Learn Intune Beginners Guide MDM MAM MIM | EndPoint Manager

Intune standalone starter kit. I think this post will help to start learning Intune from scratch. I won't cover SCCM Hybrid/Mixed Intune and Office 365 Intune MDM. In most of the scenarios (for Intune Standalone), no need/very minimal need for on-premises infrastructure. Intune standalone is the way to go when you want to take the path of modern management.

Latest updates available - https://www.anoopcnair.com/learn-microsoft-intune/

Free Intune Training Videos - https://www.youtube.com/playlist?list=PL67vGzo-INWO_0e-iSXsMHoRwB1mrTvU4

By **Anoop C Nair** - October 16, 2017 *****Updated on April 6th, 2020**

Loads of people requested for an **Intune starter kit** as I have one for SCCM. I think SCCM starter kit page was useful for the IT community. Mobile device management is new for most of the IT Pros in device management world.

TL;DR

Great Learning for Intune Beginners

SCCM is great and it's not **going to die as per Mcirosoft**. But, don't go away from Intune learning. I would strongly recommend going through Intune learning process.

What to Learn Intune? Great Resource Around you! **(1) LinkedIn Learning Courses for Microsoft Intune**, **(2) Learning How to Learn SCCM Intune**

Intune for SCCM Admins

Intune is the modern device management solution from Microsoft. My recommendation to SCCM admin is to start learning Microsoft Intune.

I have a series of post to explain the difference between SCCM and Intune administration and architecture. Check out those posts:

1. Microsoft Intune for SCCM Admins Part 1 (the video post **here**)
2. Microsoft Intune for SCCM Admins Part 2
3. Microsoft Intune for SCCM Admins Part 3 (sometime in future ;))

Introduction to Microsoft Intune for Beginners

This post would be useful for Intune **newbies**. In this post, you will see more details about "Beginners Guide to Learn Intune MDM MAM MIM – Learn Microsoft Intune."

- **My latest Intune posts are available https://www.anoopcnair.com/intune/**

This post, I will be concentrating on **Intune standalone**. I won't cover SCCM Hybrid/Mixed Intune and Office 365 Intune MDM. In most of the scenarios (for Intune Standalone), no need/very minimal need for on-premises infrastructure.

Intune standalone is the way to go when you want to take the path of **modern management**. Most of the Intune components are hosted in Microsoft Azure. I'll try to keep this post updated with new Intune features.

NOTE! – New Intune Microsoft Device Management portal. More Details https://www.anoopcnair.com/intune-microsoft-device-management-portal/

Intune Very High Level Architecture Flow
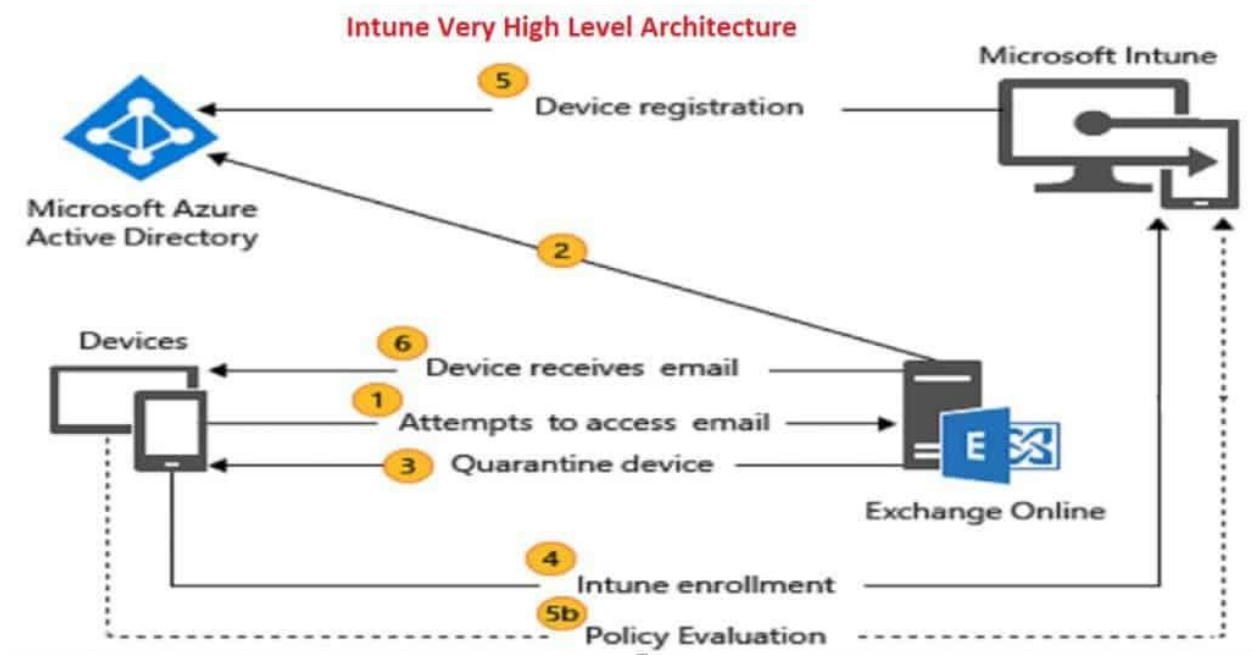
Intune Architecture

*We already have a **Facebook group for Intune Professionals**. If you would like to join the Facebook community of Intune Professionals, click here. You can also **subscribe the YouTube channel** here where you have loads of Intune tutorial.*

Why Learn Microsoft Intune as a Beginner?

