دليل إدارة الأجهزة المحمولة MDM
KAMC MDM USER MANUAL

مدينة الملك عبدالله الطبية
King Abdullah Medical City

Contents

Introduction مقدمة 2
Android Guide دليل إعداد الأندرويد 8
iOs (iPhone, iPad) Guide دليل إعداد أجهزة الأيفون والأيباد 9

مدينة الملك عبدالله الطبية
King Abdullah Medical City

Introduction مقدمة

Mobile Device Management (MDM)

A simple everyday-user guide for King Abdullah Medical City (KAMC)

Why this matters: MDM helps you access work tools securely, protect patient and hospital data, and stay compliant with KSA healthcare security requirements.

1. What is MDM?

MDM stands for Mobile Device Management. It is the system KAMC uses to manage and secure mobile access to work email, files, and internal systems on smartphones and tablets.

2. Why KAMC uses MDM

- To protect patient information and other sensitive hospital data.
- To reduce risk if a device is lost, stolen, or used on an unsafe network.
- To give staff secure access to email, documents, and internal websites from anywhere.
- To make sure devices and apps follow KAMC security policies and Saudi regulations.

إدارة الأجهزة المحمولة (MDM)

دليل مبسّط للاستخدام اليومي لمنسوبي مدينة الملك عبدالله الطبية (KAMC)

لماذا هذا مهم: يساعدك نظام MDM على الوصول إلى أدوات العمل بشكل آمن، وحماية بيانات المرضى والمستشفى، والالتزام بمتطلبات الأمن في القطاع الصحي بالمملكة العربية السعودية.

1. ما هو نظام MDM؟

MDM هو اختصار Mobile Device Management (إدارة الأجهزة المحمولة). وهو النظام الذي تستخدمه المدينة لإدارة وتأمين الوصول عبر الهواتف الذكية والأجهزة اللوحية إلى البريد الإلكتروني والملفات والأنظمة الداخلية الخاصة بالعمل.

2. لماذا تستخدم المدينة نظام MDM

- لحماية معلومات المرضى وغيرها من بيانات المستشفى الحساسة.
- للحد من المخاطر عند فقدان الجهاز أو سرقته أو استخدامه على شبكة غير آمنة.
- لتمكين الموظفين من الوصول الآمن إلى البريد الإلكتروني والمستندات والمواقع الداخلية من أي مكان.
- للتأكد من التزام الأجهزة والتطبيقات بسياسات الأمن في المدينة وأنظمة المملكة.

3. What it means for you as a user

- You can work more easily using approved mobile apps instead of personal apps.
- Your work data stays protected inside secure applications.
- You help KAMC stay safe, compliant, and ready for audits.
- You reduce service disruption caused by login issues, unsafe sharing, or data leakage.

3. ماذا يعني ذلك لك كمستخدم

- يمكنك العمل بسهولة أكبر باستخدام التطبيقات المعتمدة بدلاً من التطبيقات الشخصية.
- تبقى بيانات عملك محمية داخل التطبيقات الآمنة.
- تساهم في بقاء المدينة آمنة وملتزمة وجاهزة للمراجعة والتدقيق.
- تقلّل من انقطاع الخدمة الناتج عن مشكلات تسجيل الدخول أو المشاركة غير الآمنة أو تسرّب البيانات.

4. Your privacy

What KAMC Manages	What KAMC does not manage
Work apps, secure access, compliance settings, and corporate data inside managed apps.	Your personal photos, personal messages, personal email, and personal apps.

Important: MDM is about protecting KAMC work access and data, not monitoring your private life.

4. خصوصيتك

ما تديره المدينة	ما لا تديره المدينة
تطبيقات العمل، والوصول الآمن، وإعدادات الامتثال، وبيانات المدينة داخل التطبيقات المُدارة.	صورك الشخصية، ورسائلك الشخصية، وبريدك الإلكتروني الشخصي، وتطبيقاتك الشخصية.

مهم: يهدف نظام MDM إلى حماية الوصول إلى بيانات العمل في المدينة، وليس مراقبة حياتك الخاصة.

