MAM and MDM Deployment Manual

LSC TIG / Special Grant Work Product Notice

LSC | America’s Partner for Equal Justice

LEGAL SERVICES CORPORATION

Pre-Existing Work and Third-Party Materials

This manual may include (a) pre-existing materials developed using non-LSC funds and (b) third-party materials. Third-party materials remain subject to their owners’ rights and terms.

Microsoft / Trademark Notice

This manual discusses Microsoft products and may reference Microsoft documentation and services. Microsoft, Microsoft 365, Intune, and related marks are trademarks of Microsoft Corporation. ArchTech LLC is not affiliated with Microsoft.

Public License (Noncommercial)

Commercial Use

Attribution

No Warranty

PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND. YOU ASSUME ALL RISKS ARISING FROM USE.

Introduction to MAM and MDM 4

Deployment Roadmap 6

Phases: 7

Phase 1 - Section 1: Prerequisites 8

Default Values Disclaimer 9
Permissions 9
Target Devices for Deployment 9
Security Groups 9
Configuring Apple and Google Intune Connections 12

Phase 1 - Section 2: Choosing Your Deployment Method(s) 20

Definitions, Purpose, & Capabilities 21
Quick Comparisons 24
Choosing your Deployment Method: 28

Phase 2 - Section 1: Communications 29

Stakeholder Advisory Communication 30
Request for Test Users 32

Phase 2 - Section 2: Configuring the Deployment Method(s) 34

MDM 35
MAM 50
Work Profile MAM+MDM 57

Phase 3 – Section 1: Test Phase Communications 71

Test Users Notification of Implementation 72

Phase 3 – Section 2: Test Phase Implementation 82

Assign the test users to groups 83
Initiate Enrollments 84

Phase 4 – Section 1: Full Deployment Communications 86

All Staff Notifications of Implementation 87

Phase 4 – Section 2: Full Deployment Implementation 96

Removing Users from Test Groups 97
Initiate Enrollments 97

Relative Reference Links 107

Microsoft Links: 108
Other Links: 110

Reminders 111

Certificate Renewals 112
Bad URLs 112
Default Values Disclaimer 112
MAM or Work Profile MAM+MDM 112

Introduction to MAM and MDM

If you are not already familiar with MDM and/or MAM, this section of this manual is here to introduce two important pieces of modern device security strategy: **Mobile Application Management (MAM)** and **Mobile Device Management (MDM)**. Throughout this manual you'll be hearing these terms more often, and this introductory section is just to provide a clear, non-technical understanding of what they mean and why you will be using them.

Mobile Device Management (MDM) is used to securely manage the *devices* that access company data—phones, tablets, and sometimes laptops. With MDM, IT can make sure corporate devices have a passcode, are encrypted, are running reasonably up-to-date software, and can be locked or wiped if they're lost or stolen. Think of MDM as the set of rules that keep the overall device safe and compliant so it's trustworthy for work.

Mobile Application Management (MAM) focuses on the *apps and data*, not the whole device. It allows us to protect company information inside specific work apps like email, chat, or file storage—even on personal devices. With MAM, you can do things like prevent copying data from a work app into a personal app, require a PIN or biometric to open work apps, and remove company data from those apps if someone leaves the organization, without touching their personal photos, messages, or other apps.

Together, MDM and MAM help strike the right balance between **security and usability**: you protect your users and your business by securing devices and data, while still respecting personal privacy and supporting flexible, mobile work. This manual will go into more detail about the various methods of accomplishing this, comparisons between those methods, how this affects your users and what to expect during enrollment.

Deployment Roadmap

Phases:

This manual is written as a 4-phase deployment. Those phases and their sections are as follows:

Phase 1:

- Section 1: Prerequisites
- Section 2: Choosing Your Deployment Method

Phase 2:

- Section 1: Communications
- Section 2: Configuring the Deployment Method(s)

Phase 3:

- Section 1: Test Phase Communications
- Section 2: Test Phase Implementation

Phase 4:

- Section 1: Full Deployment Communication
- Section 2: Full Deployment Implementation

Phase 1 - Section 1: Prerequisites

Default Values Disclaimer

Steps in this guide at times will walk you through creating and configuring various policies, profiles, etc. and it is important for anyone following this guide to understand that only values for these items that differ from the default settings are listed. DO NOT change other settings from their default values unless you are certain that the results of that action are desired and realize that you are doing so at your own risk.

Permissions

Throughout this manual you will be performing various tasks that require an elevated level of Microsoft 365 permissions. While there are various privileged user roles that could accomplish each task, to keep things as straightforward as possible, it is recommended to use a MS 365 Global Administrator account for all steps. Always follow proper security measures when using global administrator accounts (MFA, Incognito Browser, etc.).

Target Devices for Deployment

Personally owned (BYOD) and corporate-owned Android/ iOS/iPadOS phones & tablets, running managed apps like Outlook, Teams, OneDrive, Edge, and LOB apps integrated with Microsoft Intune.

Security Groups

You will be creating security groups as part of this prerequisites section as well as in parts of other sections throughout this manual. All security groups in this manual will be created in Entra Groups.

CAP Exclusion Security Group

For this step you will be creating a conditional access policy (CAP) exclusion group. This exclusion group will be used to ensure that your break glass accounts as well as any other specific accounts that you would like to exclude from the CAPs that you will create later in this manual as part of your deployment are all excluded.

As a note, you are creating a single CAP exception group, that will be used across ALL mobile devices (Android and iOS) and all deployment methods (App-Level MAM, Work

Profile MAM+MDM, MDM). Should you have specific needs that require more than one exclusion group, repeat this step and give each a unique name and exclude the groups on the desired policies.

- Navigate to Azure>Microsoft EntraID> Manage>Groups (Entra Groups)
- Click "New group"
- Group Type will be Security
- Group name will be "CAPSG-MAM-MDM-NotBlocked".
- Description will be "Users in this group do not need MDM/MAM to access Applications on mobile devices <your 1st initialLast name>"
- Membership type will be Assigned
- Add the global admin account that you are using to set this up as the owner and as a member. Add any additional accounts you wish to exclude from these deployments here as well.

Dynamic Device Groups

For this step you will be creating a pair of dynamic security groups. These will be essential for an environment running multiple Mobile Device Management solutions. Even in single solution environments the groups aid in identifying devices by type.

Dynamic iOS Group

- Navigate to Azure>Microsoft EntraID> Manage>Groups (Entra Groups)
- Click "New group"
- Group Type will be Security
- Group name will be "AAD-SDG-Intune-Mobile-iOS-Devices"
- Description will be "Dynamic group of all iOS devices. <your 1st initialLast name>"
- Change the Membership type to Dynamic Device
- Add the Global Administrator account that you are using as the Owner
- Under Dynamic device members, click "edit dynamic query". The query should look like this:
    - *(device.deviceOSType -eq "iPad") -or (device.deviceOSType -eq "iPhone")*

Dynamic Android Group

- Navigate to Azure>Microsoft EntraID> Manage>Groups (Entra Groups)
- Click "New group"
- Group Type will be Security
- Group name will be "AAD-SDG-Intune-Mobile-Android-Devices"

- Description will be “Dynamic group of all Android devices. <your 1st initialLast name>”
- Change the Membership type to Dynamic Device
- Add the Global Administrator account that you are using as the Owner
- Under Dynamic device members, click “edit dynamic query”. The query should look like this:

(device.deviceOSType -eq "Android") or (device.deviceOSType -eq "AndroidForWork") or (device.deviceOSType -startsWith "AndroidEnterprise")

Assignment Filter (MAM Optional)

This optional step is used if your environment is intending to use MAM layered with another deployment type; without it, your MAM settings WILL interfere with your other deployment settings (which in some cases may be okay – it depends on your environment’s preferences and use cases – still, it’s better to have the controls, and options, available).

Navigate to Intune > Tenant administration > Assignment filters

- Click Create Managed apps filter, and select iOS or Android.
- Filter type is Managed App.
- Give it a name like: “Filter-Unmanaged-iOS-Mobile-Devices”, or “Filter-Unmanaged-Android-Mobile-Devices”.
- Description: “Filter includes unmanaged iOS devices that are not registered in Intune - thus, excludes MDM/MAMOS devices. This way, they can be excluded from MAM App Protection policies. <your 1st initialLast name>” (Change iOS to Android for Android devices)
- Platform: iOS/iPad, or Android.
- Rules syntax: (app.deviceManagementType -eq "Unmanaged")
    - Just copy and paste that clock of code into both of those rules syntaxes, and save.

Update Existing Conditional Access Policies

If there are pre-existing CAPs, it is important to review each of them as there could potentially be conflicts with the new policies that will be implemented as part of the deployment. To avoid these conflicts, you are going to add the Dynamic groups that you just created to any conflicting policies.

An Example policy that might cause a conflict would be one that applies to all devices and blocks non-compliant devices. Knowing what pre-existing policies you currently have and if they apply to android and/or iOS devices will be key to determining if exclusions need to be made.

With that in mind, for any conditional access policy that could potentially cause a conflict, perform the following:

- Navigate to Entra>Conditional Access>Policies (Conditional Access Policies)
- Find and select the CAP with the potential conflict
- Click on the hyperlinked text below Under “Users or agents”
- Click on the “Exclude” section on the right
- Check Users and groups (If not already checked)
- Add the two newly created dynamic groups to the list of excluded groups

Repeat this same process for all conflicting CAPs.

Configuring Apple and Google Intune Connections

While it is not required for every deployment method, multiple deployment methods do require Apple and Google to be connected to Intune. For this reason, you will set this up by following the steps below.

Apple Business Manager

*****Note*** Skip this step if your organization already has an Apple Business Manager account**

Apple Business Manager is an essential foundation that will be used to integrate your Apple devices with Microsoft Intune.

First, an Apple Business account is going to need to be made. To complete this step, follow the instructions below:

- Navigate to https://business.apple.com/
- Click the “Sign up now.” Link
- Select Get Started
- Input your name, the email address you want this registered to and your company name
  - Note: Use an actual name for this or you run the risk of the application being rejected.
- Input your desired login credentials
- Input an SMS capable phone number that you can receive MFA codes to.
- Input the CAPTCHA code
- Click Continue
- Verify the account
  - Click on the big verify button that should have popped up; if needed, you can also verify the account by navigating to: Devices > Verify
  - Input the D-U-N-S number of the business being verified
    - If you do not have this number and are not able to easily get it from an internal resource, you can find all of the info you need to request it here.
    - After putting in the D-U-N-S number, the form fields should be largely auto-populated. Complete any required fields that did not auto-populate, if any.
  - Input a secondary point of contact. It is a requirement that this individual works directly for the organization.
  - Submit the verification request
    - It can take Apple up to 5 business days to complete the verification.

        - It is likely that as part of the verification process Apple will reach out via email to either the primary or secondary POC (Points of Contact). Until that communication is received and responded to, the verification process will be on hold. Be sure both POCs are available to monitor their mailboxes during this time.

iOS MDM Push Certificate

In this step you will setup the iOS Push Certificate. The iOS MDM push certificate is used to establish a trusted connection between your Intune service and Apple's Push Notification service (APNs), so devices know that management commands are coming from a legitimate source. It allows the MDM server to securely send configuration updates, wipe commands, and other management notifications to enrolled Apple devices.

*****Important Note*****

This CSR must be renewed annually. It is highly recommended for both the primary and secondary Apple Business Manager points of contact to create an annual calendar reminder for this event.

To complete this step, follow the instructions below:

- Navigate to: Intune > Devices > Device onboarding > Enrollment (Device Enrollment)
- Select the Apple header
- Select "Apple MDM Push Certificate", this will open a pane with 5 numbered steps
- Check the I agree box in the right-hand pane under "1."
- Click the "Download the CSR file" link under "2."
- Click the link, which is pre-populated with the need info to connect this Intune account to Apple Business Manager.
- Open a new browser tab and navigate to Apple Business Manager, sign in, and click "Create a certificate."
- For notes, put "CSR uploaded [date] by <First initialLast name>"
- Select "Choose file" and find the above downloaded CSR file from step 2
    - It should be named "IntuneCSR.csr"
- Click Upload
- Click the Download button to get the PEM certificate from Apple, then return to Intune.

- Back in Intune under “4.”, add the Apple ID for the Apple Business Manager account as the username
- Under “5.” Click the folder icon to browse to the location of the PEM certificate you just downloaded and select it
- Click the Upload button at the bottom of the pane

iOS MDM Enrollment Token

In this step you will setup the iOS MDM Enrollment Token. This is used to securely identify and authenticate devices during the enrollment process so they can join the correct MDM tenant and receive the right profiles. In practice, it’s what links an Apple device’s setup (or enrollment profile) back to your specific MDM environment, ensuring only authorized devices are enrolled and managed.

*****Important Note*****

This token must be renewed annually. It is highly recommended for both the primary and secondary Apple Business Manager points of contact to create an annual calendar reminder for this event.

To complete this step, follow the instructions below:

- Navigate to the following location in Intune to create the token: Intune > Devices > Device onboarding > Enrollment > Apple > Enrollment Program Tokens (Apple Enrollment Program Tokens)
- Create a new Enrollment token.
- Check “I agree”
- Click “Download your public key”
- Open a new browser tab and navigate to the following Apple Business Manager location to create a token:
    - Apple Business Manager > Account (bottom left) | Device Management Services | Add
- For the service name input, “Intune_MDM_<Company Name>”
- Click Next
- Click the “Upload Public Key” button
    - Find the above downloaded PEM file from Intune (follows format "IntuneKey<date>.pem").
- Click Save
- Reopen the service you just created

- Click the Download Token button
- Return to your browser tab the has Intune open (Do not close the ABM tab yet)
- Fill in the Apple ID with your Apple Business Manager Apple ID
- In the Apple Token field, browse for the token file that was just downloaded and click Next
    - (The file name follows the format “Intune_MDM_<CompanyName>_Token_<date>_smime”)
- Click Create / Save
- After creation, you should see the new Enrollment program token listed, with Status = Active and a valid Expiration date
- Return to the browser tab with Apple Business Manager open
- Navigate to Preferences > Device Management Services
- Under that, click “Management Assignment”
- For “Default Assignment” Select Edit and update iPhone and iPad to use the Intune_MDM_<CompanyName> service you added.

iOS VPP Token

In this step you will be setting up your iOS VPP Token. This is used for linking your MDM/Intune tenant to your Apple Business Manager app licenses so Intune can see which iOS apps and how many licenses your organization owns. It lets Intune sync those apps, assign licenses to users/devices, silently deploy them to managed iOS devices, and reclaim licenses when they’re no longer needed.

*****Important Note*****

This token has to be renewed annually. It is highly recommended for both the primary and secondary Apple Business Manager points of contact to create an annual calendar reminder for this event.

To complete this step, follow the instructions below:

- Navigate to the following Apple Business Manager location to create the token: Apple Business Manager > Account (bottom left) | Payments and Billing | Content Tokens (Apple VPP Tokens)
    - Note: If you can’t see the Payments and Billing tab, navigate to the Apps and Books pane on the left, and complete the prompt asking if the organization is Tax Exempt or not.

- Click "Download" to get the needed token
- Navigate to the following location in Intune:
    - Intune > Tenant Administration > Connectors and Tokens > Apple VPP Tokens
- Click "+ Create"
- Under the Basics Header:
    - Enter the Token Name as "Apple VPP Token"
    - Enter the Apple ID you use to sign in to Apple Business Manager
    - Select VPPTokenFile as the file you just downloaded.
- Under the Settings Header
    - Set "Take control of token from another MDM" to No
    - Select the Country this is being deployed in
    - Leave "Type of VPP Account" as Business
    - Change "Automatic App Updates" to Yes
    - Check the "I Agree" box
    - Click Next
- Under the Scope Tags Header
    - Leave the scope tags on their default settings
    - Click Next
- Under the Review + Create Header
    - Click Create

iOS App Selection and Licenses

In this step you will be configuring the app selection for iOS that MDM policies will apply to as well as setting up the initial license count for those apps.

