



Comprehensive Guide for MICROSOFT INTUNE



MICROSOFT INTUNE STEP BY STEP ON AZURE PORTAL



MAI ALI

MVP MICROSOFT
AZURE



Table of Contents

Chapter 1	9
Definition of Microsoft Intune	9
What is Microsoft Intune?	9
Why Microsoft Intune?	9
Comparison between MDM for Office 365 & Microsoft Intune	10
Chapter 2	11
Configure Microsoft Intune	11
Setting up a Microsoft Intune account	11
Add Custom Domain	13
Add Intune Users	16
Create Individual Intune User	16
Create bulk Intune Users using CSV file	19
Synchronize users from Active Directory on Microsoft Intune	22
Activate Synchronized Users and Grant Licenses	32
Azure Active Directory Pass-through Authentication “PTA”	35
Configure Pass-through Authentication	35
Step 1: Check the prerequisites	35
Step 2: Configure PTA	36
Step 3: Validate PTA	43
Chapter 3	45
Organize Users & Devices in Microsoft Intune	45
Create Intune Groups to organize Users and Devices	45
Configure Security Groups	45
To Create Assigned Group	45
To Create Dynamic User Group	47
To Create Dynamic Device Group	52
Configure Device Categories	55
Device Enrollment Manager	57
Assign Additional Administrators to manage Microsoft Intune	59
Role-based administration control (RBAC) with Microsoft Intune	61
To create a custom role	62
To assign a custom role	64
Chapter 4	67
Mobile Devices Management (MDM) Authority	67

Set Mobile Device Management Authority.....	67
Prepare for Mobile Device Management Authority “iOS”	69
Prepare for Mobile Device Management Authority “Windows phone & Windows 10 MDM”	74
Set up Windows Phone Enrollment with Intune.....	74
Prepare for Mobile Device Management Authority “Android”	75
Set up Android Enrollment.....	75
Set up Android Enterprise “Android for work” Enrollment	75
Set Enrollment Restrictions	79
Manage your company's terms and conditions for user access	84
Create Terms and Conditions.....	85
Assign Terms and Conditions	86
Identify Devices as Corporate-owned	88
Identify Corporate-owned Devices with IMEI or Serial number.....	88
Manually Enter Corporate Identifiers	89
Add Corporate Identifiers by using a .csv file.....	90
Change Device Ownership	92
Set up iOS device Enrollment with Apple Configurator	92
Prerequisites for Apple Configurator	93
Create an Apple Configurator profile for devices	93
Setup Assistant Enrollment.....	95
Direct Enrollment	101
Intune Company Portal Branding.....	110
Chapter 5	113
Protect Mobile Devices Using Microsoft Intune “MDM”	113
Device configuration	113
Device Restriction Policy	113
Custom Device Settings	118
Custom Profile for Android	119
Custom Profile for iOS Devices	122
Compliance Policies in Microsoft Intune	129
Automate email and add actions for noncompliant devices.....	133
Conditional Access policies in Microsoft Intune	137
Conditional Access Policy on Exchange Online, SharePoint Online & OneDrive.....	138
Conditional Access Policy on Cloud Apps from Specific Location	141
Conditional Access Policy on Exchange On-premise.....	147

- Reset passcodes when users are locked out of their devices..... 153**
 - Reset Device Passcode Using Intune..... 154**
 - Remotely Lock Devices Using Intune..... 156**
 - Enable Supervised mode for iOS Devices 158**
 - Turn on supervised mode using Device Enrollment Program..... 158**
 - Turn on supervised mode using Apple Configurator 158**
 - Locate lost or stolen iOS devices with Intune..... 158**
 - Activate lost mode sound alert on an iOS device 161**
 - Security and privacy information for lost mode and locate device actions 162**
- Bypass Activation Lock on Supervised iOS devices with Intune..... 162**
 - Purpose of using Activation Lock..... 163**
 - Manage Activation Lock using Microsoft Intune 163**
 - Configure Activation Lock bypass 163**
 - Prerequisites for Activation Lock..... 164**
- Retire Devices and Remove Data..... 166**
 - Wipe 166**
 - Retire..... 168**
 - iOS..... 168**
 - Android 168**
 - Android Work Profile..... 170**
 - Android Enterprise Kiosk Devices 170**
 - MacOS..... 170**
 - Windows..... 170**
 - Delete Devices from the Intune portal..... 172**
 - Automatically delete devices with cleanup rules 172**
- Chapter 6 174**
- Deploy Applications Using Microsoft Intune 174**
 - Deploy Apps “Office ProPlus” to Windows 10 MDM using Intune..... 174**
 - Configure Office ProPlus App 174**
 - Assign the App..... 177**
 - Monitor the App..... 180**
 - Deploy Apps to Mobile Devices Using Microsoft Intune..... 182**
 - Configure Store App..... 183**
 - To configure Android Store App 183**
 - To configure iOS Store App..... 185**

To Configure Windows Store App	187
Configure Web App	192
Configure Built-in App	196
Configure Line of Business App	200
Monitor App	206
Deploy App to Android Enterprise “Android for Work” Mobile Devices	207
Setup Managed Google Play Store & Add App	207
Synchronize Managed Google Play App with Intune	210
Assign Specific Group on Managed Google Play App	211
Chapter 7	214
Intune App Protection “Mobile Application Management”	214
iOS App Protection Policy	214
Android App Protection Policy	218
Enforce users to use Managed App. on Mobile devices	223
Windows Information Protection (WIP) App Protection policy	226
Additional Configuration on WIP	230
Enable MAM Provider in Azure AD	234
App Configuration Policy	236
App Configuration Policies for Managed Devices	237
App Configuration Policies for Managed Apps	242
Protected Browser App on Mobile Devices	245
Monitor App Protection	249
Summary view	249
Detailed view	250
Reporting view	251
App Selective Wipe	252
Create a wipe request	253
Monitor wipe requests	255
Delete a wipe request	256
Wrap Android Apps with the Intune App Wrapping Tool for App protection policies	257
Install the App Wrapping Tool	257
Run the App Wrapping Tool	258
Configure Wrapped Line of Business App	260
Wrap iOS Apps with the Intune App Wrapping Tool for App protection policies	267
General prerequisites for the App Wrapping Tool	267

Create an Apple signing certificate	268
Create Distribution Provisioning profile	275
Configure the App Wrapping Tool	279
Run the App Wrapping Tool	280
Configure Wrapped Line of Business App	281
Chapter 8	288
Integrate between Microsoft Intune & Other Products	288
Telecom expense management service in Intune.....	288
Deploy the Intune and Datalert integrated solution	288
Integrate between Microsoft Intune & Windows Defender ATP	311
Integrate between Microsoft Intune & Lookout Mobile Threat Defense	325
Chapter 9	346
Manage Windows 10 PCs Using Microsoft Intune	346
Enroll Windows 10 MDM	346
Manually Enroll Windows 10	346
Automatically Enroll Windows 10 Using Azure AD.....	350
Join Windows 10 to Azure AD.....	353
Register Windows 10 to Azure AD.....	356
Automatically Enroll Windows 10 Using Group Policy	359
Enroll Windows 10 Devices by Using the Windows Autopilot	385
Network Connectivity Requirements	385
Windows Autopilot – Azure AD	386
Windows Autopilot – Hybrid Azure AD join	407
Manage PowerShell Scripts Using Microsoft Intune	442
Deploy Application (EXE or MSI) on Windows 10 MDM.....	449
Manage Software Updates in Intune	462
Configure Remote Assistance	468
Protect Windows 10 MDM Using Microsoft Intune	478
Configure Windows Defender Antivirus	478
Configure Identity Protection settings in Microsoft Intune	482
MDM Security Baselines – Windows 10	491
Retire Devices and Remove Data.....	491
Wipe	492
Retire.....	493
Fresh Start	494

Autopilot Reset.....	495
Remote Windows Autopilot Reset.....	496
Local Windows Autopilot Reset.....	497
Chapter 10.....	500
Intune Reporting & Alerts.....	500
Use the Intune Data Warehouse.....	500
Azure AD and Intune credential requirements.....	500
Install Power BI.....	501
Load the data in Power BI using the OData link.....	501
Load the data and reports using the Power BI file (pbix).....	508
Publish Intune Report from Power BI Desktop.....	511
Print & Export dashboards for Reports.....	513
Export reports from Power BI to PowerPoint.....	515
Export data from a visual.....	517
Share and collaborate with colleagues in Power BI.....	520
Intune APIs in Microsoft Graph.....	526
Chapter 11.....	574
Resource Access Profile with Microsoft Intune.....	574
Enable access to corporate email using email profiles.....	574
Help users connect to their work using VPN profiles.....	578
Configure VPN Profile for Windows 10 Devices.....	578
Configure VPN Profile for iOS Devices.....	586
Help users connect to company networks using Wi-Fi profiles.....	592
Configure Wi-Fi Profile for Android Devices.....	592
Import Wi-Fi settings for Windows devices in Intune (Windows 8.1 or Later).....	597
Enable access to company resources using Certificate profiles.....	601
Configure Prerequisites for Certificate Profile.....	601
Step 1 - Configure certificate templates on the certification authority.....	602
Step 2 - for SCEP profile only: Configure prerequisites on the NDES server.....	607
Step 3 - for SCEP profile only: Configure NDES for use with Intune.....	613
Step 4 - Enable, install, and configure the Intune Certificate Connector.....	620
Configuring Certificate Profiles.....	630
Step 1 - Export the Trusted Root CA certificate.....	630
Step 2 - Create Trusted CA certificate profiles.....	631
Step 3 - Create SCEP certificate profiles.....	635

Step 4 - Create PKCS certificate profiles.....	640
Chapter 12	645
Intune Scenarios & End User Actions.....	645
Intune Business Scenarios	645
Compare between Intune MDM & Intune MAM Without Enrollment	645
Secure Corporate Data & Device	646
Secure Corporate Data on Employee’s personal device “Bring your Own Device”	646
Secure Windows PCs as MDM	647
Enroll Mobile Devices Using Microsoft Intune	648
For Android.....	648
For iOS.....	651
For Windows Phone.....	657
APPENDIX.....	663
Firewall and Proxy Server Settings for MDM Devices.....	663
Required Firewall Configuration	663
Apple Device Network Information	663
Required Proxy Server Configuration.....	664
Average Network Traffic	664
Reduce Network Bandwidth Use	665
Reference	666
Other Articles	666



Mai Ali is a Solution Architect, with a strong focus in Microsoft, virtualization, Management solution and Unified Communications area. Over 8 years' study and hands on experience delivering small to large-scale projects for different industries, mainly based on Microsoft and other leading-edge technologies, systems applications and operations running on top of them. She has Broad and mixed technical background in infrastructure and communications field, systems integration, Systems Management, security, as well as an in-depth understanding of the business of computing and networking. Currently her main tasks are Architectural design and delivery of Microsoft

environments, with specific focus on multi-vendor UC solutions, based on Microsoft System Center 2007, Microsoft System Center 2012, Microsoft Lync 2013 with Enterprise Voice, Office 365, Microsoft Enterprise Mobility Suite, Azure, Microsoft Operations Management Suite, Exchange Unified Messaging, migrations from Lync 2010 and OCS 2007, load balancers, reverse proxy, firewall, Exchange UM.

Mai Ali has various [Technology Certifications and Awards](#): **Microsoft Most Valuable Professional Azure**, **Microsoft Most Valuable Professional System Center Cloud and Data Management** on 2015, **Microsoft Certified Solutions Expert** (Communication, Server Infrastructure, Private Cloud, and Messaging), **MCITP** (Office 365 Administrator), **MCITP** (Enterprise Administrator Windows 2008), **MCITP** (Enterprise Messaging Administrator), **MCITP** (Lync Server 2010 Administrator), **Microsoft Certified Systems Engineer** (Security, Messaging) Windows 2003, **MCSA** (Office 365, Windows 2012), **MCSA** Windows 2008, **MCSA** (Security) Windows 2003, **Citrix Certified Expert - Virtualization**, **Cisco Certified Network Professional**, **Red Hat Certified Engineer**, **STS** Symantec Enterprise Vault 10.0 for Exchange and **Symantec Certified Professional Program Data Protection**.

Mai Ali has been very involved with Windows Server based virtualization, communication and Management solutions including Microsoft System Center, Microsoft Lync, Enterprise Mobility, Azure and Office 365. She is currently a prolific blogger at <http://expertslab.wordpress.com> and has done many Scripts for automatic configuration on Microsoft TechNet Gallery. Mai likes giving back via community forums: She has contributed thousands of posts to Microsoft System Center, Microsoft Lync, Azure and Experts-Exchange community forums over the years.

Mai Ali's Blog: <http://expertslab.wordpress.com>

Chapter 1

Definition of Microsoft Intune

What is Microsoft Intune?

Microsoft Intune is a cloud-based desktop and mobile device management tool that helps organizations provide their employees with access to corporate applications, data, and resources from the device of their choice. Intune is the component of Enterprise Mobility + Security (EMS) that manages mobile devices and apps. It integrates closely with other EMS components like Azure Active Directory (Azure AD) for identity and access control and Azure Information Protection for data protection. When you use it with Office 365, you can enable your workforce to be productive on all their devices, while keeping your organization's information protected.

- Ability to restrict access to SharePoint Online, Exchange On-premises and Exchange Online email based upon device enrollment and compliance policies
- Management of Office mobile apps (Word, Excel, PowerPoint) for Mobile devices, including ability to restrict actions such as copy, cut, and paste outside of the managed app ecosystem
- Ability to extend application protection to existing line-of-business apps using the Intune App Wrapping Tool.
- Managed Browser app & Edge for Android/iOS devices that controls actions that users can perform, including allow/deny access to specific websites.
- Deploy certificates, Wi-Fi, VPN, and email profiles automatically once a device is enrolled, enabling users to access corporate resources with the appropriate security configurations
- Provide a self-service Company Portal for users to enroll their own devices and install corporate applications across the most popular mobile platforms
- Modernize Windows 10 management without compromising control.
- Publishing & Pushing App on managed devices.
- Reporting on and measuring device compliance to corporate standards.
- Retire device & Removing corporate data from managed devices.
- Removing corporate data from mobile apps for BYOD.

Why Microsoft Intune?

Microsoft Intune is a unified device management solution that combines cloud and on-premises capabilities. Microsoft Intune provides mobile device management, mobile application management, and PC management capabilities from the cloud. Using Intune, organizations can provide their employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure.

Comparison between MDM for Office 365 & Microsoft Intune

The following table lists compares the device and application management capabilities available to you when you use MDM for Office 365, Intune Stand alone.

Features	MDM for Office 365	Microsoft Intune (Stand-alone)
Inventory mobile devices that access corporate applications	Yes	Yes
Remove factory Reset “Full wipe”	Yes	Yes
Mobile device configuration settings “PIN length, Pin required, etc”	Yes	Yes
Provides reporting on devices that do not meet IT Policy	Yes	Yes
Root and jailbreak detection	Yes	Yes
Remove Office 365 app data from mobile devices while leaving personal data & apps	Yes	Yes
Prevent access to Office 365 corporate email & documents based on device enrolment & compliance	Yes	Yes
Application Deployment	No	Yes
Self-Service Company portal for users to enrol their own devices	No	Yes
Deploy Certificate, VPN Profiles, Wi-Fi Profile & email Profile	No	Yes
Secure access corporate information using the Office mobile and line-of business apps & prevent sharing with personal app.	No	Yes
Remote device lock	No	Yes
Manage & Secure PCs from the cloud with no infrastructure	No	Yes

Note: As of August 14, 2018, hybrid mobile device management is a [deprecated feature](#). Microsoft won't support Intune hybrid by 1 September 2019. In case, you have **System Center Configuration Manager** on your environment. You can use **Co-management** which allow windows 10 PCs to be manage with Intune & configuration Manager at the same time.

Co-management enables you to concurrently manage Windows 10 devices by using both Configuration Manager and Intune. So, the device become register on Azure AD & Intune at same time join to local domain and manage by SCCM. By this solution, you can apply conditional access policy on windows 10 PC to block non-compliance device from access corporate data. It's a solution that provides a bridge from traditional to modern management & provide the ability to offload some workload to Intune.

Note: To enable co-management, your administrative user account in Configuration Manager must be a **Full Administrator** with **All** security scopes.

To configure Co-management on your environment, you need to check [Co-management step by step guide](#).

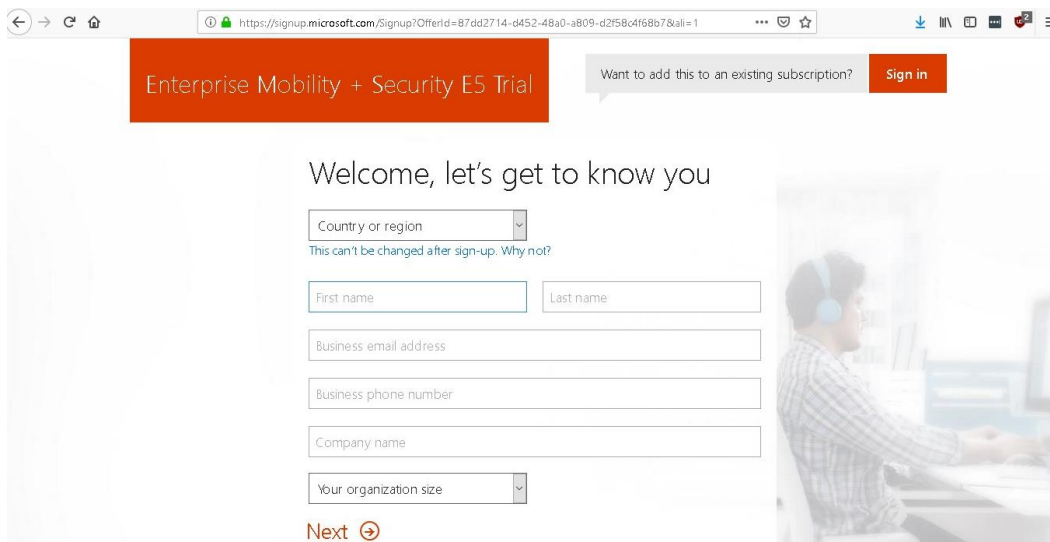
Chapter 2

Configure Microsoft Intune

Setting up a Microsoft Intune account

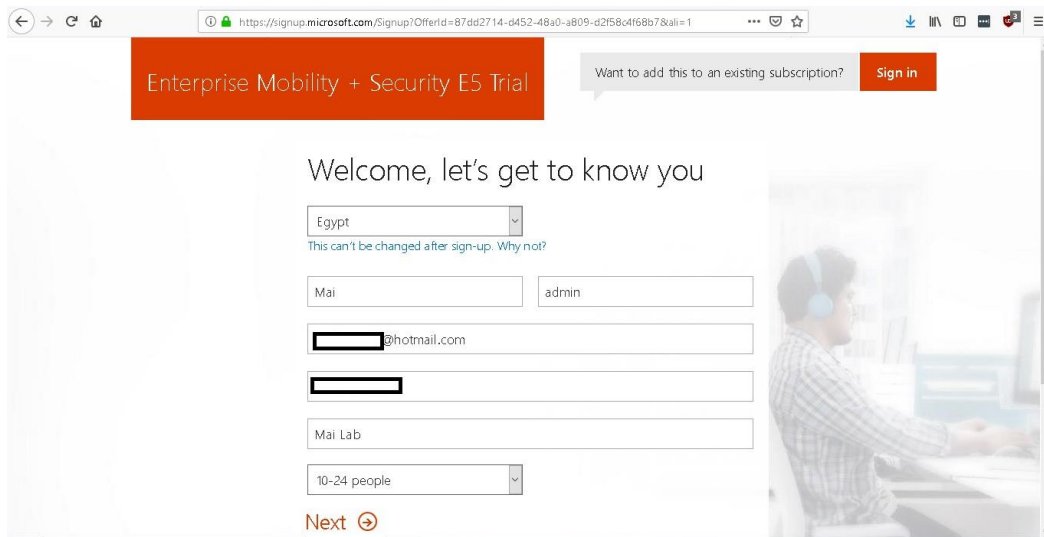
To Create Microsoft Intune Account, you need to follow below steps:

1. Create Trial Account using this [Microsoft EMS Plan](#).



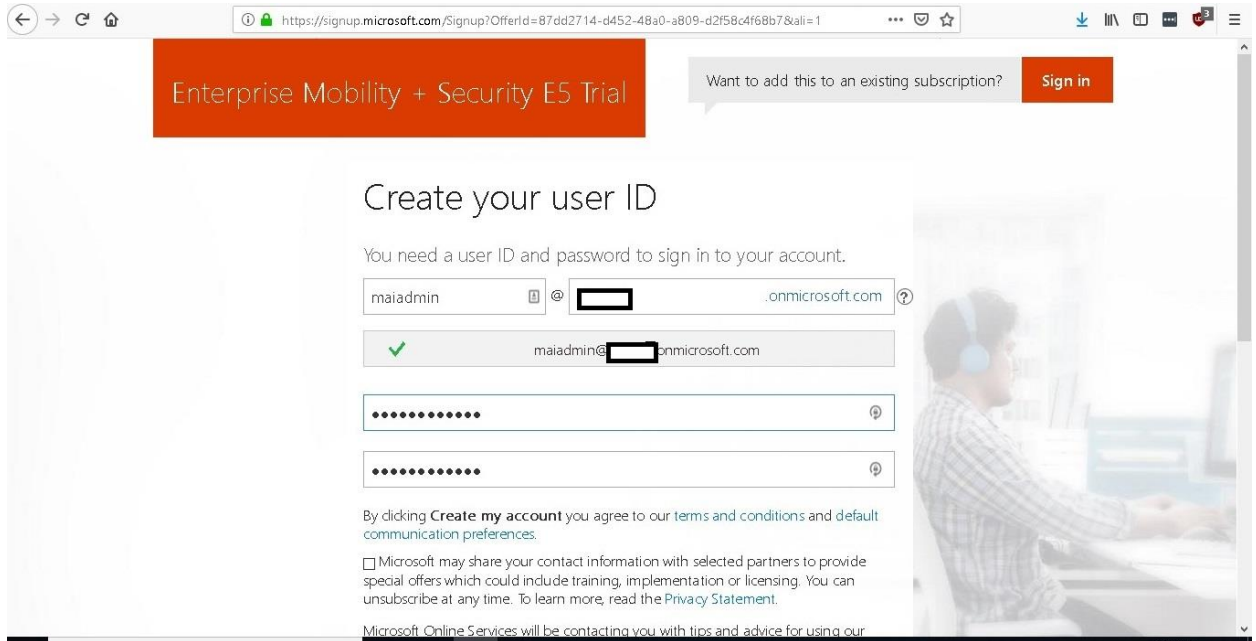
The screenshot shows the Microsoft Intune sign-up page. At the top, there is a navigation bar with the text "Enterprise Mobility + Security E5 Trial" and a "Sign in" button. Below this, the main heading reads "Welcome, let's get to know you". The form includes several input fields: "Country or region" (a dropdown menu), "First name" and "Last name" (text boxes), "Business email address" (text box), "Business phone number" (text box), "Company name" (text box), and "Your organization size" (a dropdown menu). A "Next" button with a right arrow is located at the bottom of the form. On the right side of the page, there is a blurred image of a person wearing a headset working at a computer.