5. The apps you will use every day

App	What you use it for
Mobile@Work	Device enrollment and secure access to KAMC mobile services.
Email+	Your KAMC email, calendar, contacts, notes, and tasks in a secure app.
Docs@Work	Viewing, editing, downloading, and securely sharing work documents.
Web@Work	Secure access to internal websites and portals without a separate VPN.
Tunnel	Secure connection in the background for access to protected resources.

6. What you need to do

- Install Mobile@Work and complete device enrollment using your KAMC credentials.
- Use the approved apps: Email+, and Web@Work.
- Set a passcode and keep your device updated.
- Do not move work data into personal apps or personal email.
- Report issues quickly if you cannot sign in, lose your device, or notice a security problem.

5. التطبيقات التي ستستخدمها كل يوم

التطبيق	الغرض من الاستخدام
Mobile@Work	تسجيل الجهاز والوصول الآمن إلى خدمات المدينة عبر الجوال.
Email+	بريدك الإلكتروني في المدينة والتقويم وجهات الاتصال والملاحظات والمهام في تطبيق آمن.
Docs@Work	عرض مستندات العمل وتحريرها وتنزيلها ومشاركتها بشكل آمن.
Web@Work	وصول آمن إلى المواقع والبوابات الداخلية دون الحاجة إلى VPN منفصل.
Tunnel	اتصال آمن يعمل في الخلفية للوصول إلى الموارد المحمية.

6. ما المطلوب منك

- ثبّت تطبيق Ivanti Mobile@Work وأكمل تسجيل الجهاز باستخدام بيانات دخولك إلى المدينة.
- استخدم التطبيقات المعتمدة: Email+ و Web@Work.
- عيّن رمز مرور للجهاز وحافظ على تحديثه.
- لا تنقل بيانات العمل إلى التطبيقات الشخصية أو البريد الإلكتروني الشخصي.
- بادر بالإبلاغ إذا تعذّر عليك تسجيل الدخول، أو فقدت جهازك، أو لاحظت أي مشكلة أمنية.

7. What changes in your daily use

- Use Email+ for your KAMC email, calendar, and contacts. Do not use Outlook or the built-in Mail app for KAMC email.
- Once Email+ is working, delete your old KAMC account from Outlook and the built-in Mail app to avoid duplicate accounts and sign-in lockouts.
- Open internal websites and IT services from Web@Work, not from a regular browser or a public link.
- Leave Tunnel allowed to run in the background. It is what connects you to internal systems.

8. Keep your device compliant

- Keep a screen lock (passcode, Face ID, or fingerprint) turned on at all times.
- Keep your operating system and the KAMC apps up to date.
- Do not jailbreak or root your device. Such devices are blocked from KAMC services.
- Do not delete Mobile@Work, Tunnel, or the KAMC profile from your device.
- If your device becomes non-compliant, access to KAMC services is paused. Fix the issue shown on screen and access returns. Contact ICT support if it does not.
- On Android, do not restrict battery usage or background activity for Email+ and Tunnel, or mail may stop syncing.

7. ما الذي يتغيّر في استخدامك اليومي

- استخدم Email+ للوصول إلى بريد المدينة والتقويم وجهات الاتصال. لا تستخدم Outlook أو تطبيق البريد المدمج في الجهاز لبريد المدينة.
- بعد التأكد من عمل Email+، احذف حساب المدينة القديم من Outlook ومن تطبيق البريد المدمج لتجنب تكرار الحسابات وإيقاف الحساب بسبب محاولات الدخول المتكررة.
- افتح المواقع الداخلية وخدمات تقنية المعلومات من Web@Work، وليس من المتصفح العادي أو عبر رابط عام.
- اترك Tunnel مسموحاً له بالعمل في الخلفية، فهو الذي يربطك بالأنظمة الداخلية.

8. حافظ على التزام جهازك بالمتطلبات

- أبقِ قفل الشاشة (رمز المرور أو بصمة الوجه أو بصمة الإصبع) مفعّلاً دائماً.
- حافظ على تحديث نظام التشغيل وتطبيقات المدينة.
- لا تقم بعمل Jailbreak أو Root للجهاز. الأجهزة المخترقة يتم منعها من خدمات المدينة.
- لا تحذف Mobile@Work أو Tunnel أو ملف تعريف المدينة من جهازك.
- إذا أصبح جهازك غير ملتزم، يتوقف الوصول إلى خدمات المدينة مؤقتاً. عالج المشكلة الظاهرة على الشاشة وسيعود الوصول. وتواصل مع دعم تقنية المعلومات والاتصالات إذا استمرت المشكلة.
- في أجهزة أندرويد، لا تقيّد استهلاك البطارية أو النشاط في الخلفية لتطبيقي Email+ وTunnel، وإلا قد يتوقف تحديث البريد.