*****Important Note*****

As users are added over time, you will likely run out of licenses and need to follow these steps again to assign more licenses. When adding licensing for each app, it is recommended to input more than your current needs to minimize how often you need to perform this task.

To complete this step, follow the instructions below:

- First compile a list of mobile apps that you want to manage. Below are some common examples:

    - Intune Company Portal
    - Acrobat Reader
    - Edge
    - Excel
    - MS 365 Copilot
    - OneDrive
    - OneNote
    - Outlook
    - PowerPoint
    - Teams
    - To-Do
    - Word

*****Important Note*****

Always include the Intune Company Portal app.

- Navigate to the following Apple Business Manager location to configure the apps list:
    - Apple Business Manager > Apps and Books
- Follow these steps for each app that you want to manage:
    - Search for the app in the search bar at the top
    - Assign the app to your organization
    - Add the needed license count (Current needs plus room for growth)
    - Select Get

Managed Google Play

In this step you will be setting up a connection between Google Play and Intune. This is needed so that you can properly manage your Android devices, regardless of your chosen deployment method.

To complete this step, follow the instructions below:

- Navigate to the Managed Google Play connector in Intune:
  - Navigate in Intune>Devices>Android>Android enrollment>Managed Google Play or Devices>Enrollment>Android tab>Managed Google Play, depending on the user interface (Android Enrollment)
  - Check the “I agree” box and click “Connect to Google now”
- Use your Entra identity in the Google wizard
  - A new tab opens on a Google “Create admin account / Android Enterprise” page
  - It will prefill the same email address you’re using in Intune. Choose Sign in with Microsoft when prompted
  - Sign in (if prompted) with that same Microsoft Entra account and click Accept on the permissions screen
- Complete the Android Enterprise / Managed Google Play setup
  - Fill in the basic org/admin details (company name, contact info). All about Microsoft Intune
  - On the subscriptions page, select Android Enterprise (at minimum). All about Microsoft Intune
  - Accept Google’s terms and click Agree and continue, then Allow and create account to finalize the binding between Intune and Managed Google Play. All about Microsoft Intune+1
- Verify the connection
  - Back in Intune, the Managed Google Play connector should now show as Connected
  - Intune will automatically add the standard Android Enterprise apps (Intune, Company Portal, Authenticator, etc.) into Apps → All apps.

Phase 1 - Section 2:
Choosing Your Deployment Method(s)

Section Note: This section of the manual will serve as a reference point as to the purpose of each deployment method.

Definitions, Purpose, & Capabilities

MAM:

What is MAM and what is its purpose?

The purpose of MAM (Mobile Application Management) is to keep company data secure inside mobile apps—especially on personal devices—by controlling how that data is accessed, stored, and shared, without taking over the entire device.

Microsoft MAM accomplishes this through a set of app-level tools (mostly in Microsoft Intune) that allow IT to control and protect company data inside apps without necessitating full device management.

What sorts of things can MAM do?

Typical things App-Level MAM lets admins do:

- App protection policies
  - Require a PIN or biometric to open a work app
  - Prevent copy/paste from work apps into personal apps
  - Block screenshots in sensitive apps (on some platforms)
  - Force data to be stored in managed locations (e.g., OneDrive for Business)
- Selective wipe
  - If a user leaves the company or their device is lost:
  - Only corporate data inside the apps is wiped
  - Personal photos, texts, and apps stay untouched
- App-level access control
  - Require devices to meet certain conditions before the app can access corporate data
  - For example: only allow Outlook to connect if the user signs in with a corporate account and meets security rules
- Works in BYOD (Bring Your Own Device) environments
  - Users can use their personal phones
  - Company controls only the business side of apps and data, not the full device

Work Profile MAM+MDM:

What is Work Profile MAM+MDM and what is its purpose?

In this manual, Work Profile MAM+MDM refers to managing apps and data inside Work Profiles using MAM-style controls (like Intune App Protection Policies) on top of the work container. The Work Profile itself is an OS-level "container" that separates work apps and data from the user's personal side. When you add MAM into that picture, IT can not only manage which apps live in the work profile but also enforce granular app-level rules—like blocking copy/paste out of work apps, requiring an app PIN/biometric, controlling where data can be saved, and wiping only corporate data if needed.

The purpose of Work Profile MAM is to protect corporate data while preserving user privacy and flexibility. It gives the organization stronger security and compliance (device posture checks, containerization, managed app set, certificates, VPN, etc.) and then tightens control at the app/data level inside that work profile. For users—especially in BYOD or COPE scenarios—it means their personal apps and data stay separate and largely unmanaged, while the company can confidently secure email, files, and line-of-business apps in the workspace and remove them cleanly when the user leaves or the device is lost.

What sorts of things can Work Profile MAM+MDM do?

Work Profile MAM+MDM can do all of the things that MAM can do as well as a lot of container and device level things it can't. This is because there's an enrolled work profile on the device which enables the ability to silently deploy and remove apps into that container, control which apps are allowed there at all, push Wi-Fi/VPN/certificate profiles for work apps, enforce encryption and screen-lock requirements, and use real device compliance (OS version, patch level, root status, etc.) as a condition for access. You also get cleaner UX separation: work vs personal app icons, notifications, and storage are split at the OS level, not just logically within a single app.

On the data and policy side, work profile MAM+MDM lets you control the entire flow of data into and out of the work container, not just between individual managed apps. That means you can broadly block or tightly scope sharing between work and personal profiles, centrally wipe the whole work profile in one shot (all work apps and data gone, personal untouched), and apply restrictions to any app living in the work profile—even if it doesn't have a specific MAM SDK/wrap—as long as Android's work profile policies cover it. In short: app-level MAM protects data inside specific apps; work profile MAM adds a managed "mini-device" around those apps, with compliance, networking, certificates, app set control, and one-click removal of the entire work environment.

MDM:

What is MDM and What is its Purpose?

Mobile Device Management (MDM) is a technology and set of policies that let an organization enroll, configure, secure, and monitor entire devices—like phones, tablets, and laptops—from a central system. Its purpose is to make sure any device that accesses company data is secure and compliant: enforcing things like passcodes, encryption, OS updates, and antivirus; pushing Wi-Fi, VPN, and email settings; installing or removing apps; and being able to lock or wipe a lost or stolen device. In short, MDM gives IT full-device control so they can protect corporate data, meet compliance requirements, and support users, especially when devices are corporate-owned or highly regulated.

Note When choosing your deployment method, it is important to note that IT will need to factory reset the device as part of the MDM enrollment process

---

What sorts of things can MDM do?

MDM can do a lot, but here's a practical list of what it can do:

- Enroll and inventory devices
    - Register devices with the company
    - See what devices are in use, platform, OS version, etc.
- Enforce security policies
    - Require PIN/biometrics, encryption, screen lock, OS version, antivirus, jailbreak/root detection, etc.
- Configure settings remotely
    - Push Wi-Fi, VPN, email profiles, certificates, and other system settings without users doing it manually.
- Deploy and manage apps
    - Silently install, update, or remove apps
    - Control which apps are allowed or blocked
    - Manage app licenses.
- Control access to company data
    - Combine with conditional access to only let compliant devices connect to email, files, and internal resources.
- Track compliance and report
    - See which devices meet policy
    - Generate reports for audits and compliance requirements.

- Lock, wipe, or reset devices
    - Remotely lock a device, change its passcode, wipe corporate data, or in some cases fully factory reset if lost/stolen.
- Separate work and personal (in some modes) – On platforms like Android Enterprise and iOS, it can create managed areas or profiles to keep work data separate.

In short: MDM gives IT central, remote control over devices so they can secure them, configure them, and support users at scale.

Quick Comparisons

MAM vs MDM (Mobile Device Management)

Here is a quick comparison of the major differences between MAM and MDM:

Feature	**MAM (App-Level)**	**MDM (Device Level)**
Controls entire device?	❌ No	✅ Yes
Controls specific apps?	✅ Yes	✅ Yes (but via device)
Good for BYOD?	✅ Great fit	😬 Often too invasive
Can wipe whole device?	❌ No	✅ Yes
Can wipe only corp data in apps?	✅ Yes	✅ Yes (depending on configuration)

MAM VS Work Profile MAM+MDM

Here is a quick comparison of the two types of MAM deployment methods in this manual:

Feature	**MAM (App-Level)**	**Work Profile MAM (MDM + MAM)**

Management scope	Protects data only inside supported corporate apps (e.g., Outlook, Teams, Edge, LOB apps).	Manages all work apps and data inside the Android work profile container.
Device enrollment	Not required. User just installs the app and signs in with their work account.	Required. Device (profile) enrolls into Intune as an Android Enterprise work profile device.
Data protection controls	App-level controls: copy/paste restrictions, save-location control, app PIN/biometric, in-app encryption.	Container + app-level controls: control data movement between work and personal profiles, enforce encryption and screen lock, plus APP if used.
Device posture & compliance	Limited. Relies mostly on Conditional Access and basic signals (e.g., rooted where detectable). No full device compliance.	Full device compliance checks (OS version, patch level, encryption, screen lock, root) drive access decisions.
App deployment model	Apps usually from public store or Company Portal; APP applies when user signs in with work account.	Apps are deployed to the work profile; users see separate "Work" versions of apps.
User privacy & experience	Very high privacy; only selected apps are managed. No visible device management banner for the user.	Clear work/personal separation with a dedicated work profile; users see that part of the device is managed.
Wipe / offboarding behavior	Selective wipe removes only corporate data from managed apps; personal data and apps remain.	Removing the work profile deletes all work apps and data; personal side is left intact. (Full wipe possible for corp-owned devices.)

Best suited for	BYOD and contractors where enrollment is hard to justify; focus is on protecting data in a few key apps.	BYOD/COPE where you also need device posture, managed app set, Wi-Fi/VPN/certificates, and strong separation.

Work Profile MAM+MDM vs MDM

Feature	Work Profile MAM + MDM (Android Enterprise Work Profile + Intune APP)	MDM-Only (Device-level management, no app-level MAM)
Scope of control	Manages the work profile container (work apps, work data, work settings) plus app-level protections inside those work apps.	Manages the entire device (or entire corporate side on corp-owned modes) via device settings, but has no extra app-level data controls.
Data separation	Strong OS-level separation: work profile vs personal profile. App-level MAM further locks down data flow inside work apps and between work/personal.	Depends on mode: fully managed corp devices have no personal profile; BYOD with legacy/limited MDM has weaker separation, mostly policy-based, not a dedicated container.
Data protection / DLP	Container rules (no sharing out of work profile, control between profiles) plus MAM rules: restrict copy/paste, “Open in,” save locations, app PIN, in-app encryption, selective wipe per app.	Mainly device-wide controls: device encryption, screen lock, email profiles, etc. No granular app-level policies like copy/paste restrictions or per-app DLP.
Device compliance & posture	Full device compliance (OS version, patch level, encryption, screen lock, root) and app-level health (MAM policy present, app PIN, etc.) can both feed Conditional Access.	Full device compliance only. Access decisions are based on device state; there’s no awareness of per-app protections.

App lifecycle & deployment	IT deploys apps into the work profile and can enforce which apps are present there. MAM can still apply protection if a user installs an additional supported app in the work profile.	IT deploys apps device-wide or to the “managed” area only, but has no MAM layer to protect data if an app is compromised or misused.
User privacy & BYOD fit	Excellent for BYOD: only the work profile is managed, personal side is separate; MAM adds protection without visibility into personal apps/data.	BYOD with classic MDM feels more intrusive (device shows as “managed” as a whole); user may worry about IT visibility and wipes affecting their personal content.
Wipe / offboarding	Admin can: (1) selectively wipe data from specific managed apps via MAM, and/or (2) remove the entire work profile (all work apps & data gone, personal untouched).	Wipe options are coarse: retire/remove management (may leave or remove data, depending on platform) or full device wipe on corp-owned devices. No per-app selective wipe.
Access control flexibility	Very flexible: Conditional Access can require both a compliant device and a protected app (MAM). You can also let un-enrolled devices in with just MAM for some workloads and require work profile + MAM for higher-risk ones.	More binary: either the device is compliant/managed and allowed, or it isn’t. No way to say “must use a protected app” on top of device management.
Security strength	Strongest combo: device posture + work container + app-level DLP. Great for sensitive data on BYOD or COPE devices.	Good for device posture and basic hardening, but weaker for fine-grained data protection once data is on the device.
Best use cases	BYOD or COPE needing clear separation + strong DLP (e.g., email, files, line-of-business apps with sensitive data).	Purely corporate-owned devices where personal use is limited/irrelevant, and coarse controls are acceptable
Key limitations	More moving parts: device enrollment + work profile + MAM policies. Android-specific model. Slightly more complex to explain to users.	Simpler policy model but lacks granular data control; employees may resist MDM-only on personal devices due to privacy concerns.

Choosing your Deployment Method:

There is no singular correct deployment method for everyone. It is important that you understand the differences between the 3 deployment methods and choose what makes the most sense for your specific environment. You may even find that a combination of deployment methods makes the most sense. For example, you have company owned iPads and want MDM configured to properly manage those, but you also have a BYOD mobile phone policy that you wish to deploy MAM for.

*****Important Note*****

While it may be possible to implement MAM and Work Profile MAM+MDM at the same time, this manual is not written in a way that supports it. When following this manual, you may implement either solution in conjunction with MDM ONLY. If an either-or solution for MAM or Work Profile MAM+MDM does not work for your needs, you will need to consult a professional for assistance with if you are solely reliant on this manual for deployment.

Once you feel you have a good understanding of the 3 methods and have decided on your deployment method(s), proceed to Phase 2: Configurations.

Phase 2 - Section 1: Communications

Note The following communications are only recommended and may not be mandatory depending on your organization’s approval matrix. Skip any parts of this section that you feel may not apply.

Stakeholder Advisory Communication

Below you will find a sample communication that provides a notification / advisory of the planned implementation. It is recommended to be sent to any stakeholders / executive leaders in your organization that need to be apprised of and/or provide approvals for organization wide IT changes.

Sample Communication: (Fill in parts in red)

Subject: Upcoming rollout of **Enter Your Chosen Deployment Method here (MDM, MAM, Work Profile MAM+MDM) for iOS and Android Devices**

Dear Executive Team **(Or Alternative Leadership Team name)**,

Over the next several weeks, IT will be rolling out **Enter Your Chosen Deployment Method here (MDM, MAM, Work Profile MAM+MDM) for iOS and Android** phones, tablets, and laptops used to access Company email, files, and business apps. This is a strategic security initiative aimed at better protecting our data while still supporting flexible, mobile work.

Why we're doing this

We are seeing a sharp increase industry-wide in:

- Targeted phishing and account takeovers via mobile devices
- Data loss from lost/stolen phones and unmanaged apps (e.g., personal mail and file apps)
- Regulatory and customer expectations around data protection and incident response

Today, many of our devices and apps that access company data are not consistently governed. MDM and MAM will allow us to:

- **Protect Company data** on both corporate and personal (BYOD) devices
- **Enforce minimum security standards** (screen lock, encryption, OS updates) where appropriate
- **Remotely remove corporate data** from a device that is lost, stolen, or when someone leaves the company
- **Demonstrate due diligence** to customers, auditors, and regulators

What is changing

1. **Corporate devices (Delete this section if it does not apply)**
    - Corporate-issued phones/laptops will be **fully enrolled in MDM**.