2. Enter your personal data then sign up.

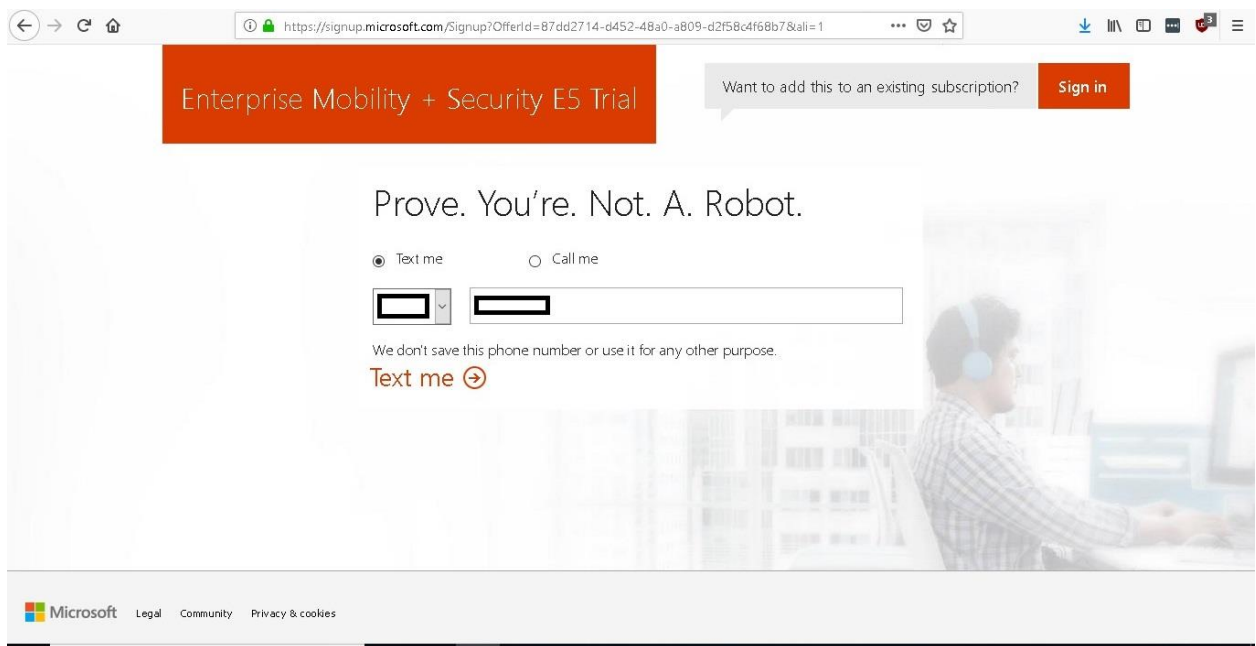


This screenshot shows the same Microsoft Intune sign-up page as the previous one, but with the form fields filled out. The "Country or region" dropdown is set to "Egypt". The "First name" field contains "Mai" and the "Last name" field contains "admin". The "Business email address" field is filled with a redacted email address followed by "@hotmail.com". The "Business phone number" field is also redacted. The "Company name" field contains "Mai Lab". The "Your organization size" dropdown is set to "10-24 people". The "Next" button is still visible at the bottom of the form.

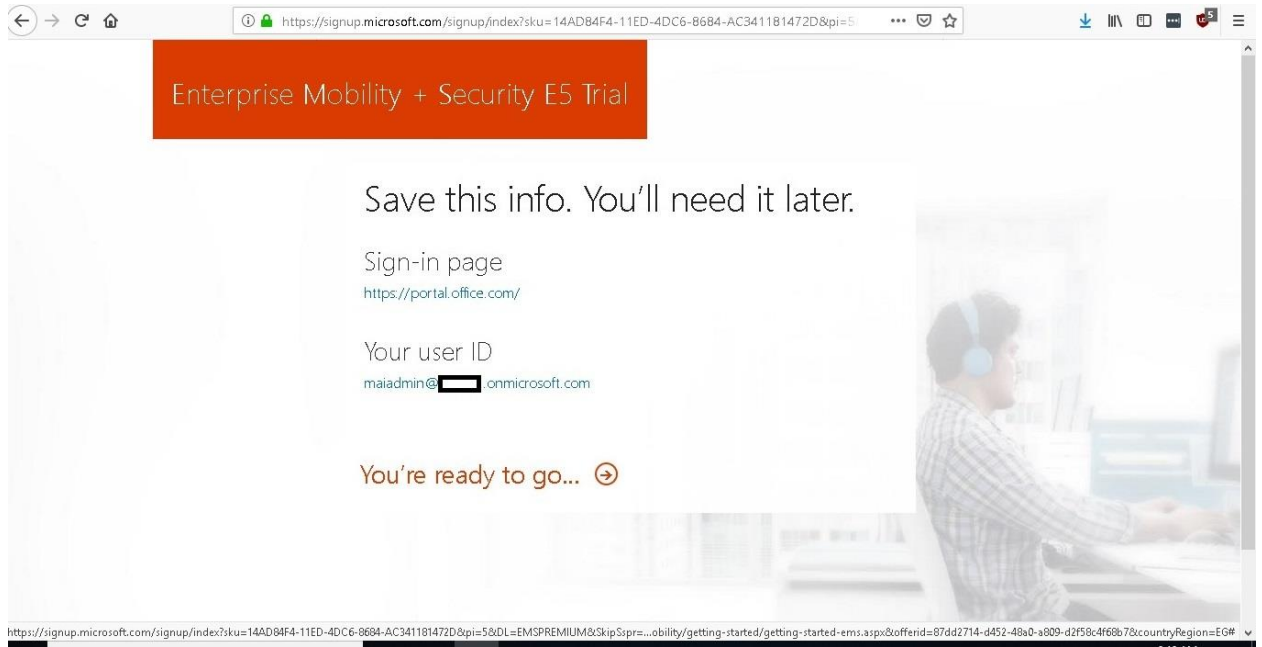
3. On “**Create your user ID**” page, enter tenant name and password.



4. On “**Prove**” page, enter your phone no. and enter verification code.



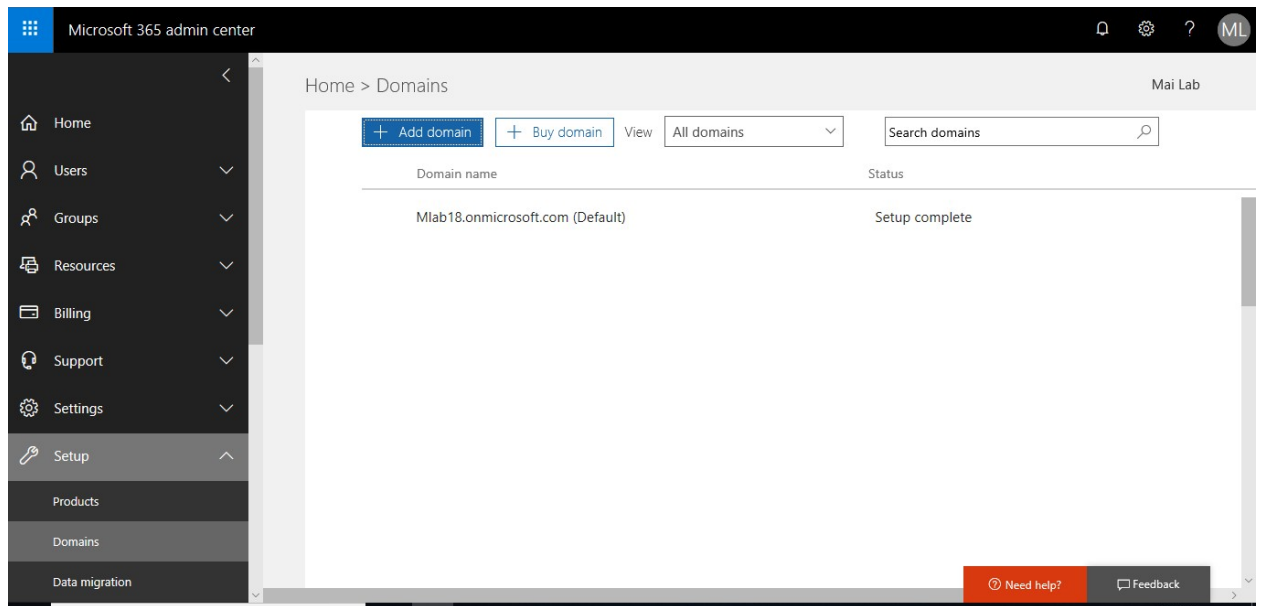
5. Now Microsoft Intune Account is created successfully.



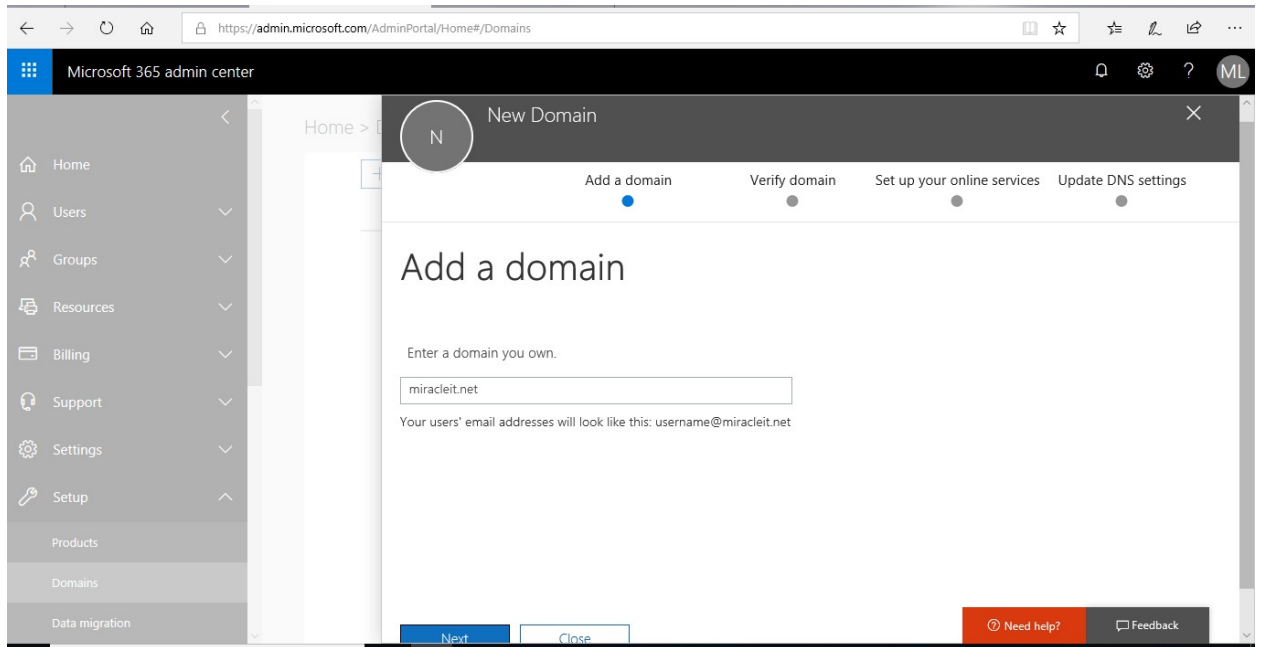
Add Custom Domain

To add custom domain, you can follow below steps:

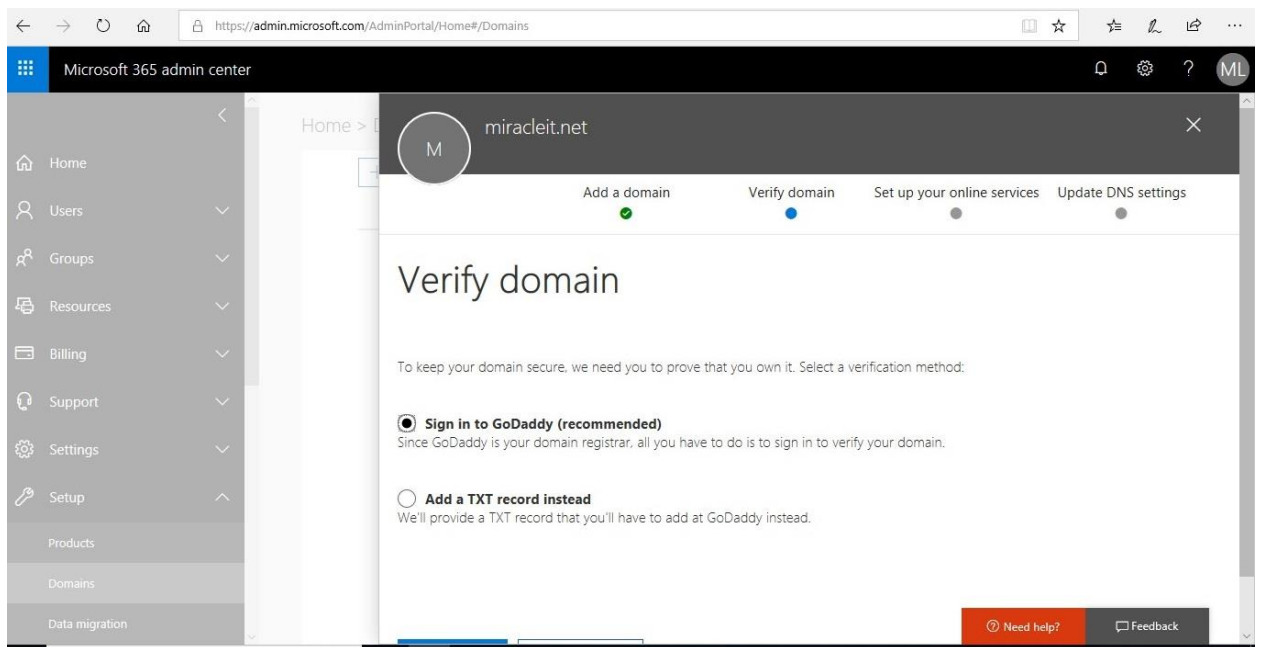
1. In the [Office365 portal](#), click **Setup > Domains** and then **Add domain**.



2. Fill your Domain Name "miracleit.net" and Click **Next**.

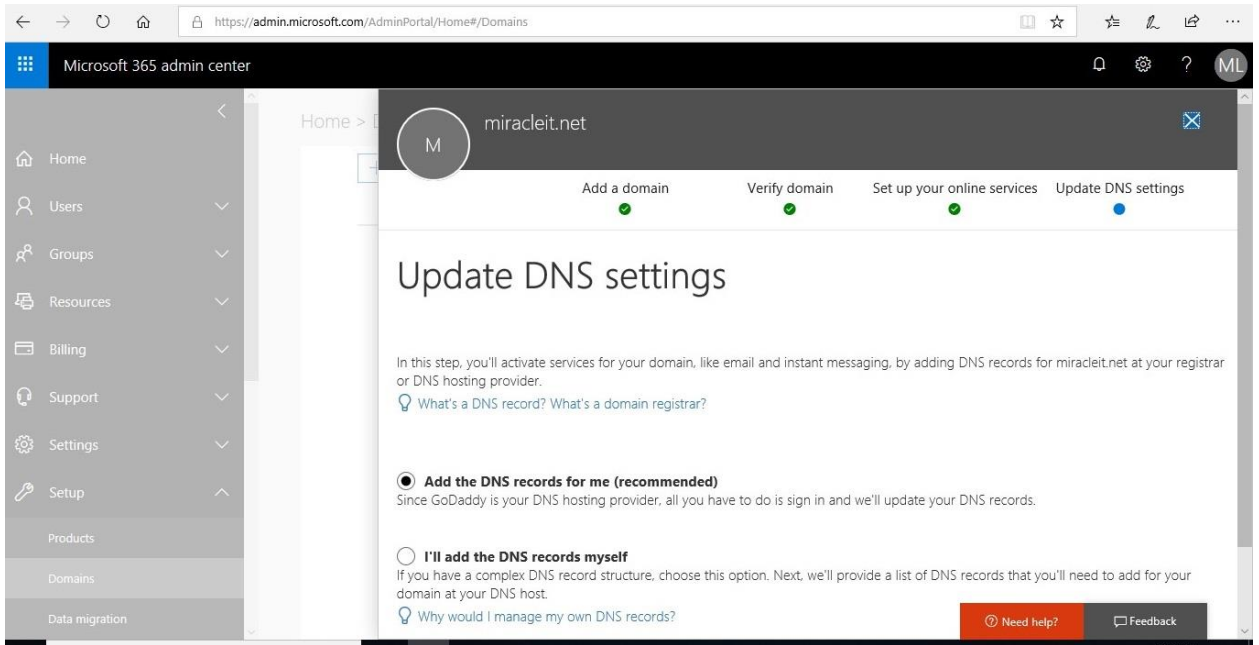


3. On **Verify domain** page, Select **Add a TXT record**. Copy **Text Record** and create it in your public DNS to verify Domain, then click **Verify**.

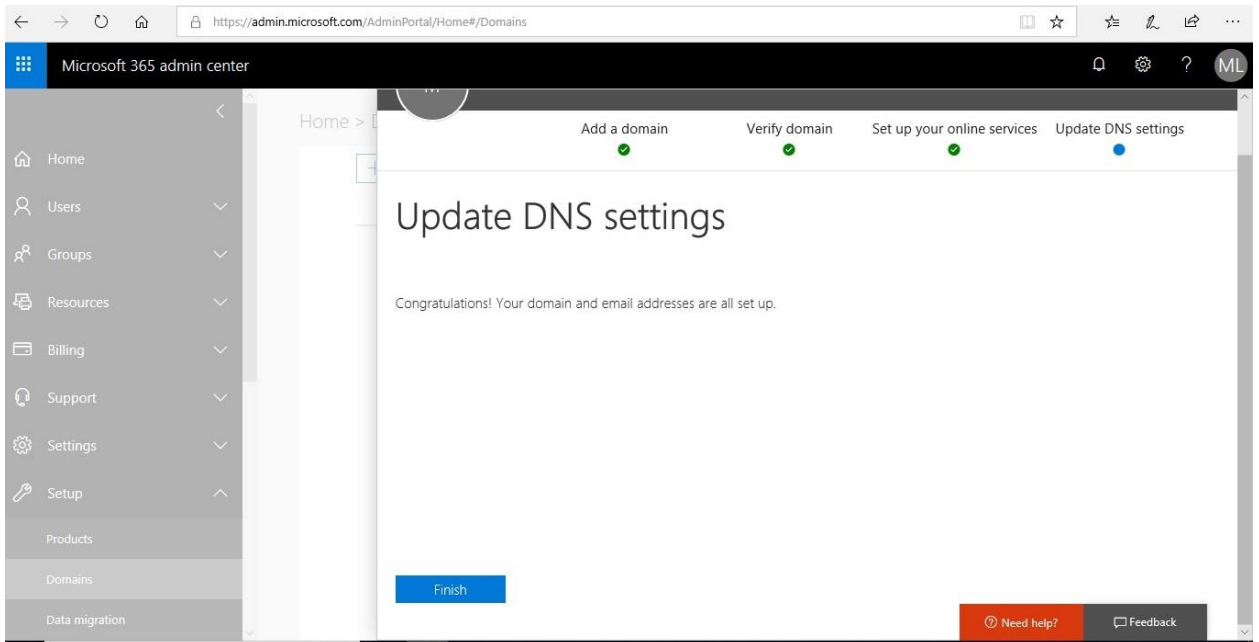


4. On **Update DNS settings**, Select **I'll add DNS by myself** in case if you have any on-Premise solution like Exchange On-premises or Skype On-Premise.