9. Stay safe: avoid scams and data leaks

- Register only through the official KAMC portal (mdmc.kamc.med.sa) and the official Google Play or App Store pages. Be careful with any other enrollment link.
- KAMC will never ask for your password or MobilePass code by phone, WhatsApp, SMS, or email. Never share them with anyone, including ICT staff.
- Do not approve a sign-in or verification request you did not start.
- Check the sender before opening links or attachments, even inside Email+.
- Install apps only from Google Play or the App Store.
- Avoid public Wi-Fi for sensitive work when possible.

10. Lost, stolen, or replaced device

- If your device is lost or stolen, report it to ICT support immediately, even if you are unsure.
- KAMC can remove work apps and data from the device and block its access to KAMC services.
- If you get a new phone, register it again using the steps in this guide, and tell IT support so the old device is removed.
- After a factory reset or restoring from a backup, you must register the device again.

9. كن آمناً: تجنب الاحتيال وتسرب البيانات

- سجّل جهازك فقط عبر بوابة المدينة الرسمية (mdmc.kamc.med.sa) وعبر صفحات Play Google أو Store App الرسمية. وكن حذراً من أي رابط تسجيل آخر.
- لن تطلب المدينة منك كلمة المرور أو رمز MobilePass عبر الهاتف أو واتساب أو الرسائل النصية أو البريد الإلكتروني. لا تشاركهما مع أي شخص، حتى موظفي تقنية المعلومات والاتصالات.
- لا توافق على أي طلب دخول أو تحقق لم تبدأه بنفسك.
- تحقق من المرسل قبل فتح الروابط أو المرفقات، حتى داخل Email+.
- ثبّت التطبيقات من Play Google أو Store App فقط.
- تجنب شبكات الواي فاي العامة في الأعمال الحساسة قدر الإمكان.

10. عند فقدان الجهاز أو سرقته أو استبداله

- إذا فُقد جهازك أو سُرق، بلّغ دعم تقنية المعلومات والاتصالات فوراً حتى لو لم تكن متأكداً.
- يمكن للمدينة إزالة تطبيقات العمل وبياناته من الجهاز ومنعه من الوصول إلى خدمات المدينة.
- عند الحصول على جهاز جديد، سجّله من جديد باتباع الخطوات الواردة في هذا الدليل، وأبلغ دعم تقنية المعلومات ليتم حذف الجهاز القديم.
- بعد إعادة ضبط المصنع أو الاستعادة من نسخة احتياطية، يجب تسجيل الجهاز من جديد.

11. Need help?

- QR code will not scan, or the registration PIN does not work: request a new PIN from the Self Service Portal and try again.
- Mail is not updating: open Email+, check your internet connection, and make sure Tunnel is allowed to run in the background.
- Message says the device is not compliant: follow the instructions on screen, then reopen the app.
- Still stuck: contact ICT support and share your name, device model, and a screenshot of the error.

12. Final message

MDM is not an extra burden. It is the secure way to access KAMC work on mobile devices. When all users adopt it correctly, KAMC improves security, compliance, and everyday productivity.

Action today: Enroll your device, use the approved apps, and contact IT support if you need help.

11. تحتاج مساعدة؟

- تعذّر مسح رمز QR أو لم يعمل رمز التسجيل (PIN): اطلب رمز PIN جديداً من بوابة الخدمة الذاتية (Portal Service Self) وحاول مرة أخرى.
- البريد لا يتحدّث: افتح Email+ وتأكد من اتصالك بالإنترنت ومن أن Tunnel مسموح له بالعمل في الخلفية.
- ظهرت رسالة أن الجهاز غير ملتزم: اتبع التعليمات الظاهرة على الشاشة ثم أعد فتح التطبيق.
- ما زالت المشكلة قائمة: تواصل مع دعم تقنية المعلومات والاتصالات وزوّدهم برقمك الوظيفي ونوع الجهاز ولقطة شاشة للخطأ.

