

Module 12

# MOBILE DEVICE SECURITY

CERTIFIED CYBERSECURITY TECHNICIAN

# INDEX

**Module 12:**  
**Mobile Device Security**

**Exercise 1:**  
Implement Enterprise Mobile Security using Miradore MDM Solution

---

**04**

## LAB SCENARIO

With the introduction of mobile phones in enterprises, enterprise security has become more complex. Enterprise mobile security is a major challenge for organizations. Therefore, it is important for organizations to address these security concerns to effectively manage the security of mobile devices.

A security professional must have the required knowledge to implement mobile device security to prevent critical assets and sensitive information from theft and unauthorized access.

## LAB OBJECTIVE

The objective of this lab is to provide expert knowledge in implementing mobile device security. This includes knowledge of the following tasks:

- Implementation of mobile device security using Miradore MDM Solution

## OVERVIEW OF MOBILE DEVICE SECURITY

The use of mobile devices in work environments has changed the security approach of organizations. It has given rise to a new set of security risks and challenges in organizational security. In addition to mobile device security risks which include weak security systems and insufficient configuration of mobile devices and platforms, enterprise mobile device security faces additional security challenges. Mobile devices are moving targets that can be used outside an organization and its security system, thereby defeating the purpose of preventing security attacks when organizations allow mobile devices at the workplace.

## LAB TASKS

A cyber security professional or a security professional use numerous tools and techniques to configure mobile device security policies. The recommended labs that will assist you in learning the implementation of mobile device security controls include:

### **01** Implement Enterprise Mobile Security using Miradore MDM Solution

**Note:** Turn on **PfSense Firewall** virtual machine and keep it running throughout the lab exercises.

## EXERCISE 1: IMPLEMENT ENTERPRISE MOBILE SECURITY USING MIRADORE MDM SOLUTION

Mobile device management (MDM) solutions are used to deploy, secure, monitor, and manage company-owned and employee-owned devices.

### LAB SCENARIO

Security professionals must use mobile device management (MDM) solutions to control and secure mobile devices. The growing variety of mobile devices such as smartphones, laptops, and tablets has made it difficult for enterprises to formulate policies for the secure management of these devices. MDM solutions help security professionals to handle the devices carefully while reducing the support cost and business discontinuity and mitigating security risks.

### LAB OBJECTIVE

The objective of this lab is to demonstrate how to implement the MDM solution. In this lab, you will learn to:

- Install Miradore online cloud-based MDM solution
- Install Miradore Online Client on Android device
- Enrol device to Miradore account as a User device
- Reset passcode
- Lock a lost device

### OVERVIEW OF MDM

An MDM solution is an application implemented by a security professional to manage, secure, and control mobile devices in a work environment. Among the different enterprise mobile security solutions, MDM has garnered significant attention owing to the implementation of policies such as bring your own device (BYOD) across organizations. The MDM solution encompasses policies aimed at helping companies to handle the devices carefully while reducing the support costs and business discontinuity and mitigating security risks.

**Note:** Turn on **PfSense Firewall** virtual machine and keep it running throughout the lab exercises.

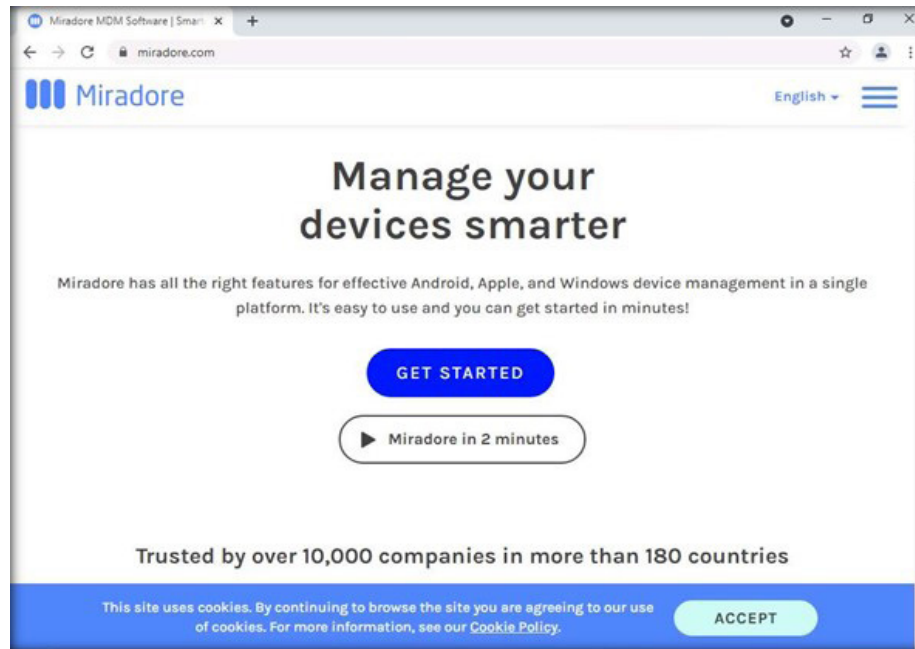
## LAB TASKS

**Note:** Before proceeding with this lab, you **must set up two Gmail** accounts—one for the Administrator, and the other for User.

**Note:** Ensure that the **PfSense Firewall** virtual machine is running.

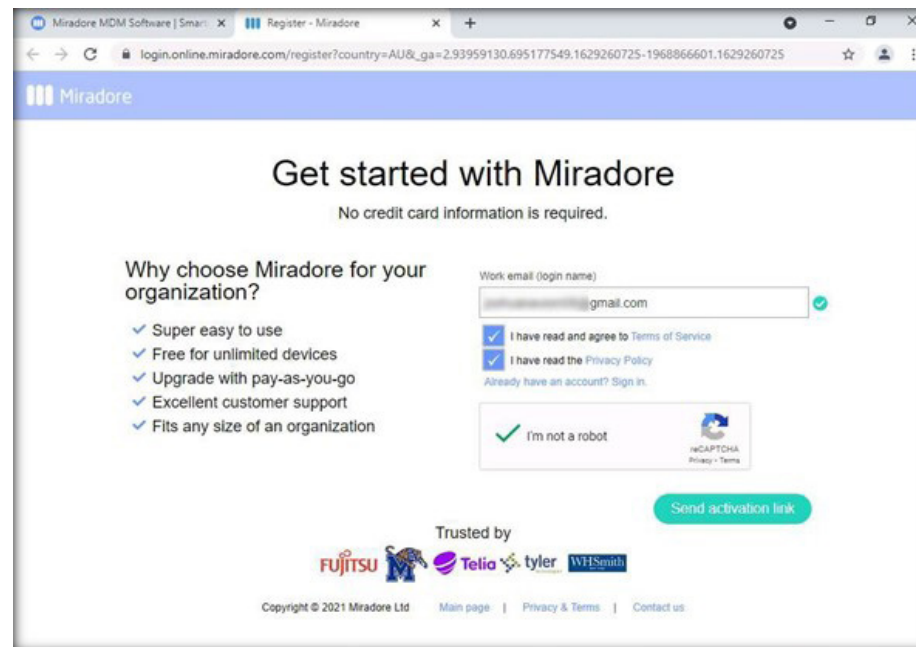
1. Turn on **Admin Machine-1** and **Android Device** virtual machines.
2. Switch to **Admin Machine-1** and log in with the credentials **Admin** and **admin@123**.  
**Note:** If the network screen appears, click **Yes**.
3. To open the browser, double-click on the **Google Chrome** icon on the **Desktop**.
4. After opening the **Google Chrome** browser, place the cursor in the address bar, type **https://www.miradore.com/**, and press **Enter**.  
**Note:** Because this is a third-party tool, the screenshot may differ from the image on your screen in the lab environment. Initially, you have to enter your email address on which Miradore will send the activation link. After clicking on the activation link, you will be directed to the Miradore home page.
5. The Miradore home page appears. Scroll down and click on the **GET STARTED** button (as visible on the page).

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



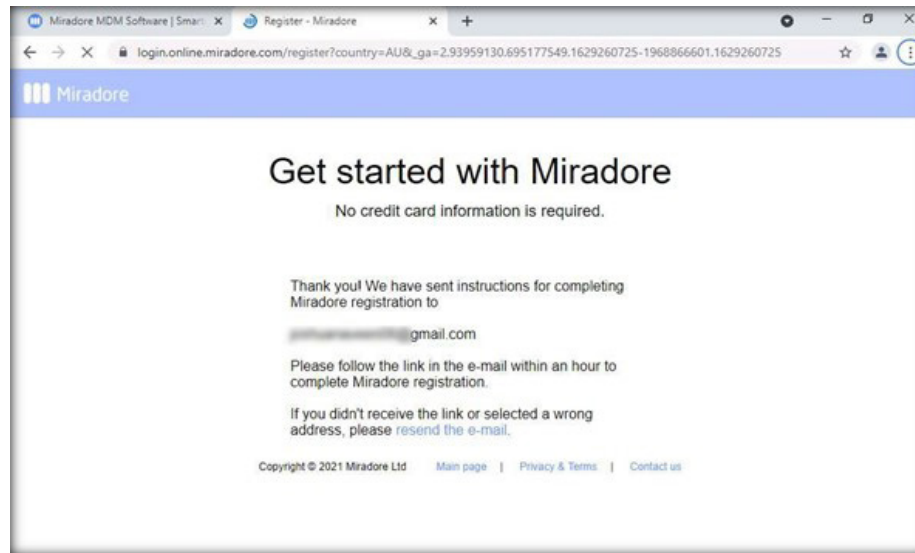
6. The **Get Started with Miradore** page will appear in a new tab. Type your email address and check the **Terms of services**, verify **I am not robot**, and click **Send activation link** button.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



7. The activation link will be sent to your email address.

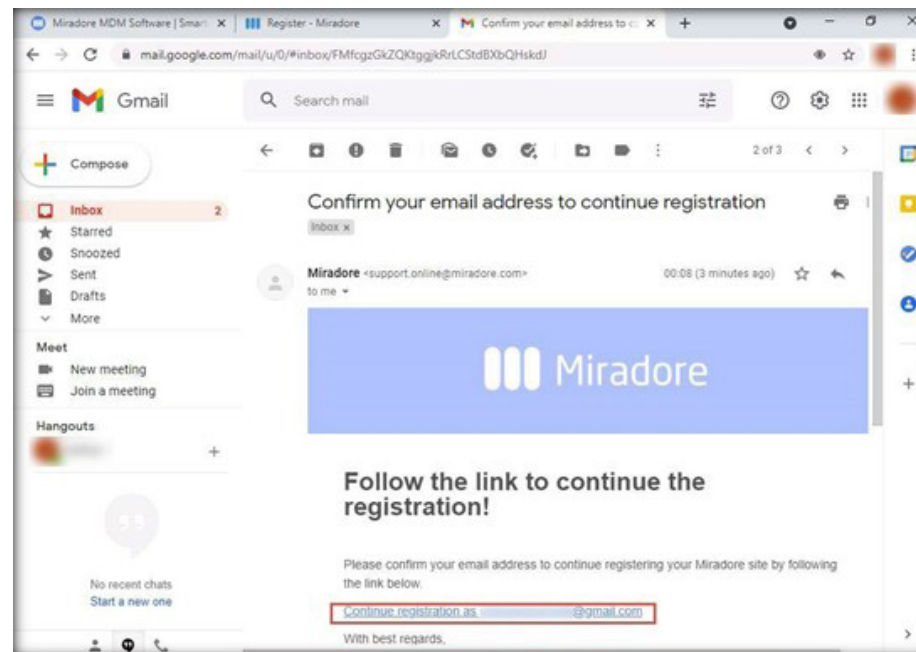
EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION





8. In a new tab, log in to the email account used for Miradore. Open the email received from **Miradore (support.online@miradore.com)**. Click the link given in the mail to continue registration.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



9. The **Get started with Miradore** page will open in a new tab, where you will be required to fill basic details such as Company, Work email, and Password. After completing this process, click on **Start now** to continue.