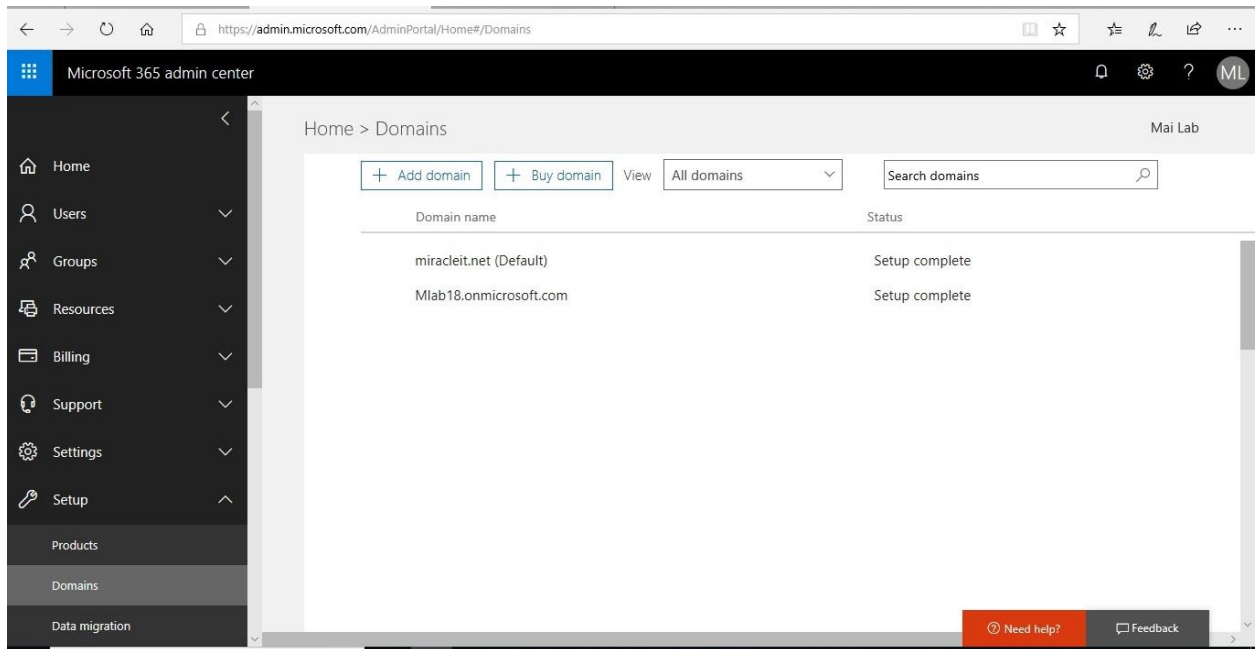
Microsoft Intune step by step on Azure portal



5. Click **Finish**.



6. Now your domain is added successfully on your tenant.



Add Intune Users

To Create Intune Users, you have 3 options:

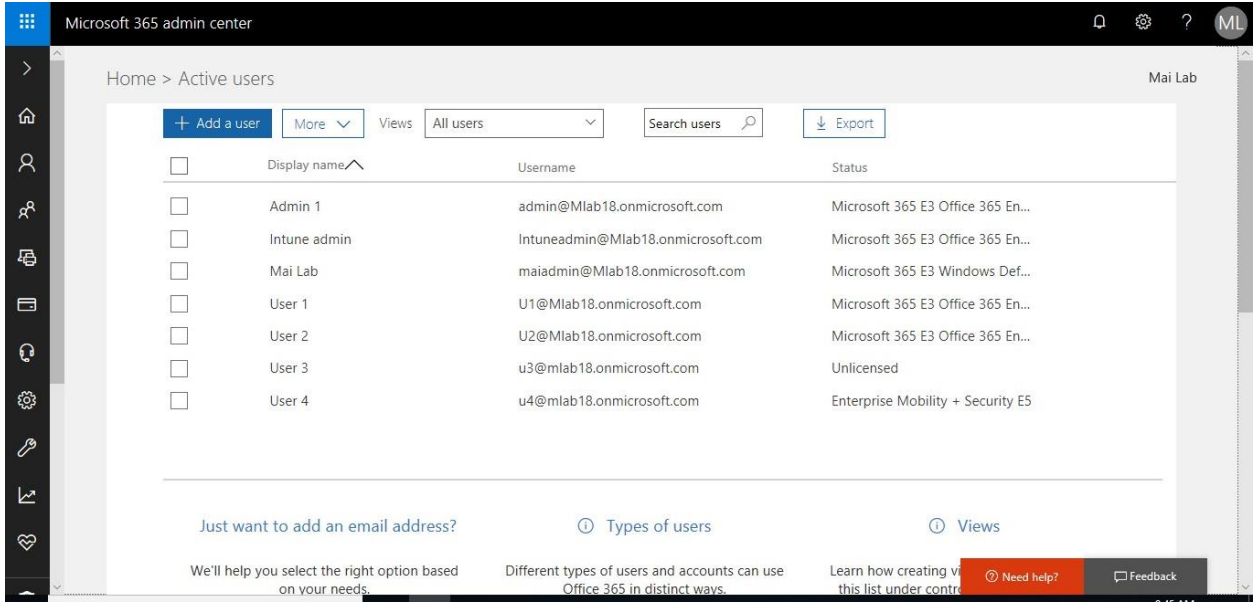
- Create Individual Intune User.
- Create bulk of Intune users using CSV file.
- Synchronize users from Active Directory on Microsoft Intune.

Create Individual Intune User

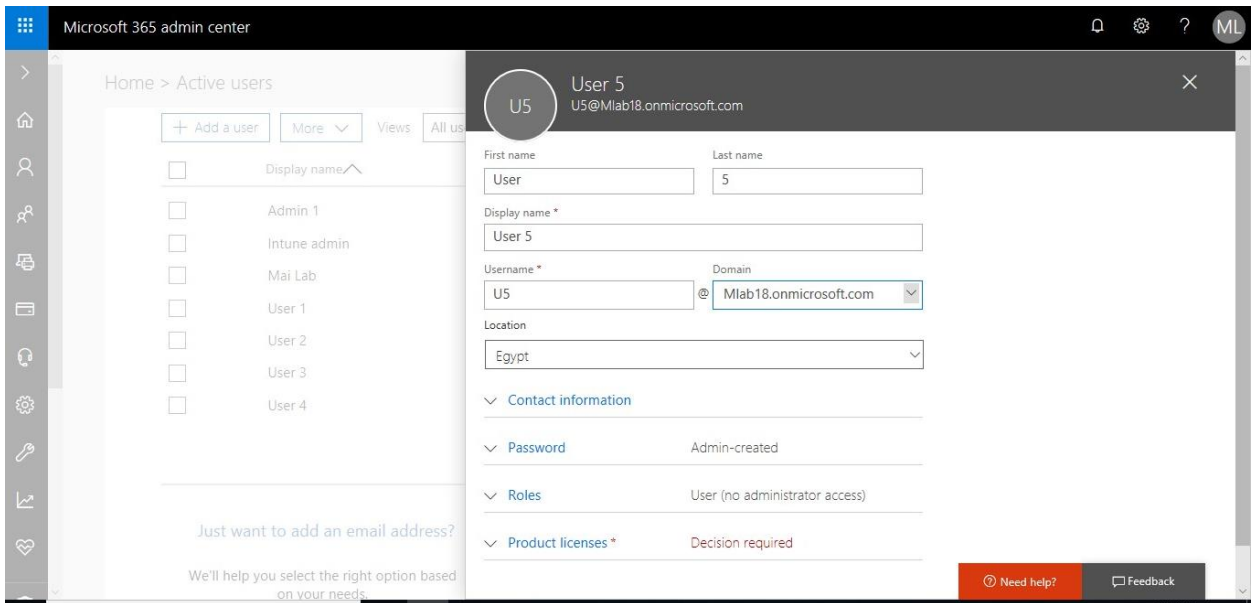
To create individual user, you can follow below steps:

1. In the [Office 365 portal](#), click **Active Users > Add Users**.

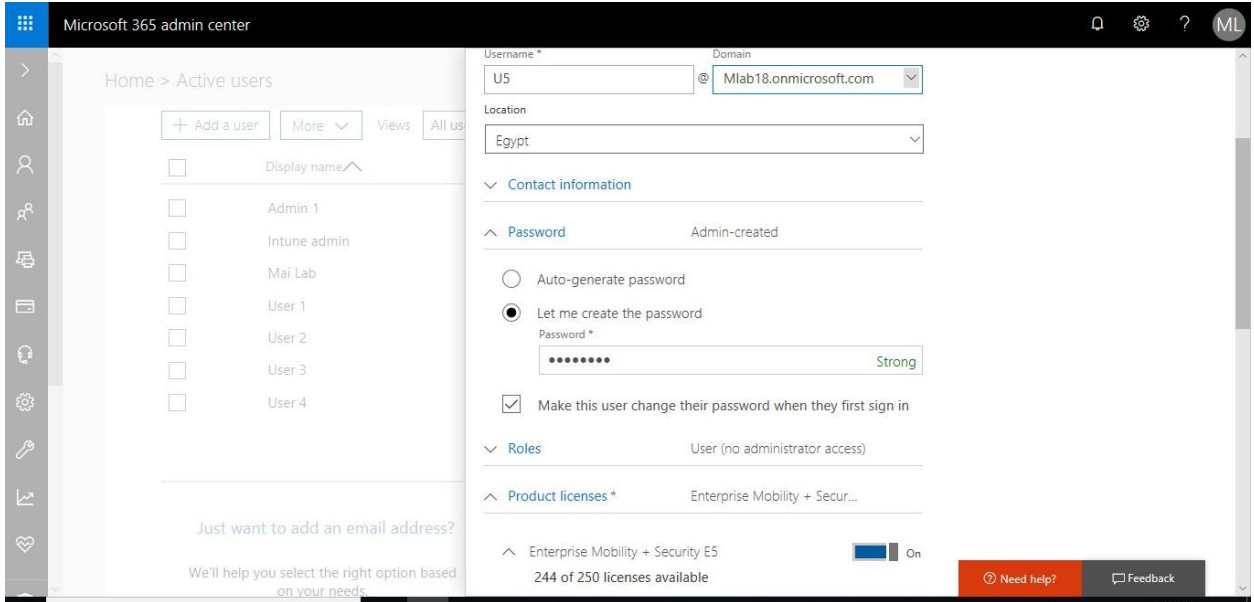
Microsoft Intune step by step on Azure portal



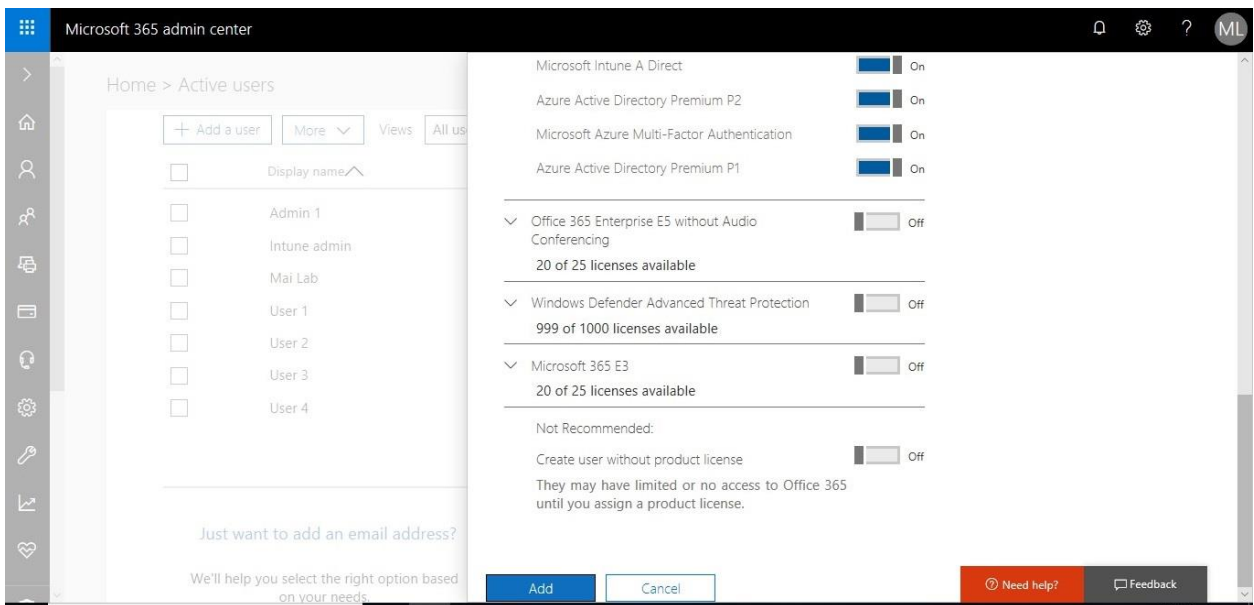
2. Fill in the required information of user you want to create. Fill the country “Egypt”.



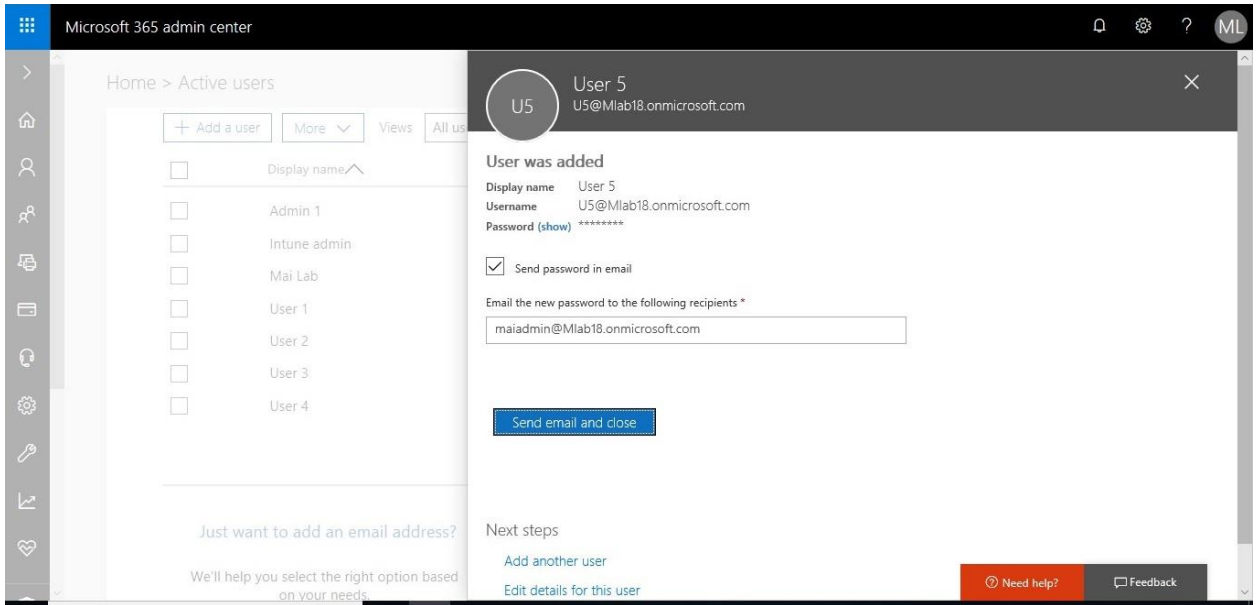
3. Enter Password or generate random password, Assign Role for this user if Administrator or not.



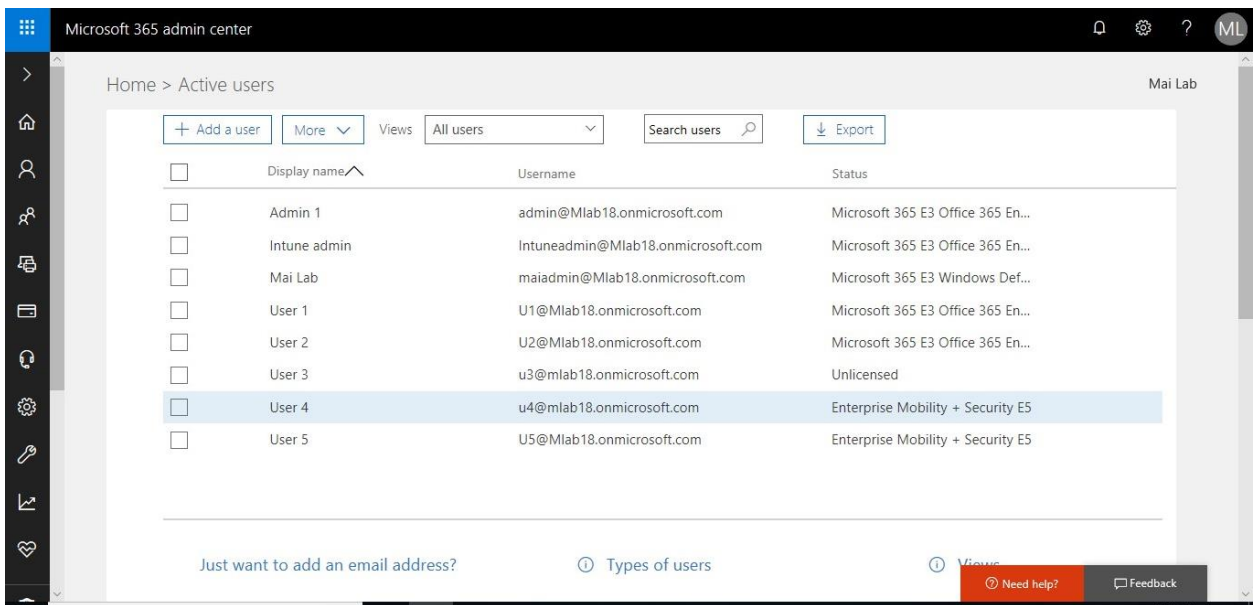
4. Select **Enterprise Mobility + Security** license then click **On**.



5. Type Email Address that you want to receive mail of this account Credential or leave it blank.



6. Now User is created Successfully.

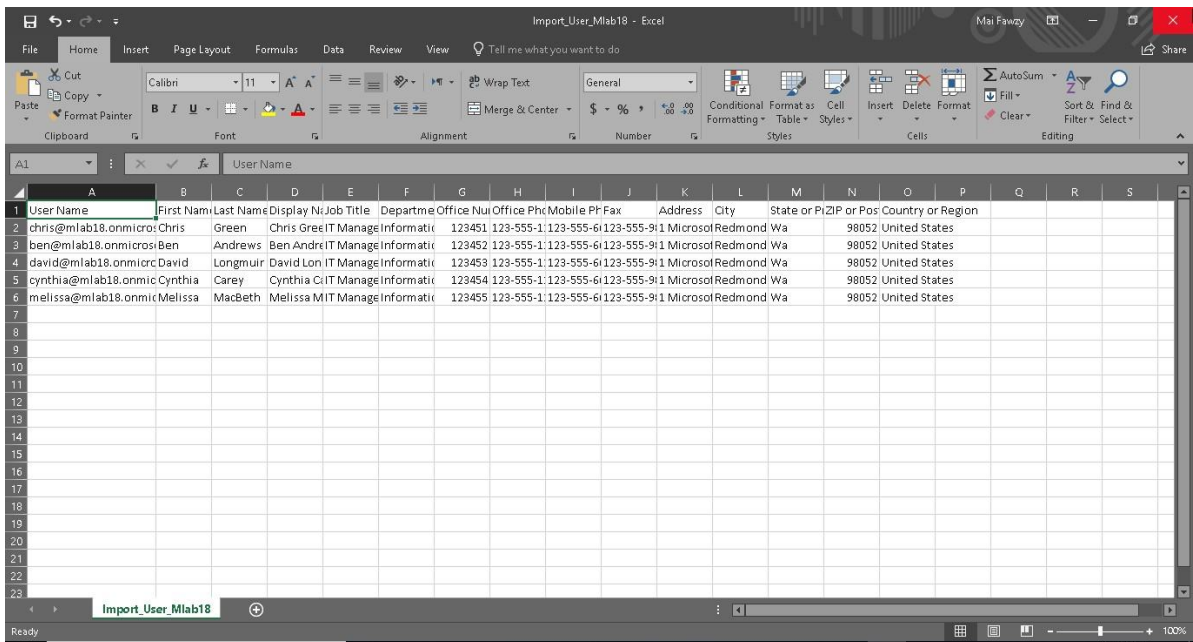


Create bulk Intune Users using CSV file

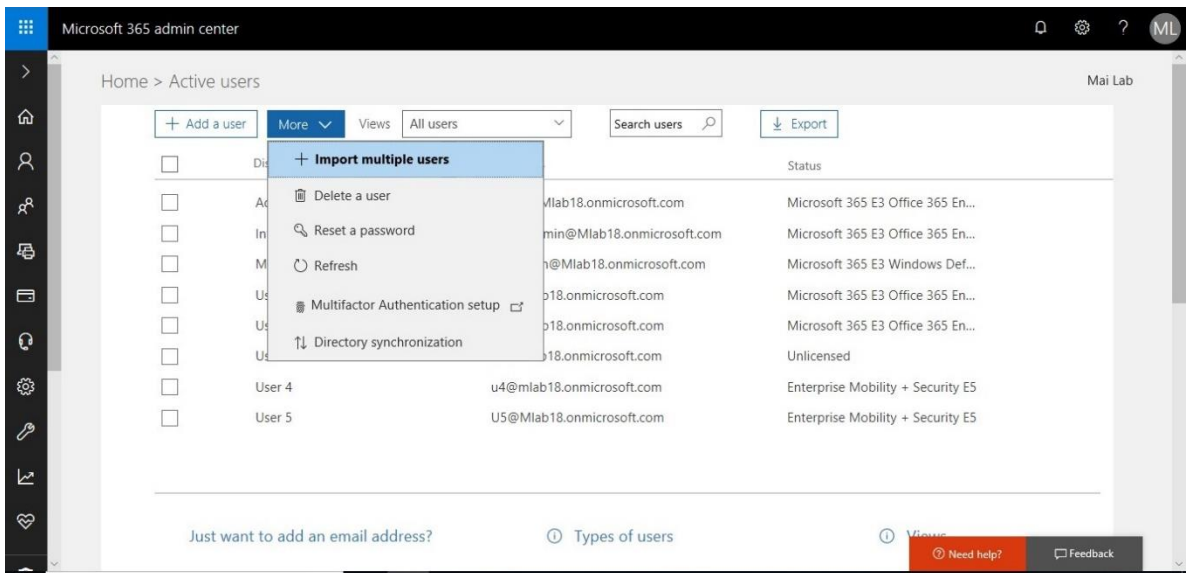
To create bulk Intune users using CSV file, you can follow below steps:

1. Create CSV file "User Name, First name, Last Name, Display Name, State, Country".

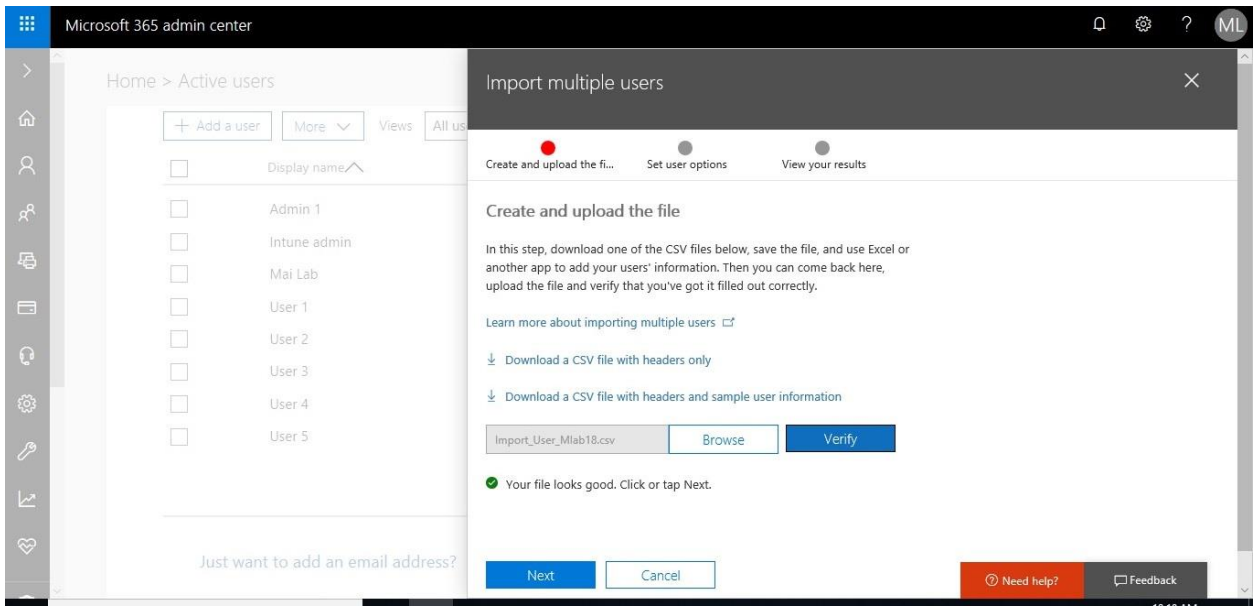
Microsoft Intune step by step on Azure portal



2. In the [Office 365 admin portal](#), click **Active Users > More > Import multiple Users**.

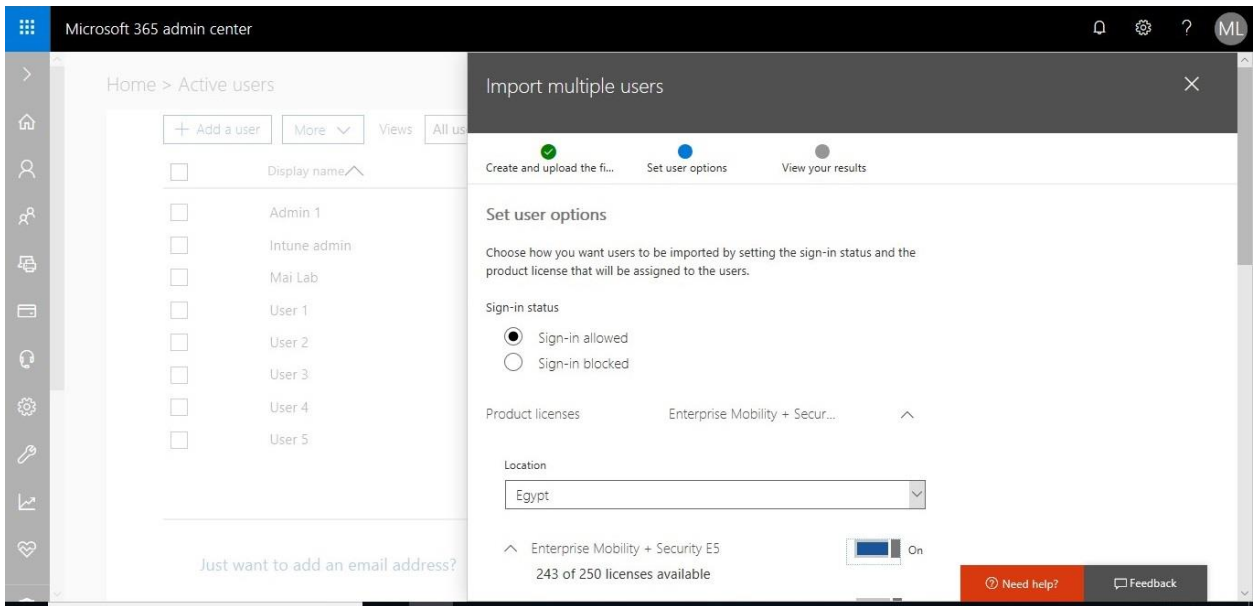


3. Select CSV file then Click **Verify > Next**.

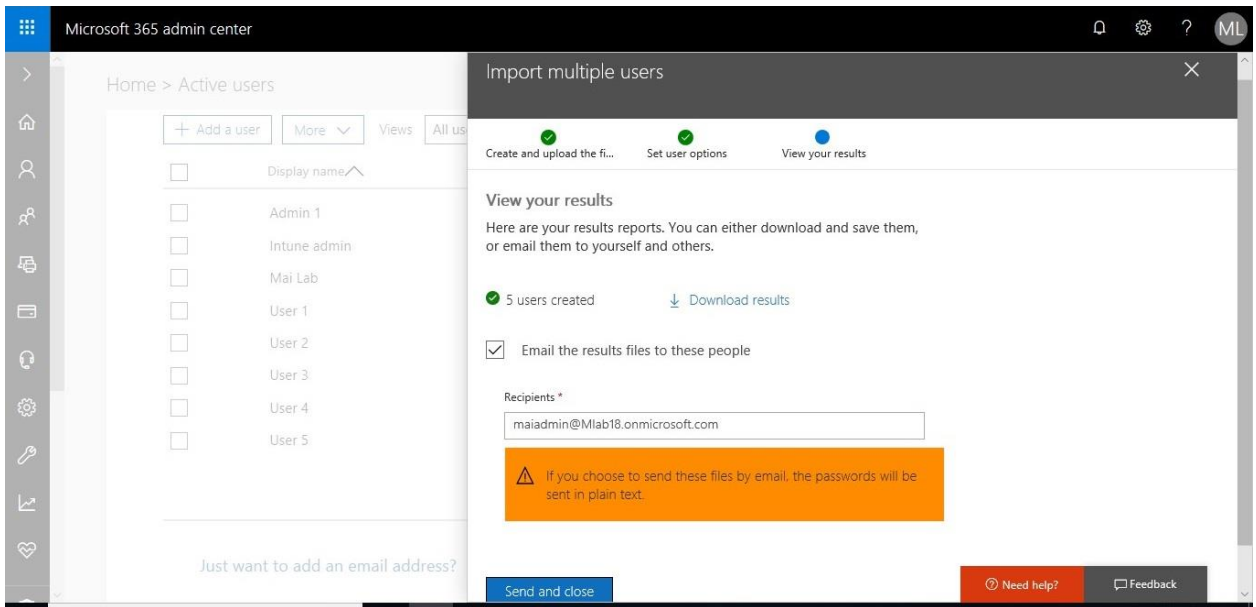


Note: You can download CSV template and add your users on it to ensure file format.

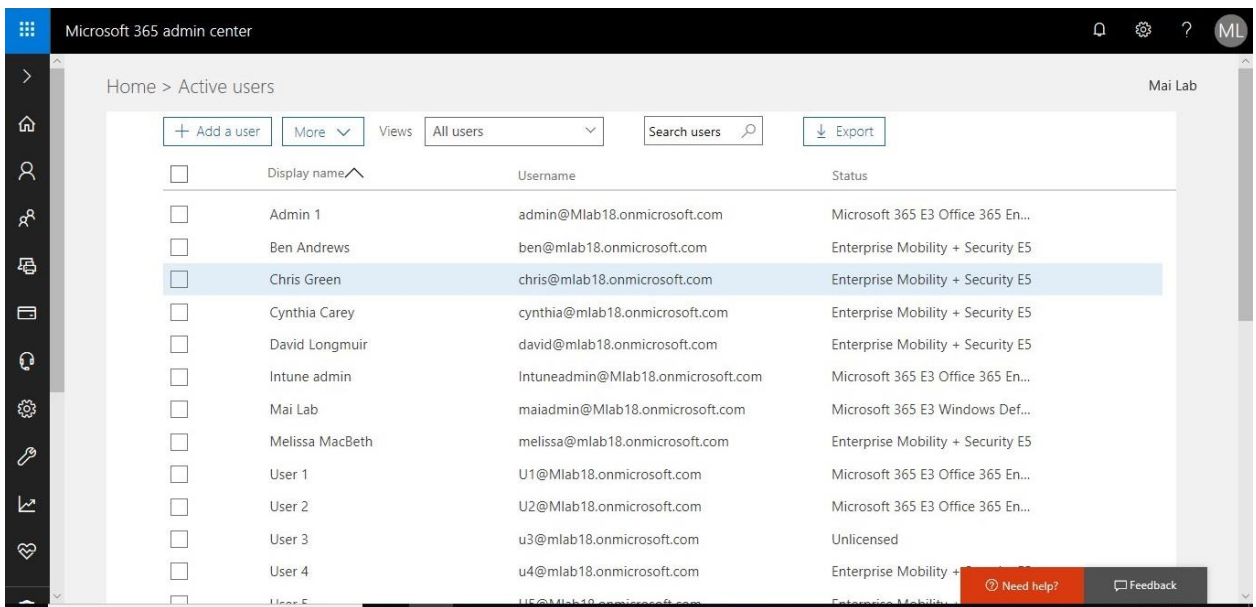
4. On “**Set user options**” Page, check **sign-in allowed** & Select Enterprise Mobility + Security Licenses Fill the country “Egypt and click **Next**.



5. On “**view your results**” Page, Type Email Address that you want to receive mail of this account Credential or leave it blank then Click **Send and Close**.



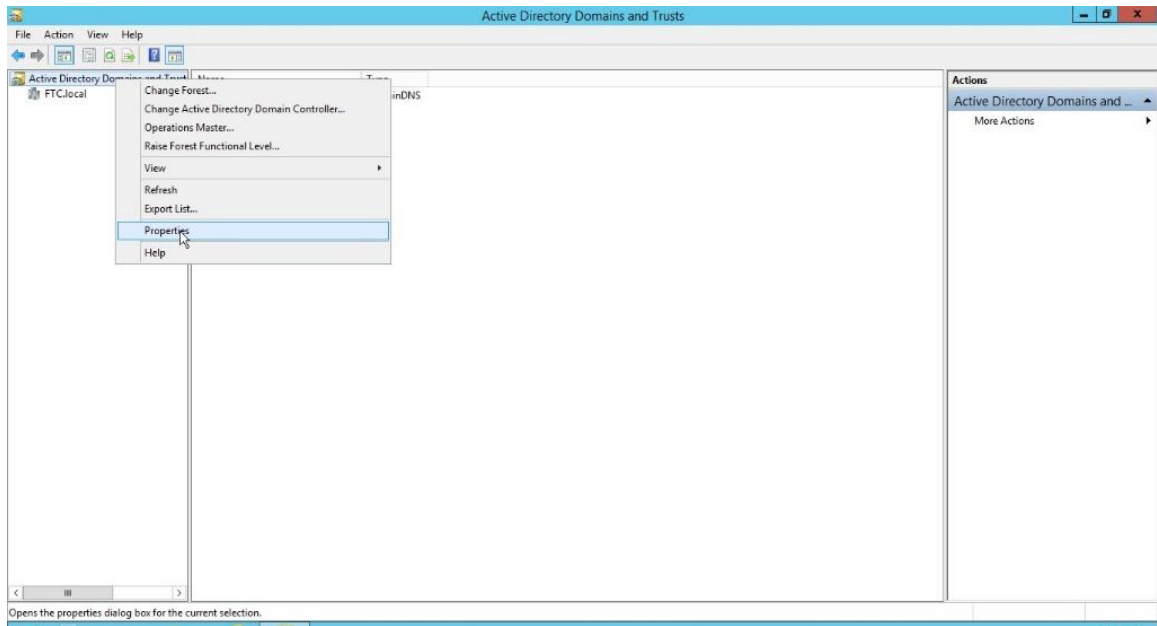
6. Now Bulk Users are created successfully.



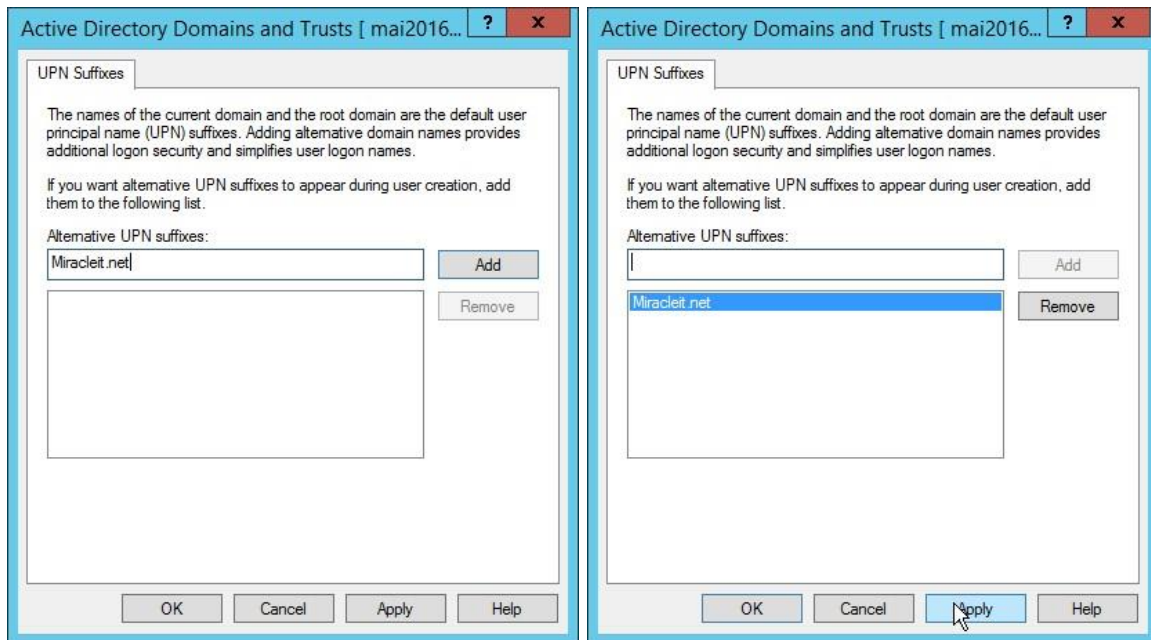
Synchronize users from Active Directory on Microsoft Intune

Add Verified domain as UPN suffix on Active Directory, you can follow below steps

1. Open **Active Directory Domains and Trusts**, Right Click **properties**.




2. Type your verified domain “miracleit.net”, Click **Add**.



3. Click Ok

Use PowerShell to Update UPN for Users, you can follow below steps

1. From the taskbar, right click the PowerShell icon , select Run as Administrator
2. Type cd C:\
3. Type [.\UPN-Update.ps1](#)

Microsoft Intune step by step on Azure portal

```
UPN-Update.ps1 X
1  ### Enter your input on Line 10 OU that contain all users that need to change user principal name on it
2
3
4  Import-Module ActiveDirectory
5
6  $ENterDomain = Read-Host 'What is the your routable domain? ie contoso.com'
7
8  $routableDomain = $ENterDomain
9
10 $users = Get-ADUser -Filter {UserPrincipalName -like '*'} -SearchBase "OU=Ftc EMS,DC=FTC,DC=local"
11 foreach ($user in $users) {
12     $userName = $user.UserPrincipalName.Split('@')[0]
13     $UPN = $userName + "@" + $routableDomain
14     Write-Host $user.Name $user.UserPrincipalName $UPN
15     $user | Set-ADUser -UserPrincipalName $UPN
16 }
17
18 }
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\ftcadmin> cd c:\
PS C:\> .\UPN-Update.ps1
what is the your routable domain? ie contoso.com: miracleit.net_
```