When you take a look at the **Desktop** (43.29%) **Vs. Mobile** (52.29%) **Vs. Tablet** (4.42%) **Market Share Worldwide** for last one year, you could see the mobile devices are leaders. So, Mobile Device Management is very critical, and this is a new world of opportunities for IT Pros like us. From my perspective, **Learn Microsoft Intune** is very important for SCCM admins.

I don't think SCCM will go away for another **5-6 years**. I know some SCCM 2007 environments are managing more than 40K devices. So, it's going to a take long time to migrate corporate organizations to move to modern device management solutions.

But, I also agree that we need to Learn Microsoft Intune **Mobile Device Management (MDM)**, **Mobile Application Management (MAM)** technologies, etc. This is why it's important to learn Microsoft Intune is important for SCCM admins.

Mobile Device Management (MDM) is not a term used only for managing or administrating mobile devices. Rather, **MDM** also includes **administration** of a wide range of new laptops, desktops etc. For example, with Windows 10 all desktops, and laptops can be managed through MDM channel.
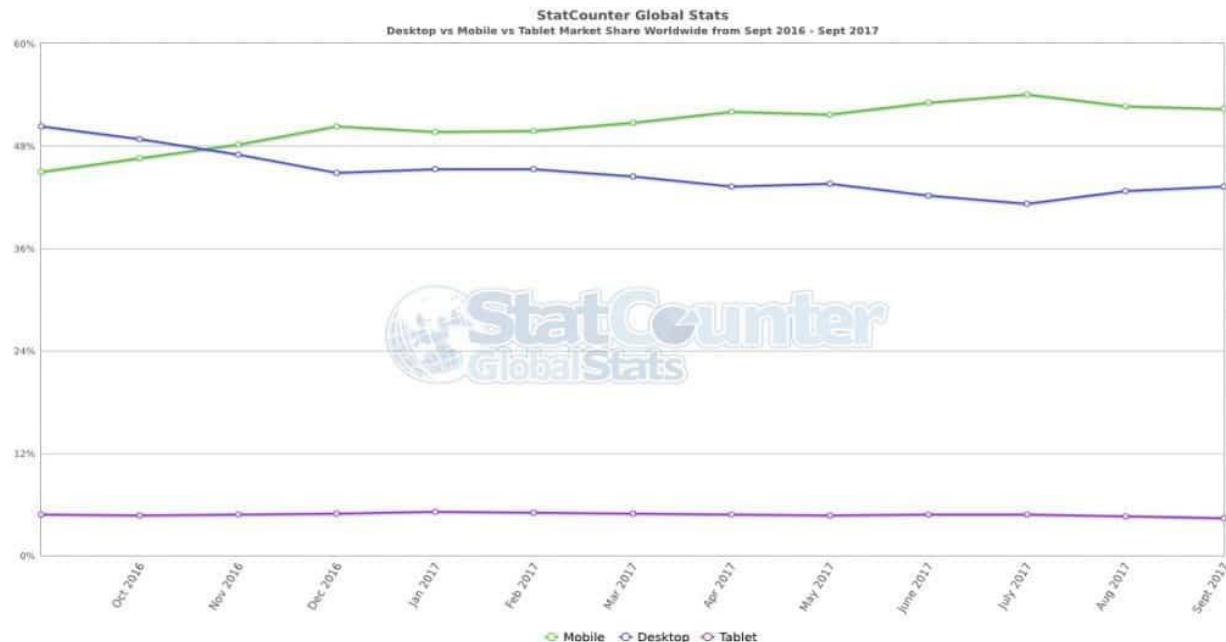
Why to Learn Intune?

What is Microsoft Intune and How is it different?

Intune is an **enterprise mobility management (EMM)** solution from Microsoft. The EMM provider helps to manage mobile devices, network settings, and other mobile services and settings.

Microsoft Intune is nothing but a combination of Device, Application, Information Protection, Endpoint Protection (antivirus software) and Security/Configuration policy management solution (SaaS) facilitated by Microsoft in Cloud.

Additionally, Azure AD has a feature where admins can create a "**Conditional Access (CA)**" policy to get access to company resources. This Azure AD CA policy can be combined with Intune compliance policies. When the devices meet those conditions then, only the Intune will provide access to company or

corporate resources (corporate email, Share point, etc…). Intune is pure cloud architecture and it's fun to Learn Microsoft Intune.
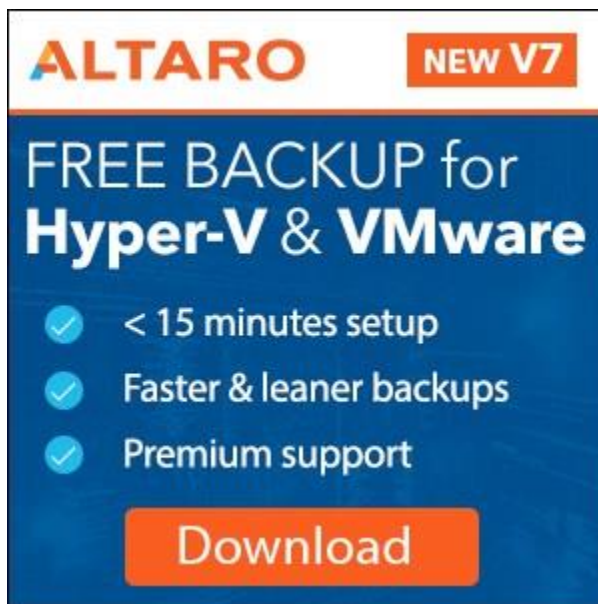
Previously, I mentioned Microsoft Intune as lighter Version of SCCM or ConfigMgr in the cloud. However, I don't want to make the comparison so simple this time.