    - IT will manage security settings (encryption, password policy, OS updates) and install required business apps.
    - If a device is lost or compromised, IT can remotely wipe corporate data (and, if needed for corp-owned devices, the full device).
2. **Personal devices (BYOD) (Delete this section if it does not apply)**
    - For employees who choose to use personal phones for work, IT will use **MAM and work profiles** (where supported) to protect only the **work side**:
        - Work apps (e.g., Outlook, Teams, OneDrive) will have additional protections like preventing copying data to unmanaged apps and requiring a PIN/biometric.
        - If someone leaves the company or loses the device, IT can **remove only corporate data and apps**, not personal photos, messages, or apps.
    - Use of personal devices for work will remain optional; however, if used, they must meet the new security standard.

What this means for you

For executives and their teams, the most visible changes will be:

- A short **enrollment step** on mobile devices that access company resources
- Work apps may prompt for a **PIN/biometric** and will enforce some restrictions (for example, how files can be saved or shared).
- In the event of a lost or stolen device, IT will be able to **quickly remove company data** without waiting for carrier support.

Privacy and boundaries – Update to your specific environment's relative devices

We know privacy is a key concern, especially on personal devices. To be clear:

- On **corporate devices**, IT manages the full device, as is standard practice.
- On **personal devices**, IT will:
    - Manage only the **work profile/apps and corporate data**.
    - Not access your personal photos, texts, call history, or personal apps.
    - Be able to remove corporate data and work apps, but not wipe the personal side of the device.

We will publish a short **"What IT can and cannot see"** summary for all employees as part of the rollout.

Timeline & next steps

Phase 1: Prerequisites and choosing the deployment method – This has been completed

Phase 2: Configurations – Current Phase

Steps:

- Stakeholder Advisory Communication
- Request for Test Users Communication
- Deployment Method Configuration(s)

Phase 3: Test Phase
Steps:

- Test Users Notification of Implementation Communication
- Test Phase Implementation

Phase 4: Full Deployment
Steps:

- Stakeholder Full Deployment Communication
- Org wide communication
- Full Deployment Implementation

You will receive a separate message with **specific dates**, enrollment instructions, and support options. Our ask from you now:

1. **Endorse the initiative** with your teams; this is a business risk reduction effort, not an IT preference.
2. **Encourage staff to participate in the pilot** and share feedback on the experience.

If you have questions or concerns—particularly about executive use cases, travel scenarios, or sensitive workflows—please reach out to me directly or to the IT Security team, and we'll address them one-on-one.
Best regards,

Request for Test Users

Below you will find a sample communication that is recommended to be sent to department leaders for assistance with putting together a list of approved test users. It is recommended that you pull test users from multiple departments / roles when possible.

Sample Communication: (Fill in the parts in red)

Subject: XYZ

Dear **Insert Leadership Team name here (Senior Leaders, Team Leads, Senior Management Etc.)**

We are pleased to announce our new **Enter Your Chosen Deployment Method here (MDM, MAM, Work Profile MAM+MDM) for iOS and Android** phones, tablets, and laptops used to access Company email, files, and business apps. This is a strategic security initiative aimed at better protecting our data while still supporting flexible, mobile work.

It is with the support of our executive leadership team (**Or Alternative Leadership Team name)** that we will be rolling this out and in order to support a smooth rollout of the new mobile management solution, we will first run a pilot with a limited test group before moving to an organization-wide deployment.

We are asking you to identify and request volunteers from your team to participate in this pilot.

Who should be included

When selecting participants, please prioritize individuals who:

- Regularly use mobile devices to access organizational resources (email, calendar, document management, case systems, etc.).
- Are willing to provide feedback on their experience.
- Are comfortable with some controlled changes to how they access organizational resources on their mobile device.

Please reply to this email with any individuals that you feel may be a good fit for this. Thank you for your collaboration and cooperation.

Phase 2 - Section 2:
Configuring the Deployment Method(s)

MDM

The purpose of this part of the section is to provide step by step instructions for configuring MDM for iOS and/or Android for managed devices. If you are not deploying MDM for iOS or Android devices as one of your chosen deployment methods, then skip this step. If you are only implementing MDM for iOS and not Android or vice versa then skip the device type you are not implementing MDM for.

Disclaimers

- Before performing any of the steps that follow in this guide, you MUST complete all steps in the "Phase 1 Section 1: Prerequisites" section that you were provided.

- Steps in this guide at times will walk you through creating and configuring various policies, profiles, etc. and it is important for anyone following this guide to understand that only values for these items that differ from the default setting are listed. DO NOT change other settings from their default values unless you are certain that the results of that action are desired and realize that you are doing so at your own risk.

Security Groups:

The first step of this deployment method is to set up a security group for the MDM test phase.

- Navigate to Azure>Microsoft EntraID> Manage>Groups (Entra Groups)
- Click "New group"
- Group Type will be Security
- Group name will be "AAD-SUG-Intune-Mobile-MDM-StaticTestGroup"
- For Description enter "Group of users to participate in testing prior to deployment. <your 1st initialLast name>".
- Assign the owner of the group to the Global Administrator account you are using for deployment

MDM for iOS

Compliance Policy

The next step to configuring MDM for iOS is to set up the compliance policy. This will ensure that the enrolled devices meet certain minimum-security requirements.

- Navigate to: Intune > Devices > Manage devices | Compliance > Policies (Compliance Policies)
- Click "+ Create policy" to create a new compliance policy
- In the Create a Policy pane, for Platform select iOS/iPadOS
- Set the profile type to iOS compliance policy (If it isn't by default)
- Click Create (or Next depending on UI)
- Name the policy "Intune-Devices-Compliance-iOS-MDM"
- Set the policy description to "Policy for MDM (AKA fully managed devices). <FirstInitial.LastName>".
- Click Next

Configure the Compliance Settings:

Device Health:

- Under the "Device Health" header:
  - Set "Jailbroken devices" to Block.

Device Properties:

- Under the "Device Properties" header:
  - Set "Minimum OS version" to 8

System Security:

- Under the "System Security" header:
  - Set "Require a password to unlock mobile devices" to Require
  - Set the "Minimum password length" to 4
  - Set the "Require password type" to Numeric
  - Set the "Maximum minutes after screen lock before password is required" to 0 minutes
  - Set the "Maximum minutes of inactivity until screen locks" to 10 minutes
  - Click Next

Configure the Actions for Non-Compliance:

- Leave the existing action (immediately mark the device as noncompliant)
- Add another action to immediately Send a push notification to the end user. (Write steps in greater detail)
- Click Next

Configure the Assignments:

- Under Included Groups, click “Add groups”
- Check the box next to the previously created test group “AAD-SUG-Intune-Mobile-MDM-StaticTestGroup” and then click Select at the bottom of the pane
- Click Next

Review + Create

- Click Create

Device Configuration Policy

In this step you will create the Device Configuration Policy. The settings in this policy will control various functions of the fully managed iOS devices.

Create the Policy:

- Navigate to: Intune > Devices > Manage devices > Configuration >Policies (Configuration Policies)
- Click “+ Create” and select “+ New Policy” in the dropdown menu
- For Platform select iOS/iPadOS devices
- For Profile Type select Templates
- Select Device Restrictions
- Click Create

Basics

- Name the policy “Intune-Devices-Config-iOS-MDM-DeviceConfig”
- Enter “Restrictions for corporate devices running MDM (AKA fully managed devices). <FirstInitial.LastName>” for the policy description
- Click Next to continue to Configuration Settings

Configuration settings

App Store, Doc Viewing, Gaming:

- Under the App Store > Doc Viewing > Gaming Header:
  - Set “Block viewing corporate documents in unmanaged apps” to Yes
  - Set “Treat AirDrop as an unmanaged destination” to Yes

    - Set “Allow copy/paste to be affected by managed open-in” to Yes
    - Set “Block playback of explicit music, podcast, and iTunes U” to Yes

General:

- Under the General Header:
    - Set “Block screenshots and screen recording” to Yes,
    - And “Block trusting new enterprise app authors” to Yes.

Password:

- Under the Password Header:
    - Set “Require password” to Yes,
    - “Required password type” to Numeric,
    - “Minimum password length” to 4,
    - “Number of sign-in failures before wiping device” to 11,
    - “Maximum minutes after screen lock before password is required” to “Immediately”,
    - And “Maximum minutes of inactivity until screen locks” to 10 minutes.

Wireless:

- Under the Wireless Header:
    - Set “Block data roaming” to Yes
- Click Next to proceed to Assignments

Configure the Assignments:

- Under Included Groups, click “Add groups”
- Check the box next to the previously created test group “AAD-SUG-Intune-Mobile-MDM-StaticTestGroup” and then click Select at the bottom of the pane
- Click Next

Review + Create

- Click Create

App List

In this step you will configure the assignment for the iOS app list the you setup in the iOS App Selection and Licenses prerequisite step. Follow the steps below to complete this task:

- Navigate to Intune>Apps>iOS/iPadOS (iOS/iPadOS apps)
- For each iOS app in the list, click the app name to open the app overview

- Under manage, click properties
- Click Edit to the right of Assignments
- Under the Required section click “Add group”:
    - Search for the “AAD-SUG-Intune-Mobile-MDM-StaticTestGroup” group, check the box next to the group and click Select
- Click Review + save

Conditional Access Policy

In this step you will be creating and configuring a new Conditional Access Policy so that you can control the availability of resources to iOS devices.

Create the Policy:

- Navigate to Entra>Conditional Access>Policies (Conditional Access Policies)
- Click “+ New policy”
- Name the policy “CAP-iOSMDM-Blocked”
- Continue to Assignments

Assignments:

- Leave “What does this policy apply to?” set to Users and groups
- Under Include:
    - Click the bubble next to “Select users and groups”
    - Check the Users and groups box
    - Search for the “AAD-SUG-Intune-Mobile-MDM-StaticTestGroup” group, check the box next to the group and click Select
- Under Exclude:
    - Check the Users and groups box
    - Search for the “CAPSG-MAM-MDM-NotBlocked” group, check the box next to the group and click Select
- Continue to Target Resources

Target Resources:

- Under Include:
- Click the bubble next to “Select resources”
- Click the “None” text hyperlink under “Select Specific Resources”
- Check the box next to Office 365 and click Select
- Continue to Conditions

Conditions:

- Under Device Platforms:
  - Select the “Not Configured” hyperlink under Device Platforms
  - Set Configure to Yes
  - Under Include, check the box next to iOS
- Under Client apps:
  - Select the “Not Configured” hyperlink under Client apps
  - Set Configure to Yes
  - Under Include, check the box next to Browser and the box next to Mobile apps and desktop clients
- Continue to Access Controls

Access Controls:

- Under Grant:
  - Select the “0 controls selected” hyperlink
  - Make sure the select bubble at the top is “Grant Access” and check the box next to “Require device to be marked as compliant” and click Select

Enable the Policy

- The final step is to enable the policy. It is important that you correctly complete all the steps in this section before enabling this policy.
- Once you have reviewed all the settings and feel confident that they are correct, at the bottom of the page, change the Enable Policy setting from “Report Only” to “On”

Enrollment Profile

Next, you will need to set up the Enrollment Profile. These profiles are part of the requirements to add fully managed devices to Intune.

- Navigate to the following location in Intune to create the token: Intune > Devices > Device onboarding > Enrollment > Apple > Enrollment Program Tokens (Apple Enrollment Program Tokens)
- Click on the existing Apple enrollment program token that was created in the prerequisite steps
- Click Manage
- Click the Profiles tab
- Click “+ Create profile”
- For Platform, choose iOS/iPad
- Navigate to Basics:
  - Name the profile “Intune-Devices-EnrollmentProfile-iOS-MDM”

  - Input “Enrollment profile for MDM (AKA Corporate owned device management). <FirstInitial.LastName>” as the device description
  - Set Device Type to iOS/iPadOS
- Navigate to Management Settings:
- Set User Affinity to “Enroll with User Affinity” (This should display more settings once chosen)
- Leave the authentication method as Company Portal
  - Under that, Install Company Portal with VPP should have “Use Token:” set to the token created during prerequisites
  - If it shows a different file or says none is available, go back to the iOS App Selection and Licenses section of the prerequisites and make sure you properly followed the steps to assign the Company Portal in Apple Business Manager
- Set Locked enrollment to “Yes”
- Set Sync with computers: to “Deny All”
- Set Apply device name template to “Yes”
- Set Device Name Template to “{{DEVICETYPE}}{{SERIAL}}”
- Set Activate cellular data to “No”.
- Under the Setup Assistant section
  - Set Department to the company name
  - Set the Department Phone to the desired IT support phone number
- Make sure the following items are toggled to “Show” (Default may be hide)
  - Passcode
  - Touch ID
  - Face ID
  - Get Started
- Navigate to Assignments
  - Assign the profile to All Devices linked to this token (Or adjust to specific devices by manually selecting them)
- Navigate to Review + create
  - Review the profile details and if everything looks correct, click Create

Enrolling Devices

Prerequisites:

- Devices are purchased as corporate devices and appear in Apple Business Manager (ABM) and Devices are assigned to the Intune MDM server in ABM.

    - If there are corporate iOS devices that are legacy devices that weren’t added into Apple Business Manager at the time of purchase they need to be added into ABM via the Apple Configurator. Here are the steps for that:
        - Note: This method requires a spare designated iOS device that will be used as the “Configurator Phone” to add all other iOS devices into the companies ABM instance as a managed device
        - On the Configurator phone:
            - Install Apple Configurator (Mac) or Apple Configurator for iPhone from the app store and sign in with a Managed Apple ID that has Device Enrollment / Administrator rights in ABM.
        - On the iOS devices to be added into ABM:
        - **Back up** any important data from the iOS devices as they **must be erased** to be added.
        - Put the devices into setup / erase it so it starts at “Hello”.
            - On the device: Settings → General → Transfer or Reset iPhone → Erase All Content and Settings.
        - Using Configurator Phone:
            - Bring the Configurator iPhone near the device at the **Wi-Fi / Country** screen and scan the pairing image to upload its info to ABM.
            - During the Configurator workflow, choose to **assign the devices to your MDM server** (Intune)
        - After the process is completed, the iOS devices appear in **ABM → Devices** like any other DEP/ADE device and will enroll into Intune the next time you run Setup Assistant.

Enrollment Steps:

- Make sure the device is either brand new or has been erased:
    - On the device: Settings → General → Transfer or Reset iPhone → Erase All Content and Settings.
- Power on the iPhone/iPad.
- Go through the initial Setup Assistant screens:
    - Choose language and region.
    - Connect to Wi-Fi (or cellular if available).
- The device contacts Apple and detects it is owned by your organization.
- When you see “Remote Management” / “This iPhone/iPad is managed by <Your Org>”:

    - Tap Next or Continue to accept management.
- Sign in with your work (Entra ID/Azure AD) account during setup.
- Allow the installation of the management profile when prompted (this happens automatically with ADE; no manual profile download needed).
- Wait while the device:
    - Enrolls into Intune MDM.
    - Applies configuration profiles (Wi-Fi, restrictions, certificates, etc.).
- Installs required apps (Company Portal, Outlook, Teams, line-of-business apps, etc.).
- Once setup completes, unlock the device and confirm:
    - Required apps are present.
    - Any enforced passcode or other compliance settings are configured.
- (Optional but recommended) Open Company Portal to verify the device shows as Compliant.

MDM for Android

Compliance Policy

The first step to configuring MDM for Android is to set up the compliance policy. This will ensure that the enrolled devices meet certain minimum-security requirements.