4. Enter your Domain Name

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

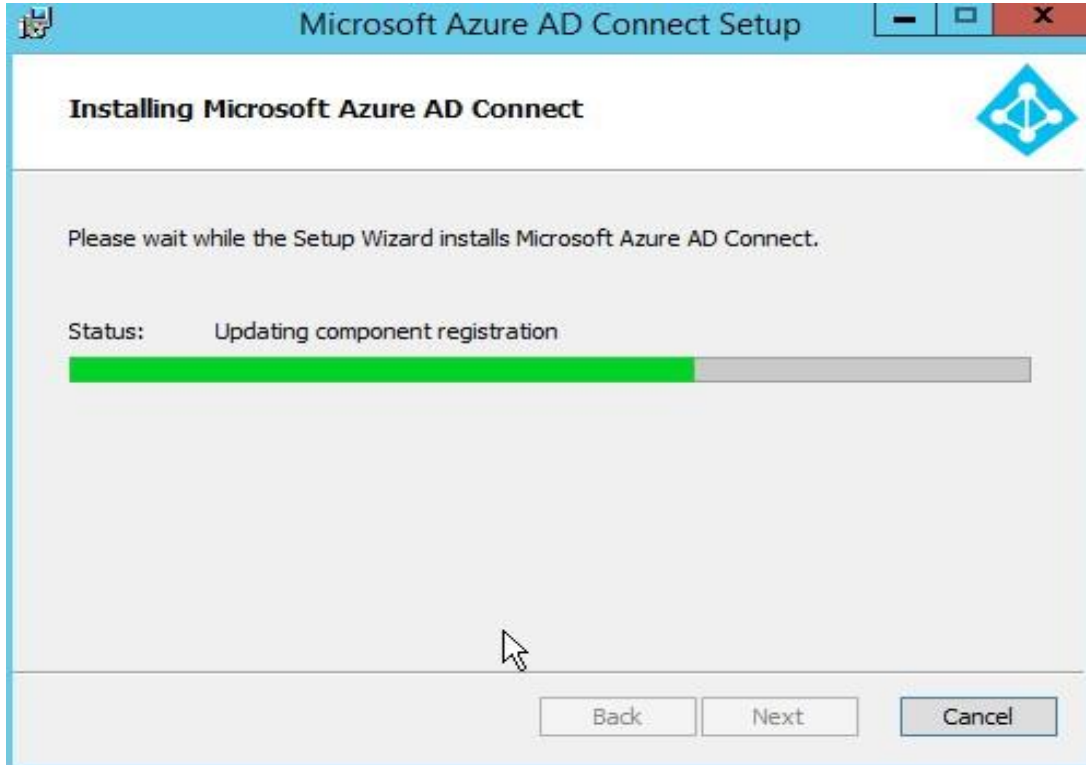
PS C:\Users\ftcadmin> cd c:\
PS C:\> .\UPN-Update.ps1
what is the your routable domain? ie contoso.com: miracleit.net
David Heriz DavidHeriz@imperialits.com DavidHeriz@miracleit.net
Anish Anish@imperialits.com Anish@miracleit.net
Vanda Carvalho Vreis@imperialits.com Vreis@miracleit.net
Magdy Magdy@imperialits.com Magdy@miracleit.net
Ghady Ghady@imperialits.com Ghady@miracleit.net
PS C:\> _
```

Note: Edit UPN-Update Script, Write OU Path that you need to update UPN suffix on it.

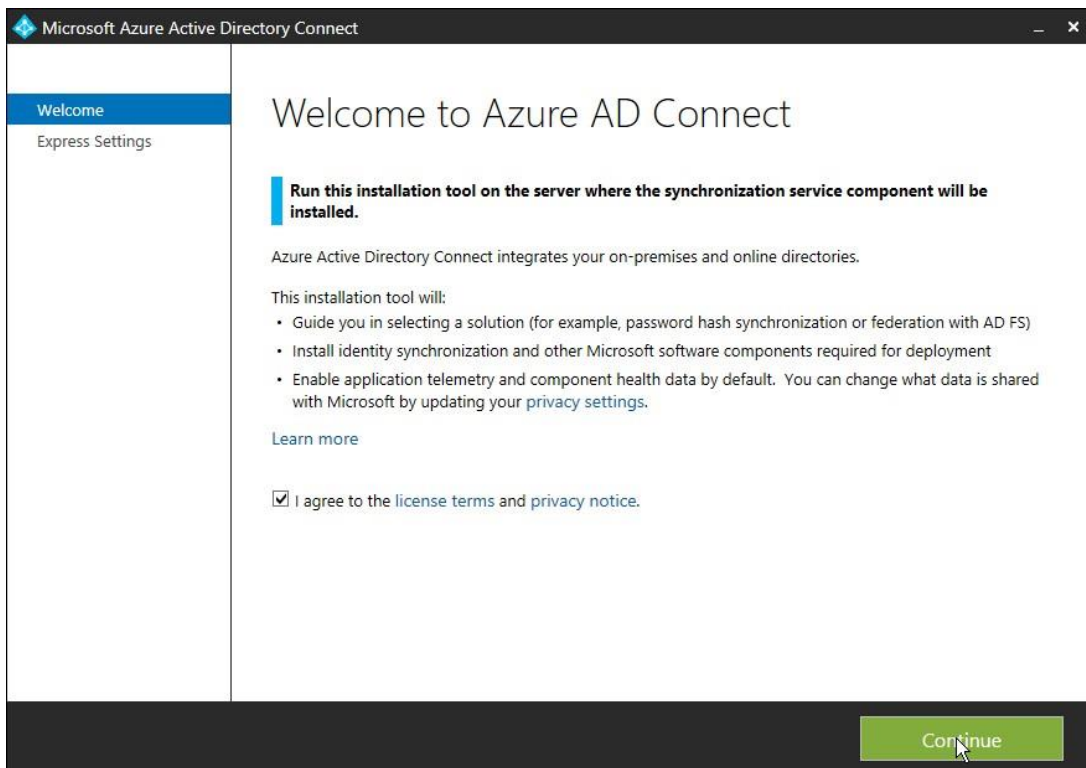
Configure Azure AD connect, you can follow below steps

Microsoft Intune step by step on Azure portal

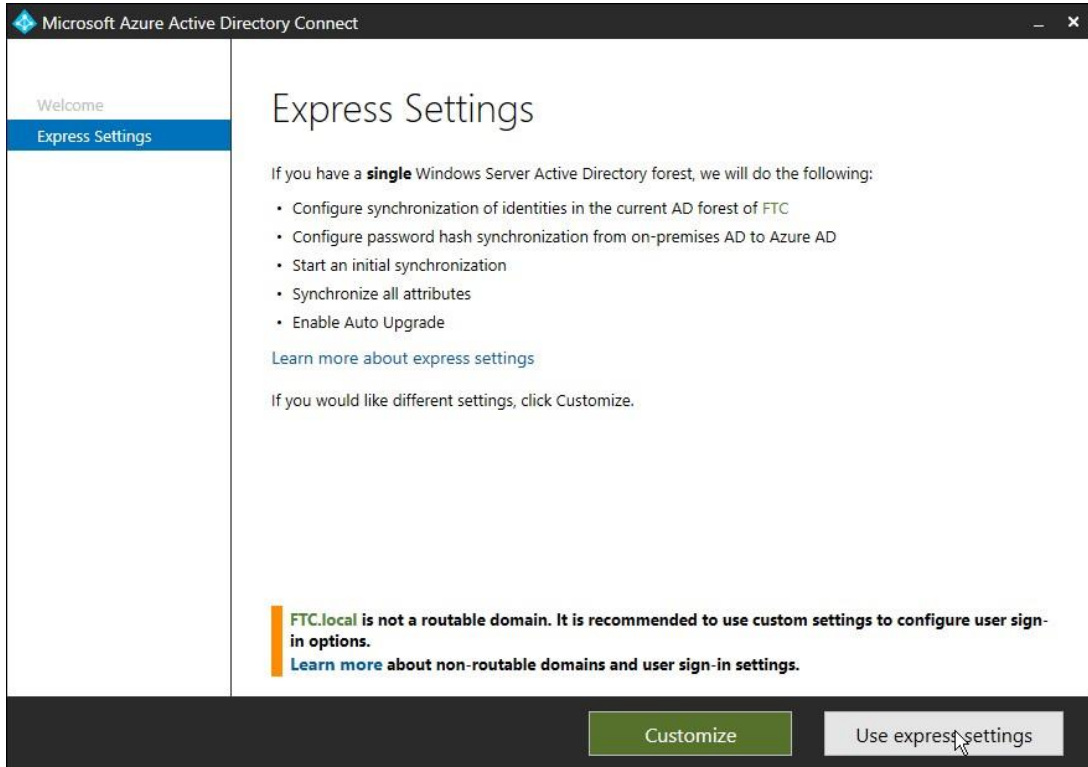
1. Download [Azure AD Connect](#), then Click **Run**.



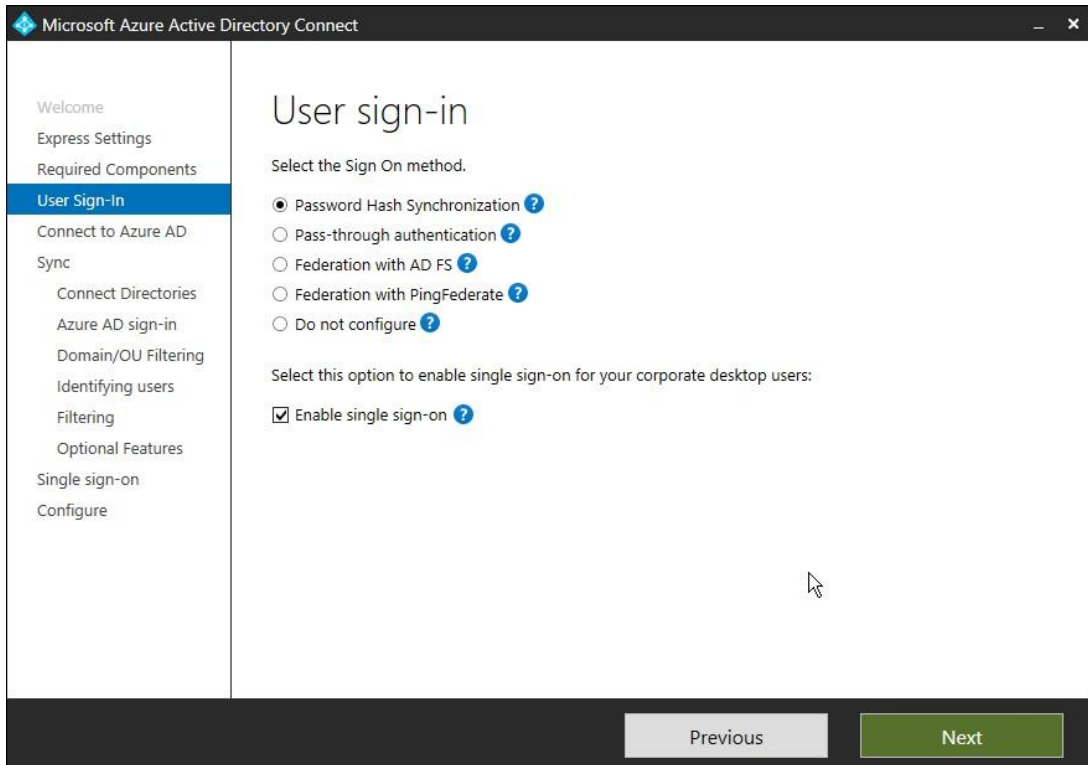
2. On **Azure AD Connect**, Check I agree and Click **Continue**



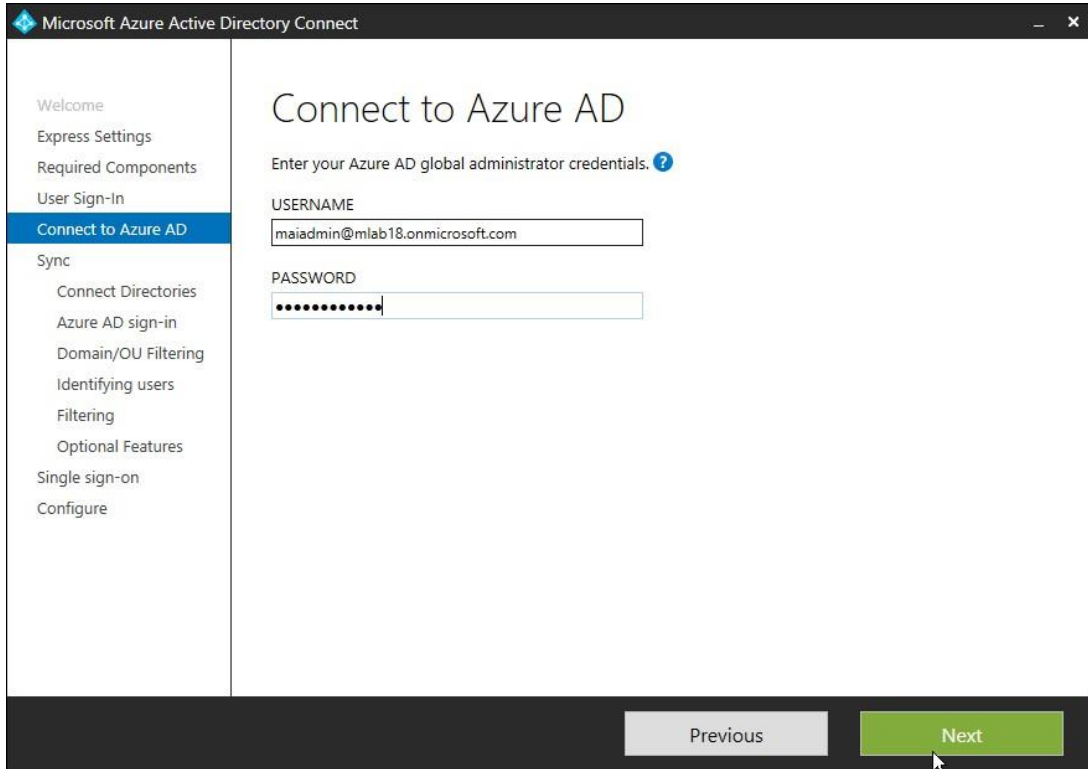
3. Use **Express settings** and Click Install.



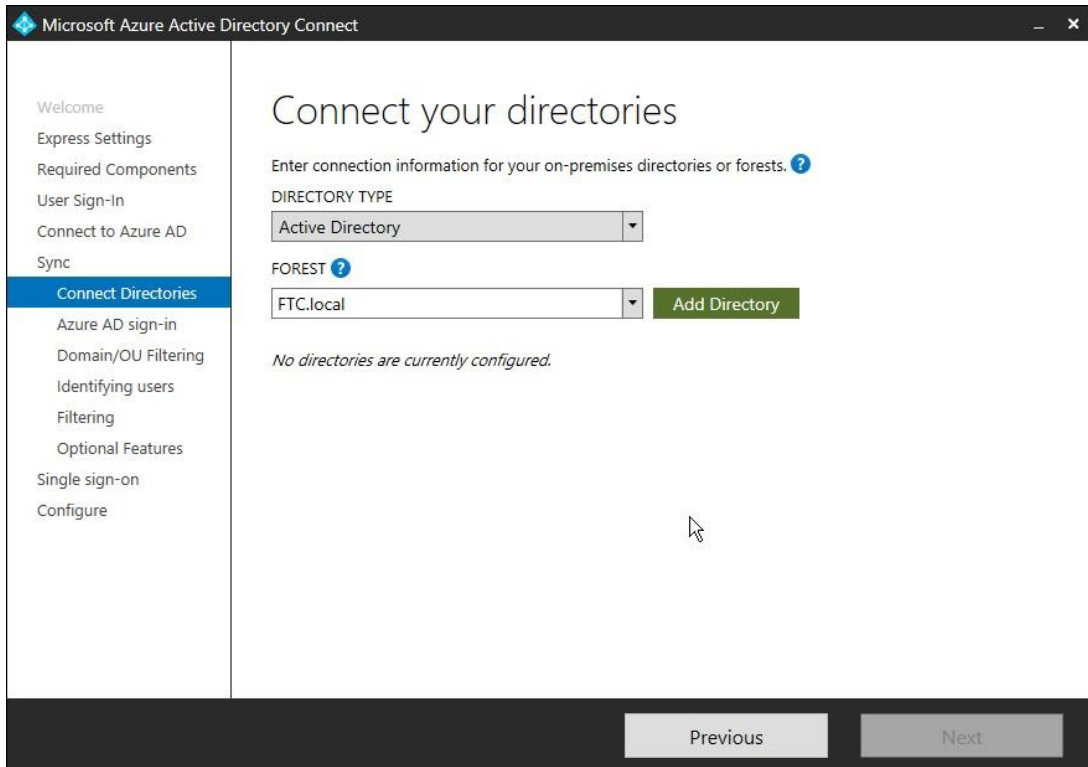
4. On “**User sign-in**” Page, Select **Password Hash Synchronization** and Click **Next**.

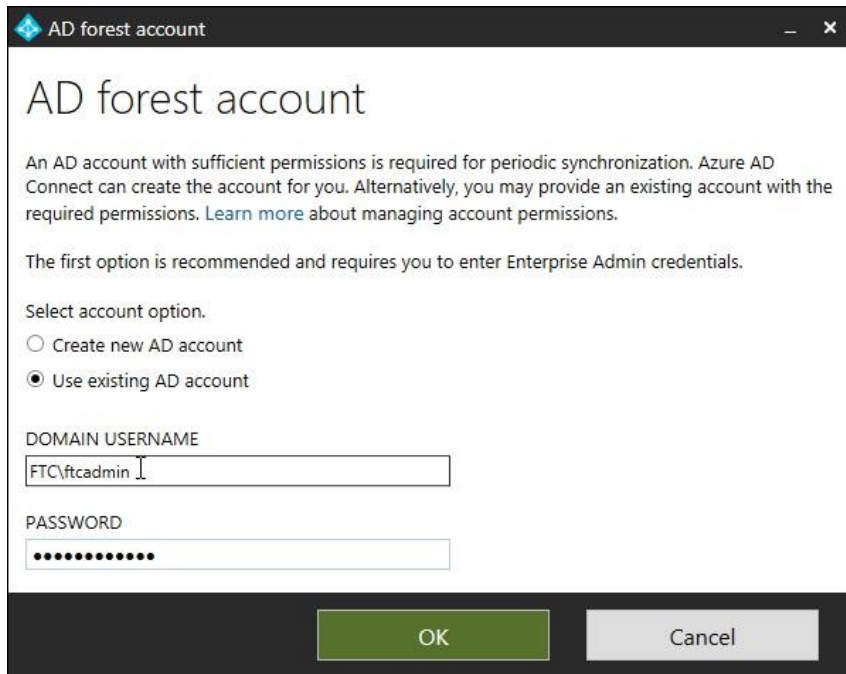


5. Enter **Global admin** credential, Click **Next**.

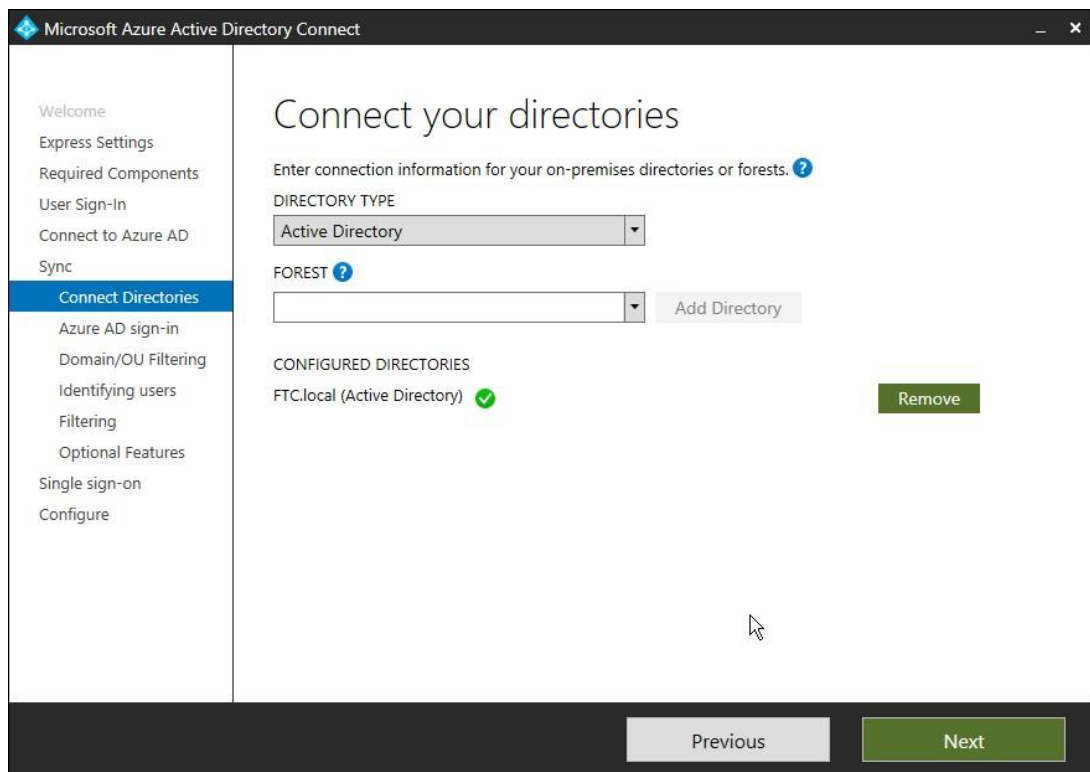


6. Click **Add Directory** & enter **Enterprise admin account** for AD On-premise

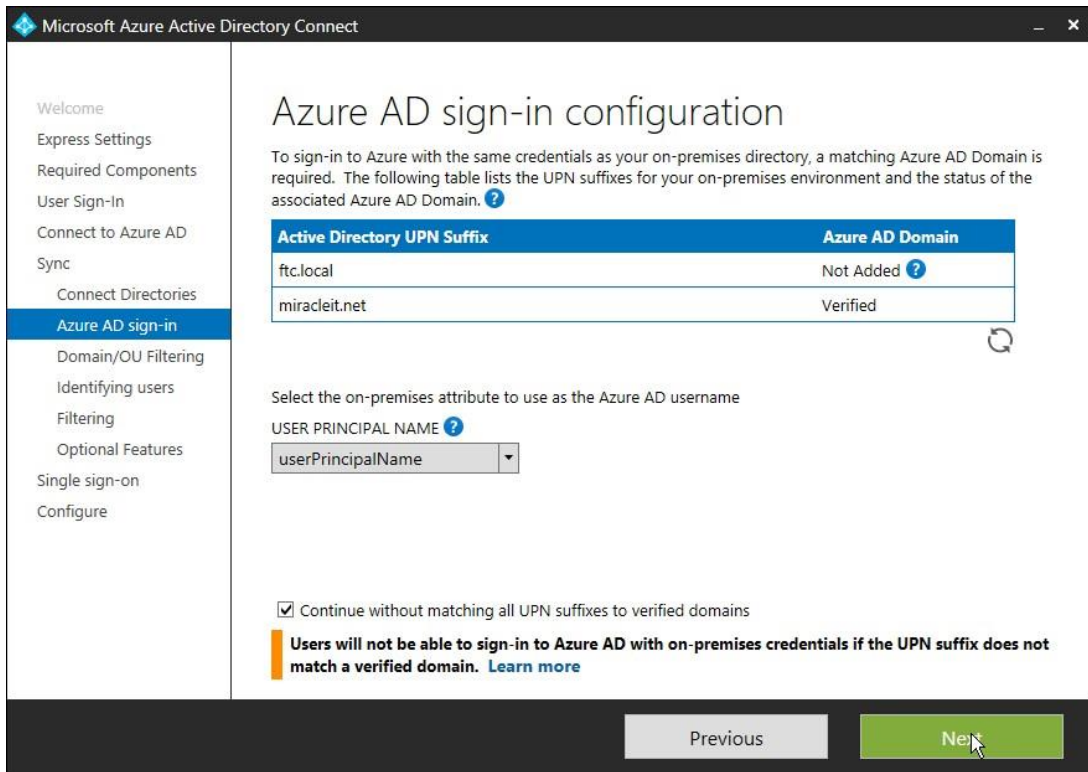




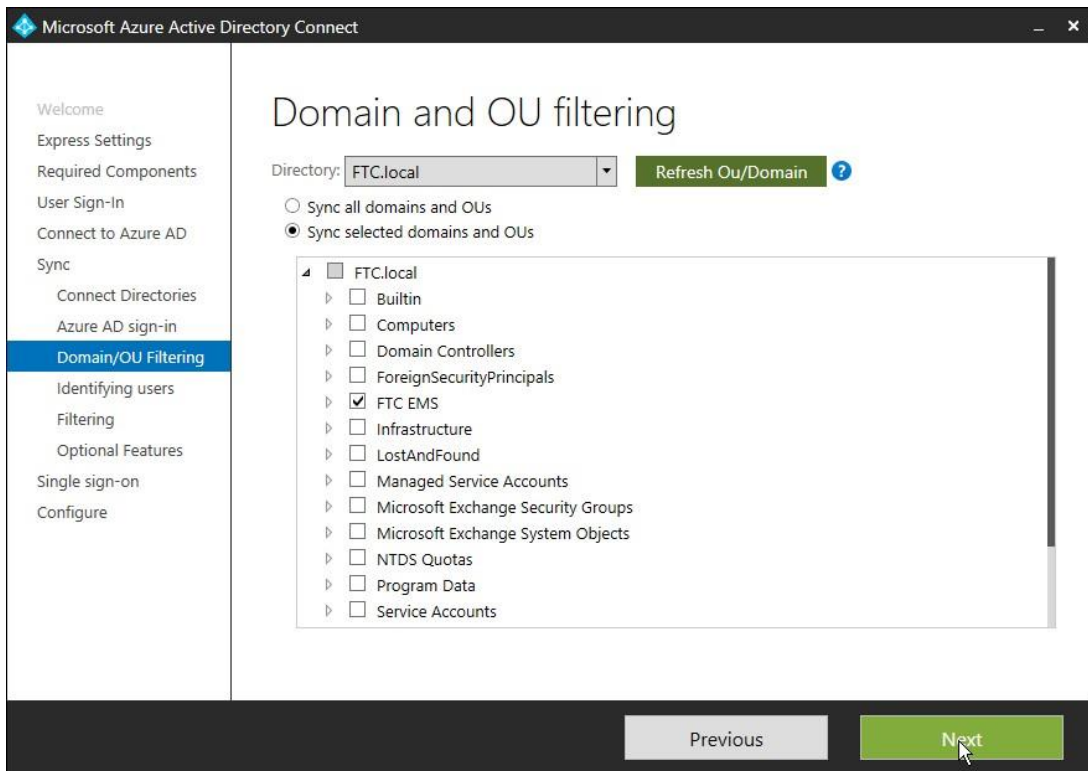
7. Click **Next** on connect your directories page.



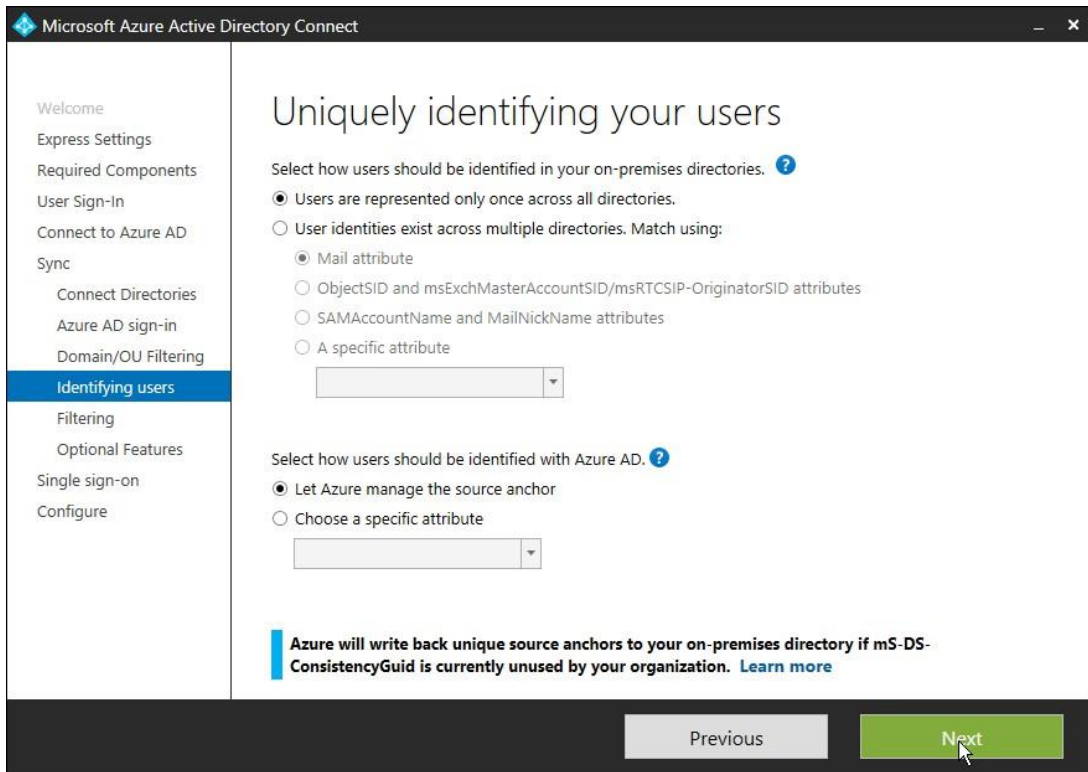
8. Check continue without matching all UPN suffix in case you will sync only specific OU and Click **Next**.



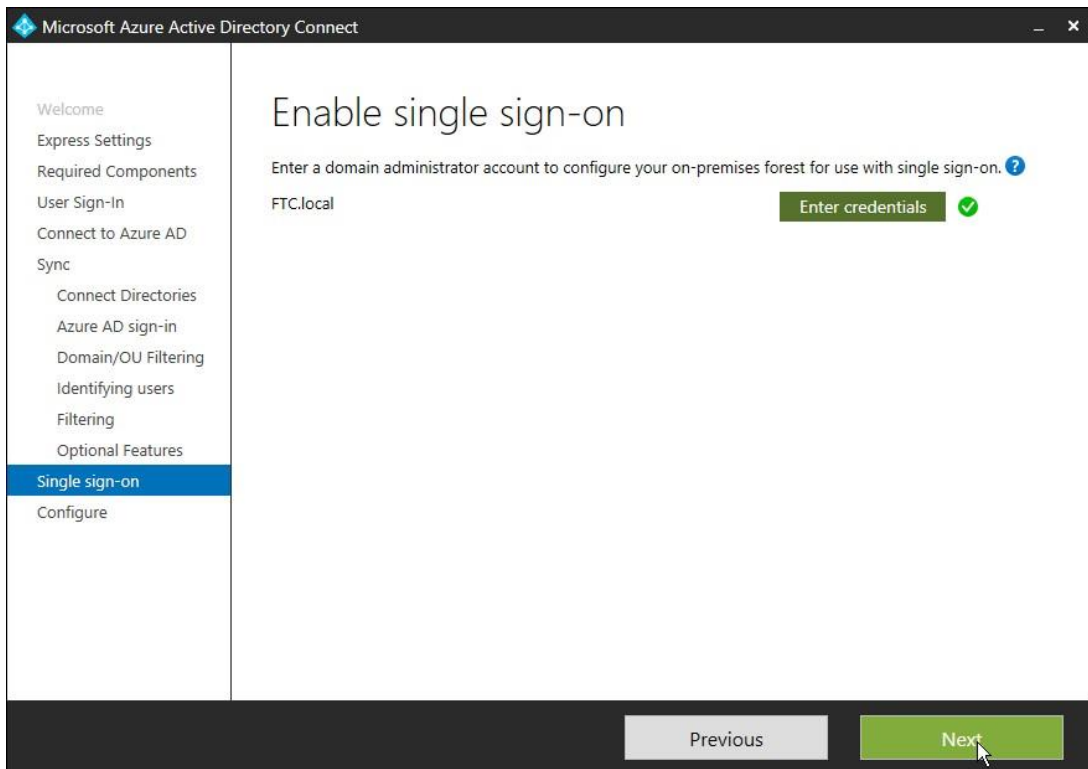
9. Select OU that you want to sync on Azure AD and Click **Next**.



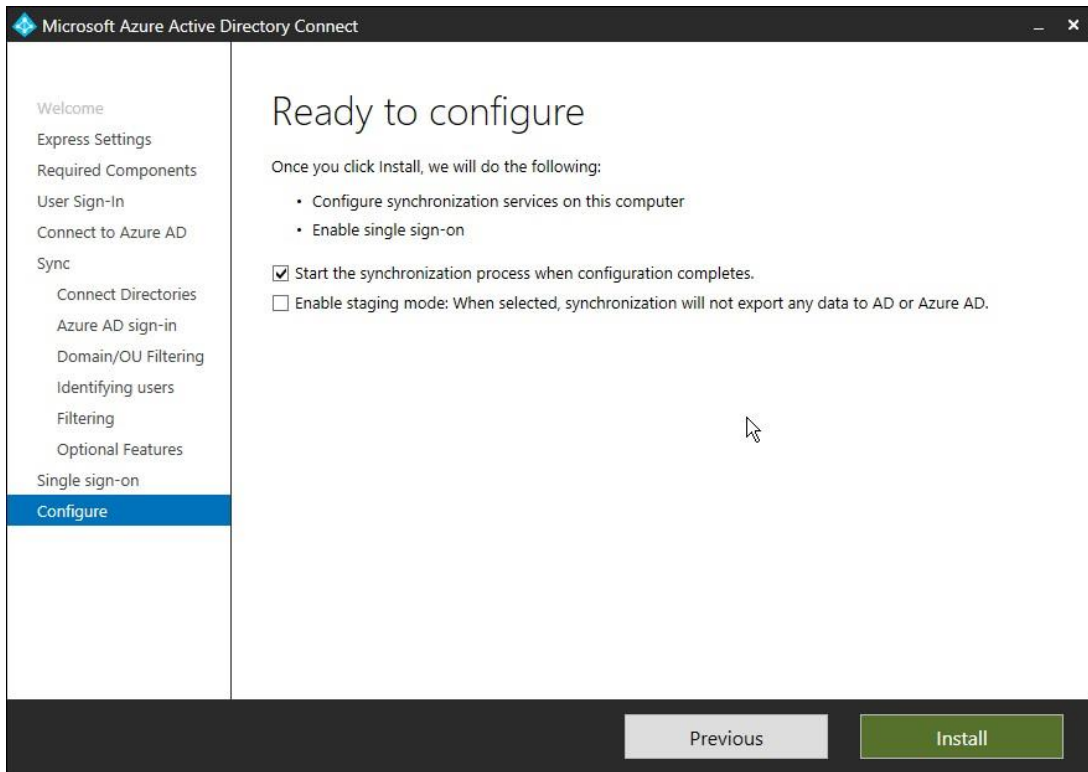
10. Click **Next**.



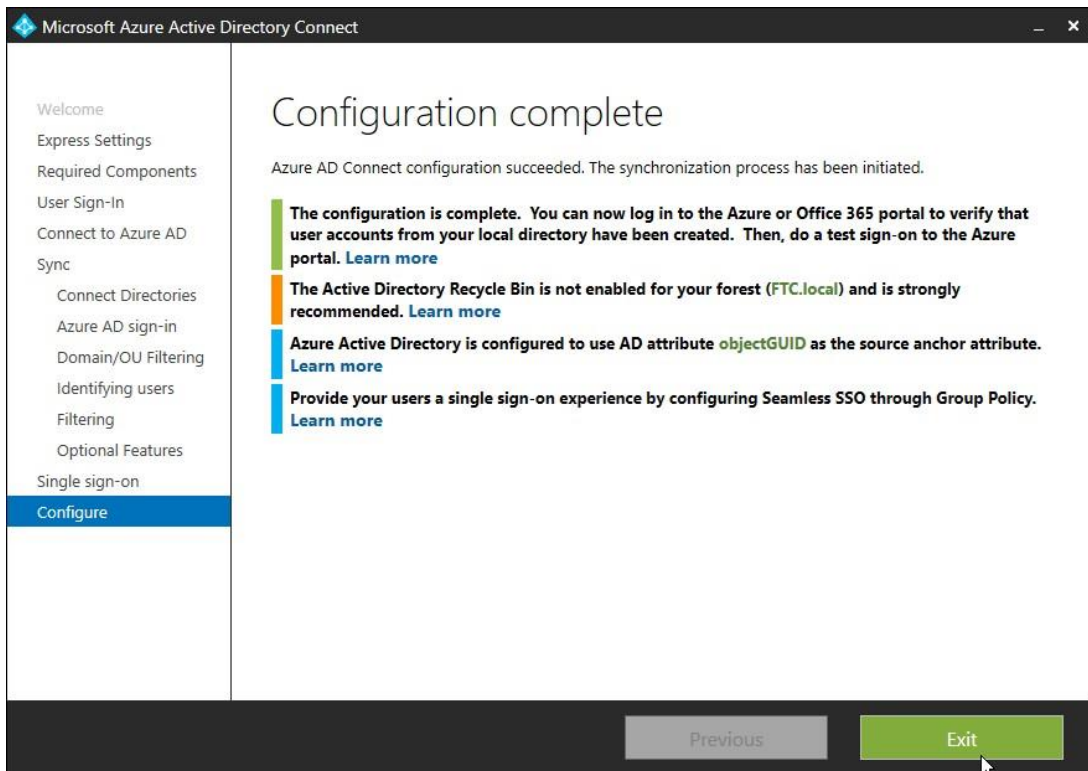
11. On the **Enable Single sign-on** page, Enter **Enterprise admin** credentials and click **Next**.



12. **Ready to configure** page. Click **Install**.

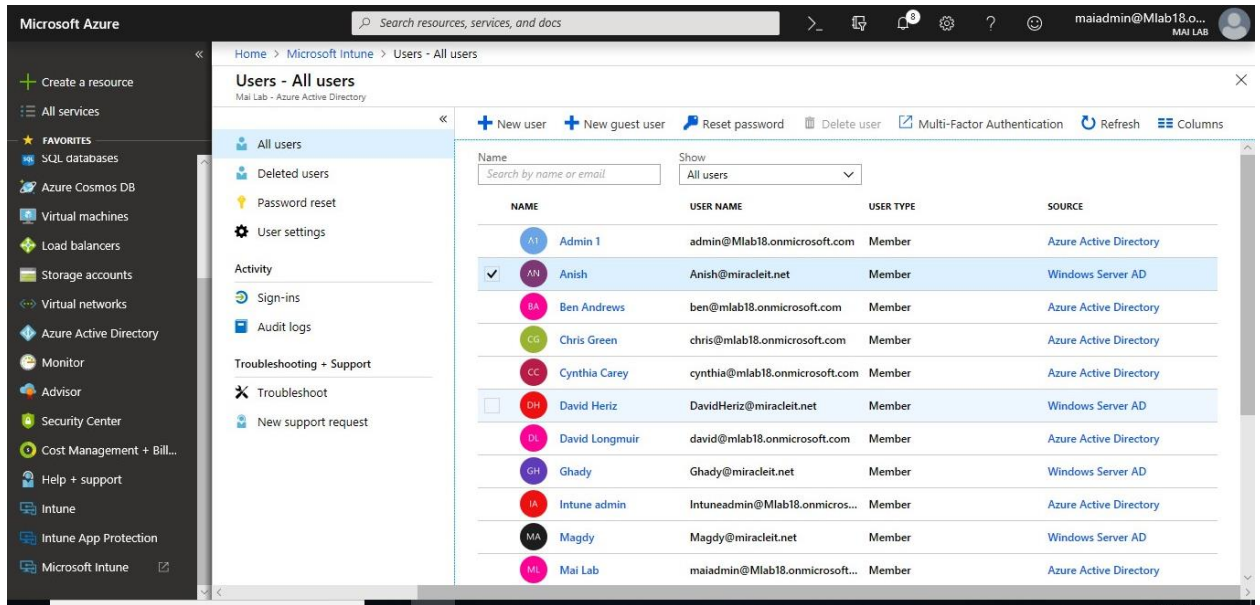