Intune architecture is entirely cloud-based and agile. Get more details idea about Microsoft Intune in the **below video**. Yes, this video is old and outdated but, very well explained.

How to Start Working with Intune as a Beginner

Download **Microsoft EMS step by step setup guide** from **here**. This guide will help you to get a trial version of Office 365, Azure AD and Intune subscription for free.

If you already have an Azure AD (Azure AD premium) subscription, then things are very straightforward as I posted on the blog **here**. First and foremost you need to have a strong desire and determination to Learn Microsoft Intune.

If you **don't have** Azure AD subscription then better to start with Enterprise Mobility Suite (EMS) trial account, Azure Free Trial Account and Office 365 free trial subscription.

The Azure trial account is already created EMS trail account. It's better to create NEW outlook.com account and get ready with Credit Card details to activate the Azure trial subscription.

Getting a trial version of Azure AD, Office 365 and Intune is very straightforward process if you have never done this same process with your credit card and mobile number. Azure AD and Office 365 are prerequisites for Intune if you want to test/trial all the features of Intune.

*Note :- **Intune can be signed up separately as well from** [here]. If you feel, you are interested in testing only Intune now then this is the way.*

Intune Quick Start Tips

- [Try Intune for free] – Create a free subscription to try Intune in a test environment.
- [Create a user] – Add a user to Intune to allow them to access company resources on mobile devices.
- [Create a group] – Organize users into groups to make it easier to manage the policies and apps they can access.
- [Set up automatic enrollment] – Set up Intune to automatically enroll devices when specific users sign in to Windows 10 devices.
- [Enroll your device] – Take the role of an Intune user and enroll your device into Intune. Then, return to Intune and confirm that the device enrolled successfully.
- [Create a device compliance policy] – Create a device compliance policy and assign a group to the policy.

- [Send notifications to noncompliant devices](#) – Send an email notification to the members of your workforce who have noncompliant devices by creating and assigning a compliance policy.
- [Add and assign an app](#) – Add and assign a client app to your company's workforce.
- [Create and assign an app protection policy](#) – Create and assign an app protection policy to a client app on an end user's device.
- [Create and assign a custom role](#) – Create and assign a custom role with specific permissions for a security operations department.
- [Create an email device profile for iOS](#) – Create an email device profile for iOS devices.
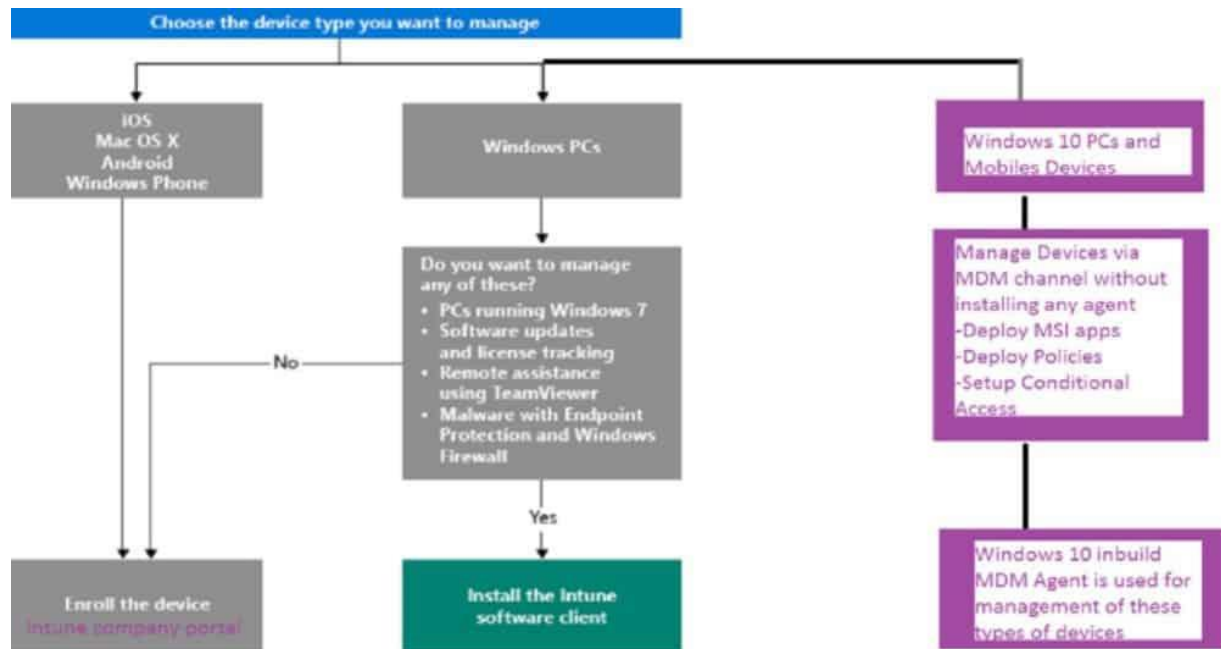- More details [here](#).

What are the Management Options in Intune?