**Note:** You need to provide a unique company name.

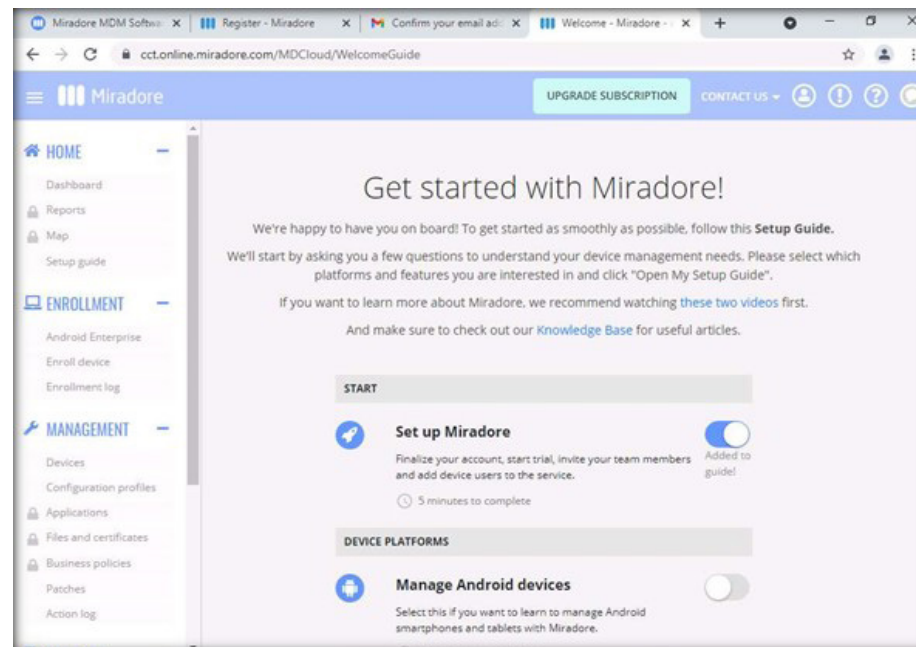
EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION

The screenshot shows a web browser window with the URL `login.online.miradore.com/RegisterConfirm?country=AU&ga=2.181597920.695177549.1629260725-1968866601.16...`. The page content includes:

- Why choose Miradore for your organization?**
  - ✓ Super easy to use
  - ✓ Free for unlimited devices
  - ✓ Upgrade with pay-as-you-go
  - ✓ Excellent customer support
  - ✓ Fits any size of an organization
- Registration Form:**
  - Company \***: CCT
  - Work email (login name) \***: [Redacted]
  - Password \***: [Redacted]
  - Country \***: United Kingdom
  - Phone number**: United Kingdom (+44) [Redacted]
- Additional Options:**
  - Already have an account? [Sign in.](#)
  - I want to subscribe to Miradore's newsletter to receive the latest product updates and news.
- Start now** button (highlighted with a red box).

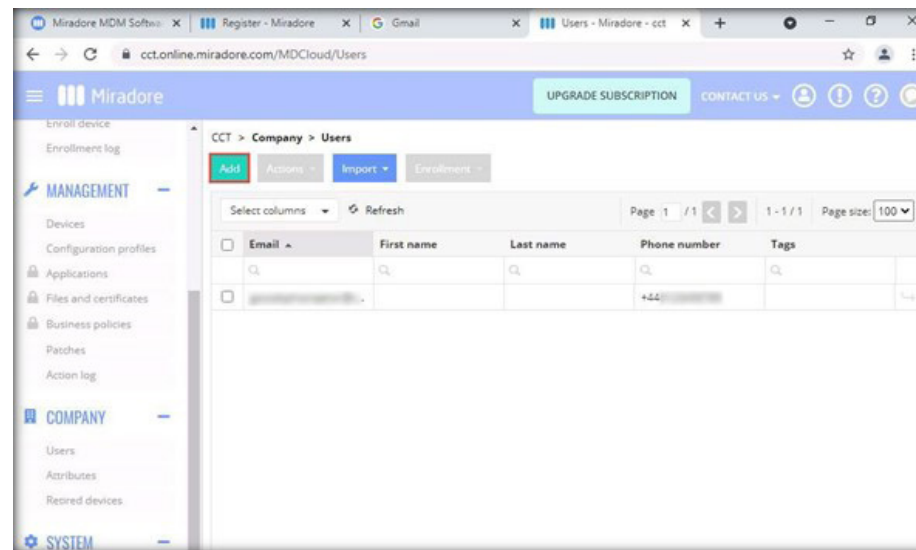
10. Next, you will be redirected to the **Get started with Miradore!** home page.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



11. Navigate to the **Company** menu on the left pane and select the **Users** option. This will open the **your company name > Company > Users** page. Click on the **Add** button.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



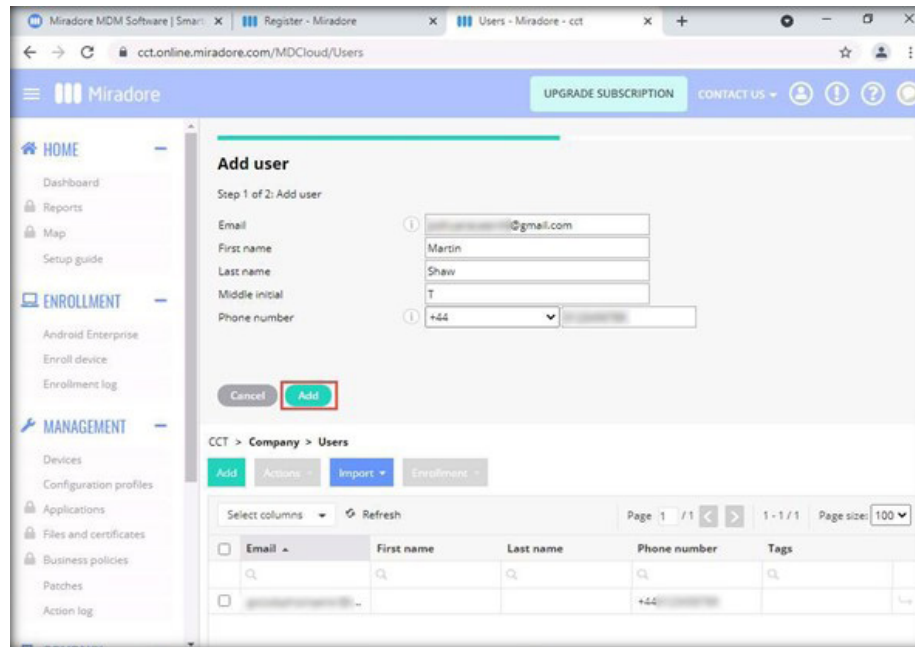
12. The **Add user** pane appears.

13. Type the following details and click **Add**.

**Email:** User email address. (We have two Gmail accounts for the purpose of demonstration; one is for the Admin and the other User. Here, type the Gmail address of User. This account may differ from that of your lab Gmail account.)

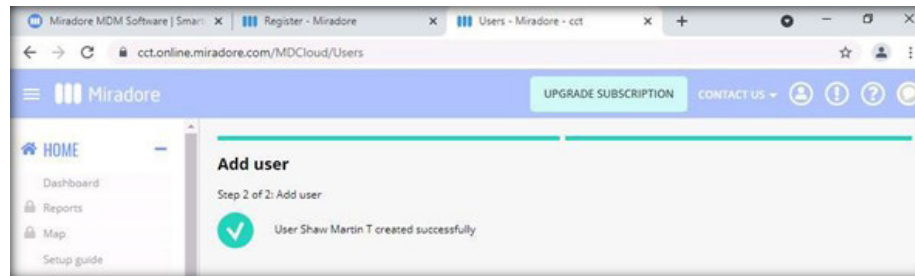
- **First name:** Martin
- **Last name:** Shaw
- **Middle Initial:** T
- **Phone number:** ----

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



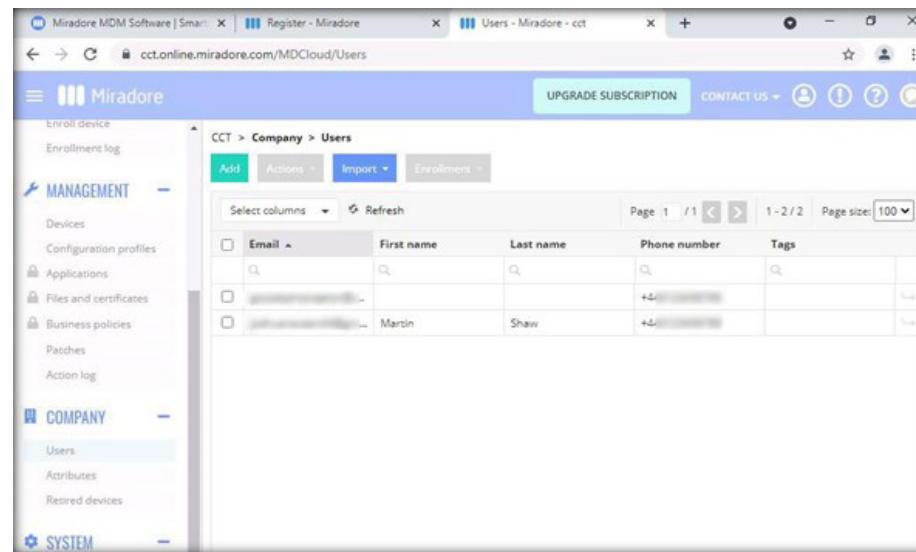
14. The User is created successfully. You can see the status.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



15. Upon clicking **Users** under **Company**, you will see the new user (in this case, **Martin**) added to the users' list.