13. Now **Configuration complete**, click **Exit**.



14. In the [Intune admin portal](#), click **Users** and verify all users synchronize on Intune Portal

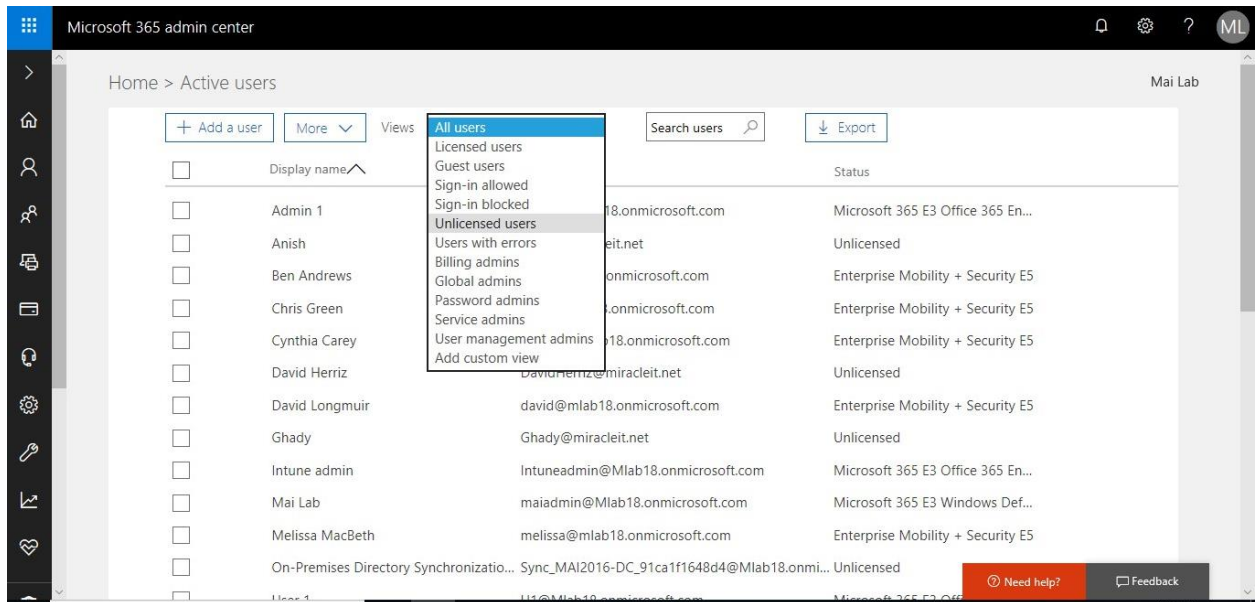
Microsoft Intune step by step on Azure portal



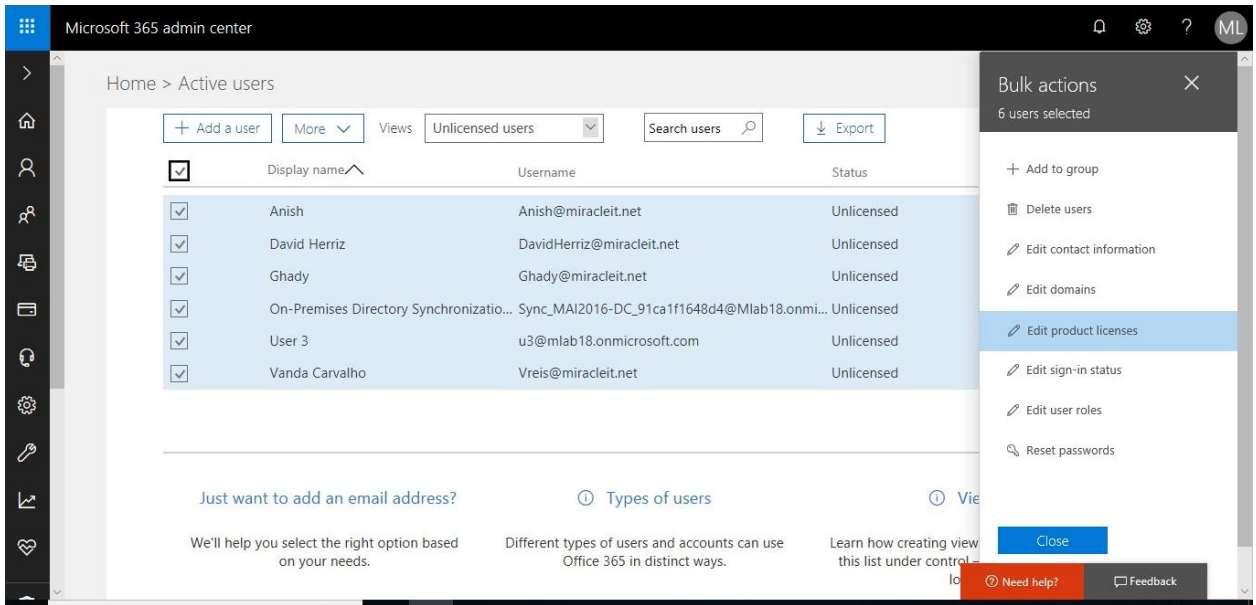
Activate Synchronized Users and Grant Licenses

To activate synchronized users, you can follow below steps

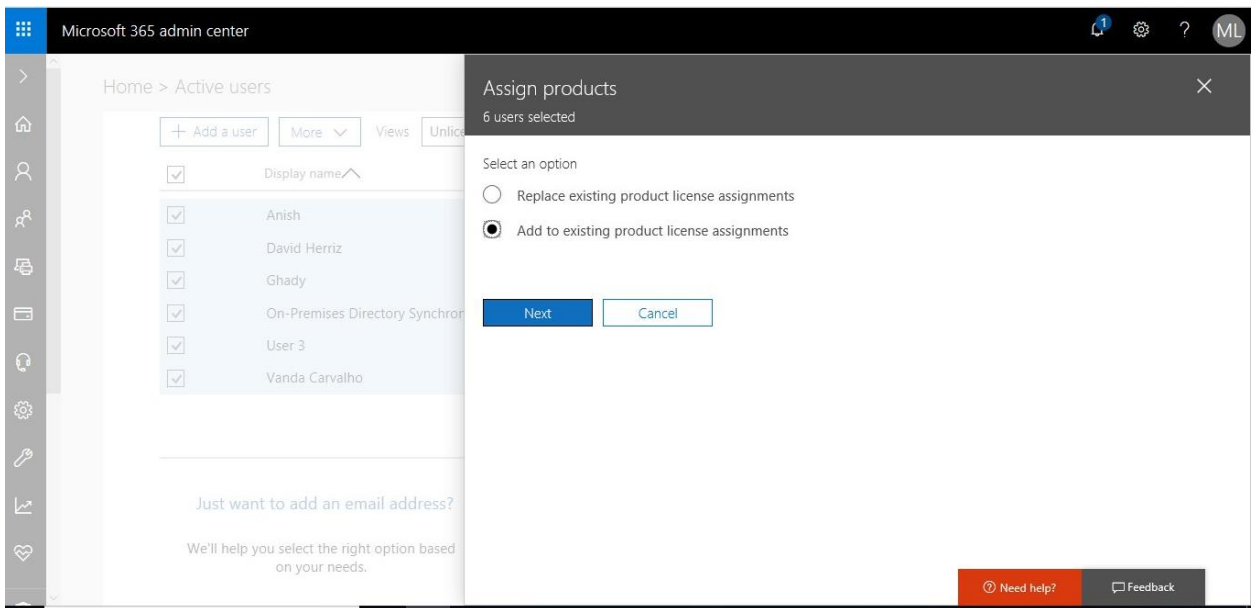
1. In the [Office admin portal](#), click **Active Users**.
2. On **views** tab, select **unlicensed users**.



3. Check the box to select all users on the page or select **Specific user** and click **Edit product licenses**.

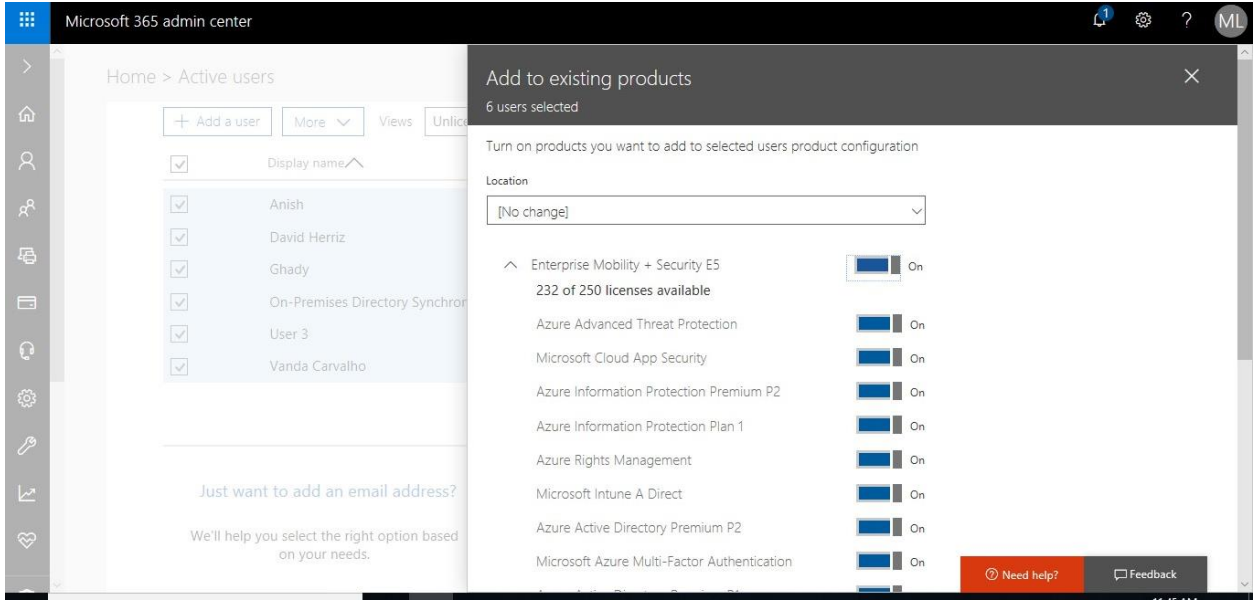


4. Select **Add to existing licenses**.

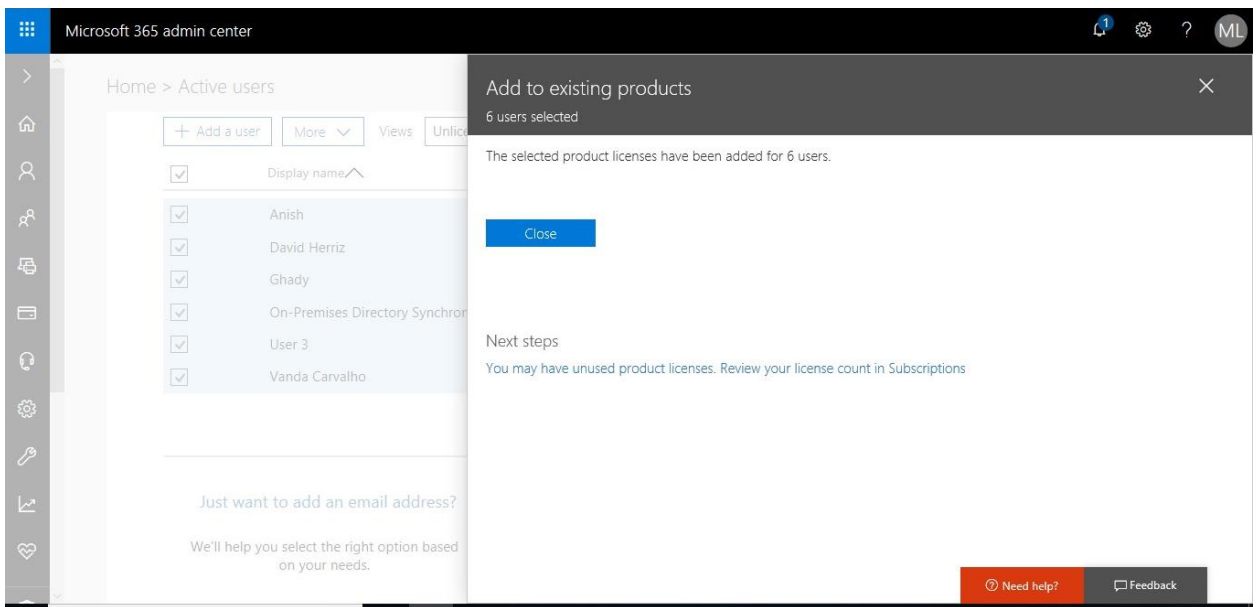


Note: When you assign licenses for EMS or Intune, try to choose add to existing Licenses to don't remove any previous licenses for office 365 or others.

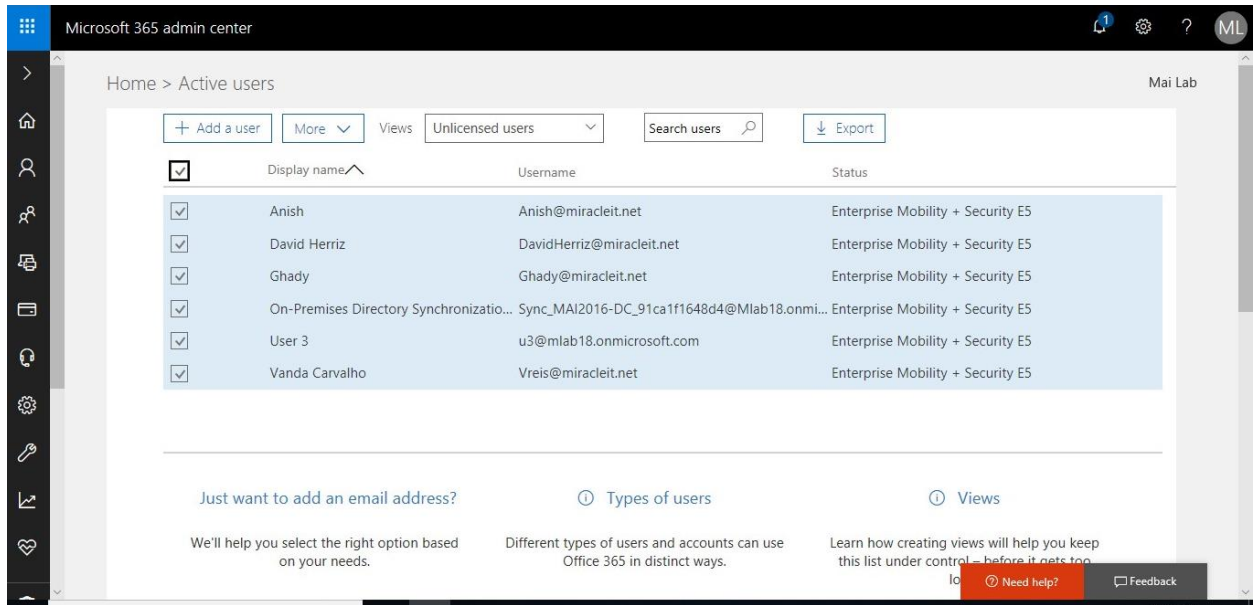
5. Select EMS licenses and Click **Add**.



6. On Add to existing product page, click **Close**.



7. Now All sync users have EMS licenses



Azure Active Directory Pass-through Authentication “PTA”

Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications by using the same passwords. Pass-through Authentication signs users in by validating their passwords directly against on-premises Active Directory.

Configure Pass-through Authentication

Step 1: Check the prerequisites

Ensure that the following prerequisites are in place.

In the Azure Active Directory admin center

1. Create a cloud-only global administrator account on your Azure AD tenant “Global admin account with onmicrosoft.com domain”. This way, you can manage the configuration of your tenant in case your on-premises services fail or become unavailable. Completing this step is critical to ensure that you don't get locked out of your tenant.
2. Add one or more custom domain names to your Azure AD tenant. Your users can sign in with one of these domain names.

In your on-premises environment