Intune can manage Mac-OS, Android, iOS and Windows devices via MDM (Mobile Device Management) channel. I cover MAM (Mobile Application Management) in the below section.

NOTE! – Different Microsoft **Intune Enrollment options** are explained in the following post. https://microscott.azurewebsites.net/2018/08/31/managing-windows-10-with-intune-the-many-ways-to-enrol/

We can manage devices (via MDM) with ~~an **Intune client agent**, and~~ arguably **without Intune client agent**. To manage iOS, Android, and Mac-OS devices, Intune needs an agent to be present in the device. Intune company portal application is the Intune agent. You can see the details in different app stores like [Google Play](#) and [Apple Store](#).

So, when you install **Intune company portal** onto your Android or iOS devices, then you are doing an Intune agent-based management. There is an Intune MSI client available to download for Windows 7, Windows 8 devices. For Windows 10, Intune uses in build MDM stack of Windows 10 operating system itself. Enrollment of devices and decision making on this is critical step to Learn Microsoft Intune.

Figure: Choose the device type you want to manage — flowchart showing iOS/Mac OS X/Android/Windows Phone, Windows PCs, and Windows 10 PCs and Mobiles Devices paths.

~~I have an old post (published on Dec 2012) here to help you understand the basic stuff about Intune MSI agent installation. Once you install Intune MSI agent on Windows machines, those machines are "fully managed" by Intune.Following are the **different ways to enroll devices into Intune** for management.~~

Windows 10 Device Enrollment – Manual

More details in the following posts:

[Windows 10 Intune Enrollment Process BYOD Scenario](#)

[Windows 10 Azure AD Join Manual Process – CYOD](#)
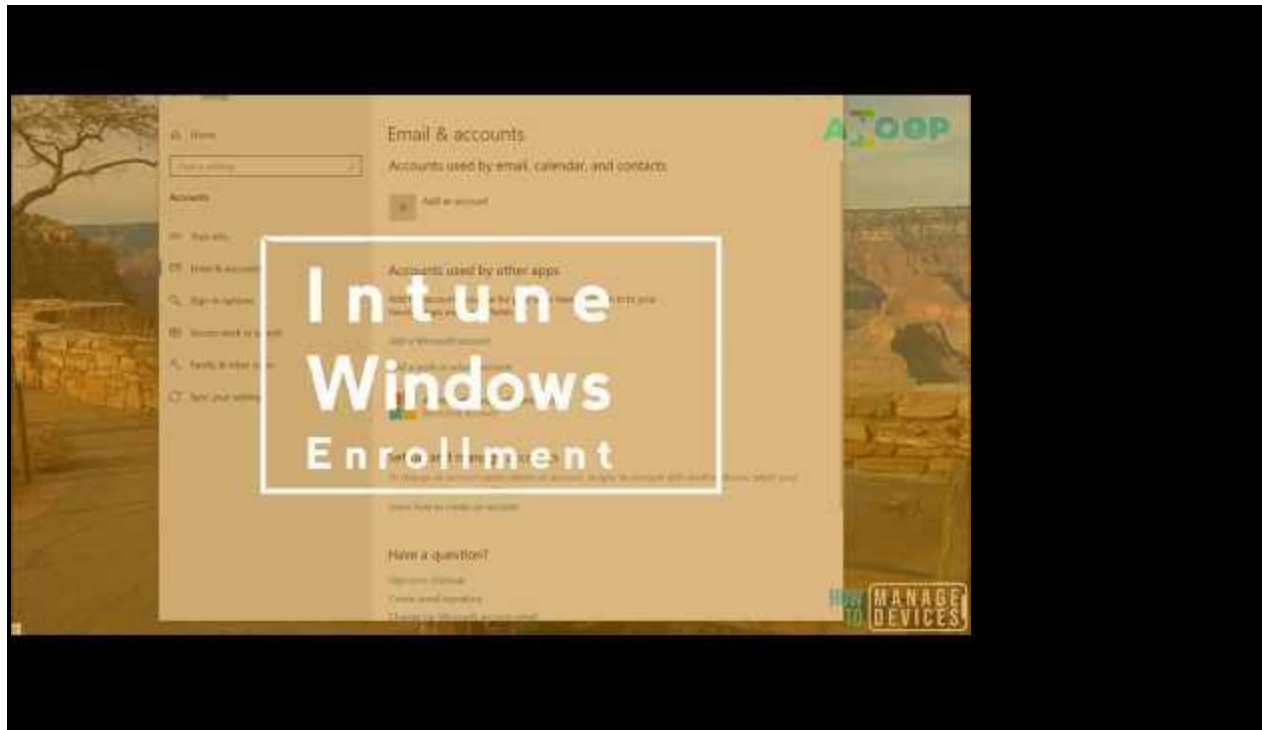
```
Enrolled via Intune company portal

Enrolled via Installation of Intune MSI client

Enrolled via Windows 10 1607 and later in build Azure AD join and
MDM enrolment

MAM without MDM enrolment
```

What is Modern Workplace OSD Replacement (Windows AutoPilot)?

I have more posts related to Windows Autopilot in the following link
– https://www.anoopcnair.com/windows-autopilot/

Intune MAM Enabled Applications

Updated List of Microsoft Intune MAM protected apps
– https://docs.microsoft.com/en-us/intune/apps-supported-intune-apps

How to Start Using Intune Console?