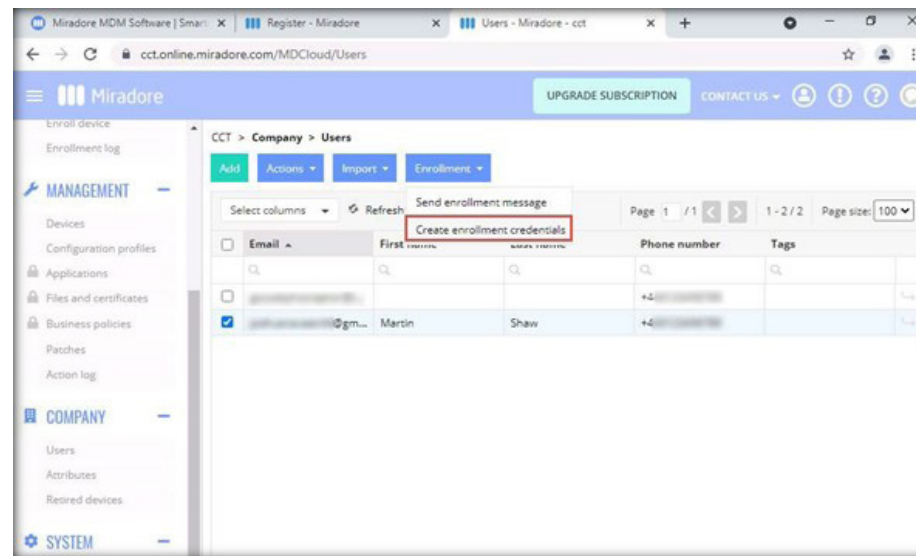
EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION





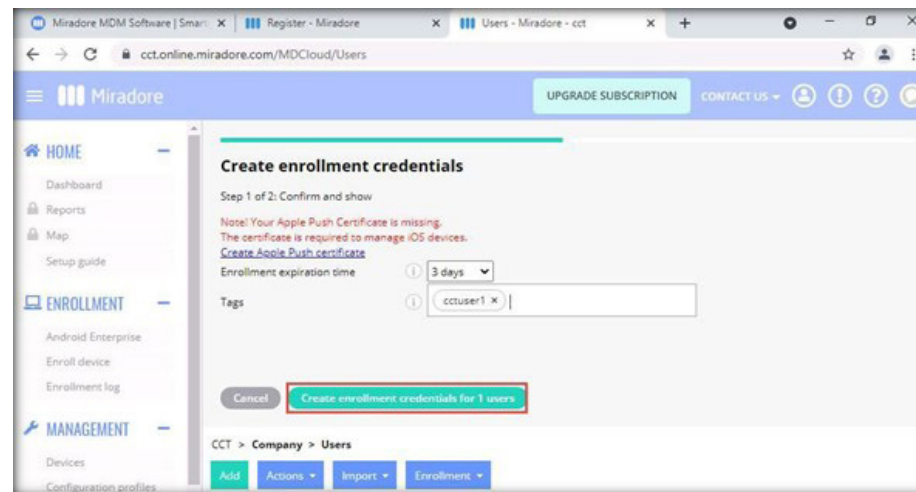
16. Select the newly added user Martin and click on **Enrollment > Create enrollment credentials**.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



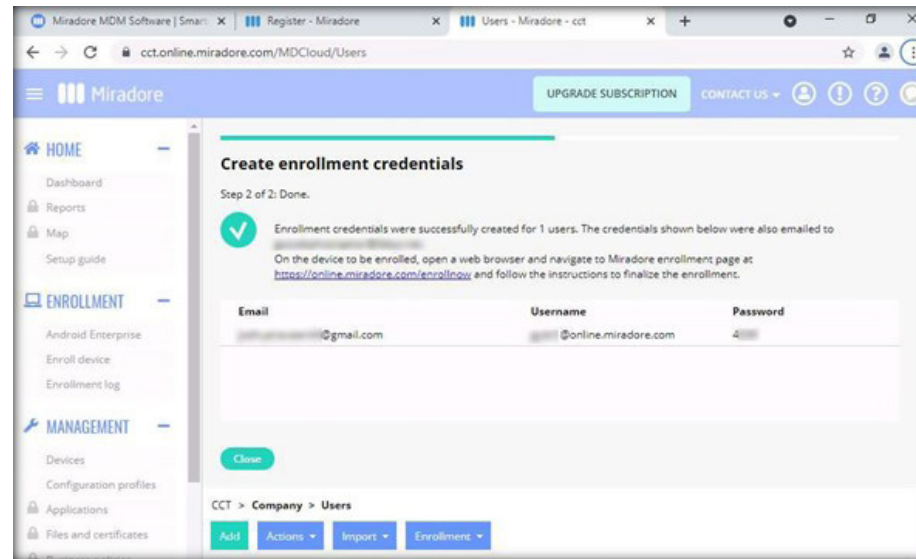
17. Add any tag name (here, it is cctuser1) in the **Tags** field and click on the **Create enrollment credentials for 1 users** button.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



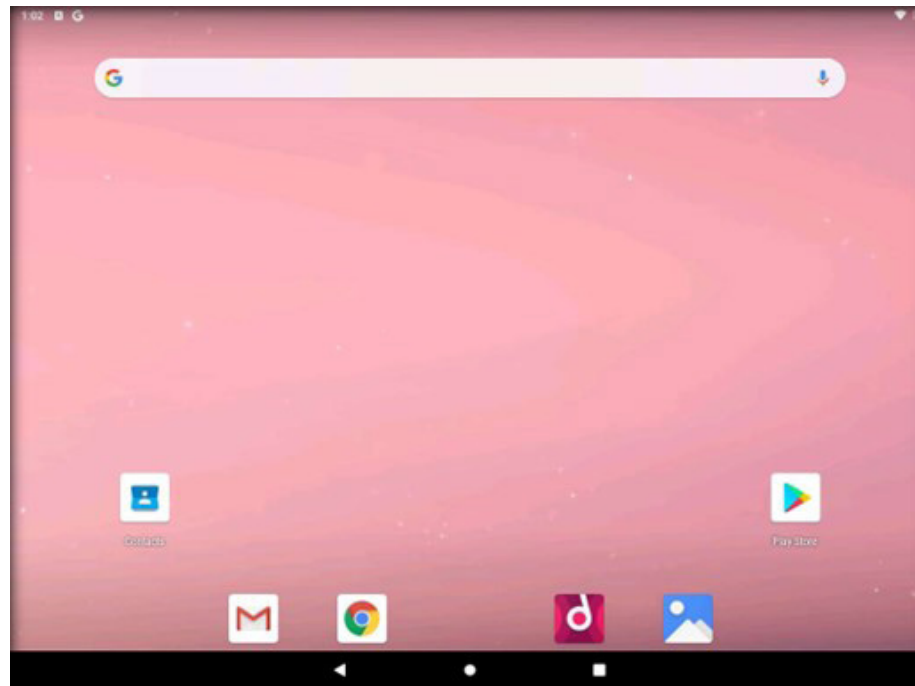
18. Thus, **Username** and **Password** are generated. Copy these credentials or save them on your host machine in any new **text file**.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



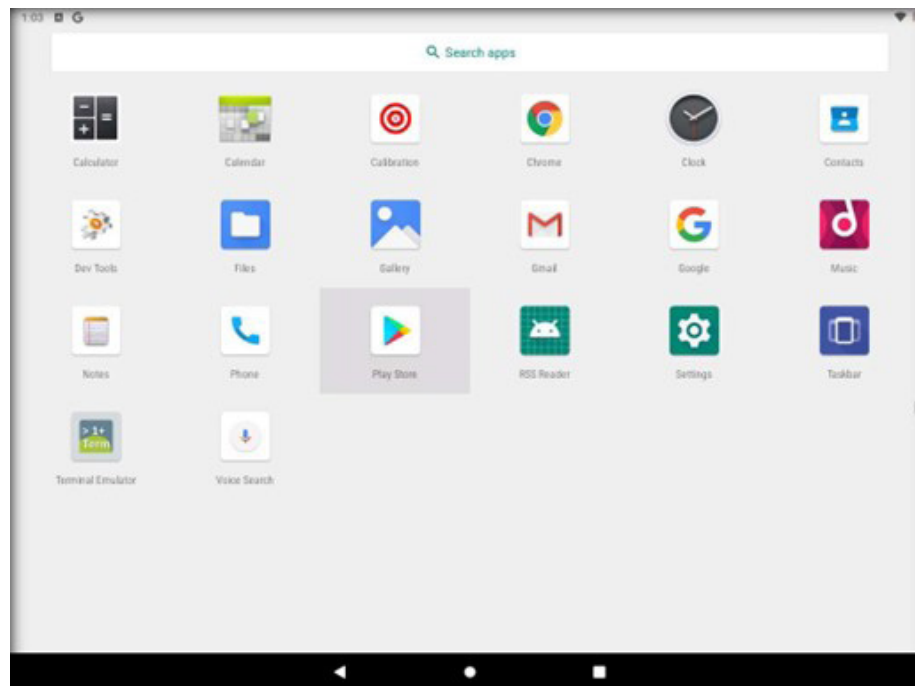
19. Switch to the **Android Device** virtual machine.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



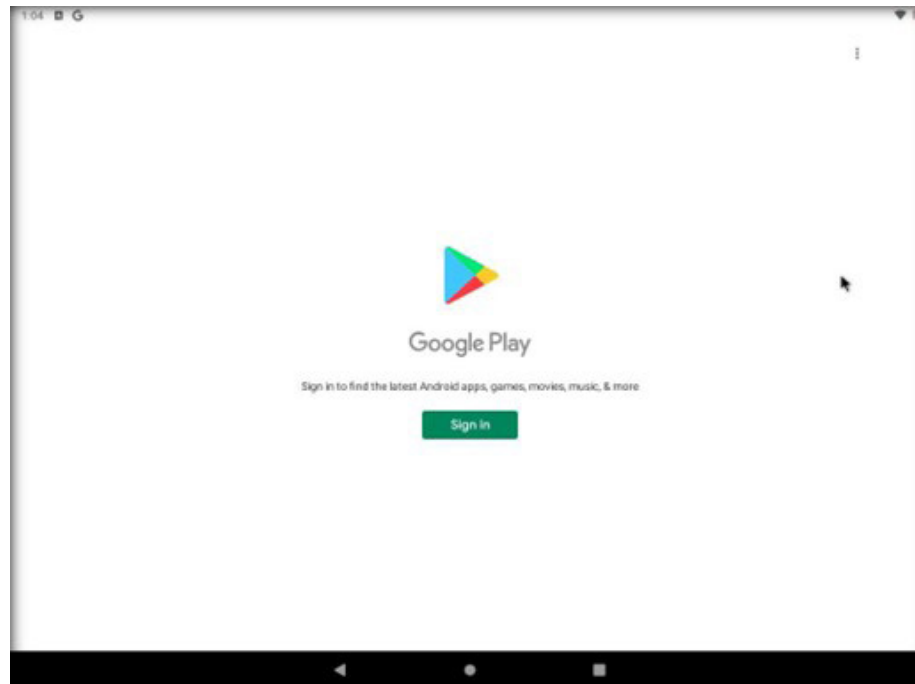
20. **Swipe-up** the Android home screen, which will show all apps. Click on the **Play Store** app.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



