**Microsoft Intune MDM setup guide**

**Introduction:**

Microsoft Intune MDM is a cloud-based client management solution that manages PCs and mobile devices. This document will walk you through on how to configure and deploying Intune as a stand-alone MDM solution. We will also walk through deploying applications to devices, configuring your Company Portal, enrolling end user devices, creating policies and more.

The tasks and configurations will need to accomplish are broken down into the components below and are our mini-goals to accomplish as we configure them component by component..

1. Configure MDM Authority
2. Configure APN Certificate
3. Configure MDM DNS Records
4. Configure Company Portal
5. Device Enrollment Administrator
6. Device Enrollment and Type Restrictions
7. Device Group Mappings
8. Intune Policies
9. Enable Windows 10 automatic enrollment
10. Enroll Devices into Intune
11. Deploy Client Apps to Managed Intune Devices

**Configure MDM Authority**

First we must configure Intune as my MDM authority. Since this is going to be stand alonewe want Intune as the only authority and not Configuration Manager.

1. Go to portal.azure.com and expand the Intune node and select “Device Enrollment”
2. Select “Intune MDM Authority” and then click “Choose”
3. There will be a notification that the changes were saved successfully

**Configure APN Certificate**

To manage iOS devices you must have an Apple Push certificate. Follow the steps below to get this;.

1. In the Intune page, go to Device Enrollment --> then Apple Enrollment → select “Apple MDM Push Certificate”
2. Agree to the terms → then download the CSR
3. It will download the file, “IntuneCSR.csr”
4. Click “Create your MDM push certificate.” This steps requires an Apple ID so if you don’t have one you will need to create one.
5. Sign in with your Apple ID into the Apple Push Certificates Portal
6. Click “Create a Certificate” after signing into the portal with your Apple ID.
7. Go to your CSR file that you downloaded from the Intune portal above and then select “Upload”
8. After you get a green confirmation, download your certificate
9. Go back to the Intune portal in section 4 on the bottom of the page enter your Apple ID you used to create the certificate.
10. In section 5 browse to the downloaded certificate and then press “Upload”
11. After the upload is done, we can scroll up and see details regarding our certificate, including the expiration data

**Configure MDM DNS Records**

For Windows devices, there are two DNS CNAME records you need to create:

1. The first CNAME to create is this

Name - Enterpriseregistration.yourdomain.com

CNAME - Enterpriseregistration.windows.net

1. The second CNAME is

Name - Enterpriseenrollment.yourdomain.com

CNAME - Enterpriseenrollment.manage.microsoft.com

1. Check your DNS for MDM again, and make sure your records are in place and valid
2. Go back Back into the Intune portal → Go to Device Enrollment,-->Windows enrollment → CNAME Validation and verify that your domain comes back successful

**Configure Company Portal**

The company portal is a web page and a mobile device application that supports BYOD users. It’s a centralized location to install published applications, self management, and retrieve information.

* Open your Intune Admin Portal → Go to Client Apps -->Branding and Customization
* On your IOS phone you open the Company Portal application and you’ll see under support you can see the email and website we specified for help. This is handy for end users as they have a very simple and clear way to contact you or your IT team.
* Once you finished customizing the logo you can save and you’re done.

**Configure Portal Terms and Conditions**

The Terms and Conditions can be prompted to users prior to them accessing the Intune Company Portal. In the Azure Intune portal you can configure your policies, apply to users or groups, and review the acceptance reporting. Here’s how:

* Open the Azure Intune Portal -->Intune blade,--> Device Enrollment --> Terms and Conditions and click “Create”
* Create the required information regarding your Terms and Conditions and then press OK
* You will get a notification that your policy must be asssigned to users or groups in your organization
* In your Terms and Conditions overview select “Assignments”
* Select the Users or Groups you want to assign the Terms and Conditions to and then click Save

The next time you or your users log into the Company Portal they will be greeted with the Terms and Conditions that were assigned to them.

Note: The default number of devices a user can enroll is 5. The only accounts that can add more are the Device Enrollment Administrator and members of Device Enrollment Administrators group.

* To Add users go back into the Intune blade → Expand “Device Enrollment” and select “Device Enrollment Managers” → Click Add and then enter your users UserPrincipalName and then select the “Add” button on the bottom

**Device Enrollment and Type Restrictions**

The default amount of devices a regular users can enroll into Intune is 5 This number can go up or down depending on your needs. To do this go to:

* Open the Intune blade -->Select “Device Enrollment” -->click “Enrollment Restrictions”
* You’ll have the option to either create a new policy or edit the current one. Just go ahead and change it to whatever number is appropriate and click save
* If I want to change the Device Type Restriction Policy, go back to the Enrollment Restrictions pane and select the Device Type Restriction policy

**Device Group Mappings**

If you use Microsoft Intune device categories to automatically add devices to groups based on categories that you define. This makes it easier for you to manage those devices.

**Step 1: Device Categories**

Start by creating two (2) device categories. One category is for BYOD devices, or personal devices. These will be devices that end users own but may use them for work. The other category will be Company Owned Devices. These devices are purchased by the company, and given to the end users through the IT department.