Intune blade (console) is part of part of the Azure portal. Intune blade in Azure portal has loads of new features and the functionalities. In this section, we will a see an overview of New Azure Intune Portal. **Try this out https://portal.azure.com**

The following documentation is the place where you can start reading about all the Intune topics:- **Microsoft documentation Intune quick start guide here**. I have another post which gives a "Quick Overview New Intune Azure." Also, you can have a look at the video tutorial to understand the Intune Azure console **here**.

What is Intune Team's Roles & Responsibilities?

In a high-level following are the **roles and responsibilities of Intune team**. Some parts of it have involvement of Azure AD and other teams of the organization. Understanding the roles and responsibilities will help the IT Pros to understand, How Intune works? And How Intune will be deployed within the organization? More details available in my previous post "Intune Team's Roles and Responsibilities."

Setting up a team is also part of Learn Microsoft Intune process.

```
User Management


Application Creation and Deployment/Assignment


Service Administration


Mobile Application Management
```

```
Device/Profile Management


Conditional Access


Company Resource Access


Software Update Management
```

What is Intune MDM Authority?

Setting up mobile device management authority is an important and first step before start working with Intune. The **M**obile **D**evice **M**anagement (MDM) authority determines where **you will perform mobile device management** tasks.

Microsoft provides **3 options to set the MDM** authority. Microsoft Intune by using the Intune Azure console, or to SCCM by using the SCCM CB console. It's important to understand the details about MDM authority when you Learn Microsoft Intune.

- **Microsoft Intune**
- ~~Configuration Manager~~ **~~(SCCM Intune Hybrid is Out of Support)~~**
- Office 365 (lightweight Intune)

In my perspective, the best **design decision** is to set **Mobile Device Management (MDM) authority** as **Intune**. You can set MDM authority **Microsoft_Intune_Enrollment** / OverviewBlade /overview section from Azure Portal.
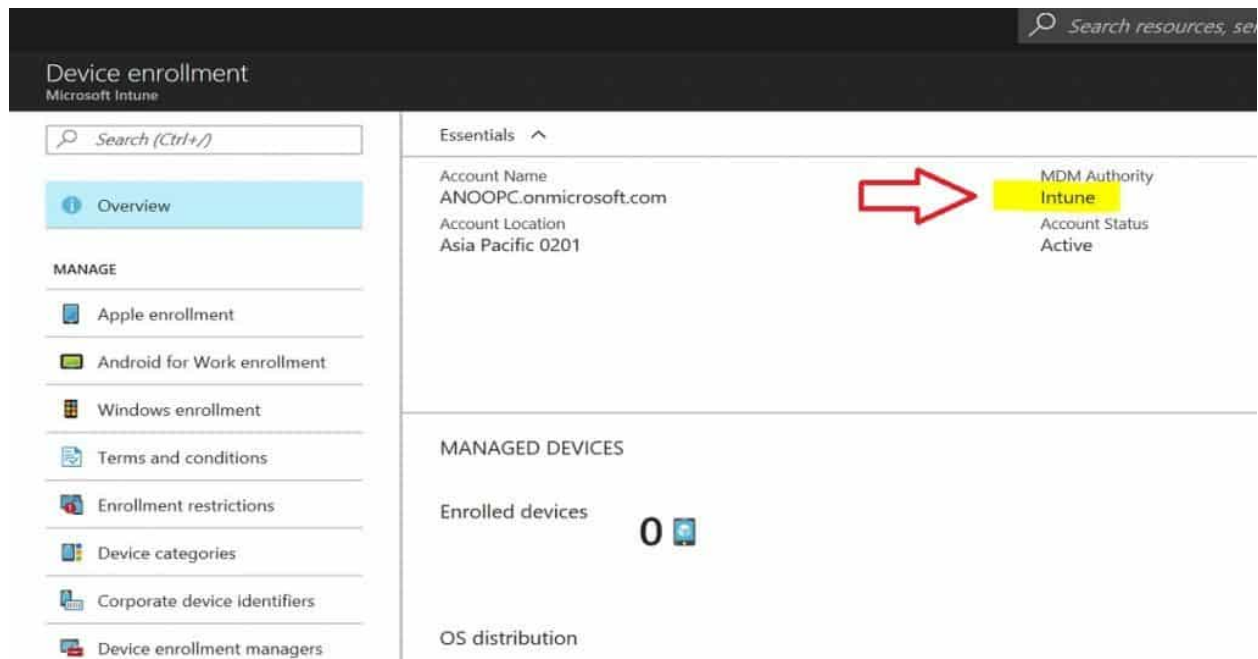
How to Start Managing Devices with Intune?

Windows 10 device management is straightforward with Intune.
It's 10 minutes work to your sync your Windows Store for Business and
Microsoft Intune. More details in the post "Integrate Windows Store for
business." Learn Microsoft Intune is important if you are in the field of Device
management.

If you want to install store apps with the corporate account then, we can sync
the Windows store for Business with Intune. Once the store apps are synced
with Intune then, we can deploy it to Windows 10 devices. Read following blog
post for more details "How to Add Apps to Business Store and Install Intune
Company Portal without Using MS Account."

Intune Windows 10 MDM YouTube Playlist

Google provides **two channels of management** for Android devices. The first
channel of management is part of **general Android** device management and
the second channel of management is **Android Work (Android for
Work)** device management.

`Android (General)`

`Android for Work`

Intune supports both channels of management. **Google's strategic approach** is to support management via only via Android Work channel. Learn Microsoft Intune should be part of strategic approach of SCCM Admin.