12. الخلاصة

نظام MDM ليس عبئاً إضافياً، بل هو الطريقة الآمنة للوصول إلى أعمال المدينة عبر الأجهزة المحمولة. وعندما يعتمده جميع المستخدمين بالشكل الصحيح، ترتفع مستويات الأمن والامتثال والإنتاجية اليومية في المدينة.

إجراء اليوم: سجّل جهازك، واستخدم التطبيقات المعتمدة، وتواصل مع دعم تقنية المعلومات إذا احتجت إلى مساعدة.

مدينة الملك عبدالله الطبية
King Abdullah Medical City

Android Guide دليل إعداد الأندرويد

1- Download **Ivanti Mobile@work** in your mobile device:
https://play.google.com/store/apps/details?id=com.mobileiron

2- From any desktop computer (or laptop), go to https://mdmc.kamc.med.sa/ and login
Use your **MoiblePass** code in "***gemalto***" screen

3- From "**Self Service Portal**" choose **Devices**, then Click on "**Register New Device**"

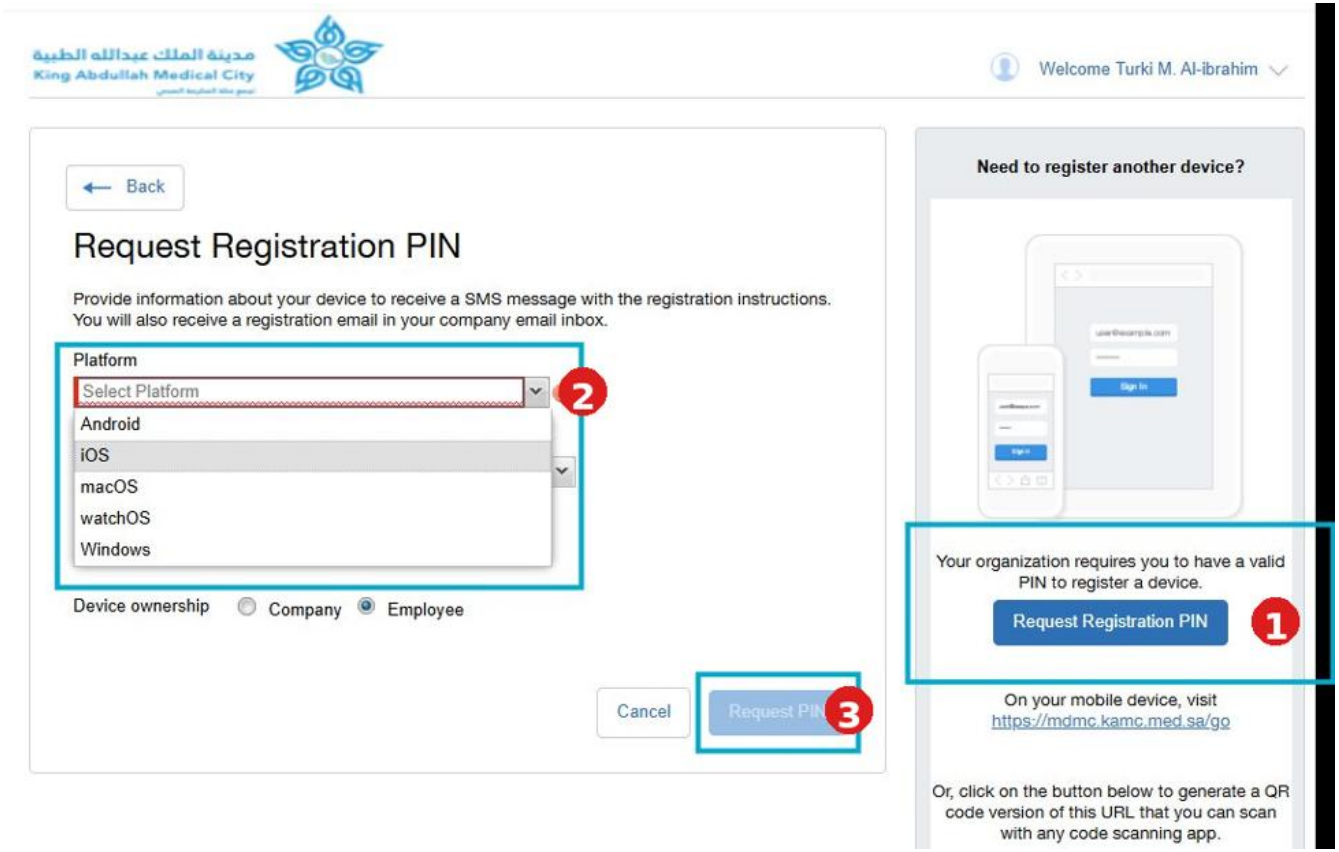
4- Click on "Request Registration PIN"