* In Intune portal select “Device Enrollment” → click “Device Categories” -->click Create Device Category → then supply a valid name and press “Create”

You can create any device categories you want. For example:

Point-of-sale device

Demonstration device

Sales

Accounting

Manager

**Step 2: Create Azure Active Directory Dynamic Device Security Groups**

In this step, you will create dynamic groups in the Azure portal, based on the device category and device category name. Use the information in this section to create a device group with an advanced rule, by using the deviceCategory attribute.

When users of iOS and Android devices enroll their device, they must choose a category from the list of categories you configured. After they choose a category and finish enrollment, their device is added to the Intune device group, or the Active Directory security group that corresponds with the category they chose. Windows users should use the Company Portal website to select a category.

Regardless of platform, your users can always go to portal.manage.microsoft.com after enrolling the device. Have the user access the Company Portal website, and go to My Devices. The user can choose an enrolled device listed on the page, and then select a category.

After choosing a category, the device is automatically added to the corresponding group you created. If a device is already enrolled before you configure categories, the user sees a notification about the device on the Company Portal website. This lets the user know to select a category the next time they access the Company Portal app on iOS or Android.

To set up the Group go to :

* Open the Intune Portal, --> select Groups → select “All Groups” -->click “New Group”
* Give your group the required properties like type, name and description, and add a dynamic membership rule. The one below will contain all devices that a user selects as their Personal Device.. Click Create when done.

**Step 3: Select Device Category**

Windows

When users enroll their Windows devices they will need to assign a category in the online Intune portal. Clicking on the device will show them the outstanding notification and allow them to select a category. In the top right of the portal they will also see a notification

Here we see the two categories I set up for the users to select. Since this machine is a Company Owned Device I will select the category. Behind the scenes, this device is added to that dynamic group and allows for a better management experience.

**iOS**

When users enroll their devices using the Company Portal application, they will select which category the device should be placed in

**Intune Policies**

**Compliance Policies**

Compliance policies in Intune define the rules and settings that a device must comply with in order to be considered compliant by conditional access policies.

* Open the Intune portal→ Select “Device Compliance” -->then “Policies” -->Click “Create Policy” and then create a policy that will apply to the end users personal devices. This will be a policy for the group we created earlier. Once we specify a name and platform we will have different compliance settings that we can configure become available. Save when done with setting the compliance settings.
* Next, we will need to assign this policy to devices or users. Click the Assignments item under Manage, click “Select groups to include” you will have the option select Intune – Personal Devices dynamic group and then save.
* If I you want to make sure the policy goes into effect immediately on a device, go to All Devices and find the device and force a resync.
* If you set a passcode setting and the users current passcode does not match, they will be greeted with a password expiration notification. From there they can set their own passcode.

**Configuration Policies**

Commonly used to manage security settings and features on your devices, including access to company resources.

Basic Configuration Policy Overview

* Go to Intune Portal -->select “Device Configuration”, -->“Profiles” -->click “Create Profile” → then .enter the appropriate information regarding your profile / policy. (ie. like making a policy that is applied to corporate owned Windows 10 devices) -->Configure the necessary settings for your specific policy → click “Create” → then click Assignments to assign this policy
* From theren select my Intune – Company Devices group to apply this policy to.

Uninstall Restricted Applications

We’ll configure a restricted application and apply it iOS devices. Restricted applications are applications that users are not allowed to install and run. Users are not prevented from installing a prohibited app, but if they do so, this is reported to you.

* In the Intune portal --> select Device configuration > Profiles -->select your profile you want to edit or create a new one → select Settings > Restricted Apps, and then under type of restricted apps list select Prohibited Apps.
* Open a tab in IE, Firefox, Chrome, etc and look up your application and note the itunes store URL→ go back to the portal paste the link → click “Add” → “Save”

The company portal will display a message that I must uninstall the xxx application since it is now a disallowed application.

**Configure Email Profiles**

* In the Intune portal --> select “Device Configuration”, --> “Profiles” --> click “Create Profile” --> Give your new profile a name and description, →Under profyle type select “Email” or the type that fits your needs → In the email blade configure the email profile --> OK →”Create”
* Click Assignments to assign your profile to a group or all devices. For testing apply it to all devices. This will apply to all iOS devices. If there are other devices, such as Android, it will just list as not applicable.

(Back on my iOS device it will automatically add the account. On an iOS device the account is in Settings > Password and Accounts. When you open the settings application it immediately asks for my password) When I go to Passwords and Accounts I can see that the account was automatically added

Modify iOS Dock

In this example we testing how Intune can modify users home docks. we’lll be making a profile / policy that will ensure the default Phone application is on the dock.

* In the Intune portal--> select “Device Configuration”,-->“Profiles” --> click “Create Profile” .

1. The platform must be iOS
2. Profile type is going to be “Device Features”.
3. In the device features blade select Home Screen Layout and select Dock.

When adding a new application you will need to know the App Bundle ID. If the application is not a default iOS application you can follow the steps in the link to obtain the bundle ID.

https://support.microsoft.com/en-us/help/4294074/how-to-find-the-bundle-id-for-an-ios-app

The application will automatically be placed on the dock on iOS devices once the profile gets pushed to the device.