I have explained the process how to setup Android Work from Intune Azure Portal in one of my previous post **here**. You need to have a Google account to complete the setup of Android for Work in Intune console. More details about Android for Work Enrolment readiness is available in the following post. **Step by Step Video Guide Intune Azure Portal How to Setup Android Work Support**.

Videos Android Devices Management via Intune

iOS\MAC OS device management has certificate requirements, and we need to go to apple portal, upload your cert for the tenant and get the certificate for your Intune tenant. Similar to Android **iOS and Mac-OS** has **two channels of management**. One is **traditional management,** and another one is advanced management via **Apple DEP** management.

The first requirement for iOS and MAC OS device enrollment is the setup of **Apple MDM push cert**. You need to download different certificate signing request (CSR) from Intune tenant and upload the same to the Apple portal. Once uploaded successfully, you will get an option to download the Apple MDM push cert from Apple portal.

I have explained iOS/MacOS on-boarding process in the following post "How to Get Intune Environment Ready for iOS and Mac OS Devices."

Intune step by step Video Tutorials for iOS

Intune Automatic Policy Refresh Update?

Intune Policy Sync Time details here. You will get more understanding of this refresh timings as part of Learn Microsoft Intune.

Following are the default Intune policy refresh intervals :-

- iOS and Mac OS X: **Every 6 hours.**
- Android: Every **8 hours.**
- Windows Phone: **Every 8 hours.**
- Windows 8.1 and Windows 10 PCs enrolled as devices: **Every 8 hours.**

When the devices have just enrolled, the Intune policy check-in frequency will be more frequent more details as follows:-

- iOS and Mac OS X: Every **15 minutes** for 6 hours, and then every 6 hours.
- Android: Every 3 minutes for **15 minutes**, then every 15 minutes for 2 hours.
- Windows Phone: Every 5 minutes for **15 minutes**, then every 15 minutes for 2 hours.
- Windows PCs enrolled as devices: Every **3 minutes** for 30 minutes.

When any type policy or an app is deployed, **Intune immediately** begins attempting to notify the device that it should check in with the Intune service. This typically takes less than five minutes.

If a device doesn't check in to get the policy after the first notification is sent, Intune makes three more attempts. If the device is offline (for example, it is turned off or not connected to a network), it might not receive the notifications.

Sequence of Intune Policy Creation

There are different types of policies in Intune. All these policies are used for managing and securing the mobile devices. In my opinion, we need to start creating **Intune policies in the following sequence**.

We will see more details about each type of Intune policies in the below sections of this post. To understand this flow is important step to Learn Microsoft Intune.

1. **Enrollment Restriction Policy**

2. **Conditional Access Policy (Azure AD)**

3. **Compliance Policy**

```
4. Configuration Policy (Device Restriction Policy)


5. Resource Policy (Wi-Fi, VPN profiles)
```

Enrollment Restrictions

Conditional Access

Compliance Policies

Configuration Policies

Why Set Enrollment Restriction Policies

Device Enrollment is the first step of Mobile Device Management (MDM). When a device is enrolled into Intune, they have issued an MDM certificate, which that device then uses to communicate with the Intune service.

So, it's a best practice from the security perspective to restrict devices from enrolling into Intune environment. This can be achieved through Enrolment restriction policies.

Difference Between Intune Enrollment Restriction Vs Device Restriction Profile

Why Deploy Intune Compliance Policies?

Compliance policy rules might include using a **password/PIN** to access devices and **encrypting data** stored on devices. These set of such rules is called a compliance policy. The best option is to use compliance policy with **Azure AD Conditional Access**.

Intune compliance policies are the first step of the protection before providing access to corporate apps and data. I have a post which explains about "**How to Plan and Design Intune Compliance Policy**."

Intune Compliance Policy Support Details

The following table lists the device types that compliance policies support. Intune can automatically remediate or quarantine. The table also describes how non-compliant settings are managed when a compliance policy is used with a conditional access policy. More details **here**.

Deploy Intune Device Restriction Policy

Intune **Device restriction profiles are the policies similar to GPO** from traditional device management world. Most of the enterprise organizations use GPO to restrict corporate-owned devices with these policies.

Restriction policies are security policies which need to apply on devices. Intune Device restriction policies control a wide range of settings and features of mobile devices (iOS, Android and Windows 10). More details in my previous blog "How to Restrict Personal Android Devices from Enrolling into Intune."

I love to learn Microsoft Intune as it has 100% return of investment (ROI).

Deploy Resource Policies (Wi-Fi Profile)

Intune Resource policies help devices to **connect to corporate resources**. Deployment of SCEP profiles to devices helps to get connected to corporate resources through Wi-Fi and VPN profiles etc. Before creating iOS SCEP profile in Intune, you need to create and deploy certificate chain.

More details about the Intune resource policy are available in my previous post. **How to Create and Deploy SCEP Profile to iOS Devices via Intune**.

Deploy Applications to Devices using Intune

One of the important use cases of Intune is to deploy applications to different flavors of devices.

The types of applications which Intune supports now are EXE, MSI (Windows Installer and Windows Installer through MDM), APK, IPA, XAP, APPX – APPXBUNDLE for Windows app package and Windows Phone app package.

Also, you can deploy store applications from Windows Store, Google Store and Apple store using Intune Azure Portal. More details about deploying the **application via Intune** is given in the following links **here** and **here**.