5- Select Device type

6- Click on "Request PIN"

7- Open "Ivanti Mobile@Work" in your mobile, click on scan QR Code, & scan the code

8- Accept/allow all following messages



مدينة الملك عبدالله الطبية
King Abdullah Medical City

iOs (iPhone, iPad) Guide دليل إعداد أجهزة الأيفون والأيباد

1- Download **Mobile@work** in your mobile device:
iPhone: https://apps.apple.com/us/app/ivanti-mobile-work-client/id320659794

2- From any desktop or laptop computer, go to https://mdmc.kamc.med.sa/ and login
Use your MoiblePass code in "*gemalto*" screen

3- From "**Self Service Portal**" choose **Devices**, then Click on "**Register New Device**"

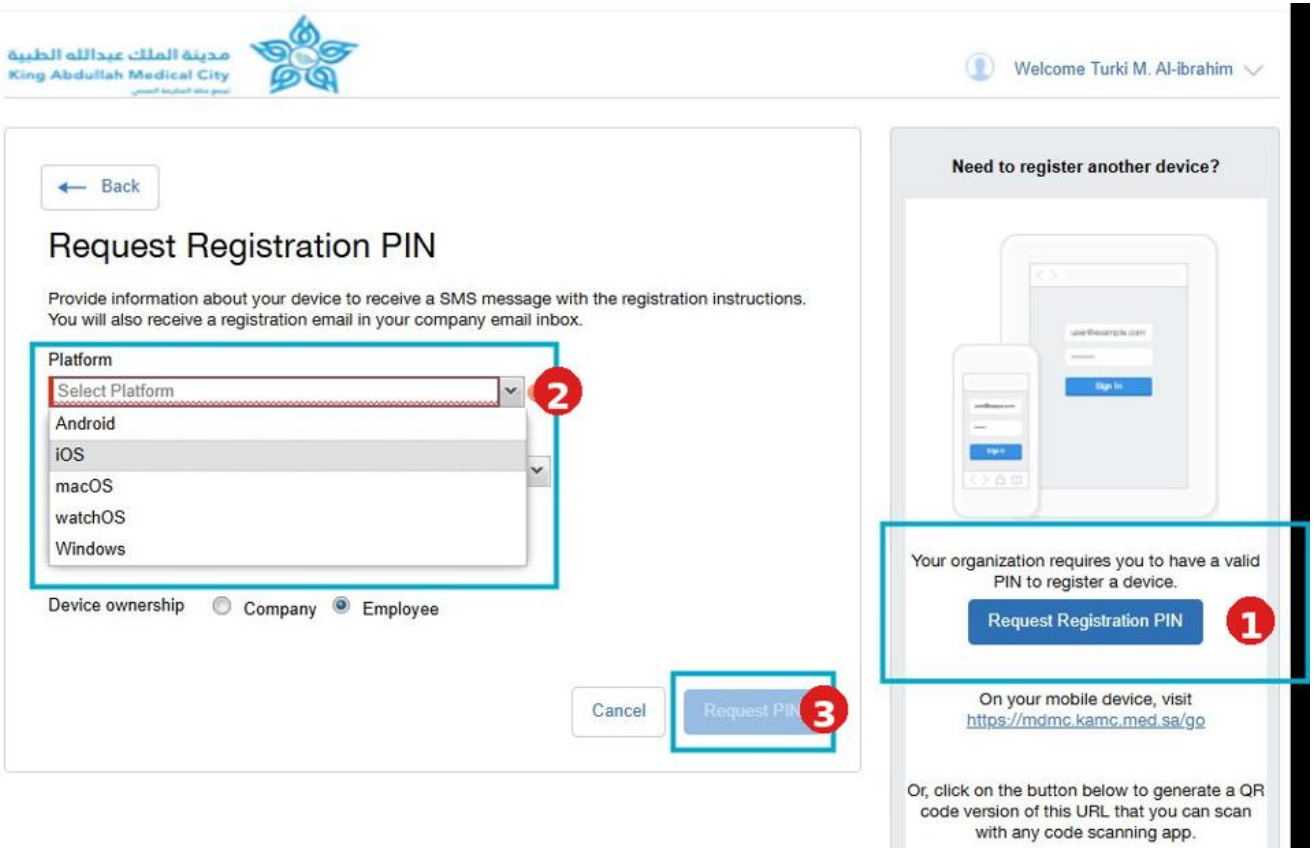
4- Click on "Request Registration PIN"