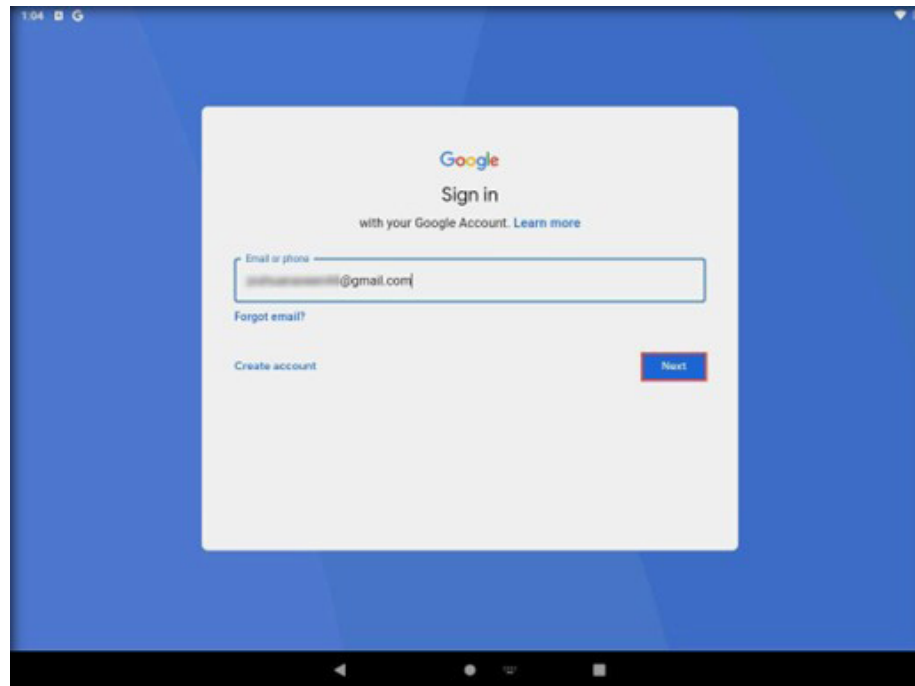
21. The Play Store **Sign in** page appears. Click on **Sign in** to continue.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



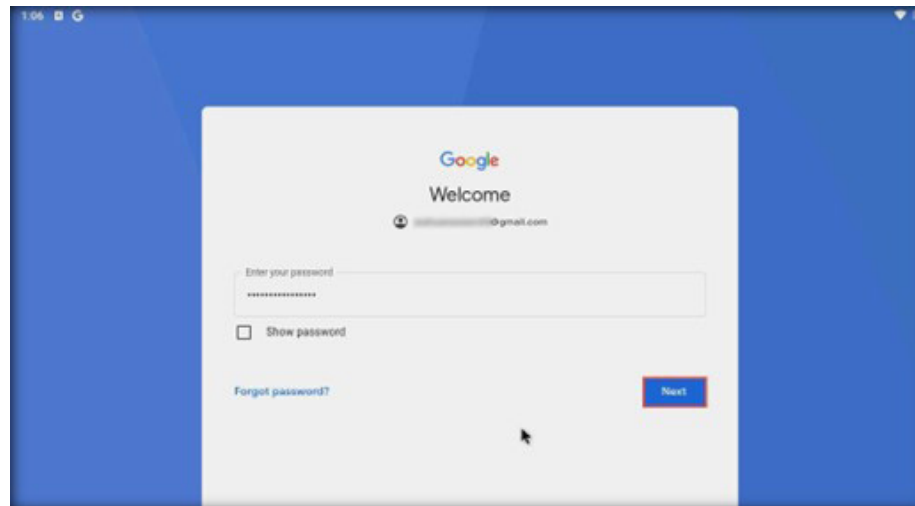
22. Type the Gmail account you have created for User; click **Next**.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



23. On the next screen, type the password of your user Gmail account and click **Next**.

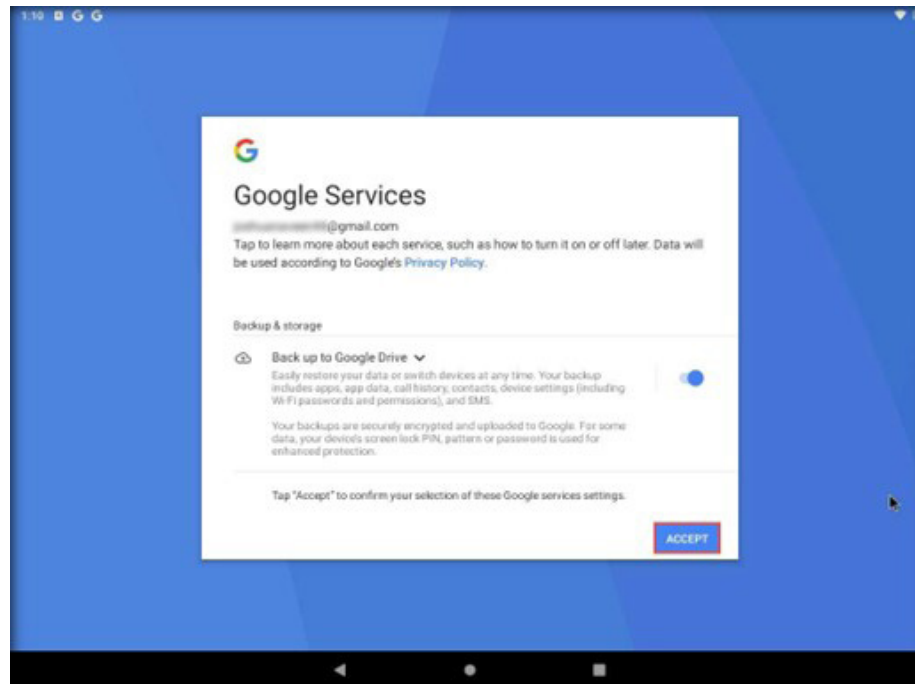
EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION





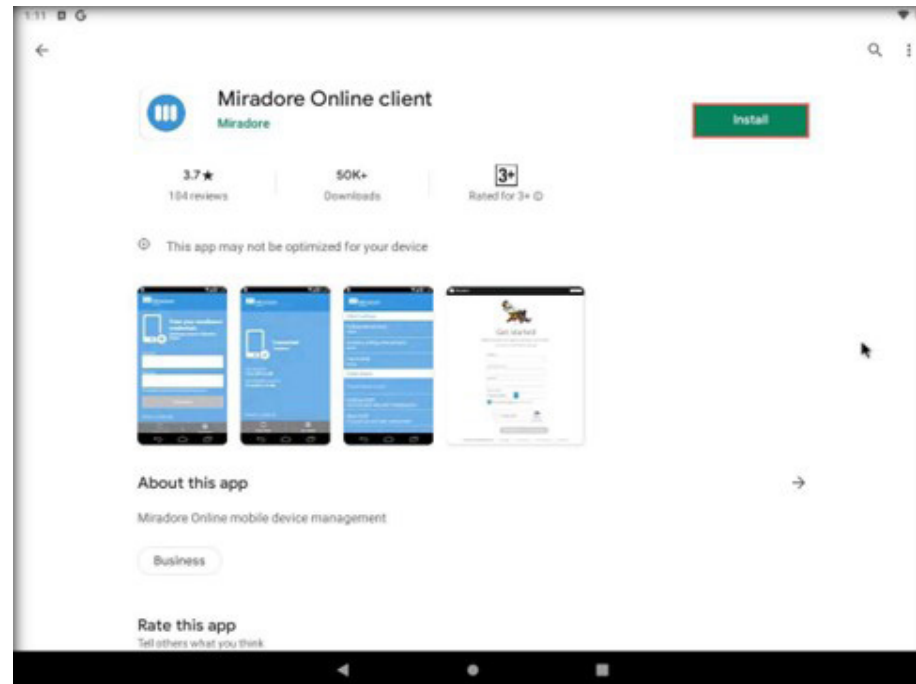
24. The **Google Terms of Service** page appears. Click on **I agree** to continue.
25. On the **Google Services** page, scroll down or click **More**; then, click **ACCEPT**.  
**Note:** If an **Introducing Google Play Points** window appears, click on **Not now**.  
**Note:** If a **You can choose additional search services for your device** page appears, click **No thanks**.

EXERCISE 1:  
 IMPLEMENT ENTERPRISE  
 MOBILE SECURITY  
 USING MIRADORE MDM  
 SOLUTION



26. The **Google Play Store** app opens. Search for **Miradore Online client** in Play Store and select the matched app to continue. Click **Install**.

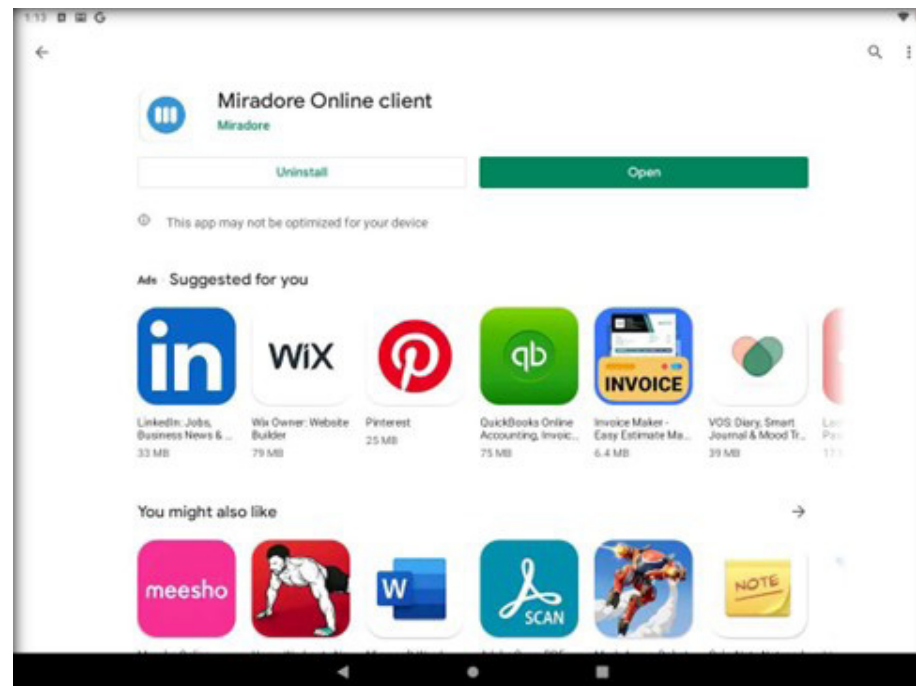
EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



