Mobile Device Management

Implementation of Miradore MDM

a cloud-based solution for managing
a fleet of mobile devices

By Ershad RAMEZANI

Table of Contents

Brief overview of the project

While waiting for the implementation of a VDI solution to provide each ADRAR user with a virtual desk allowing them to work from anywhere, including from home, you have been tasked with proposing and implementing a cost-effective solution to allow ADRAR to have control over the mobile devices of users such as laptops, tablets, and smartphones. Since ADRAR is spread across multiple sites and involves several partners, some of whom have access to internal resources such as videos and course materials, the solution should allow for quick integration of new equipment. A cloud-based solution would be desirable.

The distinction will be made between mobile equipment provided by ADRAR and personal equipment on which any intervention must be subject to acceptance. As previously mentioned, part of the mobile fleet is provided by ADRAR, but users who prefer to use their own equipment will only be able to access internal resources if their equipment meets the charter which states that:

- The owner must sign a waiver releasing ADRAR from any liability for damage to their equipment, of any kind.
- Any equipment accessing internal resources must be identified and recorded on the asset register.
- The ADRAR establishment reserves the right to inventory third-party equipment and all its components before granting access rights to its network.
- For equipment provided by the DSI for telework, the DSI reserves the right to implement a geolocation system for the equipment.
- Owners who have refused or not submitted to this charter will be able to use Wi-Fi connections and Internet access subject to authentication by a proxy, but no other resources will be accessible.

Note: The study of deploying a proxy will be the subject of another project.

Your mission:

1. Propose an MDM solution to inventory mobile devices
2. Implement a system for geolocating equipment provided by ADRAR
3. Automatically deploy on equipment provided by ADRAR:
    a. An antivirus.
    b. A VPN client (compatible with the company's VPN solution).
    c. The CA certificate used to secure connections that may need it.

Bring Your Own Device (BYOD)

In a *bring your own device* (BYOD) program, employees use their own personal mobile devices for work purposes. This is a common issue faced by many companies and universities. There are several approaches that can be taken to address this situation:

1. Completely forbid the use of personal mobile devices within the company, which means the device cannot connect to the company's network or other resources.
2. Implement rules for mobile device use:
    a. Allow mobile devices to connect to the network, but direct them to a specific VLAN with ACLs configured and limited access to resources. Additionally, require authentication through a radius server.
    b. Use a mobile device management (MDM) solution to secure any mobile device that connects to the company's network.
3. Implement a hybrid solution:
    a. Allow users to access the internet through the company's network, but monitor their activities with a proxy. In this scenario, users are responsible for any abuse of the network, as their activities will be monitored.
    b. For access to other resources, provide users with a virtual desktop infrastructure (VDI) and allow them to connect to a virtual desktop.

Company-owned devices

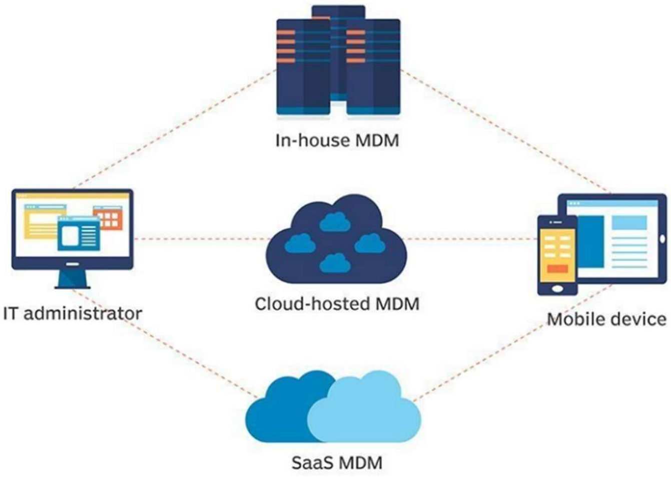
In a company-owned device scenario, the organization provides mobile devices to employees and is responsible for managing and securing those devices. This can be accomplished through the use of mobile device management (MDM) software, which allows the organization to have total control over the device. MDM in Windows 10 is similar to using group policy objects (GPOs) to limit the administration of a Windows device that is integrated into a domain.

Mobile Device Management

Mobile device management (MDM) is a type of software that allows organizations to securely manage and monitor the use of mobile devices, such as smartphones and tablets, by employees. MDM solutions typically include a range of features and capabilities, including the ability to enforce security policies, remotely wipe data from lost or stolen devices, track device location, and manage the installation and updates of apps on devices.

How MDM works

Mobile device management involves using special software, called an MDM agent, on devices and an MDM server in a data center, either on premises or in the cloud, to manage and secure mobile devices. IT administrators can set up policies on the MDM server and send them wirelessly to the MDM agent on the device and they will be applied to the operating system. The MDM server can also be used to deploy apps to managed devices.



OMA-DM protocol

MDM uses a protocol based on XML that is called OMA-DM. This is an open standard protocol. The OMA part stands for Open Mobile Alliance. And the DM part stands for Device Management. OMA-DM deals with the joining aspect of a machine to an MDM system, which is known as *enrollment*. And OMA-DM deals with sending messages to the mobile device, to deliver a new policy via push, gather its status, or perform a remote wipe.

CSPs (Configuration Service Providers)

These are the build-in mini-receivers within Windows 10’s implementation of MDM. They accept OMA-DM directives as XML, process and apply them on the client. In Group Policy-land, we used CSEs, or Client-Side Extensions. Now in MDM-land, we use CSPs.

Comparing MDM vs. Group Policy

Group Policy has been used to manage domain-joined computers for almost two decades. By creating Group Policy Objects (GPOs), you can deliver settings, enforce security, restrict software, deploy applications, and assign printers and network drives. In short, you can do a lot with Group Policy.

It looks like MDM in Windows 10 and Group Policy accomplish the same goals. The major difference between Windows 10 MDM vs Group Policy is that they each work in different environments. For example, Group Policy only supports domain-joined machines in a traditional Active Directory environment. but a Windows 10 MDM provider like *Intune* only supports MDM-enrolled machines that reside in a cloud tenant like Microsoft Azure. With MDM, machines can be non-domain-joined, or hybrid domain-joined (on-prem Active Directory vs Azure Active Directory).

