Google Play store

☐ APK download

Choose Google Play store to deploy applications from Google Play store to Android devices.

The user must be signed in to Google Play with his/her account, and accept the installation. The installations cannot be forced to a device nor can the applications be installed quietly in the background.

Paid applications are supported, but the user must purchase the application prior to installation.



CancelPreviousNext

Elegimos la aplicación correspondiente, elegimos su nombre, nombre de paquete (que podemos obtener de la página correspondiente en play store) y una descripción:

Add application

Step 3 of 4: Enter application details

Name: Evernote

Package name: com.evernote [Show in Google Play](#)

Notification to user: Se va a instalar EVERNOTE en tu tablet

Description: Aplicación para tomar notas

Add shortcut to home screen: ☒

Buttons: Cancel, Previous, Create

Pantalla de confirmación con resumen:

Add application

Step 4 of 4: Add application

✓ Application Evernote created successfully

Icon: Smartphone with Evernote logo

Name: Evernote

Package name: com.evernote

Notification to user: Se va a instalar EVERNOTE en tu tablet

Description: Aplicación para tomar notas

Add shortcut to home screen: ☒

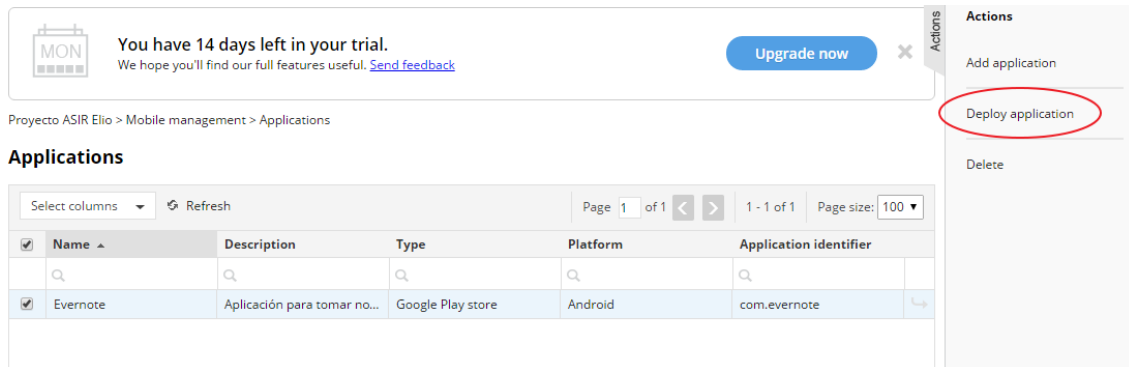
Application on Google Play: <https://play.google.com/store/apps/details?id=com.evernote>

Button: Close

Despliegue de aplicación – Android

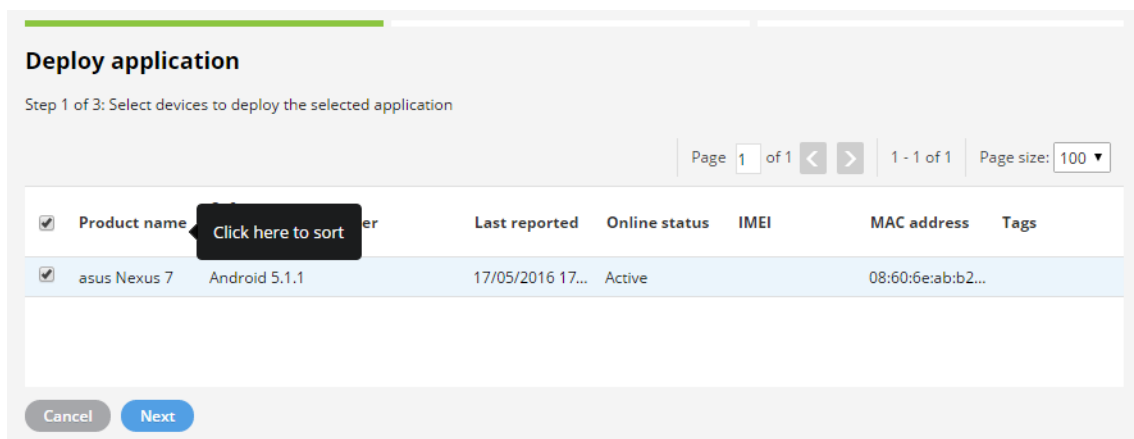
Acto seguido vamos a proceder a desplegar la aplicación en los dispositivos. Es importante saber que sólo podremos desplegar aplicaciones que previamente hemos definido en la sección aplicaciones.

La seleccionamos, y pulsamos Deploy application:



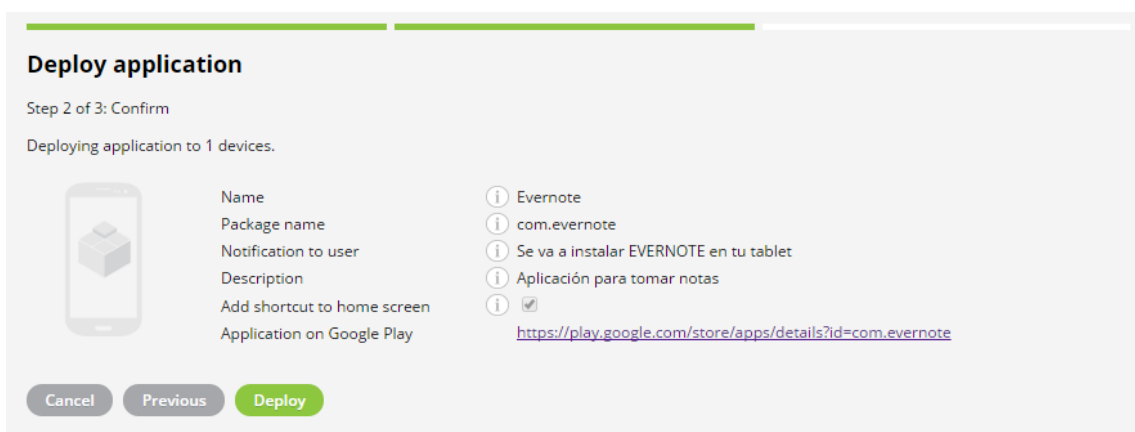
The screenshot shows the Mobile management console interface. At the top, there is a trial notice: "You have 14 days left in your trial. We hope you'll find our full features useful. [Send feedback](#)". Below this, the breadcrumb "Proyecto ASIR Elio > Mobile management > Applications" is visible. The main section is titled "Applications" and contains a table with columns: Name, Description, Type, Platform, and Application identifier. One application, "Evernote", is listed with the description "Aplicación para tomar no...", type "Google Play store", platform "Android", and identifier "com.evernote". To the right of the table is an "Actions" menu with options: "Add application", "Deploy application" (highlighted with a red circle), and "Delete".

Ahora seleccionamos el/los dispositivo(s) sobre los que instalaremos:



The screenshot shows the "Deploy application" screen, Step 1 of 3: "Select devices to deploy the selected application". It features a table with columns: Product name, Version, Last reported, Online status, IMEI, MAC address, and Tags. One device, "asus Nexus 7", is selected with version "Android 5.1.1", last reported "17/05/2016 17...", and online status "Active". A tooltip "Click here to sort" is visible over the "Version" column header. At the bottom, there are "Cancel" and "Next" buttons.

Confirmamos que la aplicación será desplegada con la configuración seleccionada. Podemos personalizar el mensaje que se mostrará al usuario antes de instalarse:



The screenshot shows the "Deploy application" screen, Step 2 of 3: "Confirm". It displays the application details for "Evernote" and the devices it will be deployed to. The details include: Name (Evernote), Package name (com.evernote), Notification to user (Se va a instalar EVERNOTE en tu tablet), Description (Aplicación para tomar notas), Add shortcut to home screen (checked), and Application on Google Play (https://play.google.com/store/apps/details?id=com.evernote). At the bottom, there are "Cancel", "Previous", and "Deploy" buttons.

Step 3 of 3: Done

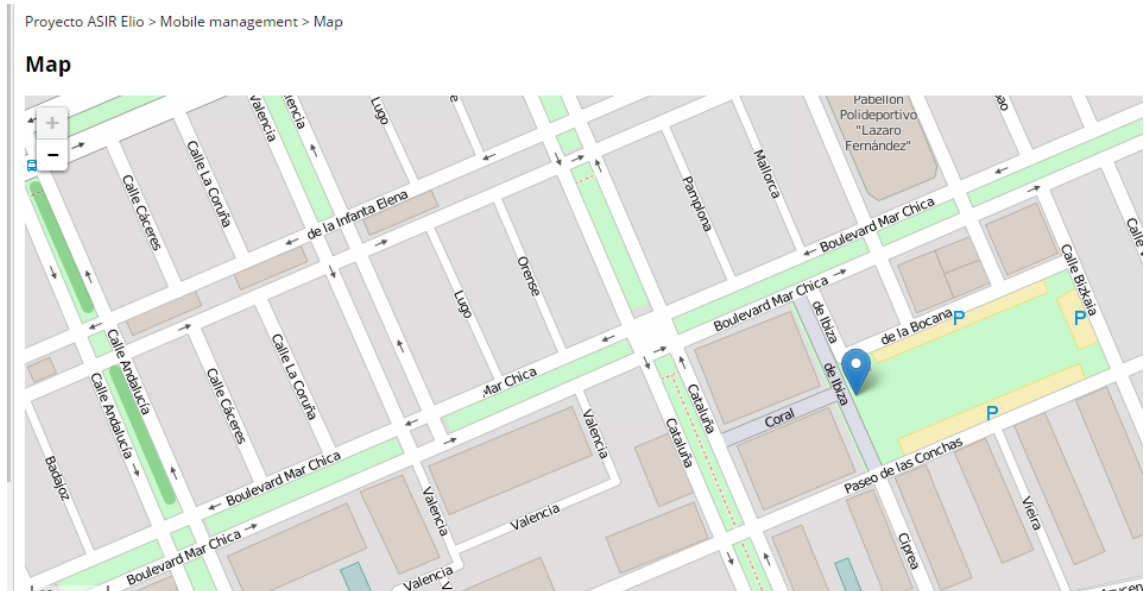


Application added to deployment queue successfully

Monitorización de ubicación

Ahora vamos a comprobar cómo podemos observar la ubicación de un dispositivo en tiempo real:

Para ello, pulsamos la pestaña Map en el menú lateral, y se nos muestra un mapa detallado con la ubicación del dispositivo:



Bloqueo remoto del dispositivo

Bloqueo de dispositivo. Esta opción es muy interesante porque podemos bloquear remotamente uno o varios dispositivos. Debemos saber que se trata de un bloqueo normal, por lo que el usuario puede desbloquearlo de la forma usual si conoce la contraseña.

Lock device

Step 1 of 2: Lock device

Device lock is an MDM feature that allows administrators to remotely lock selected device(s) from the management console of Miradore. When the device receives the lock command, the device locks immediately and a predefined password or passcode is required in order to unlock the device.

Device

asus Nexus 7

User

Cancel

Lock