27. After a few seconds, the app will be downloaded and installed automatically. If any popup appears, click **Skip**.

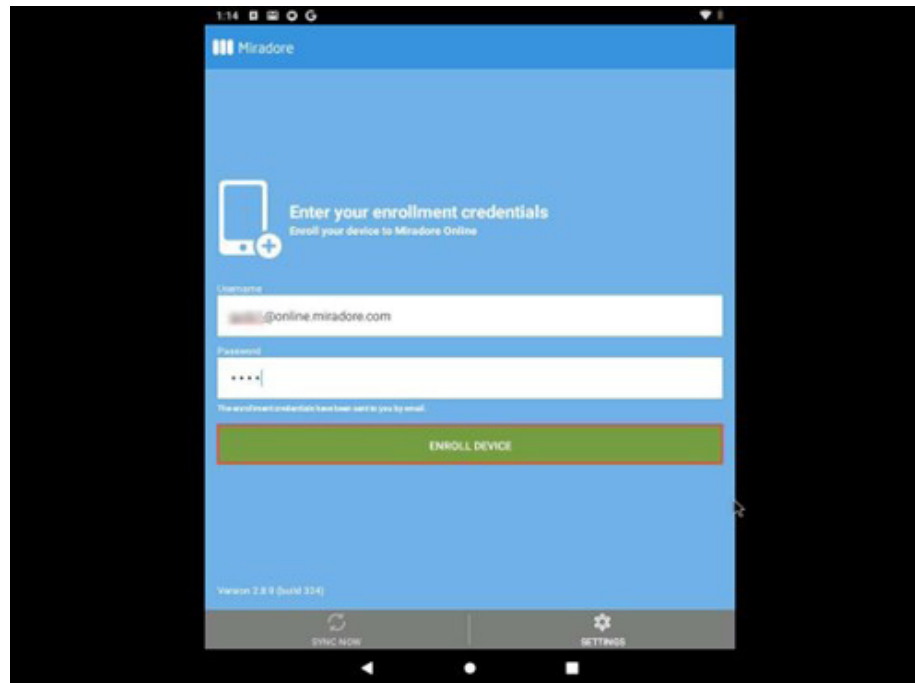
28. After installation, click on **Open**.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



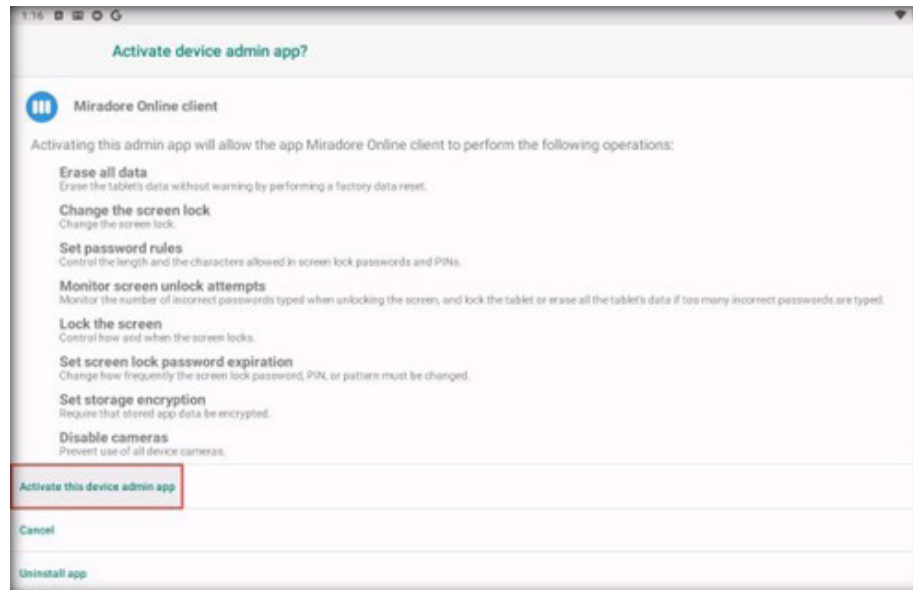
- 29. When the Miradore app screen appears, click **CONTINUE**. If you get a pop-up for permission, click on **ALLOW** for all permissions.
- 30. The **Enter your enrollment credentials** screen appears. Type the user credentials saved in **Step no. 18** and click on **ENROLL DEVICE**.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



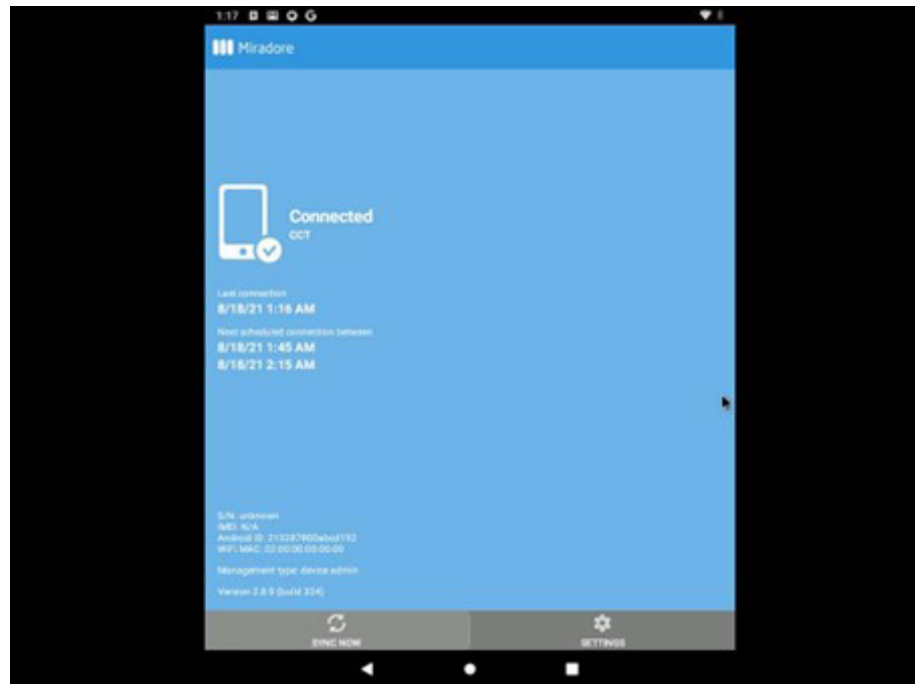
31. The **Activate device admin app?** screen appears. Click the **Activate this device admin app** option.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



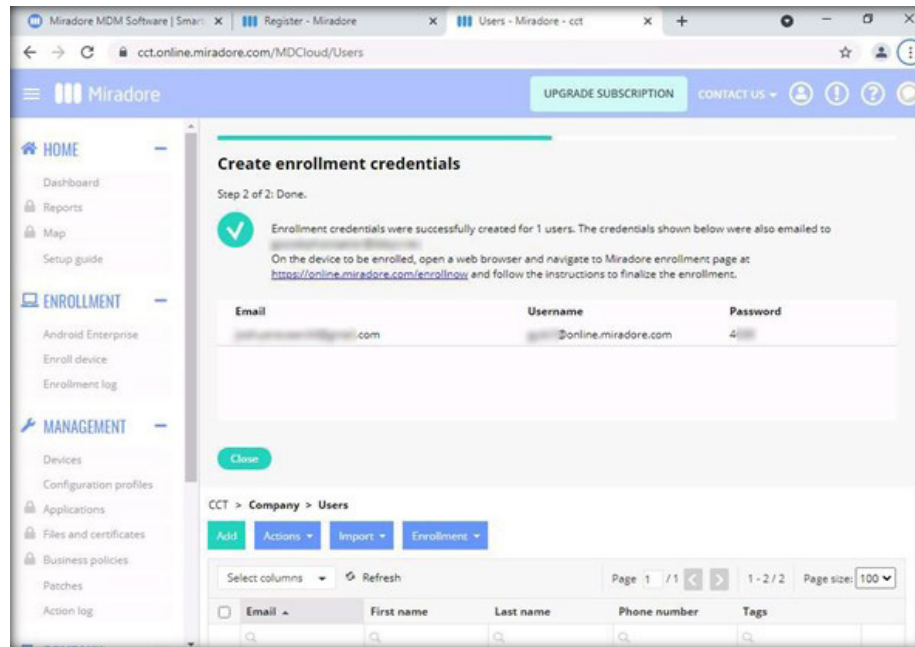
32. The app will show that the connection has been established to the Miradore online cloud-based account. Click on **SYNC NOW**.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



33. Switch back to the **Admin Machine-1** virtual machine and navigate to the opened **Chrome** browser. The Miradore account is already opened.

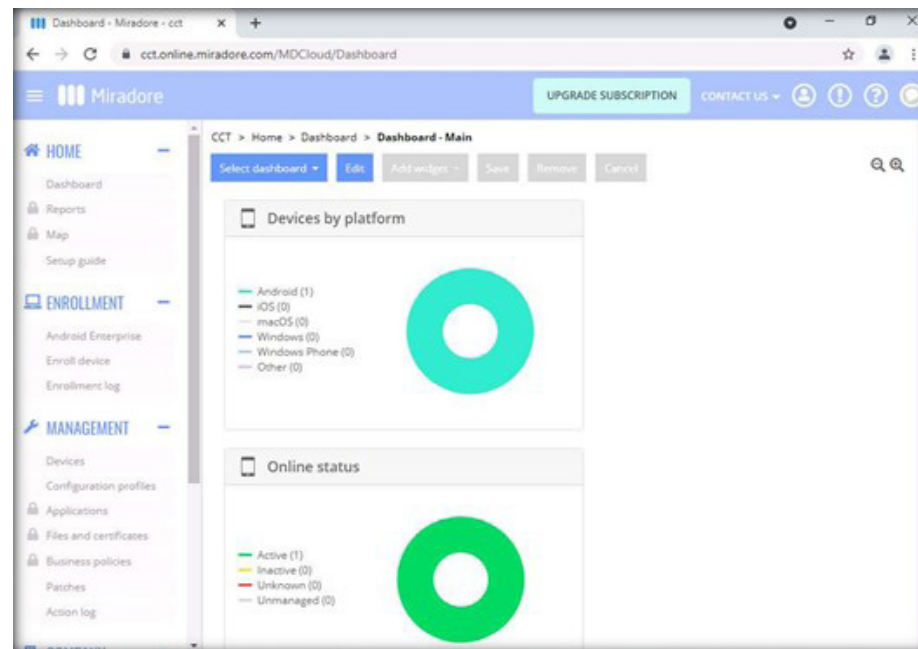
EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