Choosing a MDM solution

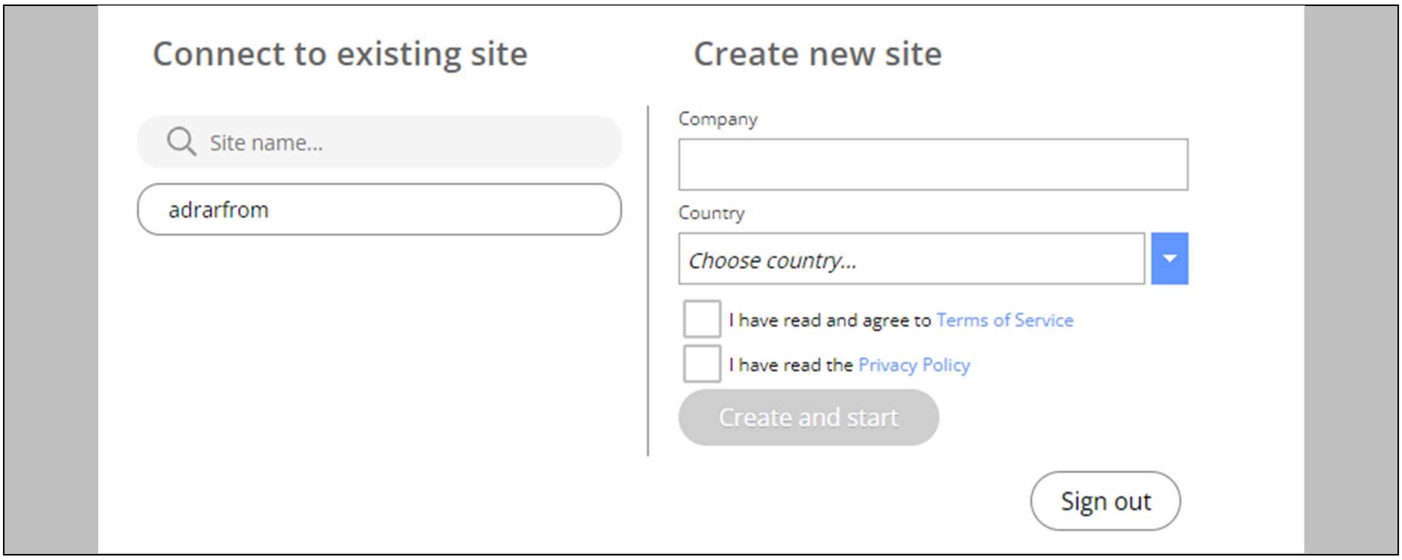
In this article, we will be discussing Miradore, which is one of three mobile device management (MDM) solutions that offer similar capabilities for managing and securing mobile devices. The other two solutions are Microsoft Intune and ManageEngine. When choosing an MDM solution, it is important to consider factors such as the specific needs of the organization, budget, and preferred deployment model (cloud-based or on-premises). All three solutions offer similar capabilities, so the choice between them may depend on these and other factors.

Miradore

Miradore offers a free account that provides a 14-day trial of the Miradore Premium plan, which allows you to access all of the features that are available with a paid subscription to Miradore. This is a great opportunity to try out the full range of capabilities offered by Miradore.

Creating an account on Miradore

Once you have connected to your new account, you can create your first site by selecting a name for your company and choosing the country in which it is located.



Connect to existing site

Site name...

adrarfrom

Create new site

Company

Country

Choose country...

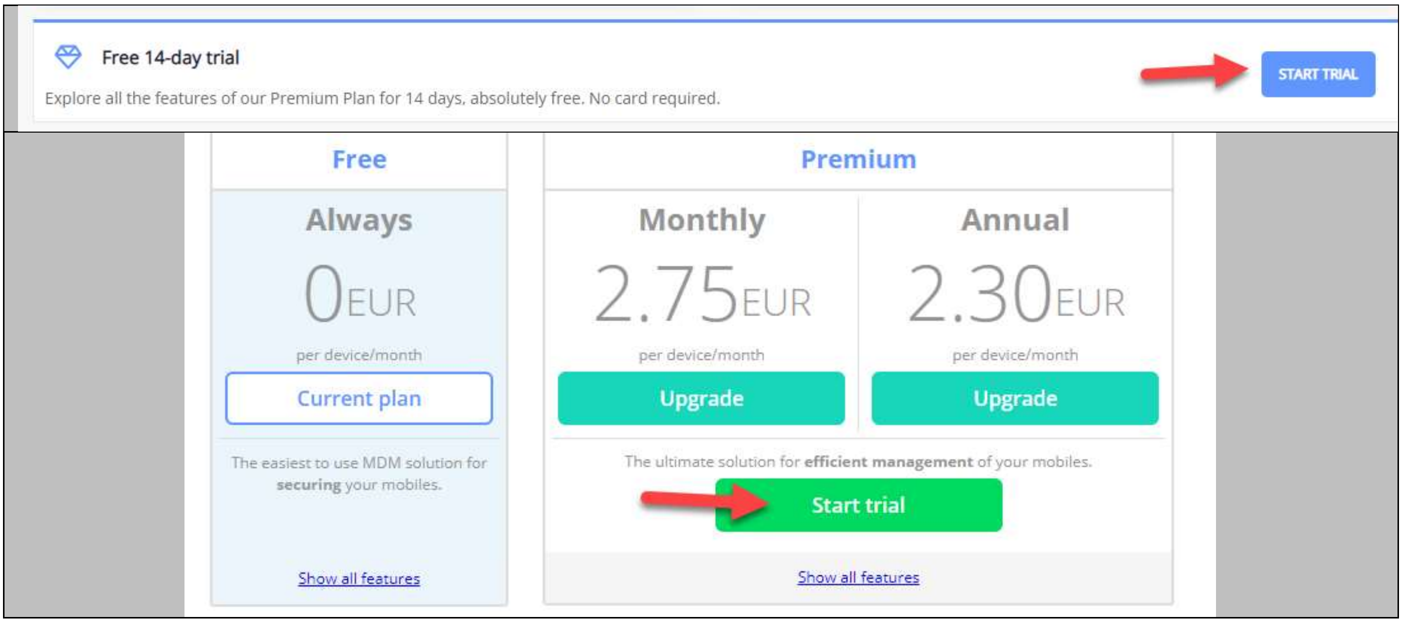
□ I have read and agree to Terms of Service

□ I have read the Privacy Policy

Create and start

Sign out

At the bottom of the welcome page, there is a button that allows you to activate the trial.