MSI application deployment is one of the best use cases of Intune for enterprise customers. More details are available in my previous post. Intune Azure **Step by Step MSI Application Deployment Video Guide**.

Intune Application Model Support (Complex MSI)

Now Intune can deploy all the complex applications to Windows 10 MDM managed Windows 10 devices using a new agent called Sidecar.

You can have more details on Vimal's posts in the following links:

[Intune Win32 App and .EXE Application Deployment using Modern Management](#)

Intune Win32 App Deployment Troubleshooting post – [Intune Win32 app Troubleshooting](#)

Mobile App Mgmt without Enrollment (MAM)

Microsoft Intune supports MAM without enrollment (MAM WE) and Conditional Access policies for Android devices. There are two types of management options for Windows, Android and iOS devices with Intune.

First one is the traditional way of MDM management and the second **method of management is the light management** of apps which are installed on Android, iOS and Windows devices via Intune.

BYOD devices are suitable for MAM WE type of Intune management. Intune can also have Conditional Access policies assigned to MAM users.

For example, if a consultant's device has already enrolled to a 3rd part EMM solution, but he wanted to have access to client's corporate email access on his mobile device for a very short period then, The "MAM WE" is the best option for that consultant.

I have a post about MAM WE "**How to Enable Intune MAM without Enrollment along with Conditional Access**."

Updated List of Microsoft Intune MAM protected apps
– https://docs.microsoft.com/en-us/intune/apps-supported-intune-apps

Intune and Mac Device Management

Intune natively support Mac Device management. But, the Intune Mac device support is very generic. Jamf is the one third party solution which Microsoft advised all the organizations to look into if they are looking for more deep level management of Mac Devices with Intune.

More details available https://nohuman.dk/ems-jamf-connect-jamf-connect-login/

Learn to Troubleshoot Intune Issues

Intune troubleshooting **made easy in the Azure portal**. It's recommended to start with "Microsoft Intune – Help and support" page in Azure portal whenever you face issue with Intune.

I have a post where I discussed "Start Troubleshooting Intune Policy Deployment Issues from Intune (new Azure) portal." More details in the Video experience **here**.
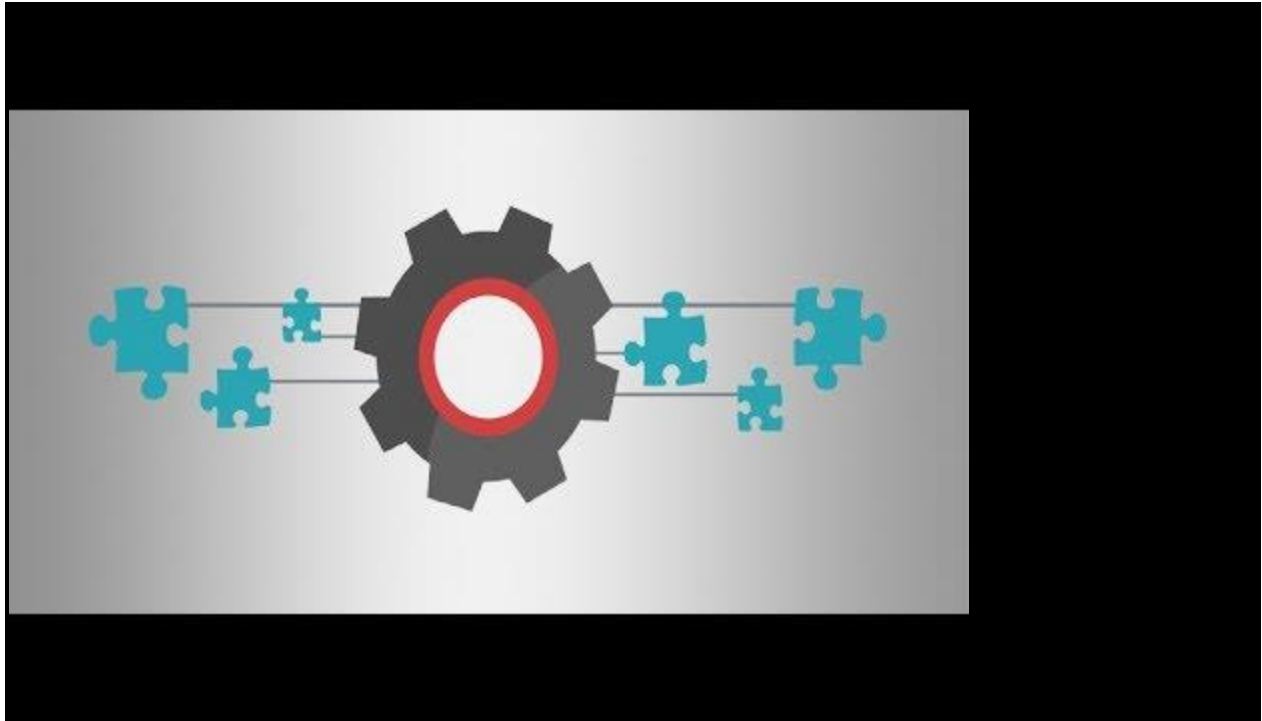
How to Troubleshoot Android Device for Intune Issue

https://docs.microsoft.com/en-us/intune/enduser/troubleshoot-your-device-android
Open the Company Portal app Menu > Help and Feedback
CompanyPortalX.log. This log file contains a lot of information about the communication between the device and Microsoft Intune.