34. Click on the **Dashboard** menu in the left sidebar.

35. The dashboard will show the enrolled device.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION

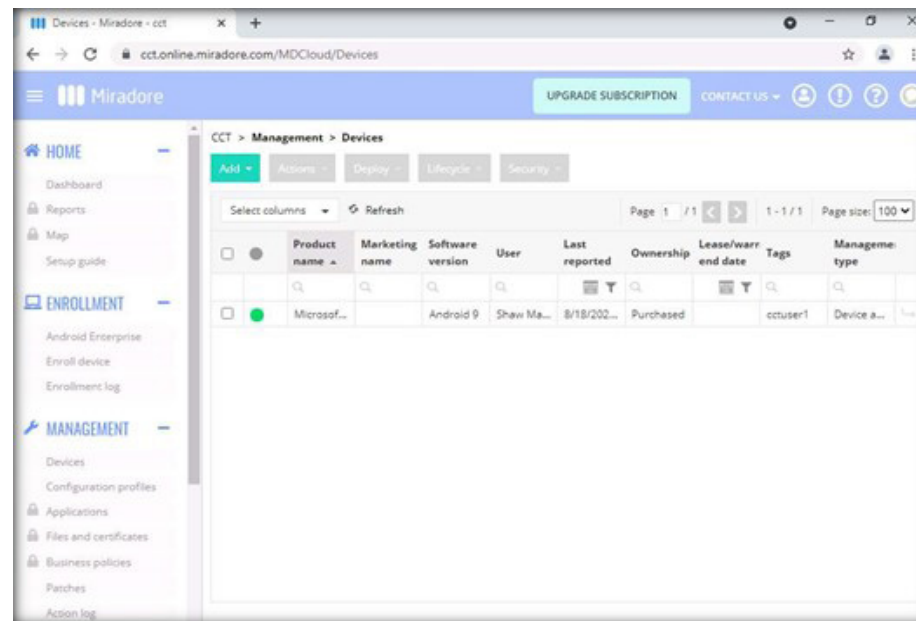




36. A security professional can manage this device online.

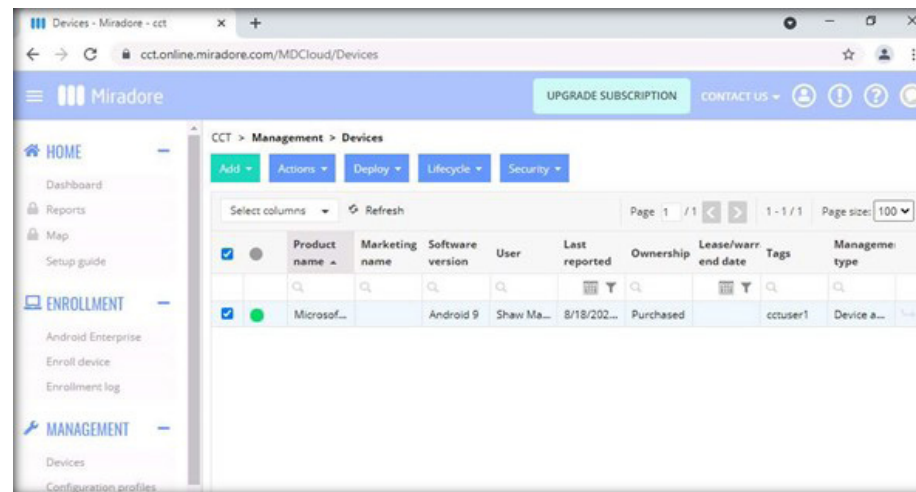
37. To manage the device, go to the **MANAGEMENT** menu and click on **Devices**.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



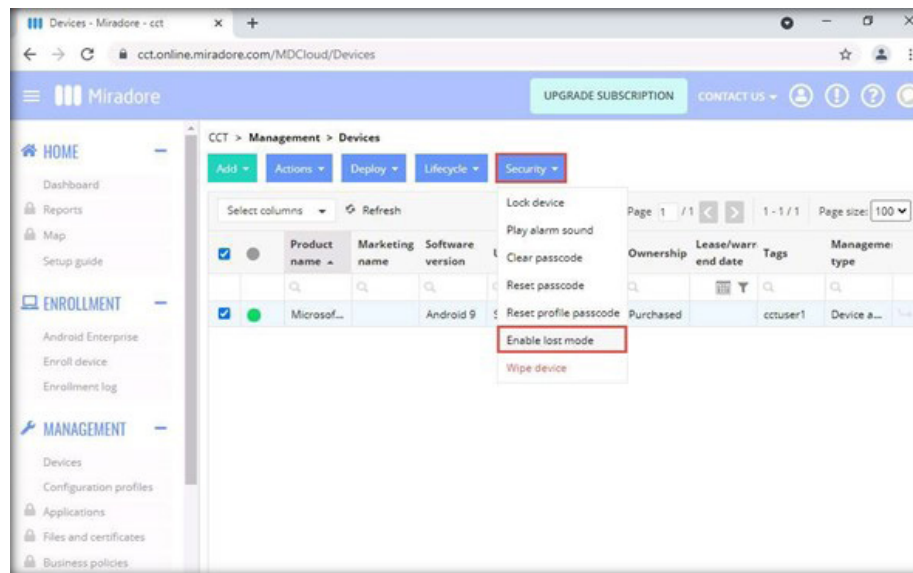
38. The **Devices** screen will show the enrolled devices. In this lab, we added **Microsoft Corporation VM with Android 9**. When you select this device, all related buttons will become visible.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



- 39. If a user loses the device, security professionals will be required to take quick action for the lost device and protect organizational data.
- 40. Admin can enable lost mode to protect the device from any malicious activity.
- 41. Click on the **Security** button and select the **Enable lost mode** option.

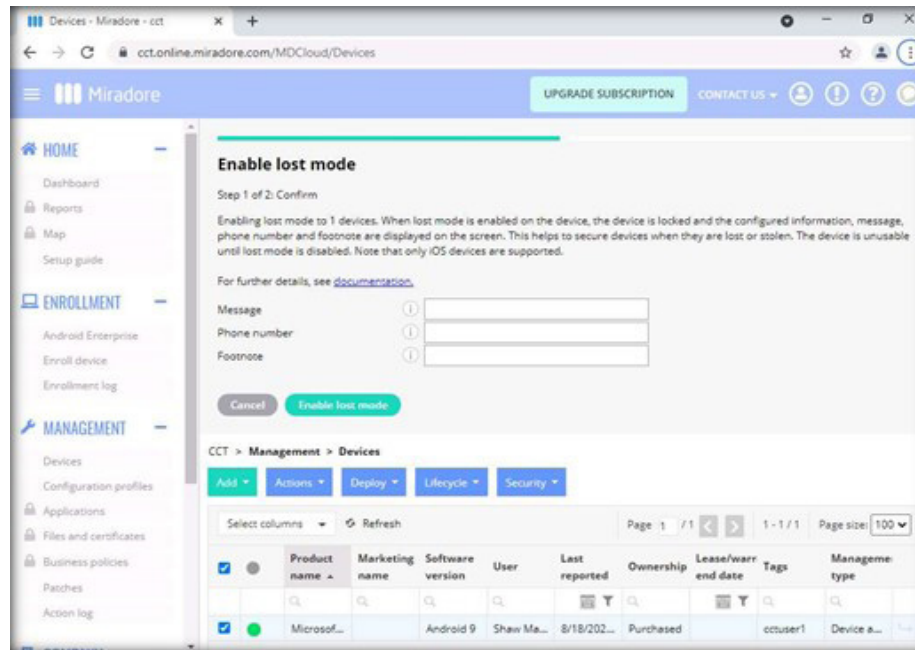
EXERCISE 1:  
 IMPLEMENT ENTERPRISE  
 MOBILE SECURITY  
 USING MIRADORE MDM  
 SOLUTION



42. The **Enable lost mode** page appears; by entering the details in this page and clicking on **Enable lost mode**, you can secure a device when it is stolen or lost, the device will be unusable until the lost mode is disabled.

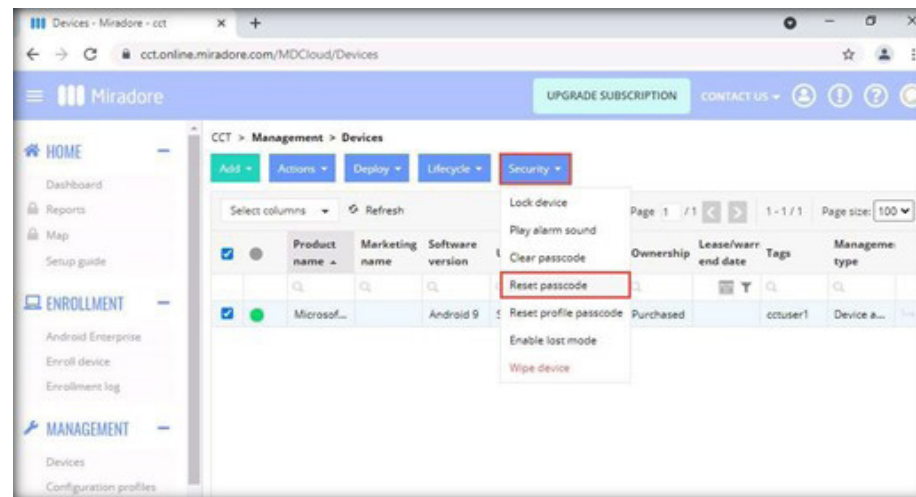
**Note:** Note that only iOS devices are supported by lost mode feature.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



- 43. In case of lost device, the Admin can reset the passcode or lock the device to protect it from any malicious activity.
- 44. To reset the passcode, click on **Devices** option under **Management** menu on the left pane.
- 45. Select the device for the related buttons to be visible, click on **Security** button and select **Reset passcode** option.

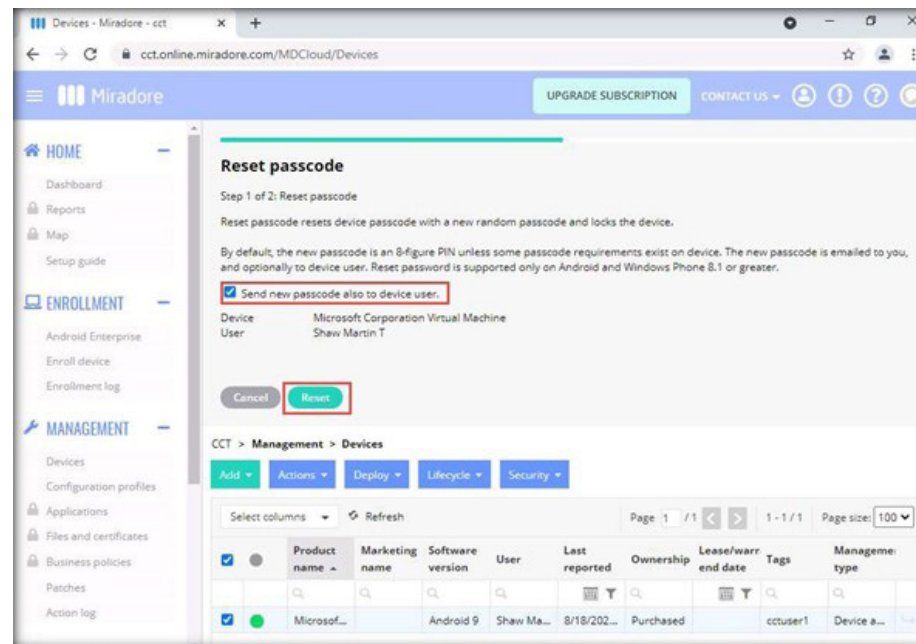
EXERCISE 1:  
 IMPLEMENT ENTERPRISE  
 MOBILE SECURITY  
 USING MIRADORE MDM  
 SOLUTION



46. The **Reset passcode** page appears, check the **Send new passcode also to device user** option and click on **Reset**.