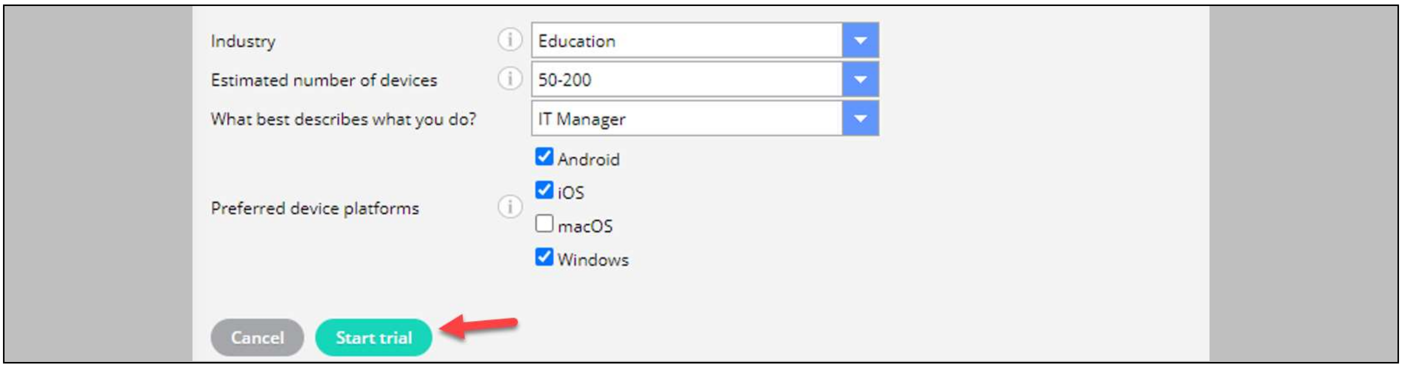


Free 14-day trial

Explore all the features of our Premium Plan for 14 days, absolutely free. No card required.

START TRIAL

Free	Premium	
Always	Monthly	Annual
0EUR	2.75EUR	2.30EUR
per device/month	per device/month	per device/month
Current plan	Upgrade	Upgrade
The easiest to use MDM solution for **securing** your mobiles.	The ultimate solution for **efficient management** of your mobiles.	
	Start trial	
Show all features	Show all features	



Industry: Education

Estimated number of devices: 50-200

What best describes what you do?: IT Manager

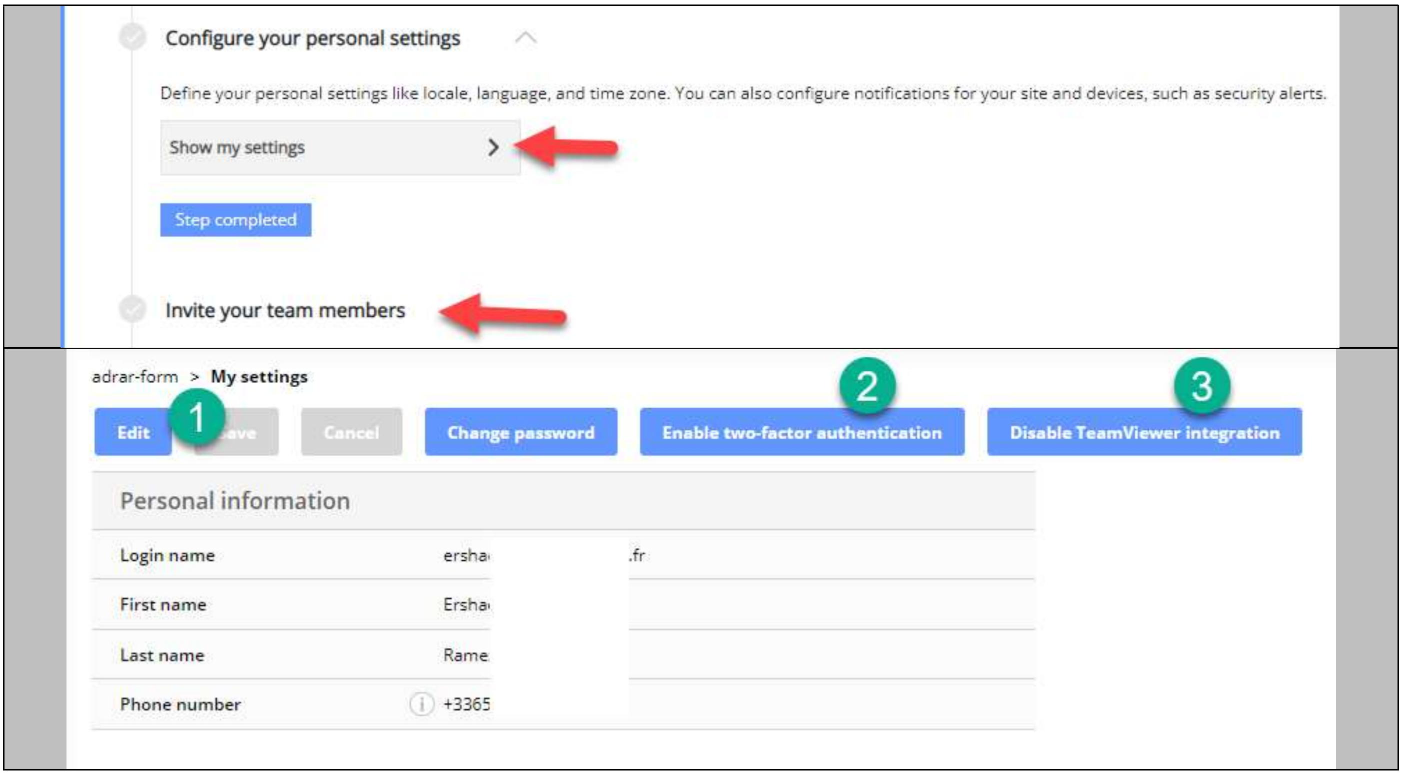
Preferred device platforms: ☑ Android ☑ iOS □ macOS ☑ Windows

Setup Guide

I recommend following the setup guide when starting with Miradore, as it provides step-by-step instructions for configuring the software. To access the setup guide, go to the vertical bar on the right side of the screen and click on "setup guide." Then, scroll to the bottom of the page and click on "open setup guide".