Create the Policy:

- Navigate to: Intune > Devices > Manage devices | Compliance > Policies (Compliance Policies)
- Click "+ Create policy" to create a new compliance policy
- In the Create a Policy pane, for Platform select Android Enterprise
- Set the Profile type to Fully Managed, dedicated, and corporate-owned work profile
- Click Create (or Next depending on UI)
- Name the policy "Intune-Devices-Compliance-Android-MDM".
  Set the description to "Policy for MDM (AKA fully managed devices).
  <FirstInitial.LastName>".
- Continue to Compliance Settings

Configure the Compliance Settings:

Device Health:

- Expand the "Device Health" section:
  - Set "Rooted devices" to Block
  - Set "Minimum OS version" to 8
- Continue to Device Properties

Device Properties

- Expand the "Device Properties" section:
  - Set "Minimum OS version" to 8
- Continue to System Security

System Security:

- Expand the "System Security" Section:
  - Set "Require a password to unlock mobile devices" to Require
  - Set "Minimum password length" to 4
  - Set "Require encryption of data storage on device" to Require
- Click Next to continue to Actions for Non-Compliance header

Actions for Non-Compliance:

- Leave the existing action (immediately mark the device as noncompliant)
- Add another action to immediately Send a push notification to the end user. (Write steps in greater detail)
- Click Next to continue to Assignments

Configure the Assignments:

- Under Included Groups, click "Add groups"
- Check the box next to the previously created test group "AAD-SUG-Intune-Mobile-MDM-StaticTestGroup" and then click Select at the bottom of the pane
- Click Next

Review + Create

- Click Create

Device Configuration Policy

In this step we will create the Device Configuration Policy. The settings in this policy will control various functions of the fully managed android devices.

Create the Policy:

- Navigate to: Intune > Devices > Manage devices > Configuration >Policies (Configuration Policies)
- Click "+ Create" and select "+ New Policy" in the dropdown menu
- For Platform Select Android Enterprise
- Select to use templates.
  - Note: The templates are divided into two sections, "Fully Managed…" and "Personally-Owned Work Profile"
  - Under the Fully Managed, Dedicated and Corporate-Owned Work Profile section, select "Device restrictions"
  - Click Create at the bottom of the pane

Basics

- Name the policy "Intune-Devices-Config-Android-MDM-DeviceConfig"
- Set the policy description to "Restrictions for corporate devices running MDM (AKA fully managed devices)."
- Click Next to continue to Configuration Settings

Configuration settings

General:

- Expand the "General" section:
  - Set "Screen capture (work profile-level)" to Block
  - Set "USB file transfer" to Block
  - Set "External media" to Block
  - Set "Beam data using NFC (work profile-level)" to Block
  - Set "Contact sharing via Bluetooth (work profile-level)" to Block

Device Password:

- Expand the "Device password" section:
  - Set "Require password type" to Numeric
  - Set "Minimum password length" to 4
  - Set "Number of sign-in failures before wiping device" to 11
- Click Next to continue to Assignments

Configure the Assignments:

- Under Included Groups, click "Add groups"
- Check the box next to the previously created test group "AAD-SUG-Intune-Mobile-MDM-StaticTestGroup" and then click Select at the bottom of the pane

- Click Next

Review + Create

- Click Create

App List

In this step you will configure the app list for Android that you would like to implement controls for. Please note this list varies environment to environment and the example apps listed in this section are just a general universal recommendation that you may wish to amend to better suit your environment's needs.

Create the list:

- Navigate to: Intune>Apps>All Apps (All Apps)
- Verify if the apps you wish to manage are already in the list.
    - Example Apps:
        - 365 Copilot
        - Acrobat Reader
        - Azure
        - Edge
        - Excel
        - OneDrive
        - Outlook
        - PowerPoint
        - Teams
        - To-Do
        - Word
        - OneNote
- For needed apps not currently in the list:
    - Click "+ Create"
    - Set the "App Type to Managed Google Play app"
    - Click Select
    - Search for and click on the app then click Select
    - Click Sync at the top
    - You should be back at the original All apps list now. Click the Intune Refresh button above search and you should now see the app in the list

Assignments:

- For each Android app in the list with Type set to "Managed Google Play store app" that you wish to manage as part of this deployment method, click the app name to open the app overview
- Under manage, click properties
- Click Edit to the right of Assignments
- Under the Required section click "Add group":

    - Search for the “AAD-SUG-Intune-Mobile-MDM-StaticTestGroup” group, check the box next to the group and click Select
- Click Review + save

Conditional Access Policy

In this step you will be creating and configuring a new Conditional Access Policy so that you can control the availability of resources to Android Devices.

Create the Policy:

- Navigate to Entra>Conditional Access>Policies (Conditional Access Policies)
- Click “+ New policy”
- Name the policy “CAP-AndroidMDM-Blocked”
- Continue to Assignments

Assignments:

- Leave “What does this policy apply to?” set to Users and groups
- Under Include:
    - Click the bubble next to “Select users and groups”
    - Check the Users and groups box
    - Search for the “AAD-SUG-Intune-Mobile-MDM-StaticTestGroup” group, check the box next to the group and click Select
- Under Exclude:
    - Check the Users and groups box
    - Search for the “CAPSG-MAM-MDM-NotBlocked” group, check the box next to the group and click Select
- Continue to Target Resources

Target Resources:

- Under Include:
- Click the bubble next to “Select resources”
- Click the “None” text hyperlink under “Select Specific Resources”
- Check the box next to Office 365 and click Select
- Continue to Conditions

Conditions:

- Under Device Platforms:
    - Select the “Not Configured” hyperlink under Device Platforms

    - Set Configure to Yes
    - Under Include, check the box next to Android
- Under Client apps:
    - Select the “Not Configured” hyperlink under Client apps
    - Set Configure to Yes
    - Under Include, check the box next to Browser and the box next to Mobile apps and desktop clients
- Continue to Access Controls

Access Controls:

- Under Grant:
    - Select the “0 controls selected” hyperlink
    - Make sure the select bubble at the top is “Grant Access” and check the box next to “Require device to be marked as compliant” and click Select

Enable the Policy

- The final step is to enable the policy. It is important that you correctly complete all the steps in this section before enabling this policy.
- Once you have reviewed all the settings and feel confident that they are correct, at the bottom of the page, change the Enable Policy setting from “Report Only” to “On”

Enrollment Profile

Next, you will need to set up the Enrollment Profile. These profiles are part of the requirements to add fully managed devices to Intune.

Create the profile:

- Navigate to: Intune > Devices > Device onboarding > Enrollment (Device Enrollment)
- Select the Android header
- Under Enrollment Profiles, select Corporate-owned, fully managed user devices
- Click “+ Create policy”

Basics

- Under the Basics Header:
    - Name it “Intune-Devices-EnrollmentProfile-Android-MDM”
    - Enter “Enrollment profile for MDM (AKA Corporate owned device management). <FirstInitial.LastName>” for the description
    - Set the token type to “Corporate-owned, fully managed (default)”
    - Set “Apply device name template” to Yes

    - Set the “Device name template” to “{{UPNPREFIX}}{{DEVICETYPE}}{{SERIALLAST4DIGITS}}”
    - Click Next to continue to the “Device group” header

Device group

- Under the Device group header
    - Make sure None is the selected Radial button
    - Click next to continue to Review + create

Review + Create

- Review the summary information and if everything looks correct click Create

Save the Enrollment Token

- Navigate to: Intune > Devices > Device onboarding > Enrollment (Device Enrollment)
- Select the Android header
- Under Enrollment Profiles, select Corporate-owned, fully managed user devices
- Select the Enrollment Profile you just created
    - Select Token
    - Select Export (This will save it to your downloads folder, move it to a known location as it will be needed for later enrollments)
    - It is also recommended to print out the QR code as it can also be used for enrolling devices.

Enrolling Devices

This step is for enrolling corporate-owned Android devices where IT controls the full device. It is important to note that this will perform a factory reset on the device and **all data will be lost**:

- Factory reset the device if it’s already in use (required for fully managed enrollment).
- Power on the device and go through the initial Android setup screens (language, Wi-Fi, etc.).
- When you reach the **Google account** or setup screen, follow the enrollment method you’ve chosen (depending on how Intune is configured):
    - QR code enrollment: On another device or printed doc, show the Intune-generated QR code. On the Android device, tap the welcome screen 6 times (or the QR icon, if available) to launch the QR scanner, then scan the Intune QR code.

    - AFW token (“androidforwork”): At the Google account screen, type afw#setup or your Intune-specific token; this will trigger downloading the **Android Device Policy** / Company Portal for enterprise.
- Accept the prompts to set the device as managed by your organization.
- Sign in with your work account when prompted.
- Let the device apply the **Intune device policy** (might reboot or take a few minutes).

Once finished, required apps and configurations (Wi-Fi, certificates, restrictions) will be pushed down from Intune and the device will appear in Intune as **enrolled and (once checks pass) compliant**.

MAM

The purpose of this part of the section is to provide step by step instructions for configuring MAM for iOS and/or Android for managed devices. If you are not deploying MAM for iOS or Android devices as one of your chosen deployment methods, then skip this step. If you are only implementing MAM for iOS and not Android or vice versa then skip the device type you are not implementing MAM for.

Disclaimers

- Before performing any of the steps that follow in this guide, you MUST complete all steps in the “Phase 1 Section 1: Prerequisites” section that you were provided.

- Steps in this guide at times will walk you through creating and configuring various policies, profiles, etc. and it is important for anyone following this guide to understand that only values for these items that differ from the default setting are listed. DO NOT change other settings from their default values unless you are certain that the results of that action are desired and realize that you are doing so at your own risk.

Security Groups:

The first step of this deployment method is to set up a security group for the MAM test phase.

- Navigate to Azure>Microsoft EntraID> Manage>Groups (Entra Groups)
- Click “New group”
- Group Type will be Security

- Group name will be “AAD-SUG-Intune-Mobile-MAM-StaticTestGroup”
- For Description enter “Group of users to participate in testing prior to deployment. <your 1st initialLast name>”
- Assign the owner of the group to the Global Administrator account you are using for deployment

MAM for Android

App Protection Policy

The first step to configuring MAM for Android is to set up an App Protection policy. This will be used to protect and control corporate data inside specific apps.

Create the Policy:

- Navigate to Intune > Apps > Protection (App Protection Policies)
- Click “+ Create” and select Android in the dropdown menu

Basics

- Name the policy “Intune-Apps-Protection-Android-4-Digit-Year-2-Digit-Month”
- Enter “App-level rules that protect this organization’s data inside supported Android apps (e.g., Outlook, Teams). <your 1st initialLast name>” as the policy description
- Click Next to continue to Apps

Apps

- Select Target Policy to Selected Apps
- Select and add the apps you wish to manage by clicking +Select public apps.
  - (This will likely match the app list you created in the prerequisite step iOS App selection and Licenses)
- If you have any non-public custom apps that your company uses on Android, select the +Select custom apps and add them.
- Click next to continue to Data Protection

Data Protection

- Set Backup org data to Android backup services to Block
- Set Send org data to other apps to Policy managed apps
- Set Save copies of org data to Block
- Set Allow user to save copies to selected services to OneDrive for Business and SharePoint
- Set Transfer messaging data to Any policy managed messaging app

- Set Screen capture and Google Assistant to Block
- Set Sync Policy managed app data with native apps or add-ins to Block
- Set Printing org data to Block
- Set Restrict web content transfer with other apps to Microsoft Edge
- Click Next to continue to Access Requirements

Access Requirements

- Change Timeout (Minutes of Inactivity) to 60
- Change Recheck the access requirements after (Minutes of Inactivity) to 60
- Click Next to continue to Conditional Launch

Conditional Launch

- Leave all settings set to Default
- Click Next to continue to Assignments

Assignments

- Under Included Groups, click "Add groups"
- Check the box next to the previously created test group "AAD-SUG-Intune-Mobile-MAM-StaticTestGroup" and then click Select at the bottom of the pane
- If you are running a multi-deployment environment and have created an assignment filter, add it here as well in the assignment filter tab.
- Click Next to continue to Review + Create

Review + Create

- Review the Summary and if everything looks correct, click Create

Conditional Access Policy

In this step you will be creating and configuring a new Conditional Access Policy so that you can control the availability of resources to Android devices.

Create the Policy:

- Navigate to Entra>Conditional Access>Policies (Conditional Access Policies)
- Click "+ New policy"
- Name the policy "CAP-Android-MAM-App-Blocked"

Assignments:

- Leave "What does this policy apply to?" set to Users and groups

- Under Include:
  - Click the bubble next to “Select users and groups”
  - Check the Users and groups box
  - Search for the “AAD-SUG-Intune-Mobile-MAM-StaticTestGroup” group, check the box next to the group and click Select
- Under Exclude:
  - Check the Users and groups box
  - Search for the “CAPSG-MAM-MDM-NotBlocked” group, check the box next to the group and click Select

Target Resources:

- Under Include:
- Click the bubble next to “All Resources” (Formerly ‘All cloud apps’)
- Continue to Conditions

Conditions:

- Under Device Platforms:
  - Select the “Not Configured” hyperlink under Device Platforms
  - Set Configure to Yes
  - Under Include, check the box next to Android

- **If you are implementing MDM in addition to MAM and ONLY if you are implementing both, perform the following:**
  - Go to Conditions
  - Filter for Devices
  - Set Configure to Yes
  - Click the radial button next to “Exclude filtered devices from policy
  - Click Edit
  - Copy and Paste the follow code:

    (device.isCompliant -eq true) -or (device.trustType -eq "ServerAD") -or (device.trustType -eq "AzureAD")

  - Click Done

Access Controls:

- Under Grant:
  - Select the “0 controls selected” hyperlink

    - Make sure the select bubble at the top is “Grant Access” and check the box next to “Require app protection policy” and click Select

Enable the Policy

- The final step is to enable the policy. It is important that you correctly complete all the steps in this section before enabling this policy.
- Once you have reviewed all the settings and feel confident that they are correct, at the bottom of the page, change the Enable Policy setting from “Report Only” to “On”

MAM for iOS

App Protection Policy

The first step to configuring MAM for iOS is to set up an App Protection policy. This will be used to protect and control corporate data inside specific apps.

Create the Policy:

- **Navigate to Intune > Apps > Protection (App Protection Policies)**
- Click “+ Create” and select iOS/iPadOS in the dropdown menu

Basics

- Name the policy “Intune-Apps-Protection-iOS-4-Digit-Year-2-Digit-Month”
- Enter “App-level rules that protect this organization’s data inside supported Android apps (e.g., Outlook, Teams). <your 1st initialLast name>” as the policy description
- Click Next to continue to Apps

Apps

- Select Target Policy to Selected Apps
- Select and add the apps you wish to manage by clicking +Select public apps.
    - (This will likely match the app list you created in the prerequisite step iOS App selection and Licenses)
- If you have any non-public custom apps that your company uses on Android, select the +Select custom apps and add them.
- Click Next to continue to Data Protection

Data Protection

- Set “Backup Org Data to iTunes and iCloud Backups” to Block
- Set “Send Org Data to Other Apps” to Policy Managed Apps
- Set “Save Copies of Org Data” to Block

- Set “Allow Users to Save Copies” to Selected Services to OneDrive for Business and SharePoint
- Set “Transfer Telecommunication Data” to None, do not transfer this data between apps
- Set “Transfer Messaging Data” to None, do not transfer this data between apps
- Set “Sync Policy Managed App Data with Native Apps or Add-ins” to Block
- Set “Printing Org Data” to Block
- Set “Restrict Web Content Transfer with Other Apps” to Microsoft Edge
- Set “Screen Capture” to Block
- Click Next to continue to Access Requirements

Access Requirements

- Change Timeout (Minutes of Inactivity) to 60
- Change Recheck the access requirements after (Minutes of Inactivity) to 60
- Click Next to continue to Conditional Launch

Conditional Launch

- Leave all settings set to Default
- Click Next to continue to Assignments

Assignments

- Under Included Groups, click “Add groups”
- Check the box next to the previously created test group “AAD-SUG-Intune-Mobile-MAM-StaticTestGroup” and then click Select at the bottom of the pane
- If you are running a multi-deployment environment and have created an assignment filter, assign it here as well in the assignment filter tab.
- Click Next to continue to Review + Create

Review + Create

- Review the Summary and if everything looks correct, click Create

Conditional Access Policy

In this step you will be creating and configuring a new Conditional Access Policy so that you can control the availability of resources to iOS devices.