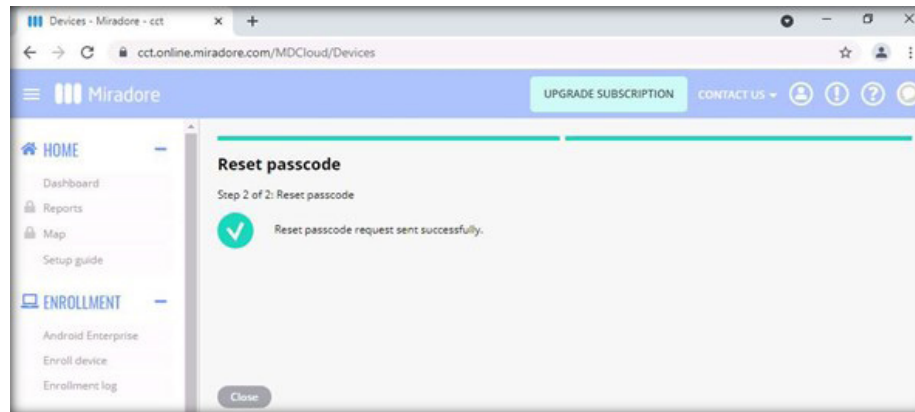
**Note:** Leave it unchecked if you do not want to send the passcode to the user.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



47. You will receive a message on the screen stating that the **Reset passcode request sent successfully.**

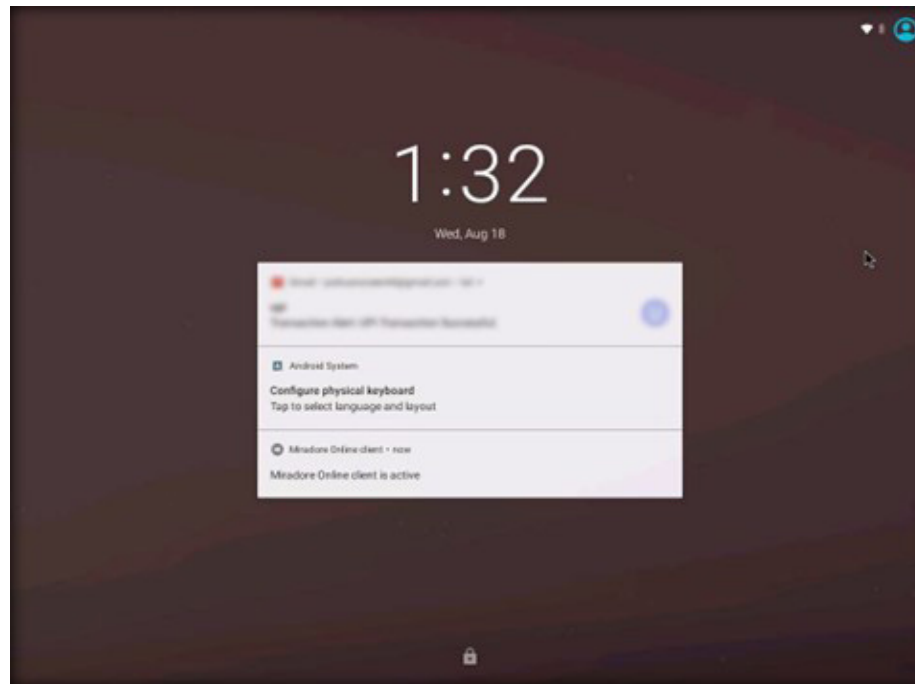
EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



48. Switch to the **Android Device** virtual machine. You can observe that the machine is locked.

**Note:** The device will take some time to lock based on the time it takes to synchronize with the MDM and the internet speed. If the device is taking long time to lock open miradore application and click on **SYNC NOW**.

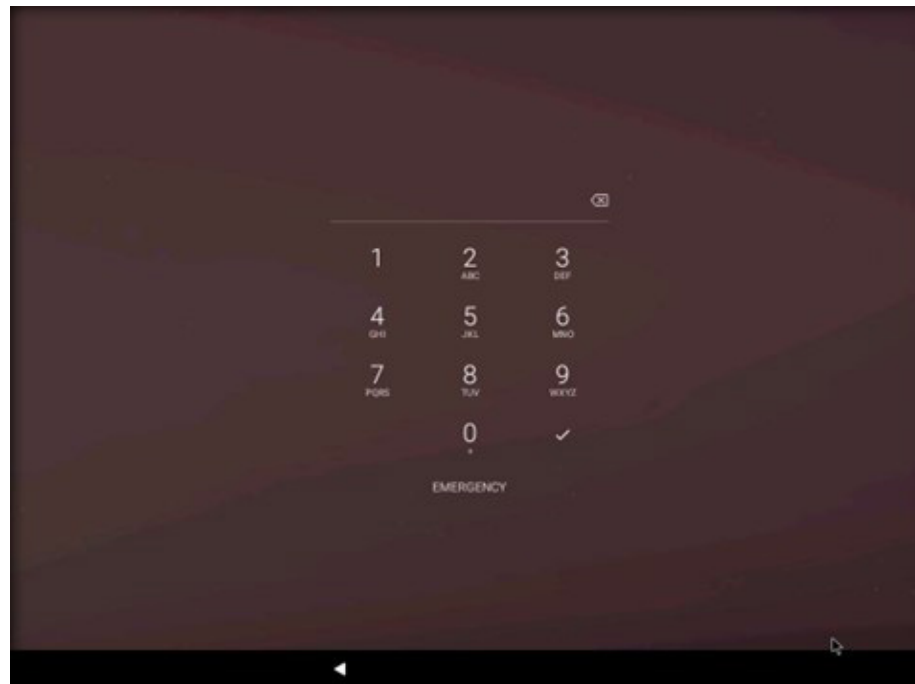
EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION





49. Swipe up to unlock the machine, you need to enter a passcode to unlock.

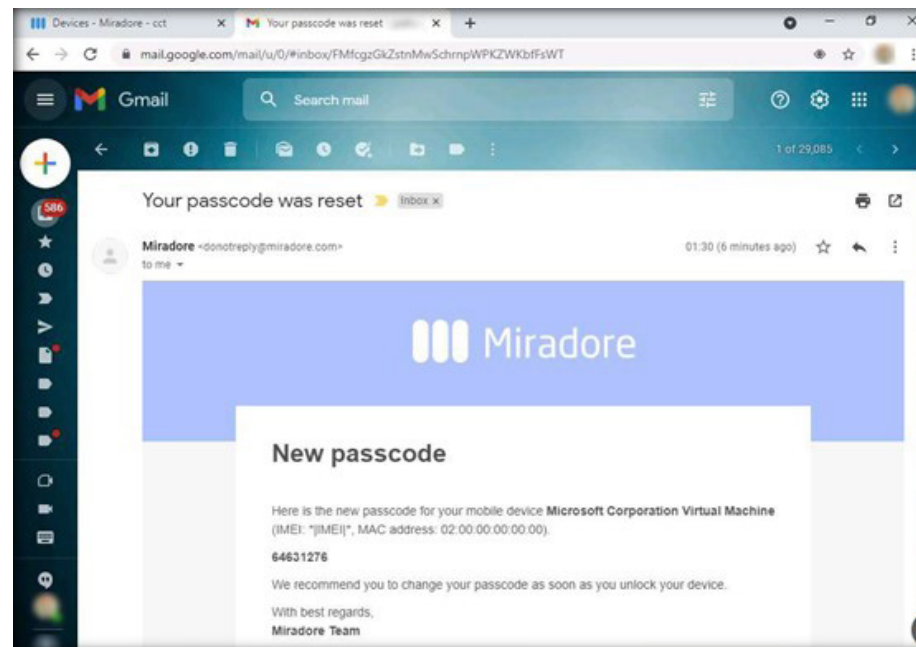
EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



50. Now, switch to the **Admin Machine-1** to virtual machine and login to the user email account. Open mail from miradore you will find the new passcode to unlock the device.

**Note:** Log into the Administrator email account if you have not checked the **Send new passcode also to device user** option in **Step#46**.

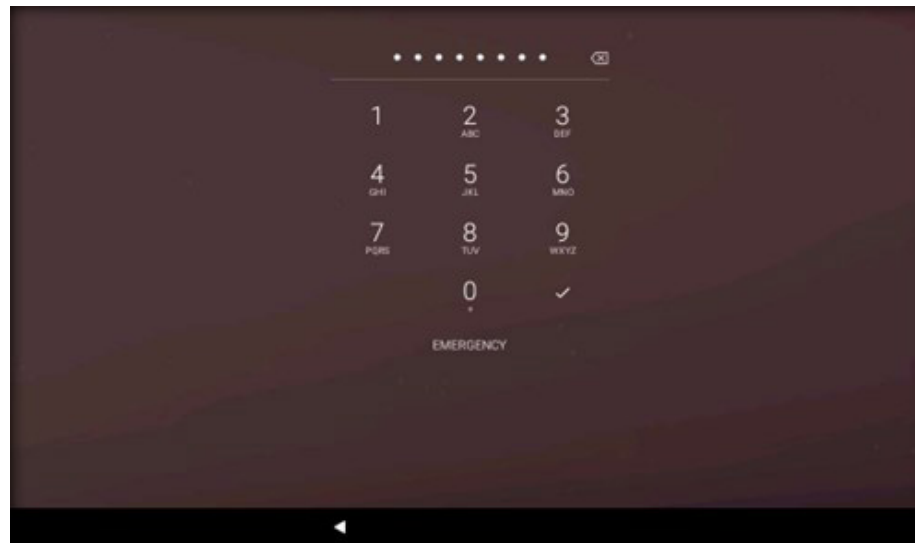
EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