Configure site and users

We have already created and activated the site, so these steps are completed. Now, we can finalize the personal settings configurations or invite our team members. Also you can connect you account to your TeamViewer account.



Configure your personal settings

Define your personal settings like locale, language, and time zone. You can also configure notifications for your site and devices, such as security alerts.

Show my settings
Step completed

Invite your team members

adrar-form > My settings

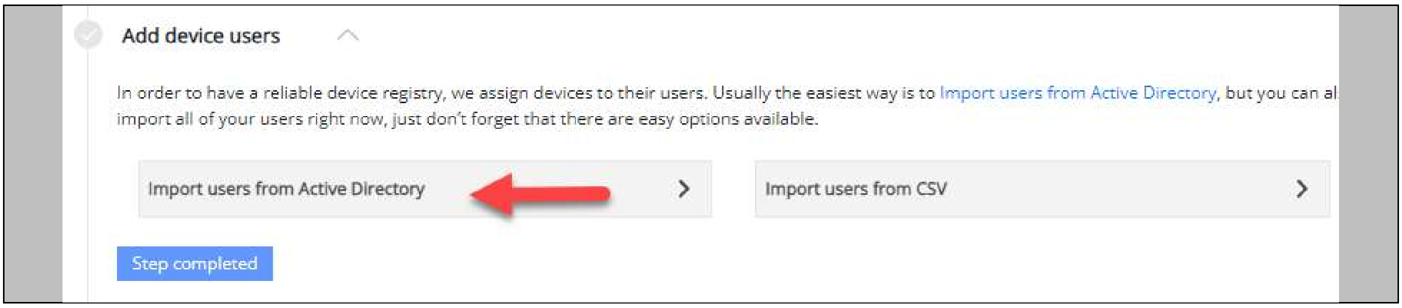
Edit
1
Save
Cancel
Change password
2
Enable two-factor authentication
3
Disable TeamViewer integration

Personal information

Login name	ersha[redacted].fr
First name	Ersha[redacted]
Last name	Rame[redacted]
Phone number	+3365[redacted]

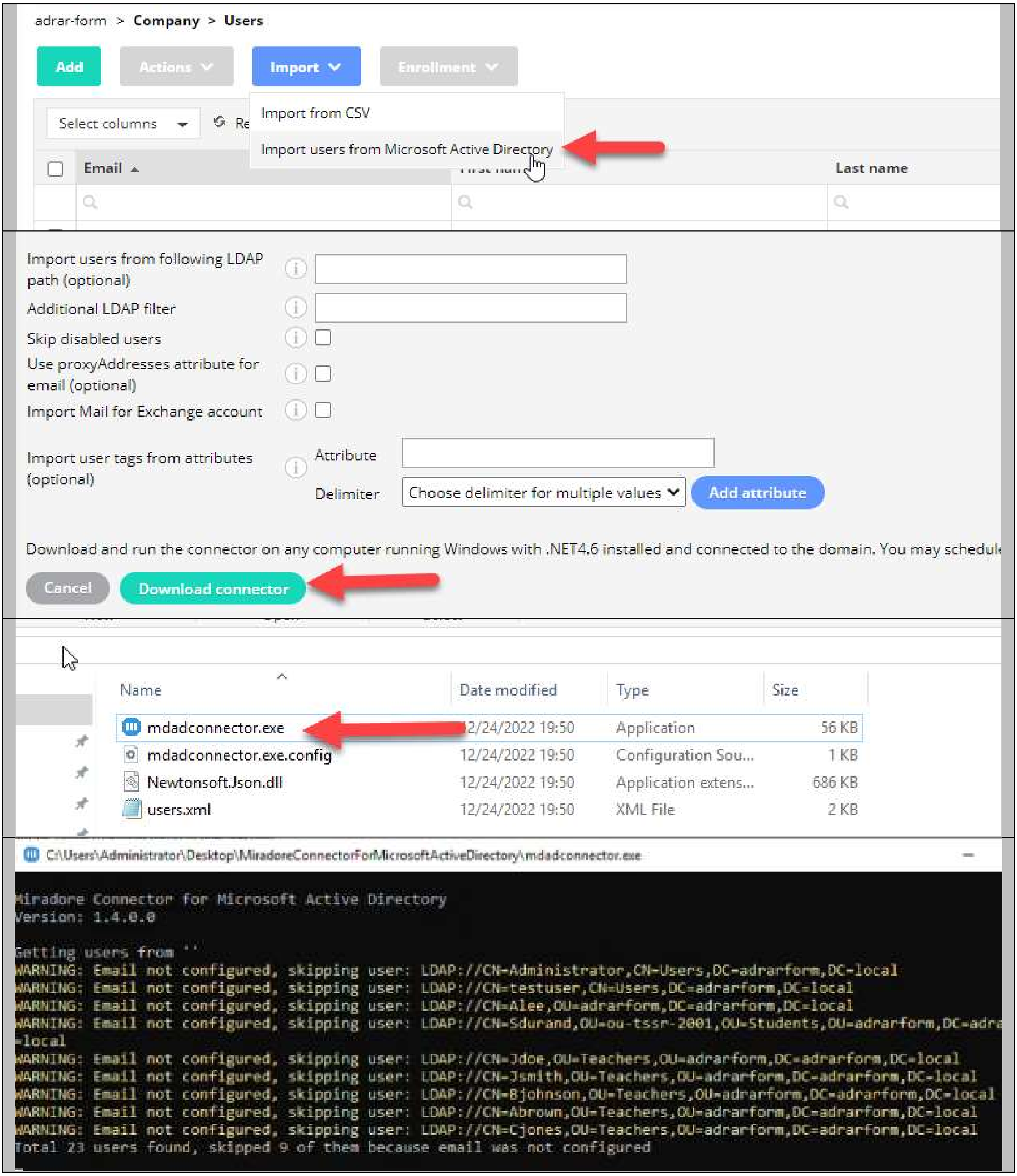
Add device users

To assign devices to their users, we can import users from Active Directory. However, the users must have an email configured in their Active Directory accounts for this to work. To start the process, download the connector executable and run it on the AD server. The connector will automatically search for users and synchronize them to your Miradore account.