**Software Update Policies**

With Software Update Policies you can control when users can update to the newest iOS, you can restrict it so they cannot download it during business hours, or how long they must wait after it has been released until they can install it. With Windows Devices you can control devices servicing channel (Insider, Semi-Annual, etc), auto updates, maintenance windows, and more.

**Windows**

To create a Windows Software Update policy

* In the intune portal-->Software Updates --> Windows 10 Update Rings,--> “Create” → Give your policy a name and description.
* In the Settings you can begin configuring the policy settings. We’ll put the devices on the Windows Insider update ring. They will also get Microsoft product updates, and drivers. You can configure a deferral period which may be recommended for a production environment.
* In the User Experience Settings administrators can configure maintenance hours, in my environment I am auto installing the updates anywhere from 3PM to 11PM. Once you have the policy settings configured to your needs you can add scope tags and then press “Create” to create the policy → , click “Assignments” to assign the policy to devices or groups.

You can apply to all devices using the “Assign to” drop down, or you can assign it to one of the dynamic groups we created earlier by click the “Select groups to include” and then selecting my “Intune – Company Devices” group.

**IOS**

* To create a Software Update policy go in the Intune Portal -->Software Updates > Update Policies for iOS, and then “Create”, give it a name and description
* Configure your settings. For an example disable users from updating to the newest iOS during the work week and during work hours. iOS updates are also deferred for 2 weeks.
* Click the Create at bottom of the blade Click “Assignment” to assign your policy to groups or devices → apply this policy to Company Devices only.

Enable Windows 10 automatic enrollment

Automatic enrollment lets users enroll their Windows 10 devices in Intune. To enroll, users add their work account to their personally owned devices or join corporate-owned devices to Azure Active Directory. In the background, the device registers and joins Azure Active Directory. Once registered, the device is managed with Intune.

1. In the Azure Portal -->select Azure Active Directory --> click “Mobility (MDM and MAM) -->select “Microsoft Intune”
2. Configure MDM User scope. Specify which users’ devices should be managed by Microsoft Intune. Windows 10 devices can automatically enroll for management with Microsoft Intune.

* None – MDM automatic enrollment disabled
* Some – Select the Groups that can automatically enroll their Windows 10 devices
* All – All users can automatically enroll their Windows 10 devices

Important Note: If both MAM user scope and automatic MDM enrollment (MDM user scope) are enabled for a group, only MAM is enabled. Only MAM is added for users in that group when they workplace join personal device. Devices are not automatically MDM enrolled.

Enroll Devices into Intune

iOS

Have your users download and install the Company Portal from the iOS App Store. Once they launch the application and sign in they can begin to Intune enrollment process. The application will show the end user the permissions the IT Administrator will have on the device. They will then be shown the step by step instructions that the application will take to enroll the device. An MDM iOS Profile will be installed on the device. And finally, the user will select a category (set up earlier) to put their device under. This allows for a better administrator management experience The Company Portal will show the end users any available apps you have granted them, all of their Intune devices, support options we set up previously and notifications.

Windows

Windows users can install the Company Portal from the Windows store, use the web Company Portal, or use the Windows Settings app to enroll their Windows devices into Intune.

* Open the Online Portal
* Navigate to the online Company Portal at <https://portal.manage.microsoft.com>
* Once the user signs into the Company Portal they can add a device under Devices -->Click “Add” → Have them sign in and then press Next
* The user will be prompted to enter their account password and then press “Sign In”. Once complete they will be prompted with a successful message.

Microsoft Store App

Have your users download and install the Company Portal application from the Microsoft Store,

* They will be prompted to sign in
* They will be prompted for the password
* Check “Allow my organization to manage my device” and then click Yes
* The Company Portal will prompt them to select a device category that we set up earlier
* The Company Portal will now show the newly enrolled device

Windows Settings App

* Open the Windows Settings application and select “Accounts”
* Select “Access work or school” in the right hand pane, and then press “Connect”
* Sign in using your work account
* Enter your work account password and then press Sign In
* Once complete you will get a successful message

Back in the Settings app you will now see your account

Deploy Client Apps to Managed Intune Devices

The Company Portal allows and administrator to push, install, uninstall, and make available, applications for end users. Applications can include Office 365 apps, web apps, Microsoft Store apps, iOS Apps and more. The Company Portal will only display applications that is relevant to the device they are on, if they are on an iPhone it will not display your published applications for Windows even if the device is in the same group.

* In Intune portal and the go to “Client Apps”,-->“Apps” -->select “Add”. For example, deploy Office 365 ProPlus to the devices so we will select Windows 10 under Office 365 Suite
* configure the app settings to fit my company needs
* configure the update channel, EULA and more
* We will make this application required for all users in my assignments setting
* After a bit we can see that Office is installing on my end user machine in Task Manager
* If we had not made the app required and just made it available, end users could choose to install it from the Company Portal
* Once the install is complete I can check the start menu to see all of my newly installed applications

In the Intune portal under my applications, you can see that I have Office 365 ProPlus successfully installed on 1 device, and not applicable on 1 device (iOS)