Omadmlog.log. OMA-DM is an open mobile standard for managing mobile devices. com.microsoft.intune.mam.managedAppName.log. For each managed application, you have a log file with the name of the managed application.

How to Troubleshoot iOS Device for Intune Issue

https://docs.microsoft.com/en-us/intune/enduser/troubleshoot-your-device-ios
Intune Company portal – User Profile – About – Send Diagnostic Report
CompanyPortal-Log.log

How to Troubleshoot Windows Device for Intune Issues

https://docs.microsoft.com/en-us/intune/enduser/troubleshoot-your-device-windows
Registry Keys
Event Logs
WMI

How to Start Learning Intune – Microsoft Graph API

More details Microsoft Intune Graph API in the following post. This post gives us the opportunity to dive into many technical areas.

https://techcommunity.microsoft.com/t5/Intune-Customer-Success/Support-Tip-Getting-Started-with-Microsoft-Graph-API/ba-p/364257

Intune PowerShell Script samples

You can download Intune PowerShell script samples from GitHub.

https://github.com/microsoftgraph/powershell-intune-samples/blob/master/AppProtectionPolicy/ManagedAppPolicy_AppRegistrationSummary.ps1

Where is the information Intune MIM in this post?

EMM, MIM, and MAM are subset of MDM. So it's very well part of your Intune MDM policies. This is not me ranting ☺ Check this out from Microsoft.

Intune Group Policy Deployment

Let's learn how to create & deploy Group policy using **Intune** Administrative Template. We can use Intune Administrative Template for deploying the "Cloud" Group Policy for modern managed devices.

NOTE! – More details available in step by step guide – https://howtomanagedevices.com/intune/1671/intune-administrative-template/

Ignite Videos Intune

- Mobile device and app management overview with Microsoft Intune
- Conduct a successful pilot deployment of Microsoft Intune
- Manage and secure Android, iOS, and MacOS devices and apps with Microsoft Intune
- Learn how to use Microsoft Intune with the new admin console and Microsoft Graph API
- Secure access to Office 365, SaaS and on-premises apps with EMS
- Manage and protect Office 365 mobile apps with Microsoft Intune
- Deploying and using Outlook mobile in the Enterprise
- Manage mobile productivity with EMS

Ignite 2017 Video Windows 10 & Office 365 ProPlus:

- Microsoft 365: Modern management and deployment (general session with Brad and Rob)
- Overview: Modern Windows 10 and Office 365 ProPlus management with EMS
- Transition to cloud-based management of Windows 10 and Office 365 ProPlus with EMS
- Modernize deployment & servicing of Windows 10 & Office 365 ProPlus with EMS
- Secure Windows 10 with Intune, Azure AD and System Center Configuration Manager

All PPT decks can be found here (updated).

Anoop C Nair

https://anoopcnair.com

Anoop is Microsoft MVP and Veeam Vanguard ! He is a Solution Architect on enterprise client management with more than 17 years of experience (calculation done on the year 2018) in IT. He is Blogger, Speaker and Local User Group Community leader. His main focus is on Device Management technologies like SCCM 2012,Current Branch, Intune. He writes about the technologies like SCCM, SCOM, Windows 10, Azure AD, Microsoft Intune, RMS, Hyper-V etc...

RELATED ARTICLESMORE FROM AUTHOR

Use Applocker to Manage Chrome Firefox in Windows from Intune – Part (3/3)

Use WDAG to Manage Chrome Firefox in Windows with Intune – Part (2/3)

Use OMA-URIs to Manage Chrome, Firefox in Windows with Intune – Part (1/3)

1. **Naushad Ali T D** October 16, 2017 at 7:33 pm

   Excellence and Brilliance what I would say.
   Many many thanks for such a detailed information for starters.

   +91779556

   Reply

2. **Migration Guide Intune Hybrid to Intune Standalone - anoopcnair.com** March 13, 2018 at 8:33 pm

   […] Start training support staff for Intune device management (Start Learning Intune) […]

   Reply

3. **Radek** April 20, 2018 at 12:59 pm

   Good job
   Maybe could you help me?
   I use autoenrolment scenario for domain joined computer. Intune is set up to standalone. I have ADFS. My device is joined to ad azure (connect type Hybrid Join) with success, device is enrolled to Intune but without user assigment. When I open company portal I see "This device hasn't been set up for corparate use yet…." . When I try assign I see message that "device is already beging managed by an organization ". In Intune console I see this device and MDM is enabled. What can I do to assign user to device? In event viewer i see 75 event Enroll success

My previous expirence is that after auto enrolment I open company portal and only choose device category .

Reply

4. **Sameer** July 31, 2018 at 12:14 am

I clicked the link for the PPT decks and they do not exist….How do I get a hold of the PPT decks?

Reply

o **Anoop C Nair** July 31, 2018 at 12:11 pm
Updated the links. Thank you

Reply

5. **Ravikaran Patel** September 3, 2018 at 12:01 am

Hi Anoop,

I need help in understanding few points.

1. Is it possible to force company portal application installation on Android, iOS and Windows phone which are not managed, not by applying conditional access. I mean to say no manual intervention required to instay app from the app store.

2. Certified based WiFi profile. My certificate is per user based, it will have password information for individual user, every user different certificate, what should I do in this case to push this certificate on every win 10 and win7 and mobile devices using Intune.

3. Intune with Sccm and cloud management gateway to manage remote machines not connected to my network.

Please share some details for this.