Add device users

In order to have a reliable device registry, we assign devices to their users. Usually the easiest way is to Import users from Active Directory, but you can al import all of your users right now, just don't forget that there are easy options available.


adrar-form > Company > Users
Add
Actions
Import
Enrollment
Select columns
Re
Import from CSV
Import users from Microsoft Active Directory
Email
Last name

Import users from following LDAP path (optional)

Additional LDAP filter

Skip disabled users ☐

Use proxyAddresses attribute for email (optional) ☐

Import Mail for Exchange account ☐

Import user tags from attributes (optional)

Attribute

Delimiter: Choose delimiter for multiple values

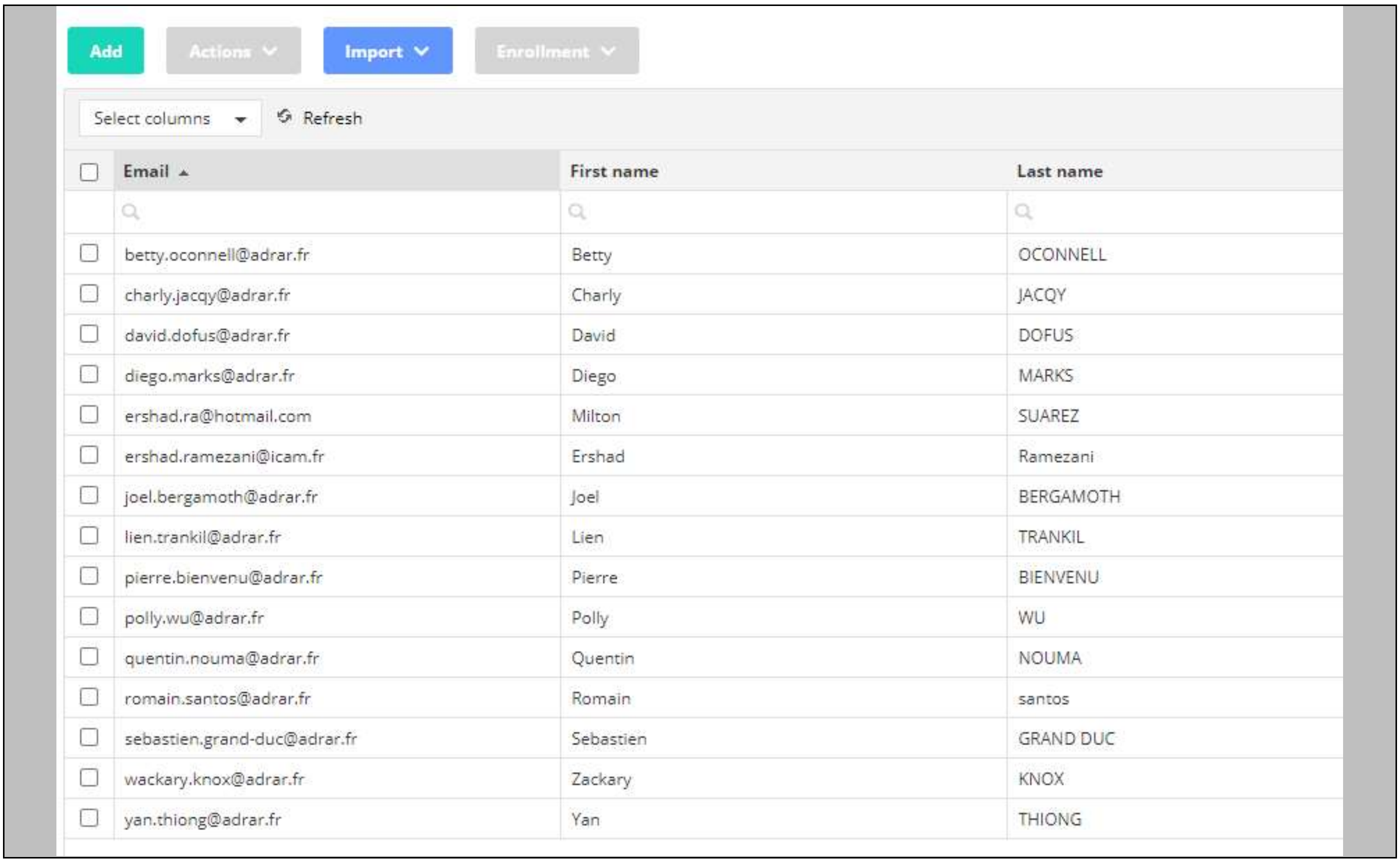
Download and run the connector on any computer running Windows with .NET4.6 installed and connected to the domain. You may schedul

Name	Date modified	Type	Size
mdadconnector.exe	12/24/2022 19:50	Application	56 KB
mdadconnector.exe.config	12/24/2022 19:50	Configuration Sou...	1 KB
Newtonsoft.Json.dll	12/24/2022 19:50	Application extens...	686 KB
users.xml	12/24/2022 19:50	XML File	2 KB