5- Select Device type

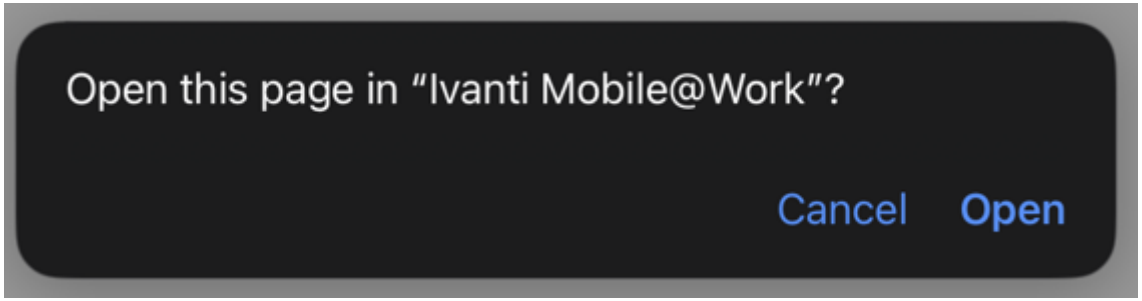
6- Click on "Request PIN"

7- Open "Ivanti Mobile@Work" in your mobile,

8- Click on scan QR Code, & scan the QR code displayed

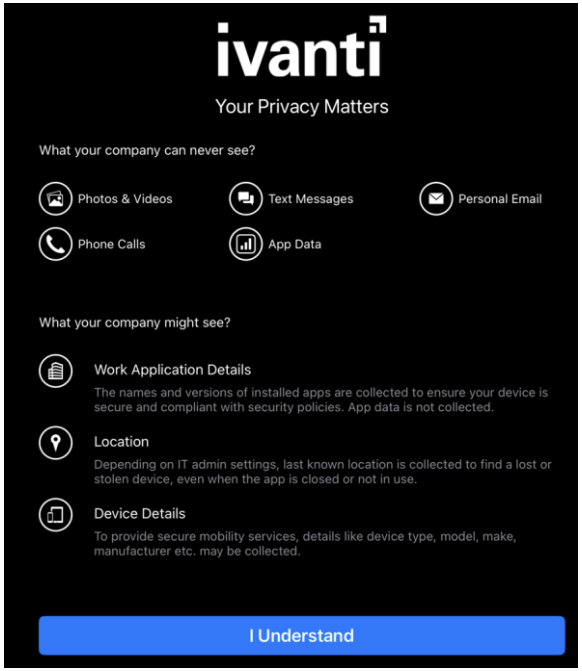


9- Click on “Open”