Create the Policy:

- Navigate to Entra>Conditional Access>Policies (Conditional Access Policies)
- Click "+ New policy"
- Name the policy "CAP-iOS-MAM-App-Blocked"

Assignments:

- Leave "What does this policy apply to?" set to Users and groups
- Under Include:
  - Click the bubble next to "Select users and groups"
  - Check the Users and groups box
  - Search for the "AAD-SUG-Intune-Mobile-MAM-StaticTestGroup" group, check the box next to the group and click Select
- Under Exclude:
  - Check the Users and groups box
  - Search for the "CAPSG-MAM-MDM-NotBlocked" group, check the box next to the group and click Select

Target Resources:

- Under Include:
- Click the bubble next to "All Resources" (Formerly 'All cloud apps')
- Continue to Conditions

Conditions:

- Under Device Platforms:
  - Select the "Not Configured" hyperlink under Device Platforms
  - Set Configure to Yes
  - Under Include, check the box next to iOS

- **If you are implementing MDM in addition to MAM and ONLY if you are implementing both, perform the following:**
  - Go to Conditions
  - Filter for Devices
  - Set Configure to Yes
  - Click the radial button next to "Exclude filtered devices from policy
  - Click Edit
  - Copy and Paste the follow code:

(device.isCompliant -eq true) -or (device.trustType -eq "ServerAD") -or (device.trustType -eq "AzureAD")

- Click Done

Access Controls:

- Under Grant:
  - Select the “0 controls selected” hyperlink
  - Make sure the select bubble at the top is “Grant Access” and check the box next to “Require app protection policy” and click Select

Enable the Policy

- The final step is to enable the policy. It is important that you correctly complete all the steps in this section before enabling this policy.
- Once you have reviewed all the settings and feel confident that they are correct, at the bottom of the page, change the Enable Policy setting from “Report Only” to “On”

Work Profile MAM+MDM

The purpose of this part of the section is to provide step by step instructions for configuring Work Profile MAM+MDM for iOS and/or Android for managed devices. If you are not deploying Work Profile MAM+MDM for iOS or Android devices as one of your chosen deployment methods, then skip this step. If you are only implementing Work Profile MAM+MDM for iOS and not Android or vice versa then skip the device type you are not implementing Work Profile MAM+MDM for.

Disclaimers

- Before performing any of the steps that follow in this guide, you MUST complete all steps in the “Phase 1 Section 1: Prerequisites” section that you were provided.

- Steps in this guide at times will walk you through creating and configuring various policies, profiles, etc. and it is important for anyone following this guide to understand that only values for these items that differ from the default setting are listed. DO NOT change other settings from their default values unless you are certain that the results of that action are desired and realize that you are doing so at your own risk.

Security Groups:

The first step of this deployment method is to set up a security group for the MDM test phase.

- Navigate to Azure>Microsoft EntraID> Manage>Groups (Entra Groups)
- Click "New group"
- Group Type will be Security
- Group name will be "AAD-SUG-Intune-Mobile-WorkProfileMAMMDM-StaticTestGroup"
- For Description enter "Group of users to participate in testing prior to deployment. <your 1st initialLast name>"
- Assign the owner of the group to the Global Administrator account you are using for deployment

Work Profile MAM+MDM for Android

App Protection Policy

The first step to configuring Work Profile MAM+MDM for Android is to set up an App Protection policy. This will be used to protect and control corporate data inside specific apps.

Create the Policy:

- Navigate to Intune > Apps > Protection (App Protection Policies)
- Click "+ Create" and select Android in the dropdown menu

Basics

- Name the policy "Intune-Apps-Protection-Android-4-Digit-Year-2-Digit-Month"
- Enter "App-level rules that protect this organization's data inside supported Android apps (e.g., Outlook, Teams). <your 1st initialLast name>" as the policy description
- Click Next to continue to Apps

Apps

- Select Target Policy to Selected Apps
- Select and add the apps you wish to manage by clicking +Select public apps.
  - (This will likely match the app list you created in the prerequisite step iOS App selection and Licenses)
- If you have any non-public custom apps that your company uses on Android, select the +Select custom apps and add them.

- Click next to continue to Data Protection

Data Protection

- Set Backup org data to Android backup services to Block
- Set Send org data to other apps to Policy managed apps
- Set Save copies of org data to Block
- Set Allow user to save copies to selected services to OneDrive for Business and SharePoint
- Set Transfer messaging data to Any policy managed messaging app
- Set Screen capture and Google Assistant to Block
- Set Sync Policy managed app data with native apps or add-ins to Block
- Set Printing org data to Block
- Set Restrict web content transfer with other apps to Microsoft Edge
- Click Next to continue to Access Requirements

Access Requirements

- Change Timeout (Minutes of Inactivity) to 60
- Change Recheck the access requirements after (Minutes of Inactivity) to 60
- Click Next to continue to Conditional Launch

Conditional Launch

- Leave all settings set to Default
- Click Next to continue to Assignments

Assignments

- Under Included Groups, click “Add groups”
- Check the box next to the previously created test group “AAD-SUG-Intune-Mobile-WorkProfileMAMMDM-StaticTestGroup” and then click Select at the bottom of the pane
- Click Next to continue to Review + Create

Review + Create

- Review the Summary and if everything looks correct, click Create

Compliance Policy

The next step to configuring Work Profile MAM+MDM for Android is to set up the compliance policy. This will ensure that the enrolled devices meet certain minimum-security requirements.

Create the Policy:

- Navigate to: Intune > Devices > Manage devices | Compliance > Policies (Compliance Policies)
- Click "+ Create policy" to create a new compliance policy
- In the Create a Policy pane, for Platform select Android Enterprise
- Set the Profile type to Personally Owned Work Profile
- Click Create (or Next depending on UI)
- Name the policy "Intune-Devices-Compliance-Android-WorkProfile-MAM+MDM". Set the description to "Policy for WorkProfile-MAM+MDM (AKA fully managed devices). <FirstInitial.LastName>".
- Continue to Compliance Settings

Configure the Compliance Settings:

Device Health:

- Expand the "Device Health" section:
  - Set "Rooted devices" to Block
  - Set "Google Play Services is configured" to Require
- Continue to Device Properties

Device Properties

- Expand the "Device Properties" section:
  - Set "Minimum OS version" to 8
- Continue to System Security

System Security:

- Expand the "System Security" Section:
  - Set "Require a password to unlock mobile devices" to Require
  - Set "Block apps from unknown sources" to Block
  - Set "Company Portal app runtime integrity" to Require
  - Set "Block USB debugging on device" to Block
  - Set "Require encryption of data storage on device" to Require
- Click Next to continue to Actions for Non-Compliance header

Actions for Non-Compliance:

- Leave the existing action (immediately mark the device as noncompliant)
- Add another action to immediately Send a push notification to the end user. (Write steps in greater detail)
- Click Next to continue to Assignments

Configure the Assignments:

- Under Included Groups, click “Add groups”
- Check the box next to the previously created test group “AAD-SUG-Intune-Mobile-WorkProfileMAMMDM-StaticTestGroup” and then click Select at the bottom of the pane
- Click Next

Review + Create

- Click Create

Device Configuration Policy

Next, we will create the Device Configuration Policy. Follow the steps below to complete this task.

Create the Policy:

- Navigate to: Intune > Devices > Manage devices > Configuration >Policies (Configuration Policies)
- Click “+ Create” and select “+ New Policy” in the dropdown menu
- For Platform, Select Android Enterprise
- Select to use templates.
  - Note: The templates are divided into two sections, “Fully Managed…” and “Personally-Owned Work Profile”
  - Under the Personally-Owned Work Profile, select “Device restrictions”
  - Click Create at the bottom of the pane

Basics

- Name the policy “Intune-Devices-Config-Android-WorkProfile-MAM-MDM”
- Set the policy description to “Restrictions Enabling the Work Profile MAM-MDM.<FirstInitial.LastName>
- Click Next to continue to Configuration Settings

Configuration settings

Work Profile Settings

- Expand the “Work Profile Settings” section:
  - Under General Settings:
    - Set “Data sharing between work and personal profiles” to “Apps in work profile can handle sharing request from personal profile”,
    - And “Default app permissions” to Prompt.

    - Under All Android devices:
        - Set “Require Work Profile Password” to Required,
        - And “Number of sign-in failures before wiping the work profile” to 10.
        - Continue to Assignments

Configure the Assignments:

- Under Included Groups, click “Add groups”
- Check the box next to the previously created test group “AAD-SUG-Intune-Mobile-WorkProfileMAMMDM-StaticTestGroup” and then click Select at the bottom of the pane
- Click Next

Review + Create

- Click Create

App List

In this step you will configure the app list for Android that you would like to implement controls for. Please note this list varies environment to environment and the example apps listed in this section are just a general universal recommendation that you may wish to amend to better suit your environment’s needs.

Create the list:

- Navigate to: Intune>Apps>All Apps (All Apps)
- Verify if the apps you wish to manage are already in the list.
    - Example Apps:
        - 365 Copilot
        - Acrobat Reader
        - Azure
        - Edge
        - Excel
        - OneDrive
        - Outlook
        - PowerPoint
        - Teams
        - To-Do
        - Word
        - OneNote
- For needed apps not currently in the list:
    - Click “+ Create”
    - Set the “App Type to Managed Google Play app”
    - Click Select
    - Search for and click on the app then click Select
    - Click Sync at the top

    - You should be back at the original All apps list now. Click the Intune Refresh button above search and you should now see the app in the list

Assignments:

- For each Android app in the list with Type set to “Managed Google Play store app” that you wish to manage as part of this deployment method, click the app name to open the app overview
- Under manage, click properties
- Click Edit to the right of Assignments
- Under the Required section click “Add group”:
    - Search for the “AAD-SUG-Intune-Mobile-WorkProfileMAMMDM-StaticTestGroup” group, check the box next to the group and click Select
- Click Review + save

Enrollment Profile

Next you will need to setup the BYOD Work Profile Enrollment Profile

Create the Profile

- Navigate to Intune > Devices > Android > Enrollment > (Under) Enrollment options > Device platform restrictions (Enrollment Restrictions)
- Click the Android restrictions header
- Click Create restriction

Basics

- Name the restriction “Android-BYOD-WorkProfile-Enrollment-Restrictions”
- Enter “Enrollment Restrictions for Android BYOD Devices using Work Profile”
- Click Next

Platform Settings

- Android Enterprise (work profile): Allow; Personally owned: Allow
- Android device administrator: Block
- Click Next

Scope Tags

- Leave all Settings to Default
- Click Next

Assignments:

- Click Add groups

- Search for the “AAD-SUG-Intune-Mobile-WorkProfileMAMMDM-StaticTestGroup” group, check the box next to the group and click Select
- Click Next

Review + Create

- Review the Summary and if everything looks correct click Create

Enrolling Devices

Below are the instructions for your users to enroll their devices into Work Profile MAM+MDM.

---

1. On your Android device, install or update:
    - **Intune Company Portal** from the Google Play Store.
2. Open Company Portal and tap Sign in
3. Sign in with your work (Microsoft 365 / Entra ID) account and complete any MFA prompts
4. Review the privacy / what your organization can see information, then tap Continue or Begin
5. On the “Set up your work profile” or “Set up your device” screen, tap Begin / Continue.
6. Company Portal will prompt you to create a work profile:
    - Tap Next / Set up when asked to create a work profile
    - Accept any Android system dialogs (e.g., “Set up a work profile?”, “Allow Company Portal to manage this profile”)
7. Wait while Android creates the work profile (this may take a few minutes)
8. When setup finishes, you’ll see a message that your work profile is ready, and you’ll have a new “Work” tab/section in your app drawer with briefcase icons on work apps
9. Back in Company Portal (Work), let it run device checks (e.g., screen lock, encryption, OS version)
10. If you see actions required (like “Set a screen lock” or “Update your device”), follow the instructions in Settings, then return to Company Portal and tap Retry or Check again
11. Use the **work apps with the briefcase icon** (e.g., Outlook [work], Teams [work]) for company email, chats, and files.

12. Use your **personal apps** as you normally would for personal activities.
13. Over **1–2 weeks**, note anything confusing, disruptive, or unclear so you can provide feedback.

Once all checks pass, the device status in Company Portal will show as Compliant (or similar), and required work apps (Outlook, Teams, etc.) will install into the work profile.

Note Users can tell they're using the work side when they see the briefcase icon on apps and a Work label on notifications.

Work Profile MAM+MDM for iOS

App Protection Policy

The first step to configuring Work Profile MAM+MDM for iOS is to set up an App Protection policy. This will be used to protect and control corporate data inside specific apps.

Create the Policy:

- Navigate to Intune > Apps > Protection (App Protection Policies)
- Click "+ Create" and select iOS/iPadOS in the dropdown menu

Basics

- Name the policy "Intune-Apps-Protection-iOS-4-Digit-Year-2-Digit-Month"
- Enter "App-level rules that protect this organization's data inside supported iOS apps (e.g., Outlook, Teams). <your 1st initialLast name>" as the policy description
- Click Next to continue to Apps

Apps

- Select Target Policy to Selected Apps
- Select and add the apps you wish to manage by clicking +Select public apps.
  - (This will likely match the app list you created in the prerequisite step iOS App selection and Licenses)
- If you have any non-public custom apps that your company uses on Android, select the +Select custom apps and add them.
- Click next to continue to Data Protection

Data Protection

- Set "Backup Org Data to iTunes and iCloud Backups" to Block

- Set “Send Org Data to Other Apps” to Policy Managed Apps
- Set “Save Copies of Org Data” to Block
- Set “Allow Users to Save Copies” to Selected Services to OneDrive for Business and SharePoint
- Set “Transfer Telecommunication Data” to None, do not transfer this data between apps
- Set “Transfer Messaging Data” to None, do not transfer this data between apps
- Set “Sync Policy Managed App Data with Native Apps or Add-ins” to Block
- Set “Printing Org Data” to Block
- Set “Restrict Web Content Transfer with Other Apps” to Microsoft Edge
- Set “Screen Capture” to Block
- Click Next to continue to Access Requirements

Access Requirements

- Change Timeout (Minutes of Inactivity) to 60
- Change Recheck the access requirements after (Minutes of Inactivity) to 60
- Click Next to continue to Conditional Launch

Conditional Launch

- Leave all settings set to Default
- Click Next to continue to Assignments

Assignments

- Under Included Groups, click “Add groups”
- Check the box next to the previously created test group “AAD-SUG-Intune-Mobile-WorkProfileMAMMDM-StaticTestGroup” and then click Select at the bottom of the pane
- Click Next to continue to Review + Create

Review + Create

- Review the Summary and if everything looks correct, click Create

Conditional Access Policy

In this step you will be creating and configuring a new Conditional Access Policy so that you can control the availability of resources to iOS devices.