C:\Users\Administrator\Desktop\MiradoreConnectorForMicrosoftActiveDirectory\mdadconnector.exe

```
Miradore Connector for Microsoft Active Directory
Version: 1.4.0.0

Getting users from ''
WARNING: Email not configured, skipping user: LDAP://CN=Administrator,CN=Users,DC=adrarform,DC=local
WARNING: Email not configured, skipping user: LDAP://CN=testuser,CN=Users,DC=adrarform,DC=local
WARNING: Email not configured, skipping user: LDAP://CN=Alee,OU=adrarform,DC=adrarform,DC=local
WARNING: Email not configured, skipping user: LDAP://CN=Sdurand,OU=ou-tssr-2001,OU=Students,OU=adrarform,DC=adra
=local
WARNING: Email not configured, skipping user: LDAP://CN=Jdoe,OU=Teachers,OU=adrarform,DC=adrarform,DC=local
WARNING: Email not configured, skipping user: LDAP://CN=Jsmith,OU=Teachers,OU=adrarform,DC=adrarform,DC=local
WARNING: Email not configured, skipping user: LDAP://CN=Bjohnson,OU=Teachers,OU=adrarform,DC=adrarform,DC=local
WARNING: Email not configured, skipping user: LDAP://CN=Abrown,OU=Teachers,OU=adrarform,DC=adrarform,DC=local
WARNING: Email not configured, skipping user: LDAP://CN=Cjones,OU=Teachers,OU=adrarform,DC=adrarform,DC=local
Total 23 users found, skipped 9 of them because email was not configured
```



☐	Email ▲	First name	Last name
☐	betty.oconnell@adrar.fr	Betty	OCONNELL
☐	charly.jacqy@adrar.fr	Charly	JACQY
☐	david.dofus@adrar.fr	David	DOFUS
☐	diego.marks@adrar.fr	Diego	MARKS
☐	ershad.ra@hotmail.com	Milton	SUAREZ
☐	ershad.ramezani@icam.fr	Ershad	Ramezani
☐	joel.bergamoth@adrar.fr	Joel	BERGAMOTH
☐	lien.trankil@adrar.fr	Lien	TRANKIL
☐	pierre.bienvenu@adrar.fr	Pierre	BIENVENU
☐	polly.wu@adrar.fr	Polly	WU
☐	quentin.nouma@adrar.fr	Quentin	NOUMA
☐	romain.santos@adrar.fr	Romain	santos
☐	sebastien.grand-duc@adrar.fr	Sebastien	GRAND DUC
☐	wackary.knox@adrar.fr	Zackary	KNOX
☐	yan.thiong@adrar.fr	Yan	THIONG

Android Enterprise

Some MDM platforms offer app wrapping, which provides a secure wrapper on mobile apps and enables IT to enforce strong security controls. For Android devices, organizations can use Android Enterprise, Google's enterprise mobility program that integrates with EMM (Enterprise Mobility Management) and MDM platforms.

Android Enterprise is a set of tools and services provided by Google to help businesses manage and secure Android devices. It provides a range of features that allow businesses to set up and manage devices in a way that is tailored to their specific needs.

Two ways to use Android Enterprise

There are two main ways that businesses can use Android Enterprise to manage and secure devices:

1. **Device owner mode**: This mode is used to manage corporate-owned devices, such as those provided to employees as part of their job. In device owner mode, the business has full control over the device, including the ability to install and remove apps, set policies, and enforce security measures.
2. **Profile owner mode**: This mode is used to manage personally-owned devices that are being used for work purposes. In profile owner mode, the business can create a separate, secure, and managed space on the device called a "work profile," which is used to store and manage work-related apps and data. The employee's personal apps and data are kept separate from the work profile.

Work profile

Work profile is a specific feature of Android Enterprise that allows businesses to create a separate, secure, and managed space on an employee's personal device. Work profile is typically used in conjunction with profile owner mode, but it can also be used in other Android Enterprise modes, such as device owner mode.

Managed Google Play Enterprise

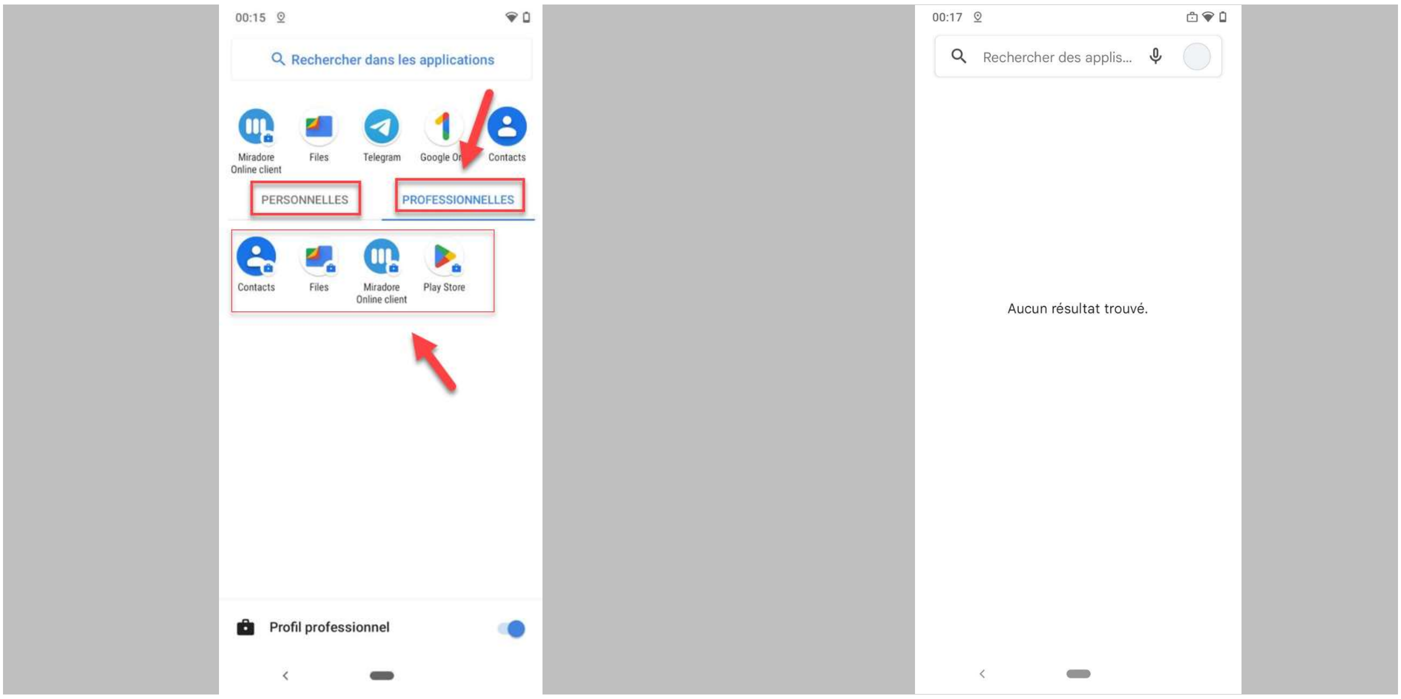
Managed Google Play is a feature of Android Enterprise that allows businesses to securely distribute and manage apps on Android devices. It is a private version of the Google Play Store that is only available to businesses, and it allows businesses to control which apps are available to their employees and how they can be used.