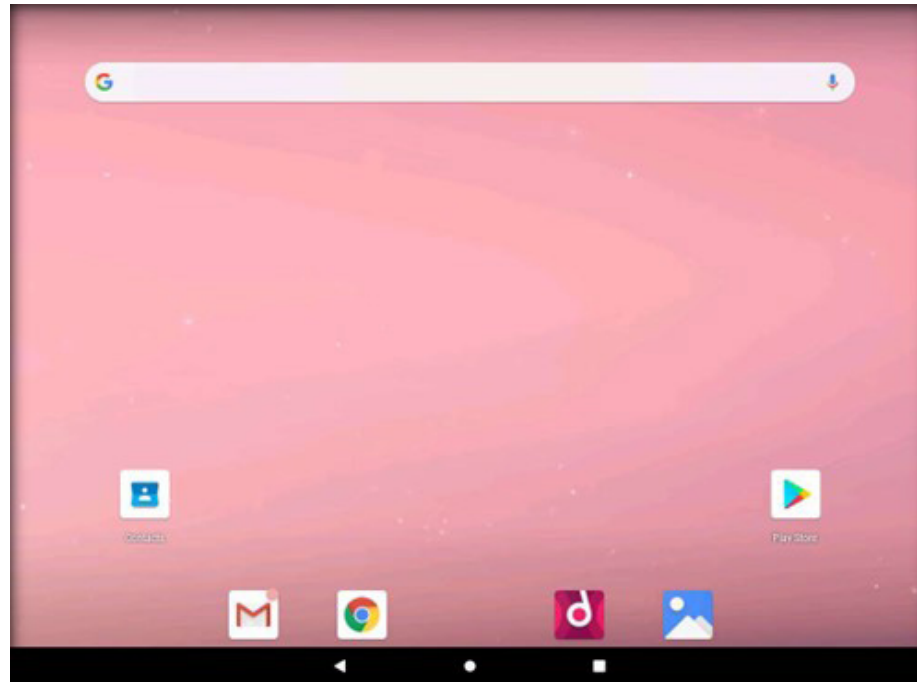
51. Note down the passcode in the host machine and switch back to the **Android Device** virtual machine; enter the passcode and press Enter to unlock the device.

**Note:** If the device is non-responsive reboot it.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION

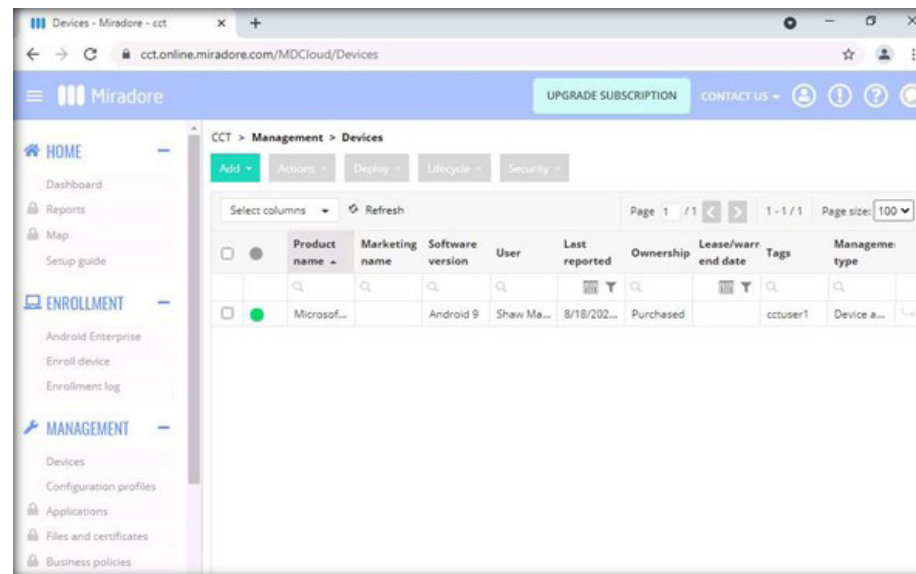


EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



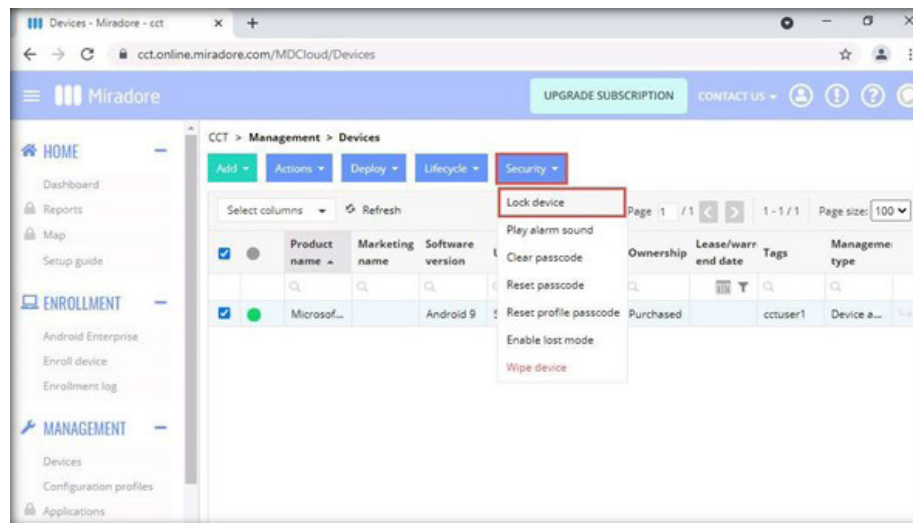
52. Now, to lock the device, switch to the **Admin Machine-1** virtual machine and navigate to the opened **Chrome** browser. The Miradore account is already opened, click on **Devices** option under **Management** menu on the left pane.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



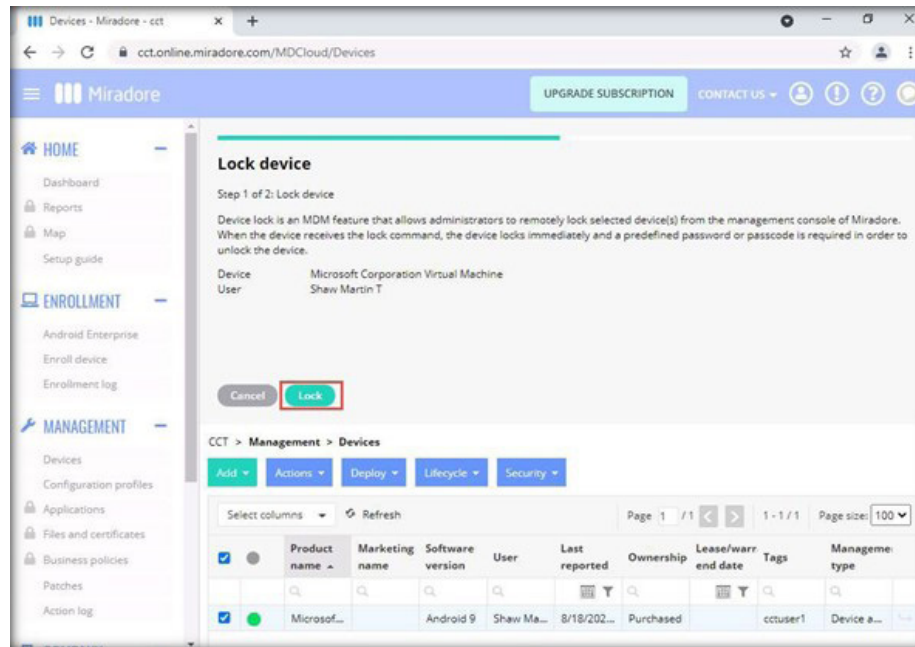
53. Select the device and click on the **Security** button and select the **Lock device** option.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



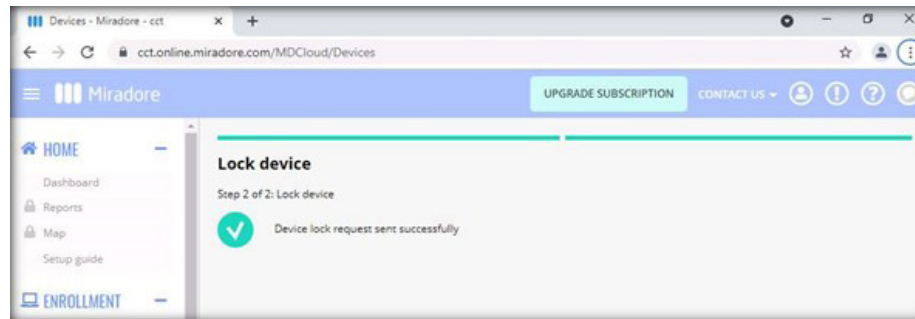
54. The **Lock device** page will show the details of the device to be locked. Click on **Lock** to continue.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



55. You will receive a message on the screen stating that the **Device lock request sent successfully**.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION

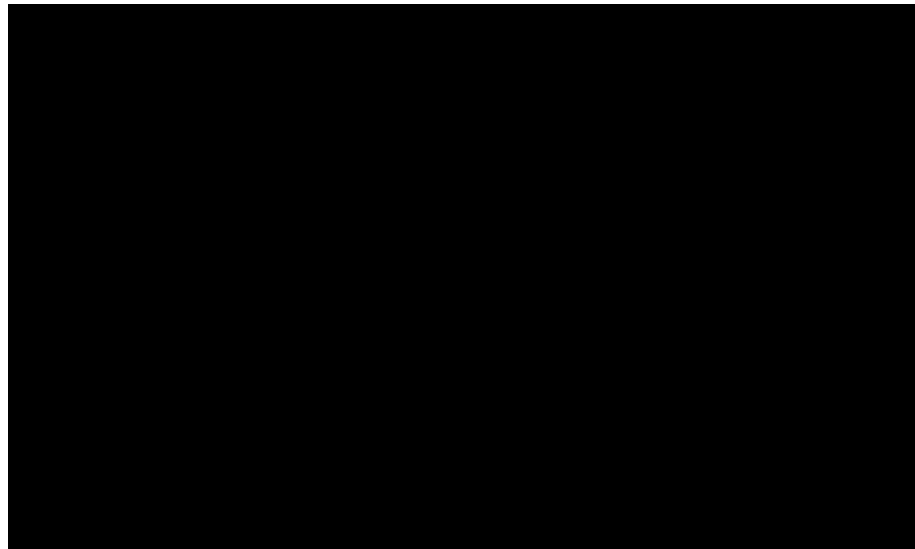




56. After switching on the **Android Device**, you will see a black screen, indicating that the device has been blocked and locked.

**Note:** The device will take some time to lock based on the time it takes to synchronize with the MDM and the Internet speed. If the device is taking long time to lock open miradore application and click on **SYNC NOW**.

EXERCISE 1:  
IMPLEMENT ENTERPRISE  
MOBILE SECURITY  
USING MIRADORE MDM  
SOLUTION



57. By locking the device, the security professional performs the security action to protect the data in the lost device.
58. This concludes the demonstration showing how to implement mobile device security using Miradore MDM Solution.
59. Close all open windows.
60. Turn off **Admin Machine-1**, **Android Device** and **PfSense Firewall** virtual machines.

# EC-Council