Create the Policy:

- Navigate to Entra>Conditional Access>Policies (Conditional Access Policies)
- Click "+ New policy"
- Name the policy "CAP-iOS-WorkProfile-Blocked"

Assignments:

- Leave "What does this policy apply to?" set to Users and groups
- Under Include:
    - Click the bubble next to "Select users and groups"
    - Check the Users and groups box
    - Search for the "AAD-SUG-Intune-Mobile-WorkProfileMAMMDM-StaticTestGroup" group, check the box next to the group and click Select
- Under Exclude:
    - Check the Users and groups box
    - Search for the "CAPSG-MAM-MDM-NotBlocked" group, check the box next to the group and click Select

Target Resources:

- Under Include:
- Click the bubble next to "All Resources" (Formerly 'All cloud apps')
- Continue to Conditions

Conditions:

- Under Device Platforms:
    - Select the "Not Configured" hyperlink under Device Platforms
    - Set Configure to Yes
    - Under Include, check the box next to iOS

- **If you are implementing MDM in addition to MAM and ONLY if you are implementing both, perform the following:**
    - Go to Conditions
    - Filter for Devices
    - Set Configure to Yes
    - Click the radial button next to "Exclude filtered devices from policy
    - Click Edit
    - Copy and Paste the follow code:

(device.isCompliant -eq true) -or (device.trustType -eq "ServerAD") -or (device.trustType -eq "AzureAD")

    - Click Done

Access Controls:

- Under Grant:
    - Select the "0 controls selected" hyperlink
    - Make sure the select bubble at the top is "Grant Access" and check the box next to "Require app protection policy" and click Select

Enable the Policy

- The final step is to enable the policy. It is important that you correctly complete all the steps in this section before enabling this policy.
- Once you have reviewed all the settings and feel confident that they are correct, at the bottom of the page, change the Enable Policy setting from "Report Only" to "On"

Device Configuration Policy:

Next you will create a configuration profile for iOS devices. To do so perform the following:

Create the Policy:

- Navigate to: Intune > Devices > Manage devices > Configuration >Policies (Configuration Policies)
- Click "+ Create" and select "+ New Policy" in the dropdown menu
- For Platform select iOS/iPadOS devices
- For Profile Type select Templates
- Select Device Features
- Click Create

Basics

- Name the policy "Intune-Devices-Config-iOS-Workprofile-MAM+MDM-DeviceConfig"
- Enter "Enable SSO extension for account-driven enrollment<FirstInitial.LastName>" for the policy description
- Click Next to continue to Configuration Settings

Configuration settings

Single Sign-on app extension:

- Expand the Single sign-on app extension section:

- For SSO app extension type, click the drop-down and select Microsoft Entra ID.
- Below that, under Additional configuration enter the following keys:
  - Key: device_registration
    Type: String
    Value: {{DEVICEREGISTRATION}})
  - Key: browser_sso_interaction_enabled
    Type: Integer
    Value: 1

NOTEMake sure there are no extra spaces around the braces. Also, all values are case sensitive.

- Click Next to continue to Assignments

Configure the Assignments:

- Under Included Groups, click "Add groups"
- Check the box next to the previously created test group "AAD-SUG-Intune-Mobile-WorkProfileMAMMDM-StaticTestGroup" and then click Select at the bottom of the pane
- Click Next

Review + Create

- Click Create

Enrolling Devices

End User Enrollment via the Company Portal is the deployment method that will be used in this manual for devices that are being configured for Work Profile MAM+MDM. Have your users this is being deployed to follow the enrollment instructions below:

1. On your iPhone/iPad, open the App Store.
2. Search for "Intune Company Portal" and install the app.
3. Open Company Portal.
4. Tap Sign in and enter your work (Entra ID / Microsoft 365) account and password.
5. Review the privacy / what your organization can see info, then tap Continue or Begin.
6. On the "Set up your device" screen, tap Begin / Continue.
7. The app will prompt you to install a management profile:

8. Tap Continue in Company Portal to download the profile.
9. When you see the message that the profile is downloaded, go to Settings on the device.
10. In Settings, tap Profile Downloaded (near the top), or go to Settings → General → VPN & Device Management and select the downloaded profile.
11. Tap Install in the top-right, enter your device passcode if asked, then tap Install again and Trust if prompted.
12. After the profile installs, tap Done, then return to the Company Portal app.
13. Company Portal will now finish enrolling the device and run device checks (passcode, encryption, OS version, etc.).
14. If it shows any actions required (e.g., “Set a passcode” or “Update iOS”), follow the prompts in Settings, then return to Company Portal.

*****NOTE*****

Once everything passes, the device status in Company Portal should show “This device is compliant” (or similar), and you’re done. Intune can now push work apps and settings to the device.

Phase 3 – Section 1: Test Phase Communications

*****Note*****

The following communications are only recommended and may not be mandatory depending on your organization's approval matrix. Skip any parts of this section that you feel may not apply.

Test Users Notification of Implementation

For all Sample Communications: Complete / replace /remove the sections of red text.

MAM Communication:

Subject: Upcoming Test: Mobile App Protection for iOS & Android Devices

Hi everyone,

You've been selected to participate in a test of our new **Mobile Application Management (MAM)** setup using **Microsoft Intune**. This will help us protect company data inside key work apps (like Outlook, Teams, OneDrive) on **iOS and Android** devices, without taking control of your entire phone.

This pilot is focused on **app-level protection**, not full device management (MDM). You'll still use your phone as normal for personal calls, texts, photos, and apps.

What's changing

During this test, when you use certain work apps on your phone (for example, Outlook, Teams, OneDrive):

- You may be prompted to **sign in with your work account**.
- You may see new **security prompts**, like setting an app PIN or using Face ID/Touch ID.
- You may notice **restrictions** such as:
    - Blocking copy/paste from work apps into personal apps
    - Limiting where files can be saved (e.g., OneDrive/SharePoint instead of personal storage)
    - Requiring you to use the **Intune Company Portal** app for registration

These controls apply **only** to work apps and work data.

What IT can and cannot see

Because this is app-level management (MAM), there are clear boundaries around your privacy:

What IT can see / manage

- That your device is **registered for app protection** (basic device details like model, OS version, compliance status)
- The **work apps** we manage (e.g., Outlook, Teams, OneDrive, approved business apps)
- **Security posture** related to work apps (e.g., whether you have an app PIN, if the app is up to date, if policy checks pass)
- The ability to **remove company data** from managed work apps (for example, if you leave the company or opt out of using your phone for work)

What IT cannot see / do

- The **content** of your personal email, text messages, photos, and personal apps
- Your **personal browsing history** or personal app usage
- Your **personal contacts**, photos, or files stored outside the managed work apps
- Your **personal passwords** or personal device PIN/passcode
- **Remotely wiping your entire device** in this MAM-only pilot (we can only remove company data from managed work apps)

In short, IT is protecting **company data inside company apps**, not monitoring or controlling your personal life on the device.

What we need you to do

1. **Install or update** the latest versions of:
    - **Intune Company Portal**
    - **Microsoft Outlook**
    - **Microsoft Teams**
    - **OneDrive**

    - **Any other managed company apps**

2. **Sign in** with your work account when prompted.
3. **Follow the on-screen steps** if you're asked to:

    - Set an app PIN or enable biometric sign-in
    - Accept app protection or "this app is managed by your organization" prompts

4. Use your device normally for **1–2 weeks**, paying attention to anything that feels confusing, disruptive, or unclear.

This rollout will go live on **XX/XX/XXXX**. We appreciate your cooperation and collaboration on this matter. Should you have any questions or concerns don't hesitate to reach out and let us know. Thank you.

Work Profile MAM+MDM Communication:

Subject: Upcoming iOS and Android Work Profile MAM + MDM Rollout

Hi everyone,

You've been selected to participate in a test of our new iOS and Android Work Profile MAM + MDM setup using **Microsoft Intune**. This combines **Mobile Device Management (MDM)** and **Mobile Application Management (MAM)** on your iOS and Android phones and tablets to better protect company data, while keeping your **personal side separate and private**.

With a Work Profile, your phone will have two spaces: a **personal side** (your existing apps, photos, texts) and a **work side** (apps and data managed by IT). The work side is where Intune will apply security controls.

What's changing

During this test, your iOS or Android device will be enrolled into Intune using a **Work Profile**:

- A dedicated **Work** area will be created on your phone.

- You’ll see **“work” versions** of apps (with a briefcase icon), such as Outlook, Teams, and other business apps.
- IT will be able to:
    - Ensure basic security settings on the **work side** (screen lock, encryption, OS version, etc.).
    - Push and update **required work apps** into the Work Profile.
    - Apply **app-level protections** (MAM), such as:
        - Restricting copy/paste from work apps to personal apps
        - Controlling where work files can be saved (e.g., OneDrive/SharePoint, not personal storage)
        - Requiring a PIN/biometric to access work apps
- If you leave the company or opt out of using your device for work, IT can **remove the entire work profile** (all work apps and data) without touching your personal side.

Your **personal side** remains yours to manage: your personal apps, photos, texts, and settings are not brought under full IT control.

What IT can and cannot see

Because this is **Work Profile MAM + MDM**, there are clear boundaries between what IT manages and what stays private.

What IT can see / do

- See and manage the **work profile** on your device (not the personal side).
- See **basic device and work profile information**, such as:
    - Device model, OS version, storage and security posture
    - Compliance status (e.g., passcode set, encryption enabled)
- Manage and configure **work apps** (e.g., Outlook, Teams, OneDrive, approved business apps).
- Apply **data protection rules** inside work apps (copy/paste restrictions, save locations, app PIN, etc.).

- **Remove the work profile** (and all corporate apps/data) if:
    - You leave the company
    - The device is lost/stolen and reported
    - You choose to stop using the device for work

What IT cannot see / do

- View the **content** of your personal text messages, photos, or personal apps.
- See your **personal browsing history** or personal app usage.
- Read your **personal email** accounts or access your social media.
- Access your **personal photos, videos, or files** stored outside the Work Profile.
- See your **personal passwords** or your personal device PIN/passcode.
- **Remotely wipe** your entire phone as part of this Work Profile pilot; they can remove only the **work profile** (the managed side).

In short: IT manages the **work side** of your device so company data stays secure, but your **personal side remains private and under your control**.

What we need you to do on the day of this rollout:

For Android Devices:

1. On your Android device, install or update:
    - **Intune Company Portal** from the Google Play Store.
2. Open Company Portal and tap Sign in
3. Sign in with your work (Microsoft 365 / Entra ID) account and complete any MFA prompts
4. Review the privacy / what your organization can see information, then tap Continue or Begin
5. On the “Set up your work profile” or “Set up your device” screen, tap Begin / Continue.
6. Company Portal will prompt you to create a work profile:
    - Tap Next / Set up when asked to create a work profile
    - Accept any Android system dialogs (e.g., “Set up a work profile?”, “Allow Company Portal to manage this profile”)

7. Wait while Android creates the work profile (this may take a few minutes)
8. When setup finishes, you'll see a message that your work profile is ready, and you'll have a new "Work" tab/section in your app drawer with briefcase icons on work apps
9. Back in Company Portal (Work), let it run device checks (e.g., screen lock, encryption, OS version)
10. If you see actions required (like "Set a screen lock" or "Update your device"), follow the instructions in Settings, then return to Company Portal and tap Retry or Check again

11. Use the **work apps with the briefcase icon** (e.g., Outlook [work], Teams [work]) for company email, chats, and files.

12. Use your **personal apps** as you normally would for personal activities.

13. Over **1–2 weeks**, note anything confusing, disruptive, or unclear so you can provide feedback.

For iOS Devices:

1. On your iPhone/iPad, open the App Store.
2. Search for "Intune Company Portal" and install the app.
3. Open Company Portal.
4. Tap Sign in and enter your work (Entra ID / Microsoft 365) account and password.
5. Review the privacy / what your organization can see info, then tap Continue or Begin.
6. On the "Set up your device" screen, tap Begin / Continue.
7. The app will prompt you to install a management profile:
8. Tap Continue in Company Portal to download the profile.
9. When you see the message that the profile is downloaded, go to Settings on the device.
10. In Settings, tap Profile Downloaded (near the top), or go to Settings → General → VPN & Device Management and select the downloaded profile.
11. Tap Install in the top-right, enter your device passcode if asked, then tap Install again and Trust if prompted.
12. After the profile installs, tap Done, then return to the Company Portal app.
13. Company Portal will now finish enrolling the device and run device checks (passcode, encryption, OS version, etc.).
14. If it shows any actions required (e.g., "Set a passcode" or "Update iOS"), follow the prompts in Settings, then return to Company Portal.

This rollout will go live on **XX/XX/XXXX**. We appreciate your cooperation and collaboration on this matter. Should you have any questions or concerns don't hesitate to reach out and let us know. Thank you.

MDM Communication:

*****Note*** This communication is only needed if the users in your test group already have corporate owned iOS or Android devices deployed to them.**

Subject: Upcoming Test: Mobile Device Management (MDM) for iOS & Android Devices

Hi everyone,

You've been selected to participate in a test of our new **Mobile Device Management (MDM)** setup using **Microsoft Intune**. This will allow us to securely manage **corporate-owned iOS and Android devices** that access company email, Teams, files, and other business apps. MDM helps us ensure these devices meet basic security standards (encryption, screen lock, updates) and can be locked or wiped if they're lost, stolen, or repurposed.

This test is focused on **full device management for corporate devices**. Your personal devices will not be enrolled in this pilot unless explicitly communicated otherwise.

What's changing

As part of this pilot, your **corporate iPhone/iPad or Android phone** will be enrolled into Intune MDM:

- Your device will be marked as **corporate-owned and managed** by [Company].
- IT will be able to enforce **core security settings**, such as:
  - Requiring a **passcode/screen lock**
  - Enforcing **device encryption**
  - Blocking high-risk settings (e.g., rooted/jailbroken devices)

- Required **work apps** (Outlook, Teams, OneDrive, business apps) may be **pushed automatically** to your device.
- If a device is **lost, stolen, or retired**, IT can remotely **wipe corporate data** and, if needed, fully wipe the device so it can be safely reassigned or decommissioned.

You'll still be able to use the device for normal day-to-day work as you do today—this change is about adding a consistent security and management layer underneath.

What IT can and cannot see

Because this is full **MDM** on corporate-owned devices, IT will have more control than with app-only management, but there are still clear boundaries on what is and is not monitored.

What IT can see / do

- See that your device is **enrolled** and associated with your work account.
- View **device details**, such as:
  - Model, operating system version, serial number
  - Storage/encryption status, compliance status (passcode set, OS up to date, etc.)
- See and manage **installed work apps** (and, depending on the platform, a list of installed apps for security/compliance purposes).
- Push and configure:
  - **Work apps** (Outlook, Teams, OneDrive, line-of-business apps)
  - **Configuration profiles** (Wi-Fi, certificates, VPN, basic restrictions)
- Enforce **security policies** (screen lock requirements, OS version requirements, blocking risky configurations).
- **Remotely wipe**:
  - Corporate data, and
  - If necessary for lost/stolen/retired **corporate devices**, the **entire device**.

What IT cannot see / do

- Read the **content** of your personal email accounts (e.g., Gmail, personal Outlook) or personal messaging apps.
- View the **content** of your personal photos, texts, or documents stored in personal apps.
- Listen to calls or read the content of SMS/iMessage conversations.
- See your **personal passwords** or your device passcode.
- Remotely access your screen in real time (this pilot does not include remote screen viewing/recording tools).

Our goal is to manage **corporate devices and data**, not to monitor your personal life. If you use a corporate device for some personal tasks, normal incidental use is expected, but the device is still managed as company property.

What we need you to do

1. As part of this rollout, IT will need to coordinate briefly capturing your corporate-owned device to enroll it into the new MDM solution. This is for the following reasons:
    - IT will need to factory reset the device as part of the enrollment process
    - The device will be wiped as part of that factory reset and capturing the device allows IT to inspect the device for personal data that may need to be backed up prior to wiping. If personal data is found, IT will make sure you are given the opportunity to backup the data with hands on assistance.
2. **Once IT returns your device:**
    - **Sign in** with your work account when prompted.
    - Accept any **management / “this device is managed by your organization”** prompts.
    - Allow required **work apps** to install and keep them updated.
    - If the device asks you to set a **passcode**, enable encryption, or update the OS to meet policy, please complete those actions.

The test phase will run for **1–2 weeks** while we validate policies, performance, and user experience and the rollout will go live on **XX/XX/XXXX**. IT will reach out to you to coordinate the retrieval of your corporate owned device prior to the rollout date. We appreciate your cooperation and collaboration on this matter. Should you have any questions or concerns don’t hesitate to reach out and let us know. Thank you.

Phase 3 – Section 2: Test Phase Implementation

Assign the test users to groups

Once you have completed the configurations for your deployment method(s) and sent your communications to the test users letting them know of the planned implementation you will need to assign those test users to the appropriate groups. Follow the instructions for each deployment below to accomplish this.