La version complète est disponible aussi mais protéger par un mot de passe.

Merci de me contacter par email :

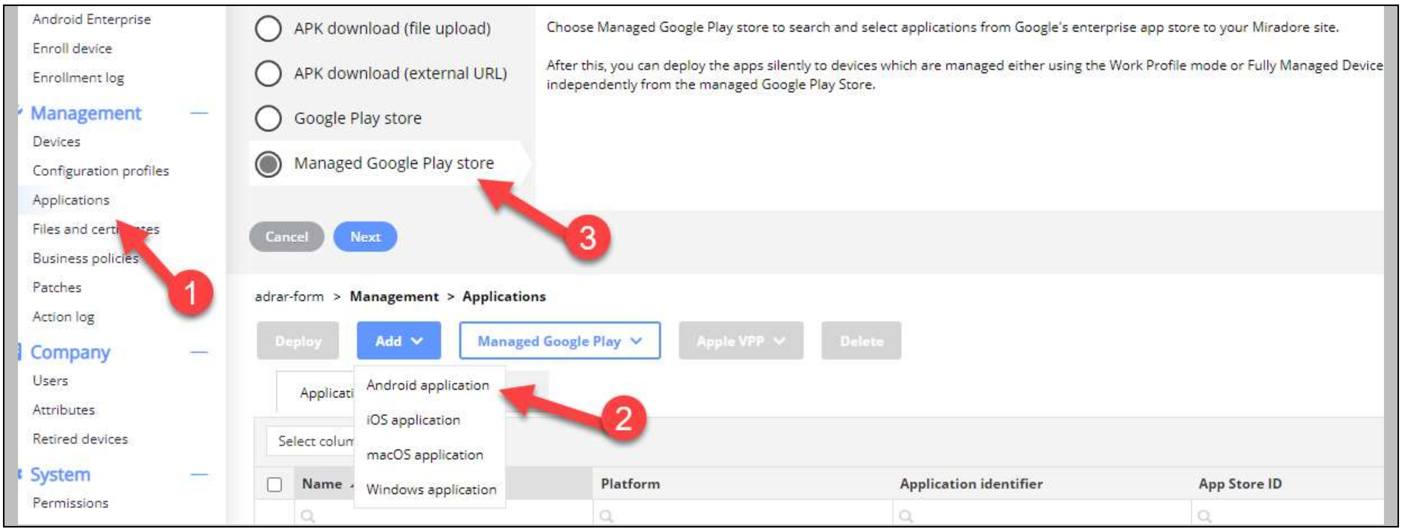
Ershad.ra@gmail.com

However, upon accessing the managed google play app, the user will not find any available applications (although they still have access to their personal profile google play app). To make our previously created managed google play enterprise apps available to this user's device, we need to assign them.



Allow app installation for profile owner

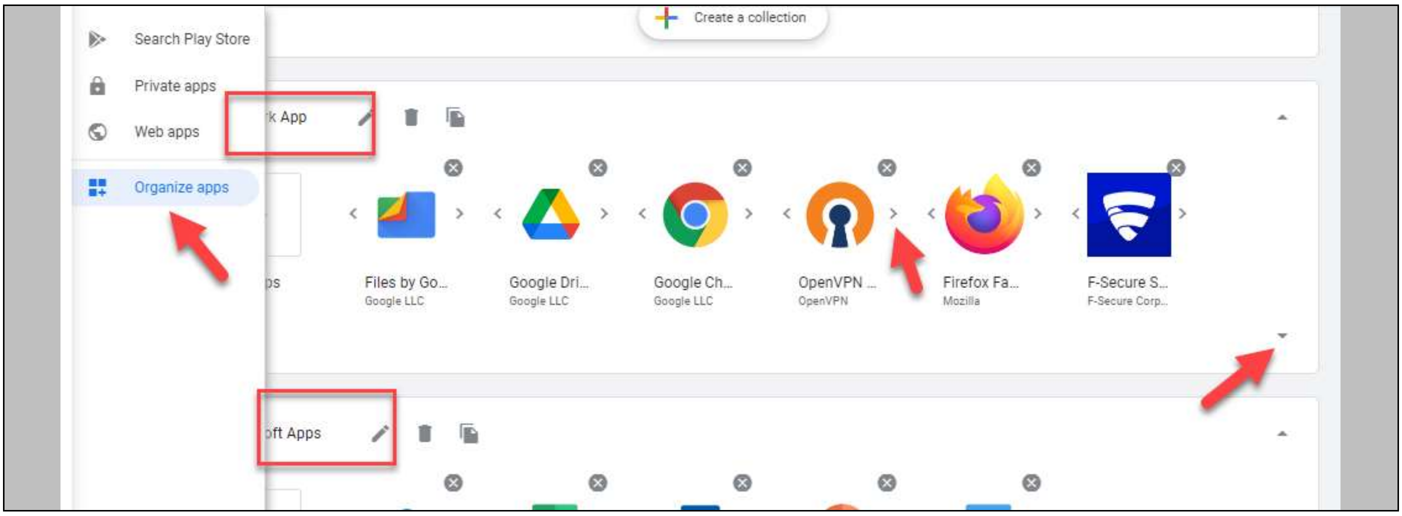
To do so, click on add > android application > managed google play store:



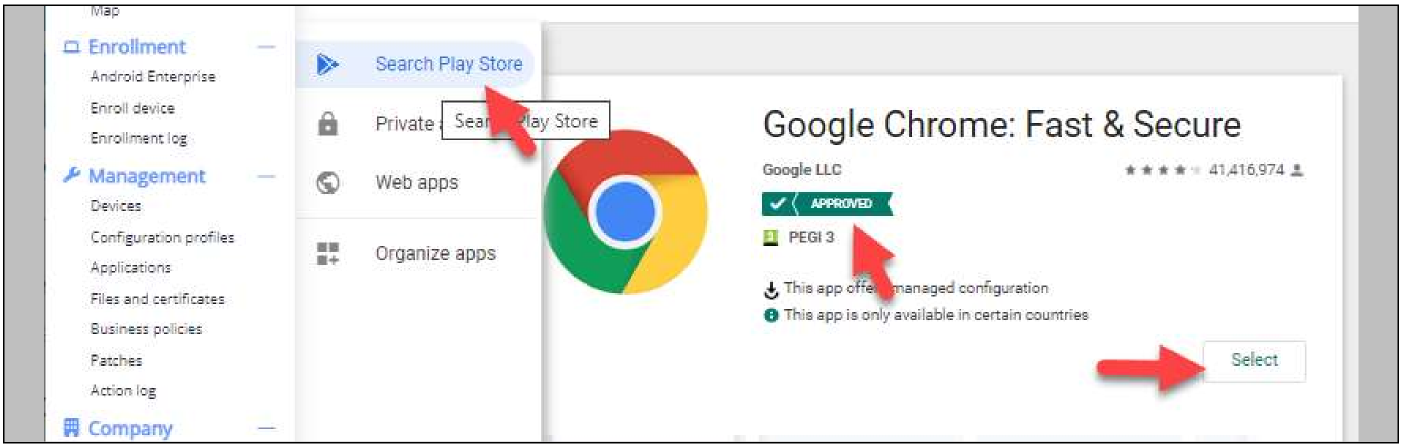
Choose Managed Google Play store to search and select applications from Google's enterprise app store to your Miradore site.

After this, you can deploy the apps silently to devices which are managed either using the Work Profile mode or Fully Managed Device independently from the managed Google Play Store.

If you click on the Next button, you will be redirected to your managed Google Play account. Once there, you can access the "organize apps" option from the side bar. Within this menu, you will see the collections that were previously created. You have the ability to rearrange the collections or the apps within each collection.



First, access the search function on the play store. Next, type in and select the desired app(s) you want to make available to users. For instance, I selected the Chrome browser. Then, click on the "select" button. As shown, the Chrome app has already been approved by us.



Google Chrome: Fast & Secure

Google LLC

41,416,974

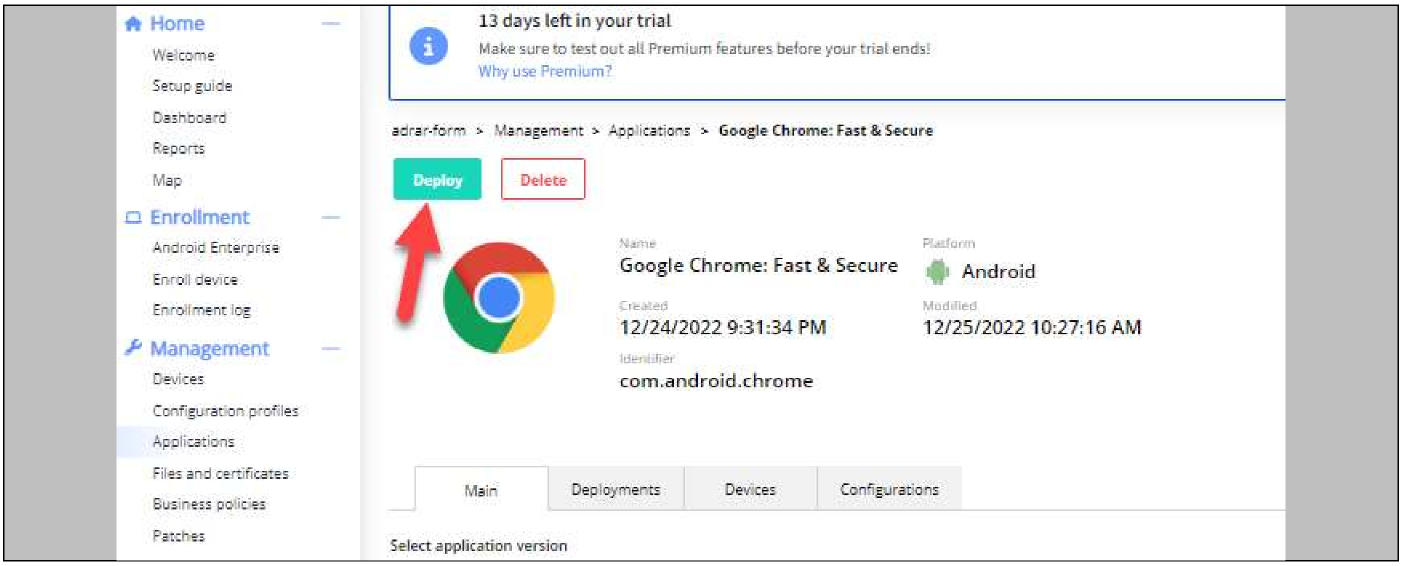
APPROVED

PEGI 3

This app offers managed configuration

This app is only available in certain countries

By clicking on the "select" button, we have added this app to our list of available apps in Miradore. From here, we have the option to deploy or allow the installation of this app to users through the managed Google Play app. Additionally, we can directly deploy this app to a user's device from this location.



13 days left in your trial

Make sure to test out all Premium features before your trial ends!

Why use Premium?

adrar-form > Management > Applications > Google Chrome: Fast & Secure

Name
Google Chrome: Fast & Secure

Platform
Android

Created
12/24/2022 9:31:34 PM

Modified
12/25/2022 10:27:16 AM

Identifier
com.android.chrome

Select application version

For the other applications we approved and added to collections earlier, follow the same process. You have the option to deploy them directly to one or multiple devices, or allow users to install them through the managed Google Play app.