**Office 365 Device Management**

**Introduction:**

First, to be clear so that there’s no confusion, this is not the same as enabling a full Microsoft Intune subscription. The Office 365 MDM solution is based off of Intune but think of it as a “lite” version of the Intune service.

**Setting up MDM**

**Setup a security group in Groups**

* Add a new group, and choose the type Security.
* Give it a name that describes the purpose–MDM Policy add users, or apply the MDM policy, etc.

For me, I usually just add all users, but in this case you can actually have multiple MDM policies with different users in each group, if you so choose accordingly to your needs.

**Configure domains for MDM**

If you manage your DNS through Office 365 go to DNS management otherwise you’ll have to go to your domain registrar. You’ll need to add the following 2 records.

Host name Record type Address

EnterpriseEnrollment CNAME EnterpriseEnrollment-s.manage.microsoft.com

EnterpriseRegistration CNAME EnterpriseRegistration.windows.net

**Admin Portal**

In Office 365 Admin portal go to - the bottom left and show all admin portals and find Device Management. OR, you an go to Security & Compliance Center and find Device Management

**Set up your Apple Push Notification Certificate**

1. To configure a APNs Certificate for iOS devices, select Set up.
2. Select Download your CSR file and save the Certificate signing request to a somewhere on your computer that you'll remember.
3. Click Next.
4. To create an APN certificate - Select Apple APNS Portal to open the Apple Push Certificates Portal
5. Sign in with an Apple ID. Try to use a company Apple ID associated with an email account that will remain with your organization even if the user who manages the account leaves. Save this ID because you'll need to use the same ID when it's time to renew the certificate.
6. Select Create a Certificate and accept the Terms of Use
7. Browse to the Certificate signing request you downloaded to your computer from Office 365 and select Upload.
8. Download the APN certificate created by the Apple Push Certificate Portal to your computer.
9. Go back to Office 365 and select Next to get to the Upload APNS certificate page.
10. Browse to the APN certificate you downloaded from the Apple Push Certificates Portal.
11. Click Finish.

**Creating a MDM Policy**

1. Go back to the Device Management Portal
2. Click Device policies.
3. Create a policy.
4. Give it a name. Although you could have multiple and apply them to different groups, etc., I usually just create a global one for the entire organization and then create more specific ones for different needs.
5. Make your selections, there are two pages of options, I usually select the more important ones like require a non-simple password, and other restrictions is up to what your organization needs.

* There is an additional page with more options, such as Require encrypted backup, and others. Most small organizations have no interest in controlling these items on personal mobile phones, tablets, etc. You can either enable the policy, or just save it without turning it on

1. Specify the group to which the policy will and click Next.
2. Review your settings and Create this policy.

**Manage organization-wide device access settings.**

Go back on the MDM page

* I usually opt to choose to Allow or Block devices that are not compliant with the MDM policy. I can see that this could be annoying for some people, but as an admin you ask yourself why use an incompatible device or app? Why bother trying to support it when it’s not compatible? You’re just asking for more support issues.
* When you are done with all of this, your users will need to go enroll their devices. See link for more information:

<https://support.office.com/en-us/article/enroll-your-mobile-device-in-office-365-c8ac722d-dcaf-4135-8345-3e6327f5d3c5?ui=en-US&rs=en-US&ad=US>

The main feature leveraged in O365 MDM is probably Selective wipe –invaluable for those situations where you need to remove the corporate data of a departed employee’s personal device, without causing an upsetting situation–by wiping ALL of the data, and affecting a full factory reset on the device. Here’s more on this feature:

<https://support.office.com/en-US/article/Wipe-a-mobile-device-in-Office-365-9d727c7d-8b47-4499-bf24-d046b449214c>

You can also add in Multi-Factor Authentication if your organization requires it. Below is the link the the Microsoft instructions:

<https://docs.microsoft.com/en-us/office365/admin/security-and-compliance/set-up-multi-factor-authentication?redirectSourcePath=%252farticle%252f8f0454b2-f51a-4d9c-bcde-2c48e41621c6&view=o365-worldwide>