*****Note*** Do not add the test users or their devices to these groups until the planned Test Phase implementation date. The groups and policies are already on and all that is required for implementation is to add the users to the groups.**

For MDM Deployments:

- Navigate to Azure>Microsoft EntraID> Manage>Groups (Entra Groups)
- Click All Groups
- Click the group named “AAD-SUG-Intune-Mobile-MDM-StaticTestGroup”
- Click Members
- Click + Add members
- Use the search box to find the users and their devices that you would like to add
- Click on each entry to select it
- Once you’ve selected all the needed devices and users, click Select (or Add) at the bottom of the pane
- You’ll be returned to the Members list which should now show the new members of the group (Refresh if needed)

For MAM Deployments:

- Navigate to Azure>Microsoft EntraID> Manage>Groups (Entra Groups)
- Click All Groups
- Click the group named “AAD-SUG-Intune-Mobile-MAM-StaticTestGroup”
- Click Members
- Click + Add members
- Use the search box to find the users that you would like to add
- Click on each entry to select it
- Once you’ve selected all the needed devices and users, click Select (or Add) at the bottom of the pane

- You’ll be returned to the Members list which should now show the new members of the group (Refresh if needed)

For Work Profile MAM+MDM Deployments:

- Navigate to Azure>Microsoft EntraID> Manage>Groups (Entra Groups)
- Click All Groups
- Click the group named “AAD-SUG-Intune-Mobile-WorkProfileMAMMDM-StaticTestGroup”
- Click Members
- Click + Add members
- Use the search box to find the users that you would like to add
- Click on each entry to select it
- Once you’ve selected all the needed devices and users, click Select (or Add) at the bottom of the pane
- You’ll be returned to the Members list which should now show the new members of the group (Refresh if needed)

Initiate Enrollments

For MDM Deployments:

This deployment method requires devices to be factory reset. If you have iOS or Android corporate devices already deployed in your environment that you are enrolling into MDM, you will need to coordinate with the users to capture the devices.

You will also need to make sure that the end users’ data (if any) is backed up on the device. Because the types of data that can be found on a device vary user to user and the methods of backing that data up also vary, this manual will not provide the steps for doing that. It is recommended to consult a specialist if needed to provide the steps for those backups.

Once you feel confident that you have corporate owned devices in hand that you are ready to start enrolling following the enrollment instructions located in “Phase 2 - Section 2 Configuring Deployment Methods”. The iOS instructions will be a subsection under “MDM for iOS” titled “Enrolling Devices” and the Android instructions will be a subsection under “MDM for Android” also titled “Enrolling Devices”.

When you reach the part of enrollment where the iOS or Android device requires a sign-in to a 365-work account, return the device to the user and have them sign-in and finish the device enrollment. It is recommended that you stay with them until the enrollment is complete, when possible, in case they run into any technical issues and so that you can verify that enrollment is completed as expected with all required apps installed.

For MAM Deployments:

MAM Deployments will not require any manual enrollment efforts. It is however recommended that you ask the users to update to the latest versions of their work apps on their devices and that you send a follow-up email to the test users on the day before or the day of rollout, reminding them of the deployment.

For Work Profile MAM+MDM Deployments:

Enrollment into Work Profile MAM+MDM is completely user driven and the instructions for how to do this were included in the “Phase 3 – Section 1: Test Phase Communications” > “Work Profile MAM+MDM Communication:” subsection.

It is recommended however, that you send a follow-up email to the test users on the day before or the day of rollout, reminding them of the go deployment and asking them to complete those steps.

Phase 4 – Section 1:
Full Deployment Communications

*****Note*****

The following communications are only recommended and may not be mandatory depending on your organization's approval matrix. Skip any parts of this section that you feel may not apply. Also, If you are implementing more than one deployment method, you will likely want to combine the communications in a more simplified way that makes logical sense.

All Staff Notifications of Implementation

For all sample communications: Complete / replace /remove the sections of red text.

MAM Communication:

Subject: Upcoming Rollout of Mobile App Protection for iOS & Android Devices

Hi everyone,

We are pleased to announce our new **Mobile Application Management (MAM)** setup using **Microsoft Intune**. This will help us protect company data inside key work apps (like Outlook, Teams, OneDrive) on **iOS and Android** devices, without taking control of your entire phone.

This deployment is focused on **app-level protection**, not full device management (MDM). You'll still use your phone as normal for personal calls, texts, photos, and apps.

What's changing

During this test, when you use certain work apps on your phone (for example, Outlook, Teams, OneDrive):

- You may be prompted to **sign in with your work account**.
- You may see new **security prompts**, like setting an app PIN or using Face ID/Touch ID.
- You may notice **restrictions** such as:
  - Blocking copy/paste from work apps into personal apps
  - Limiting where files can be saved (e.g., OneDrive/SharePoint instead of personal storage)
  - Requiring you to use the **Intune Company Portal** app for registration

These controls apply **only** to work apps and work data.

What IT can and cannot see

Because this is app-level management (MAM), there are clear boundaries around your privacy:

What IT can see / manage

- That your device is **registered for app protection** (basic device details like model, OS version, compliance status)
- The **work apps** we manage (e.g., Outlook, Teams, OneDrive, approved business apps)
- **Security posture** related to work apps (e.g., whether you have an app PIN, if the app is up to date, if policy checks pass)
- The ability to **remove company data** from managed work apps (for example, if you leave the company or opt out of using your phone for work)

What IT cannot see / do

- The **content** of your personal email, text messages, photos, and personal apps
- Your **personal browsing history** or personal app usage
- Your **personal contacts**, photos, or files stored outside the managed work apps
- Your **personal passwords** or personal device PIN/passcode
- **Remotely wiping your entire device** in this MAM-only deployment (we can only remove company data from managed work apps)

In short, IT is protecting **company data inside company apps**, not monitoring or controlling your personal life on the device.

What we need you to do

5. **Install or update** the latest versions of:
    - **Intune Company Portal**
    - **Microsoft Outlook**
    - **Microsoft Teams**
    - **OneDrive**
    - **Any other managed company apps**

6. **Sign in** with your work account when prompted.
7. **Follow the on-screen steps** if you're asked to:
    - Set an app PIN or enable biometric sign-in
    - Accept app protection or "this app is managed by your organization" prompts

This rollout will go live on **XX/XX/XXXX**. We appreciate your cooperation and collaboration on this matter. Should you have any questions or concerns don't hesitate to reach out and let us know. Thank you.

Work Profile MAM+MDM Communication:

Subject: Upcoming iOS and Android Work Profile MAM + MDM Rollout

Hi everyone,

We are excited to announce our new iOS and Android Work Profile MAM + MDM setup using **Microsoft Intune**. This combines **Mobile Device Management (MDM)** and **Mobile Application Management (MAM)** on your iOS and Android phones and tablets to better protect company data, while keeping your **personal side separate and private**.

With a Work Profile, your phone will have two spaces: a **personal side** (your existing apps, photos, texts) and a **work side** (apps and data managed by IT). The work side is where Intune will apply security controls.

What's changing

During this test, your iOS or Android device will be enrolled into Intune using a **Work Profile**:

- A dedicated **Work** area will be created on your phone.
- You'll see **"work" versions** of apps (with a briefcase icon), such as Outlook, Teams, and other business apps.
- IT will be able to:

    - Ensure basic security settings on the **work side** (screen lock, encryption, OS version, etc.).
    - Push and update **required work apps** into the Work Profile.
    - Apply **app-level protections** (MAM), such as:
        - Restricting copy/paste from work apps to personal apps
        - Controlling where work files can be saved (e.g., OneDrive/SharePoint, not personal storage)
        - Requiring a PIN/biometric to access work apps
- If you leave the company or opt out of using your device for work, IT can **remove the entire work profile** (all work apps and data) without touching your personal side.

Your **personal side** remains yours to manage: your personal apps, photos, texts, and settings are not brought under full IT control.

What IT can and cannot see

Because this is **Work Profile MAM + MDM**, there are clear boundaries between what IT manages and what stays private.

What IT can see / do

- See and manage the **work profile** on your device (not the personal side).
- See **basic device and work profile information**, such as:
    - Device model, OS version, storage and security posture
    - Compliance status (e.g., passcode set, encryption enabled)
- Manage and configure **work apps** (e.g., Outlook, Teams, OneDrive, approved business apps).
- Apply **data protection rules** inside work apps (copy/paste restrictions, save locations, app PIN, etc.).
- **Remove the work profile** (and all corporate apps/data) if:
    - You leave the company
    - The device is lost/stolen and reported

  - You choose to stop using the device for work

What IT cannot see / do

- View the **content** of your personal text messages, photos, or personal apps.
- See your **personal browsing history** or personal app usage.
- Read your **personal email** accounts or access your social media.
- Access your **personal photos, videos, or files** stored outside the Work Profile.
- See your **personal passwords** or your personal device PIN/passcode.
- **Remotely wipe** your entire phone as part of this Work Profile deployment; they can remove only the **work profile** (the managed side).

In short: IT manages the **work side** of your device so company data stays secure, but your **personal side remains private and under your control**.

What we need you to do on the day of this rollout:

For Android Devices:

1. On your Android device, install or update:
    - **Intune Company Portal** from the Google Play Store.
2. Open Company Portal and tap Sign in
3. Sign in with your work (Microsoft 365 / Entra ID) account and complete any MFA prompts
4. Review the privacy / what your organization can see information, then tap Continue or Begin
5. On the “Set up your work profile” or “Set up your device” screen, tap Begin / Continue.
6. Company Portal will prompt you to create a work profile:
    - Tap Next / Set up when asked to create a work profile
    - Accept any Android system dialogs (e.g., “Set up a work profile?”, “Allow Company Portal to manage this profile”)
7. Wait while Android creates the work profile (this may take a few minutes)
8. When setup finishes, you’ll see a message that your work profile is ready, and you’ll have a new “Work” tab/section in your app drawer with briefcase icons on work apps

9. Back in Company Portal (Work), let it run device checks (e.g., screen lock, encryption, OS version)
10. If you see actions required (like “Set a screen lock” or “Update your device”), follow the instructions in Settings, then return to Company Portal and tap Retry or Check again
11. Use the **work apps with the briefcase icon** (e.g., Outlook [work], Teams [work]) for company email, chats, and files.
12. Use your **personal apps** as you normally would for personal activities.
13. Over **1–2 weeks**, note anything confusing, disruptive, or unclear so you can provide feedback.

For iOS Devices:

1. On your iPhone/iPad, open the App Store.
2. Search for “Intune Company Portal” and install the app.
3. Open Company Portal.
4. Tap Sign in and enter your work (Entra ID / Microsoft 365) account and password.
5. Review the privacy / what your organization can see info, then tap Continue or Begin.
6. On the “Set up your device” screen, tap Begin / Continue.
7. The app will prompt you to install a management profile:
8. Tap Continue in Company Portal to download the profile.
9. When you see the message that the profile is downloaded, go to Settings on the device.
10. In Settings, tap Profile Downloaded (near the top), or go to Settings → General → VPN & Device Management and select the downloaded profile.
11. Tap Install in the top-right, enter your device passcode if asked, then tap Install again and Trust if prompted.
12. After the profile installs, tap Done, then return to the Company Portal app.
13. Company Portal will now finish enrolling the device and run device checks (passcode, encryption, OS version, etc.).
14. If it shows any actions required (e.g., “Set a passcode” or “Update iOS”), follow the prompts in Settings, then return to Company Portal.

This rollout will go live on **XX/XX/XXXX**. We appreciate your cooperation and collaboration on this matter. Should you have any questions or concerns don’t hesitate to reach out and let us know. Thank you.

MDM Communication:

*****Note*** This communication is only needed if the users in your organization already have corporate owned iOS or Android devices deployed to them.**

Subject: Upcoming Test: Mobile Device Management (MDM) for iOS & Android Devices

Hi everyone,

We are excited to announce our new **Mobile Device Management (MDM)** setup using **Microsoft Intune**. This will allow us to securely manage **corporate-owned iOS and Android devices** that access company email, Teams, files, and other business apps. MDM helps us ensure these devices meet basic security standards (encryption, screen lock, updates) and can be locked or wiped if they're lost, stolen, or repurposed.

This test is focused on **full device management for corporate devices**. Your personal devices will not be enrolled in this pilot unless explicitly communicated otherwise.

What's changing

As part of this pilot, your **corporate iPhone/iPad or Android phone** will be enrolled into Intune MDM:

- Your device will be marked as **corporate-owned and managed** by [Company].
- IT will be able to enforce **core security settings**, such as:
    - Requiring a **passcode/screen lock**
    - Enforcing **device encryption**
    - Blocking high-risk settings (e.g., rooted/jailbroken devices)
- Required **work apps** (Outlook, Teams, OneDrive, business apps) may be **pushed automatically** to your device.
- If a device is **lost, stolen, or retired**, IT can remotely **wipe corporate data** and, if needed, fully wipe the device so it can be safely reassigned or decommissioned.

You'll still be able to use the device for normal day-to-day work as you do today—this change is about adding a consistent security and management layer underneath.

What IT can and cannot see

Because this is full **MDM** on corporate-owned devices, IT will have more control than with app-only management, but there are still clear boundaries on what is and is not monitored.

What IT can see / do

- See that your device is **enrolled** and associated with your work account.
- View **device details**, such as:
  - Model, operating system version, serial number
  - Storage/encryption status, compliance status (passcode set, OS up to date, etc.)
- See and manage **installed work apps** (and, depending on the platform, a list of installed apps for security/compliance purposes).
- Push and configure:
  - **Work apps** (Outlook, Teams, OneDrive, line-of-business apps)
  - **Configuration profiles** (Wi-Fi, certificates, VPN, basic restrictions)
- Enforce **security policies** (screen lock requirements, OS version requirements, blocking risky configurations).
- **Remotely wipe**:
  - Corporate data, and
  - If necessary for lost/stolen/retired **corporate devices**, the **entire device**.

What IT cannot see / do

- Read the **content** of your personal email accounts (e.g., Gmail, personal Outlook) or personal messaging apps.
- View the **content** of your personal photos, texts, or documents stored in personal apps.
- Listen to calls or read the content of SMS/iMessage conversations.

- See your **personal passwords** or your device passcode.
- Remotely access your screen in real time (this pilot does not include remote screen viewing/recording tools).

Our goal is to manage **corporate devices and data**, not to monitor your personal life. If you use a corporate device for some personal tasks, normal incidental use is expected, but the device is still managed as company property.

What we need you to do

1. As part of this rollout, IT will need to coordinate briefly capturing your corporate-owned device to enroll it into the new MDM solution. This is for the following reasons:
    - IT will need to factory reset the device as part of the enrollment process
    - The device will be wiped as part of that factory reset and capturing the device allows IT to inspect the device for personal data that may need to be backed up prior to wiping. If personal data is found, IT will make sure you are given the opportunity to backup the data with hands on assistance.
2. **Once IT returns your device:**
    - **Sign in** with your work account when prompted.
    - Accept any **management / “this device is managed by your organization”** prompts.
    - Allow required **work apps** to install and keep them updated.
    - If the device asks you to set a **passcode**, enable encryption, or update the OS to meet policy, please complete those actions.

The rollout will go live on **XX/XX/XXXX**. IT will reach out to you to coordinate the retrieval of your corporate owned device prior to the rollout date. We appreciate your cooperation and collaboration on this matter. Should you have any questions or concerns don’t hesitate to reach out and let us know. Thank you.