1. Identify a server running Windows Server 2012 R2 or later to run Azure AD Connect. Add the server to the same Active Directory forest as the users whose passwords you need to validate.

2. Install the [latest version of Azure AD Connect](#) on the server identified in the preceding step. If you already have Azure AD Connect running, ensure that the version is 1.1.750.0 or later.
3. Identify one or more additional servers (running Windows Server 2012 R2 or later) where you can run standalone Authentication Agents. These additional servers are needed to ensure the high availability of requests to sign in. Add the servers to the same Active Directory forest as the users whose passwords you need to validate.
4. If there is a firewall between your servers and Azure AD, configure the following items:
 - o Ensure that Authentication Agents can make *outbound* requests to Azure AD over the following ports:

Port number	How it's used
80	Downloads the certificate revocation lists (CRLs) while validating the SSL certificate
443	Handles all outbound communication with the service
8080 (optional)	Authentication Agents report their status every ten minutes over port 8080, if port 443 is unavailable. This status is displayed on the Azure AD portal. Port 8080 is <i>not</i> used for user sign-ins.

- o If your firewall enforces rules according to the originating users, open these ports for traffic from Windows services that run as a network service.
- o If your firewall or proxy allows DNS whitelisting, whitelist connections to ***.msapproxy.net** and ***.servicebus.windows.net**. If not, allow access to the [Azure datacenter IP ranges](#), which are updated weekly.
- o Your Authentication Agents need access to **login.windows.net** and **login.microsoftonline.com** for initial registration. Open your firewall for those URLs as well.
- o For certificate validation, unblock the following URLs: **mscrl.microsoft.com:80**, **crl.microsoft.com:80**, **ocsp.msocsp.com:80**, and **www.microsoft.com:80**. Since these URLs are used for certificate validation with other Microsoft products you may already have these URLs unblocked.