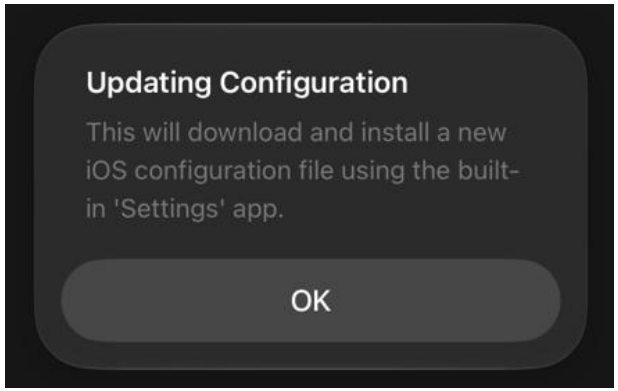


10- In the Credentials (PIN) screen, Click on Register

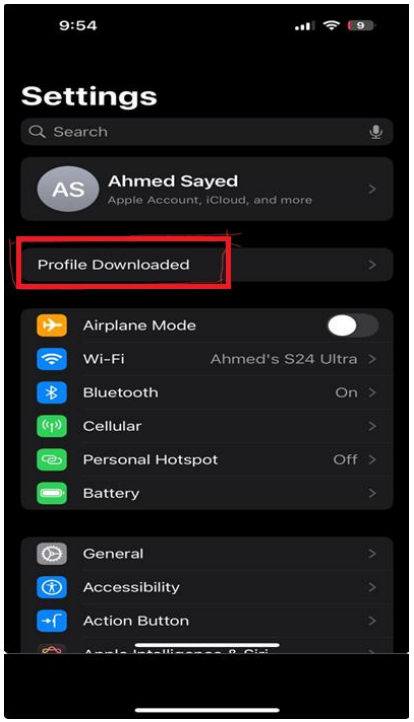
11- Click on “I Understand”



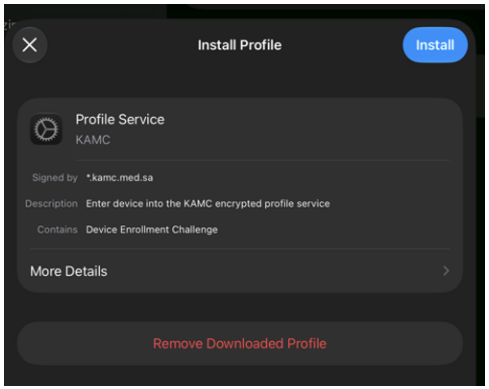
12- Click on ”OK” on Updating Configuration screen



13- Open iPhone settings, then select “Profile Downloaded”

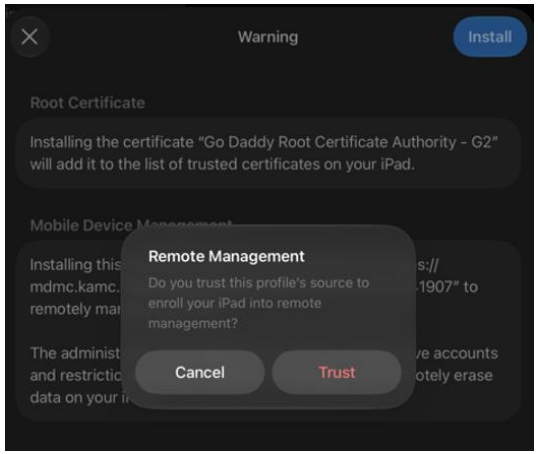


14- Click Install

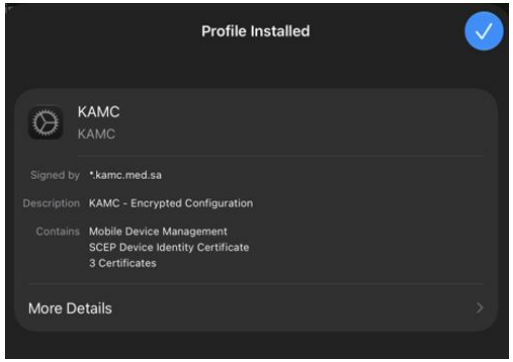


15- If asked, enter your iOS password or Face ID

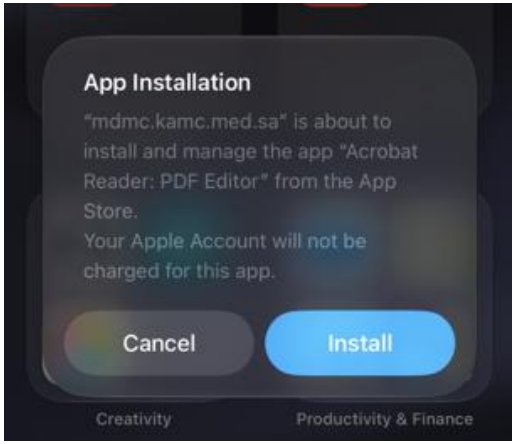
16- Click Trust



17- Click on the blue tick



18- Click on install



7. You will receive multiple pop-ups to allow work apps installation, click Install
You are done