Phase 4 – Section 2:
Full Deployment Implementation

Removing Users from Test Groups

For MDM Deployments:

- Navigate to Azure>Microsoft EntraID> Manage>Groups (Entra Groups)
- Click All Groups
- Find and select the group named "AAD-SUG-Intune-Mobile-MDM-StaticTestGroup"
- Click Members
- Check the boxes next to each member
- Click Remove
- Confirm when prompted

For MAM Deployments:

- Navigate to Azure>Microsoft EntraID> Manage>Groups (Entra Groups)
- Click All Groups
- Find and select the group named "AAD-SUG-Intune-Mobile-MAM-StaticTestGroup"
- Click Members
- Check the boxes next to each member
- Click Remove
- Confirm when prompted

For Work Profile MAM+MDM Deployments:

- Navigate to Azure>Microsoft EntraID> Manage>Groups (Entra Groups)
- Click All Groups
- Find and select the group named "AAD-SUG-Intune-Mobile-WorkProfileMAMMDM-StaticTestGroup"
- Click Members
- Check the boxes next to each member
- Click Remove
- Confirm when prompted

Initiate Enrollments

For MDM Deployments:

Assign the iOS Compliance Policy:

- Navigate to: Intune > Devices > Manage devices | Compliance > Policies (Compliance Policies)
- Select the policy named “Intune-Devices-Compliance-iOS-MDM”
- Select Properties
- Locate “Assignments” and click Edit to the right of it
- Click Add groups
- Check the box next to the previously created dynamic device group “AAD-SDG-Intune-Mobile-iOS-Devices” and then click Select at the bottom of the pane
- Click the Remove link to the right of the AAD-SUG-Intune-Mobile-MDM-StaticTestGroup

Assign the Android Compliance Policy:

- Navigate to: Intune > Devices > Manage devices | Compliance > Policies (Compliance Policies)
- Select the policy named “Intune-Devices-Compliance-Android-MDM”
- Select Properties
- Locate “Assignments” and click Edit to the right of it
- Click Add groups
- Check the box next to the previously created dynamic device group “AAD-SDG-Intune-Mobile-Android-Devices” and then click Select at the bottom of the pane
- Click the Remove link to the right of the AAD-SUG-Intune-Mobile-MDM-StaticTestGroup

Assign the iOS Device Configuration Policy:

- Navigate to: Intune > Devices > Manage devices > Configuration >Policies (Configuration Policies)
- Select the policy named “Intune-Devices-Config-iOS-MDM-DeviceConfig”
- Locate “Assignments” and click Edit to the right of it
- Click Add groups
- Check the box next to the previously created dynamic device group “AAD-SDG-Intune-Mobile-iOS-Devices” and then click Select at the bottom of the pane
- Click the Remove link to the right of the AAD-SUG-Intune-Mobile-MDM-StaticTestGroup

Assign the Android Device Configuration Policy:

- Navigate to: Intune > Devices > Manage devices > Configuration >Policies (Configuration Policies)
- Select the policy named “Intune-Devices-Config-Android-MDM-DeviceConfig”
- Locate “Assignments” and click Edit to the right of it
- Click Add groups
- Check the box next to the previously created dynamic device group “AAD-SDG-Intune-Mobile-Android-Devices” and then click Select at the bottom of the pane
- Click the Remove link to the right of the AAD-SUG-Intune-Mobile-MDM-StaticTestGroup

Assign the App List for iOS

- Navigate to Intune>Apps>iOS/iPadOS (iOS/iPadOS apps)
- For each iOS app in the list, click the app name to open the app overview
- Under manage, click properties
- Click Edit to the right of Assignments
- Under the Required section click “Add group”:
  - Search for the “AAD-SDG-Intune-Mobile-iOS-Devices” group, check the box next to the group and click Select
  - Click the three dots to the far right of the included line that lists the AAD-SUG-Intune-Mobile-MDM-StaticTestGroup and select Delete
- Click Review + save

Assign the App List for Android

- Navigate to: Intune>Apps>All Apps (All Apps)
- For each Managed Google Play app in the list, click the app name to open the app overview
- Under manage, click properties
- Click Edit to the right of Assignments
- Under the Required section click “Add group”:
  - Search for the “AAD-SDG-Intune-Mobile-Android-Devices” group, check the box next to the group and click Select

  - Click the three dots to the far right of the included line that lists the AAD-SUG-Intune-Mobile-MDM-StaticTestGroup and select Delete
- Click Review + save

Assign the iOS Conditional Access Policy

- Navigate to Entra>Conditional Access>Policies (Conditional Access Policies)
- Select the policy named “CAP-iOSMDM-Blocked”
- Click the “Specific Users Included” Under Assignments
- Under the Select section, click the “1 group” link
- Search for the “AAD-SDG-Intune-Mobile-iOS-Devices” group, check the box next to the group and click Select
- Click the three dots to the right of the AAD-SUG-Intune-Mobile-MDM-StaticTestGroup and select Remove
- Click Save

Assign the Android Conditional Access Policy

- Navigate to Entra>Conditional Access>Policies (Conditional Access Policies)
- Select the policy named “CAP-AndroidMDM-Blocked”
- Click the “Specific Users Included” Under Assignments
- Under the Select section, click the “1 group” link
- Search for the “AAD-SDG-Intune-Mobile-Android-Devices” group, check the box next to the group and click Select
- Click the three dots to the right of the AAD-SUG-Intune-Mobile-MDM-StaticTestGroup and select Remove
- Click Save

Enroll the Devices

This deployment method requires devices to be factory reset. If you have iOS or Android corporate devices already deployed in your environment that you are enrolling into MDM, you will need to coordinate with the users to capture the devices.

You will also need to make sure that the end users’ data (if any) is backed up on the device. Because the types of data that can be found on a device vary user to user and the methods of backing that data up also vary, this manual will not provide the steps for doing that. It is recommended to consult a specialist if needed to provide the steps for those backups.

Once you feel confident that you have corporate owned devices in hand that you are ready to start enrolling following the enrollment instructions located in “Phase 2 - Section 2 Configuring Deployment Methods”. The iOS instructions will be a subsection under “MDM for iOS” titled “Enrolling Devices” and the Android instructions will be a subsection under “MDM for Android” also titled “Enrolling Devices”.

When you reach the part of enrollment where the iOS or Android device requires a sign-in to a 365-work account, return the device to the user and have them sign-in and finish the device enrollment. It is recommended that you stay with them until the enrollment is complete when possible, in case they run into any technical issues and also so that you can verify that enrollment completed as expected and that all required apps were installed.

For MAM Deployments:

Assign the iOS App Protection Policy

- Navigate to Intune > Apps > Protection (App Protection Policies)
  - Open the policy named Name the policy “Intune-Apps-Protection-iOS-4-Digit-Year-2-Digit-Month”
- Under Manage, Click Properties
- Click Edit to the right of Assignments
- Add the Entra All-User group for your tenant. (Possibly Named AADSG-All-Users or something similar)
- Remove the test group “AAD-SUG-Intune-Mobile-MAM-StaticTestGroup” from the assignments

Assign the Android App Protection Policy

- Navigate to Intune > Apps > Protection (App Protection Policies)
  - Open the policy named Name the policy “Intune-Apps-Protection-Android-4-Digit-Year-2-Digit-Month”
- Under Manage, Click Properties
- Click Edit to the right of Assignments

- Add the Entra All-User group for your tenant. (Possibly Named AADSG-All-Users or something similar)
- Remove the test group “AAD-SUG-Intune-Mobile-MAM-StaticTestGroup” from the assignments

Assign the iOS Conditional Access Policy

- Navigate to Entra>Conditional Access>Policies (Conditional Access Policies)
- Select the policy named “CAP-iOS-MAM-App-Blocked”
- Click the “Specific Users Included” Under Assignments
- Under the Select section, click the “1 group” link
- Search for the Entra All-User group for your tenant (Possibly Named AADSG-All-Users or something similar), check the box next to the group and click Select
- Click the three dots to the right of the AAD-SUG-Intune-Mobile-MAM-StaticTestGroup and select Remove
- Click Save

Assign the Android Conditional Access Policy

- Navigate to Entra>Conditional Access>Policies (Conditional Access Policies)
- Select the policy named “CAP-Android-MAM-App-Blocked”
- Click the “Specific Users Included” Under Assignments
- Under the Select section, click the “1 group” link
- Search for the Entra All-User group for your tenant (Possibly Named AADSG-All-Users or something similar), check the box next to the group and click Select
- Click the three dots to the right of the AAD-SUG-Intune-Mobile-MAM-StaticTestGroup and select Remove
- Click Save

Enroll the Devices

MAM Deployments will not require any manual enrollment efforts. It is however recommended that you ask the users to update to the latest versions of their work apps on their devices.

For Work Profile MAM+MDM Deployments:

Assign the iOS App Protection Policy

- Navigate to Intune > Apps > Protection (App Protection Policies)
  - Open the policy named Name the policy “Intune-Apps-Protection-iOS-4-Digit-Year-2-Digit-Month”
- Under Manage, Click Properties
- Click Edit to the right of Assignments
- Add the Entra All-User group for your tenant. (Possibly Named AADSG-All-Users or something similar)
- Remove the test group “AAD-SUG-Intune-Mobile-MAM-StaticTestGroup” from the assignments

Assign the Android App Protection Policy

- Navigate to Intune > Apps > Protection (App Protection Policies)
  - Open the policy named Name the policy “Intune-Apps-Protection-Android-4-Digit-Year-2-Digit-Month”
- Under Manage, Click Properties
- Click Edit to the right of Assignments
- Add the Entra All-User group for your tenant. (Possibly Named AADSG-All-Users or something similar)
- Remove the test group “AAD-SUG-Intune-Mobile-MAM-StaticTestGroup” from the assignments

Assign the Android Device Configuration Policy:

- Navigate to: Intune > Devices > Manage devices > Configuration >Policies (Configuration Policies)
- Select the policy named “Intune-Devices-Config-Android-MDM-DeviceConfig”
- Locate “Assignments” and click Edit to the right of it
- Click Add groups
- Check the box next to the previously created dynamic device group “Intune-Devices-Config-Android-MDM-DeviceConfig”
- Check the box next to your Entra All-User group for your tenant. (Possibly Named AADSG-All-Users or something similar)
- Click Select at the bottom of the pane

- Click the Remove link to the right of the AAD-SUG-Intune-Mobile-WorkProfileMAMMDM-StaticTestGroup

Assign the Android Compliance Policy:

- Navigate to: Intune > Devices > Manage devices | Compliance > Policies (Compliance Policies)
- Select the policy named "Intune-Devices-Compliance-Android-Work Profile MAMMDM"
- Select Properties
- Locate "Assignments" and click Edit to the right of it
- Click Add groups
- Check the box next to the previously created dynamic device group "AAD-SDG-Intune-Mobile-Android-Devices" and then click Select at the bottom of the pane
- Click the Remove link to the right of the AAD-SUG-Intune-Mobile-MDM-StaticTestGroup

Assign the Android App List:

- Navigate to: Intune>Apps>All Apps (All Apps)
- For each Managed Google Play app in the list, click the app name to open the app overview
- Under manage, click properties
- Click Edit to the right of Assignments
- Under the Required section click "Add group":
    - Search for the Entra All-User group for your tenant. (Possibly Named AADSG-All-Users or something similar), check the box next to the group and click Select
    - Click the three dots to the far right of the included line that lists the AAD-SUG-Intune-Mobile-MDM-StaticTestGroup and select Delete
- Click Review + save

Assign the Android Enrollment Profile

- Navigate to Intune > Devices > Android > Enrollment > (Under) Enrollment options > Device platform restrictions (Enrollment Restrictions)

- Select the restriction profile titled “Android-BYOD-WorkProfile-Enrollment-Restrictions”
- Navigate to Assignments
- Under Assignments:
    - Click Edit to the right of Assignments
    - Assign it to Add the previously created dynamic device group “AAD-SDG-Intune-Mobile-Android-Devices”
    - Add the Entra All-User group for your tenant. (Possibly Named AADSG-All-Users or something similar)
    - Remove the previously created test group “AAD-SUG-Intune-Mobile-WorkProfileMAMMDM-StaticTestGroup”

Assign the iOS Conditional Access Policy

- Navigate to Entra>Conditional Access>Policies (Conditional Access Policies)
- Select the policy named “CAP-iOS-WorkProfile-Blocked”
- Click the “Specific Users Included” Under Assignments
- Under the Select section, click the “1 group” link
- Search for the Entra All-User group for your tenant. (Possibly Named AADSG-All-Users or something similar), check the box next to the group and click Select
- Click the three dots to the right of the AAD-SUG-Intune-Mobile-WorkProfileMAMMDM-StaticTestGroup and select Remove
- Click Save

Assign the iOS Configuration Profile

- Navigate to: Intune > Devices > Manage devices > Configuration >Policies (Configuration Policies)
- Open the profile named " Intune-Devices-Config-iOS-Workprofile-MAM+MDM-DeviceConfig "
- To the right of “Assignments” click Edit
- Under Included Groups, click “Add groups”
- Check the box next to the Entra All-User group for your tenant. (Possibly Named AADSG-All-Users or something similar) and then click Select at the bottom of the pane
- Click the Remove link to the right of the “AAD-SUG-Intune-Mobile-WorkProfileMAMMDM-StaticTestGroup” group

Enroll the Devices

Enrollment into Work Profile MAM+MDM is completely user driven and the instructions for how to do this were included in the “Phase 3 – Section 1: Test Phase Communications” > “Work Profile MAM+MDM Communication:” subsection.

It is recommended however, that you send a follow-up email to the test users on the day before or the day of rollout, reminding them of the go live date and asking them to complete those steps.

Relative Reference Links

Note

This section contains URLs to relevant locations referenced in this manual. These links are subject to change over time and are not absolute. This means that there may occasionally be broken links that you will have to web search for the correct URL address.

Microsoft Links:

Entra Groups:

https://portal.azure.com/#view/Microsoft_AAD_IAM/GroupsManagementMenuBlade/~/Overview

---

Conditional Access Policies:

https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/Policies/menuId//fromNav/Identity

---

Apple Enrollment Tokens:

https://intune.microsoft.com/#view/Microsoft_Intune_Enrollment/DepTokensPaging.ReactView

---

Apple VPP Tokens:

https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/TenantAdminConnectorsMenu/~/appleVpp

---

Compliance Polices:

https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/DevicesMenu/~/compliance

---

Configuration Policies:

https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/DevicesMenu/~/configuration

---

---

iOS/iPadOS apps:

https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/AppsIosMenu/~/iosApps

---

All Apps:

https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/AppsMenu/~/allApps

---

Device Enrollment:

https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/DevicesMenu/~/enrollment

---

App Protection Policies:

https://intune.microsoft.com/#view/Microsoft_Intune_DeviceSettings/AppsMenu/~/protection

---

Enrollment Restrictions:

https://intune.microsoft.com/#view/Microsoft_Intune_Enrollment/DeviceTypeRestrictions.ReactView

---

Other Links:

Apple Business Manager:

https://business.apple.com/

DUNS Number Lookup:

https://www.dnb.com/en-us/smb/duns/duns-lookup.html

Reminders

Certificate Renewals

You will need to annually renew your iOS VPP Token, iOS Enrollment Token and iOS Push Certificate in Apple Business Manager. Intune will then need to be updated with the renewed tokens and certificate.

Bad URLs or GUI changes

The URLs and step by step GUI walk throughs at the time of this manual's writing are accurate, however over time these are subject to change and cause broken links or inaccuracies. It is recommended that you conduct web searches on where items have moved to if this happens and you need assistance.

Default Values Disclaimer

Steps in this guide at times will walk you through creating and configuring various policies, profiles, etc. and it is important for anyone following this guide to understand that only values for these items that differ from the default settings are listed. DO NOT change other settings from their default values unless you are certain that the results of that action are desired and realize that you are doing so at your own risk.

MAM or Work Profile MAM+MDM

This manual is written to only support the singular deployment of MAM or Work Profile MAM+MDM. While either deployment should work in conjunction with an MDM deployment, this manual is not written in a way to support a tandem of MAM and Work Profile MAM+MDM. It's either or.