Note: In production environments, we recommend that you have a minimum of 3 Authentication Agents running on your tenant. There is a system limit of 12 Authentication Agents per tenant.

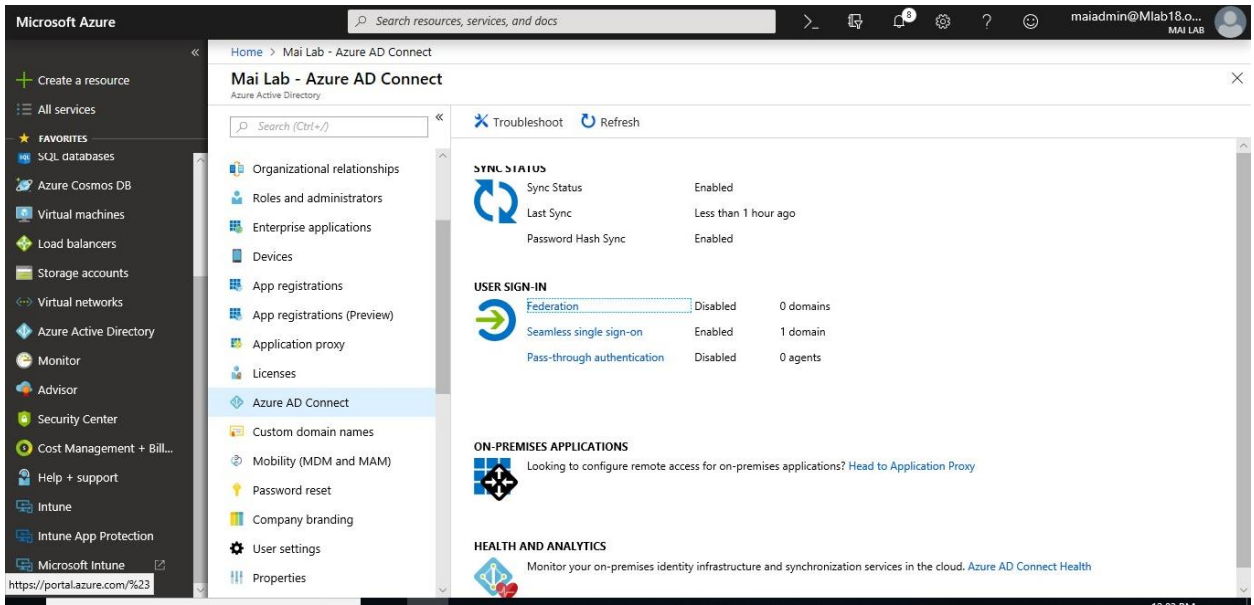
Step 2: Configure PTA

If you plan to deploy Pass-through Authentication in a production environment, you should install additional standalone Authentication Agents. Install these Authentication Agent(s) on server(s) other than the one running Azure AD Connect. This setup provides you with high availability for user sign-in requests.

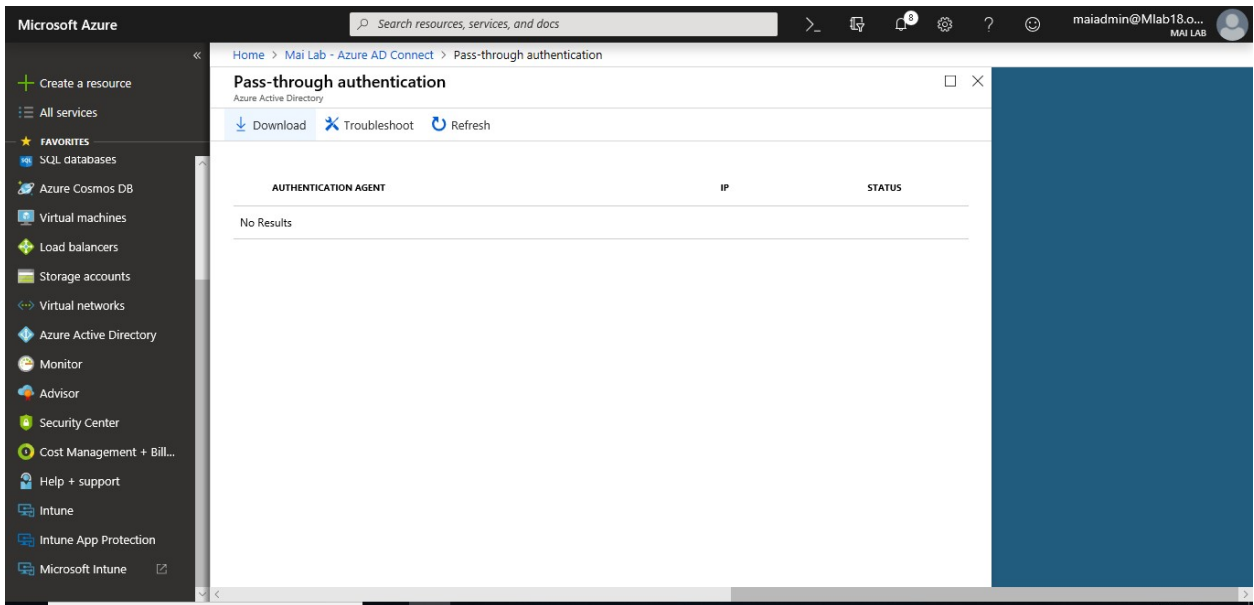
Follow these instructions to download & install the Authentication Agent software:

1. Sign in [Azure Portal](#), Select **Azure Active Directory** in the left pane.
2. Select **Azure AD Connect**, select **Pass-through authentication**.

Microsoft Intune step by step on Azure portal

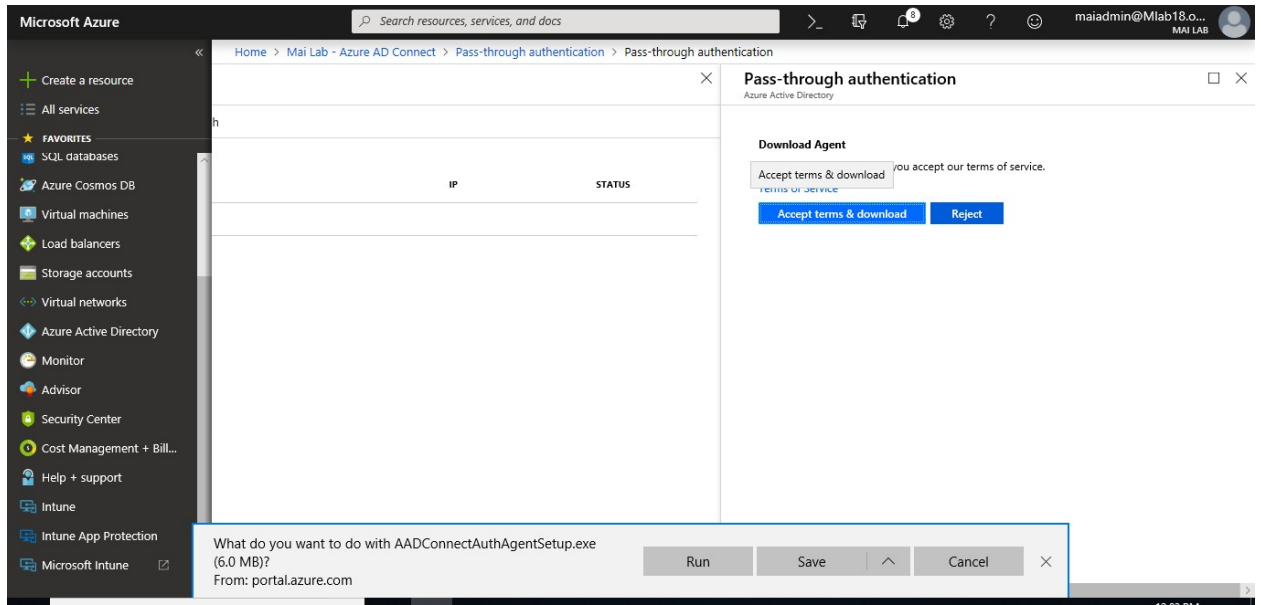


3. Select **Download Agent**.

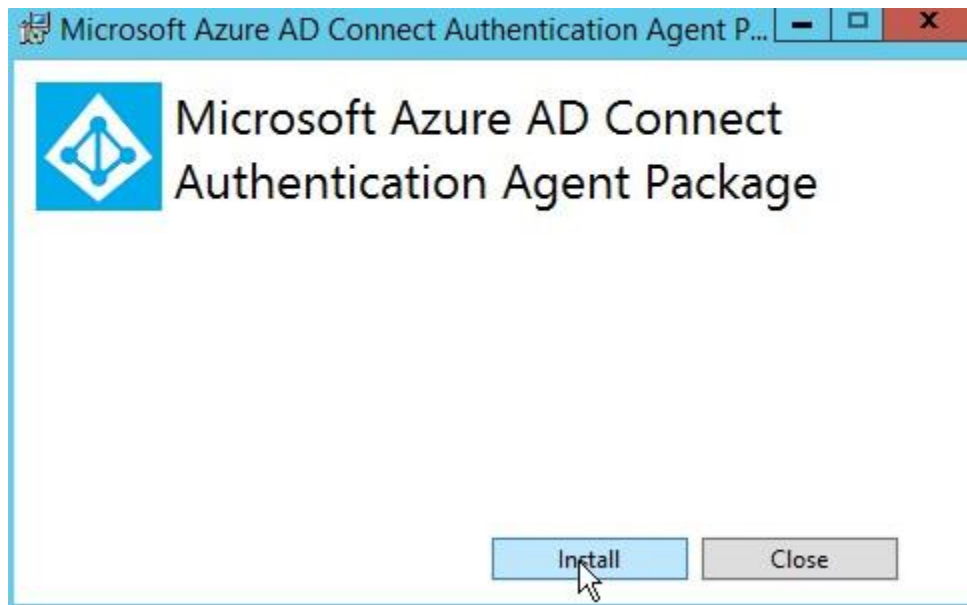


4. Select the **Accept terms & download** button.

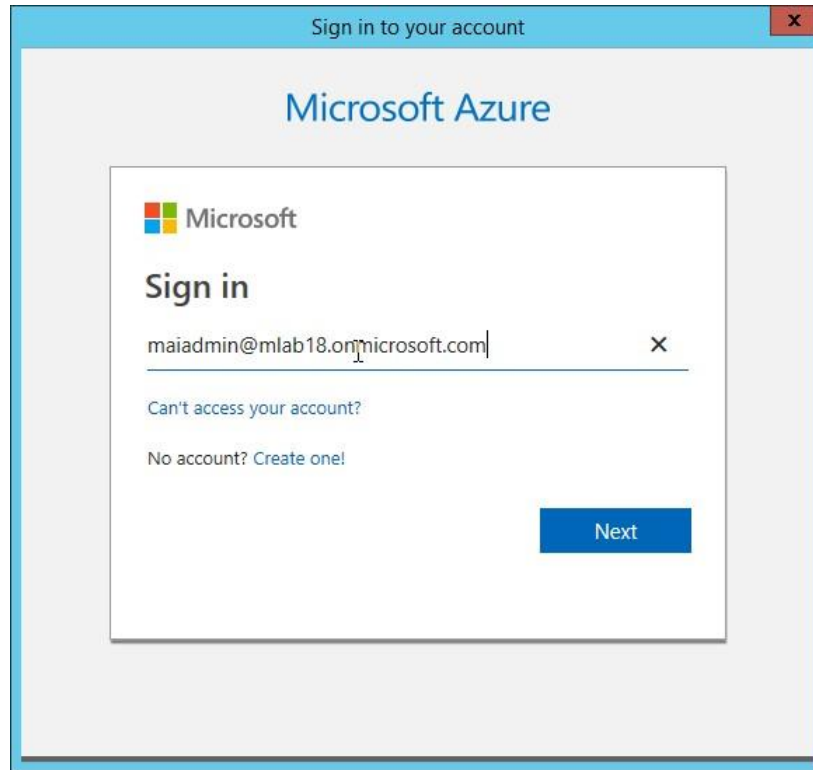
Microsoft Intune step by step on Azure portal



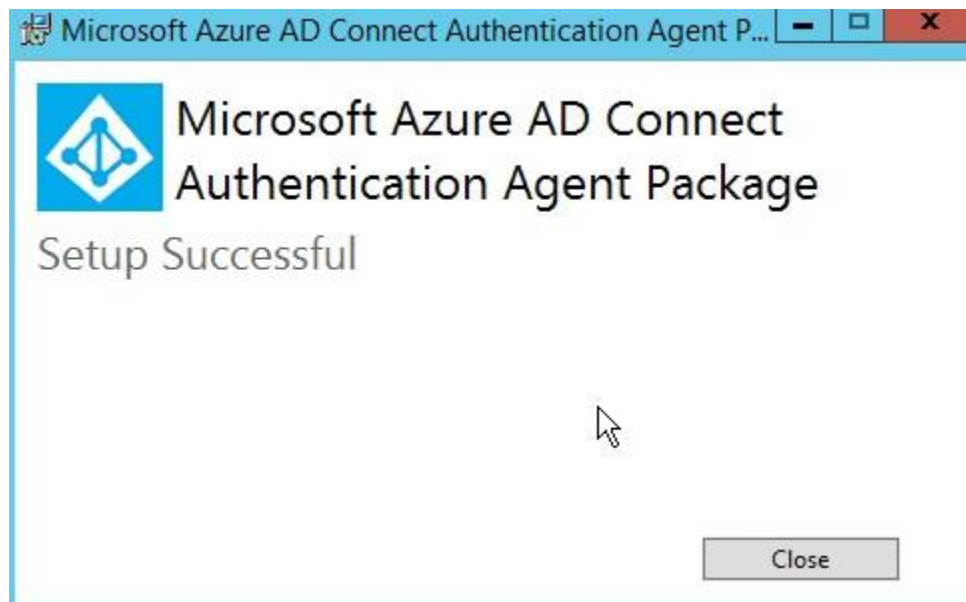
5. On the server for PTA, Install **Authentication Agent**.



6. Enter **global admin** credential for your tenant.



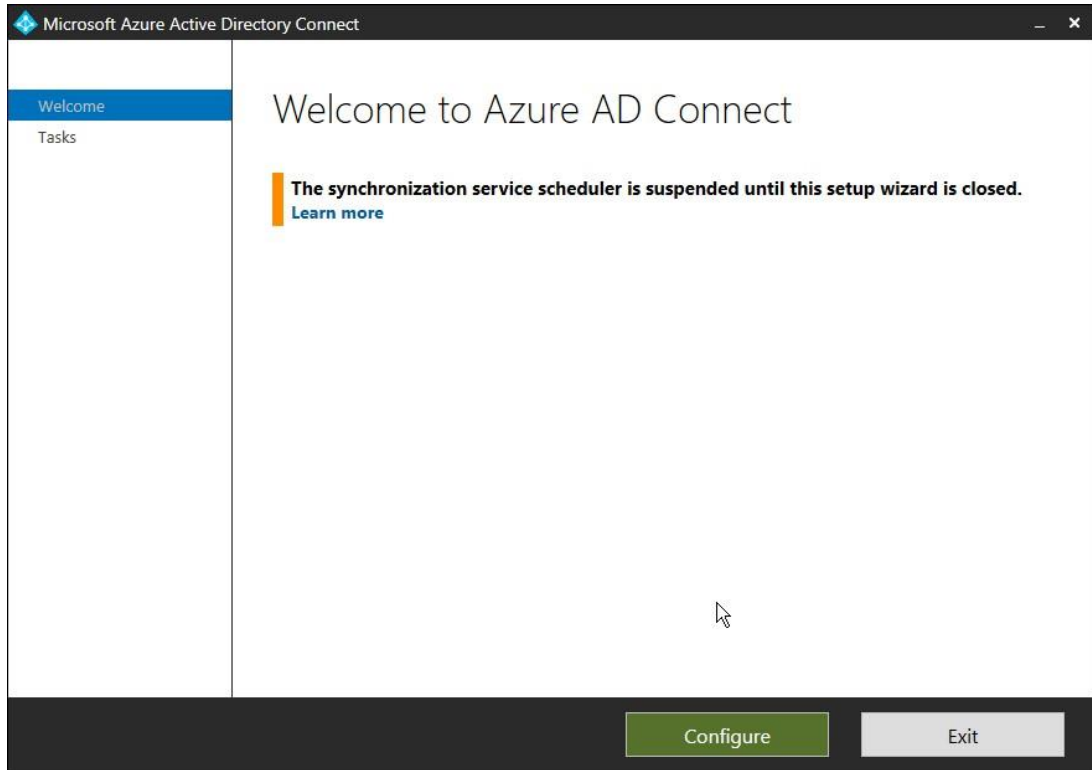
7. Click **Close**.



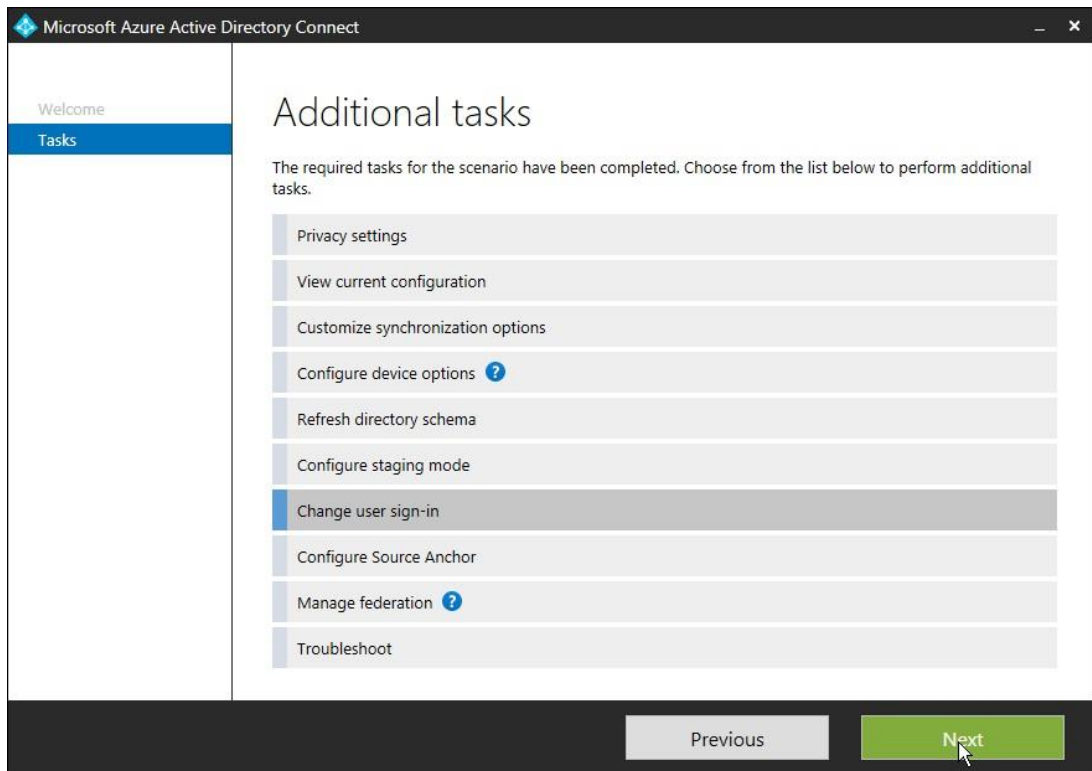
8. Repeat same steps 5-7 for install authentication agent on another server.

Enable Pass-through Authentication through Azure AD Connect.

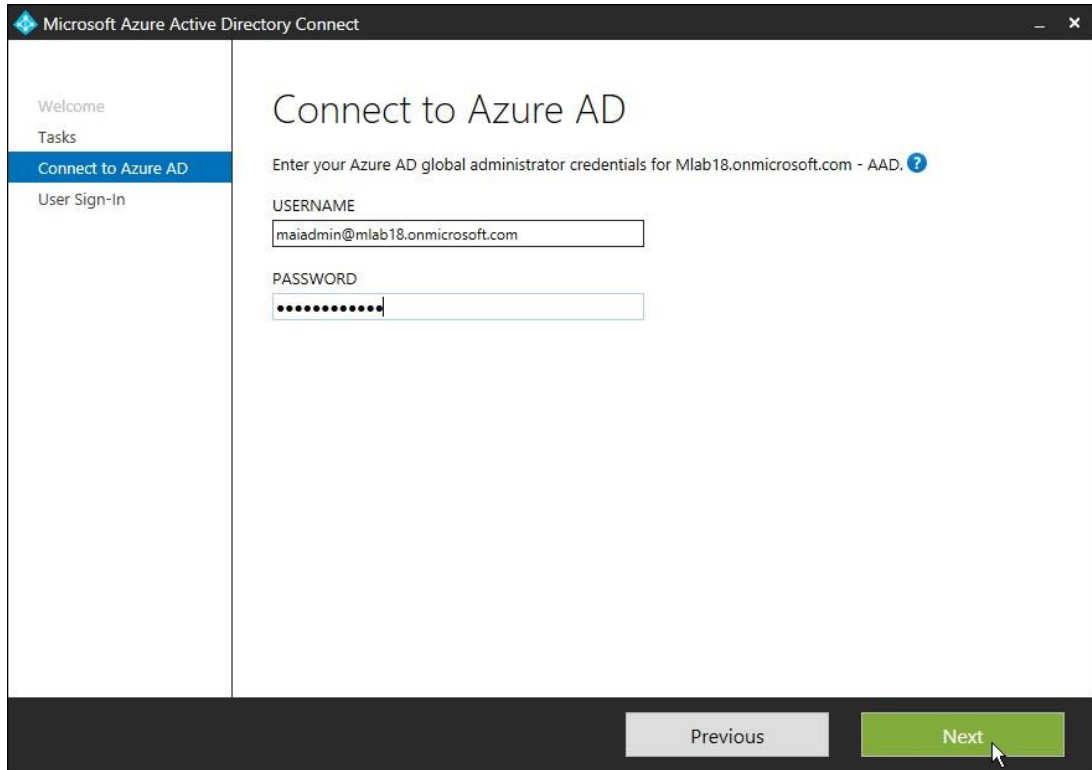
1. On Azure AD Connect Server, Click Azure AD Connect > Select **Configure**.



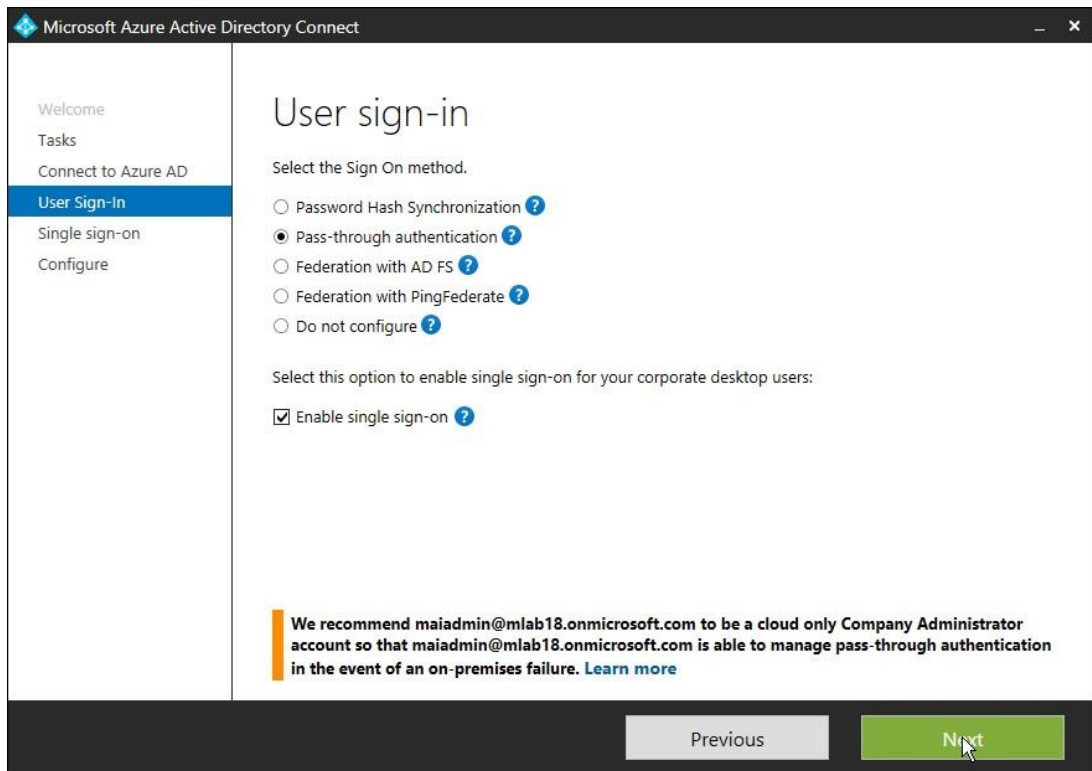
2. Select the **Change user sign-in**.



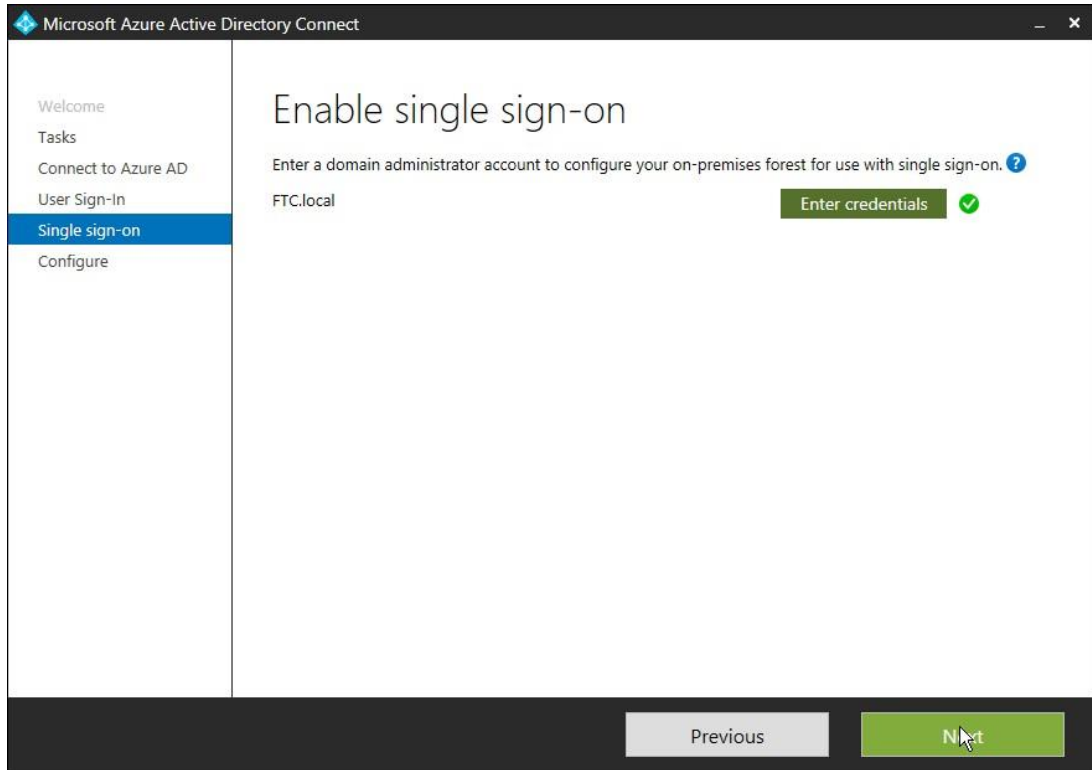
3. Enter Global admin account, Select **Next**.



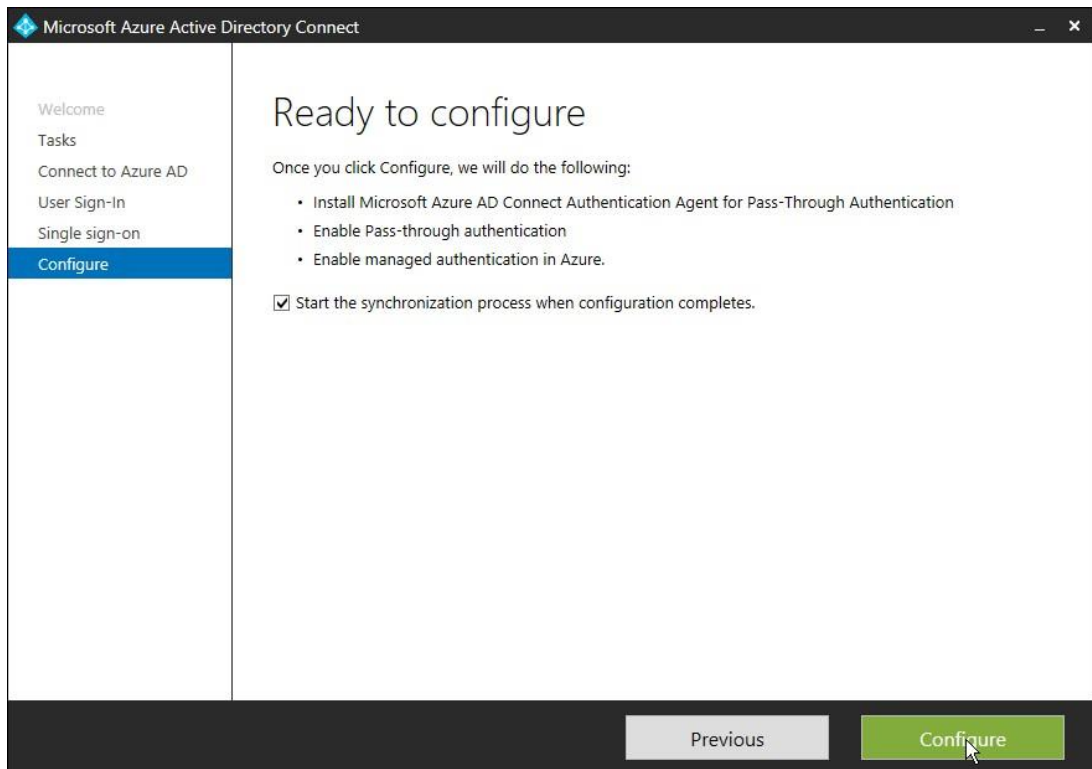
4. Then select **Pass-through Authentication** as the sign-in method.



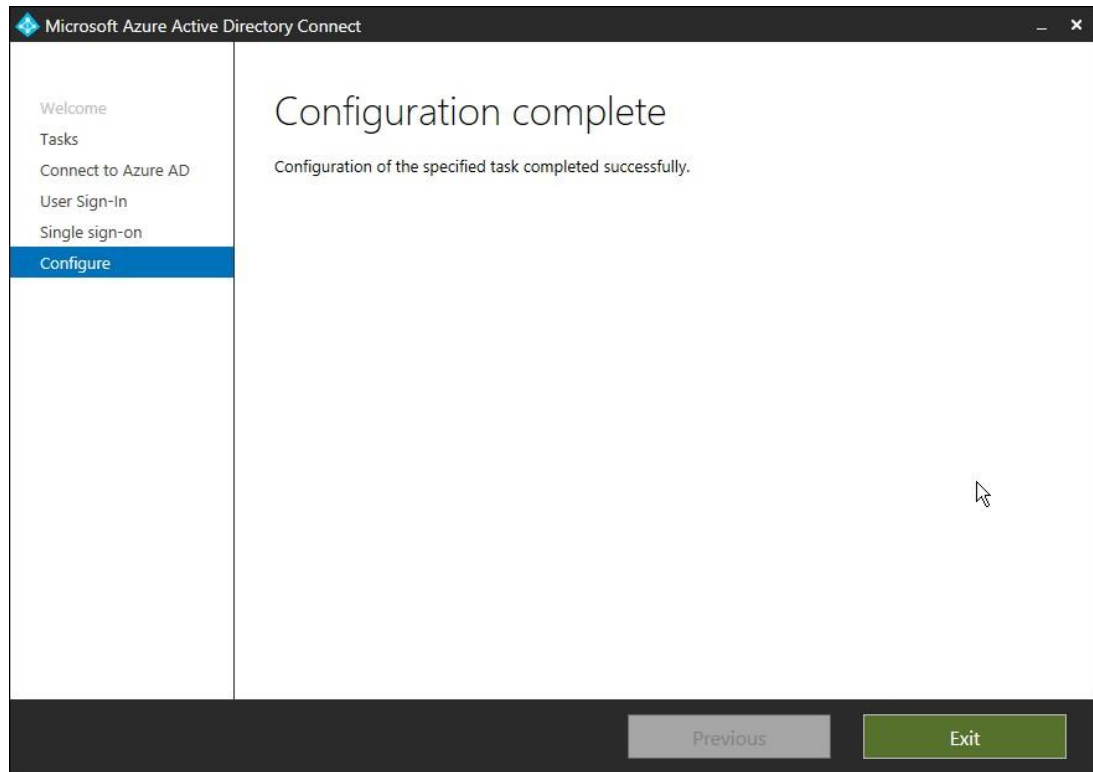
5. On Enable Single sign-on page, Click **Next**.



6. Click **Configure**.



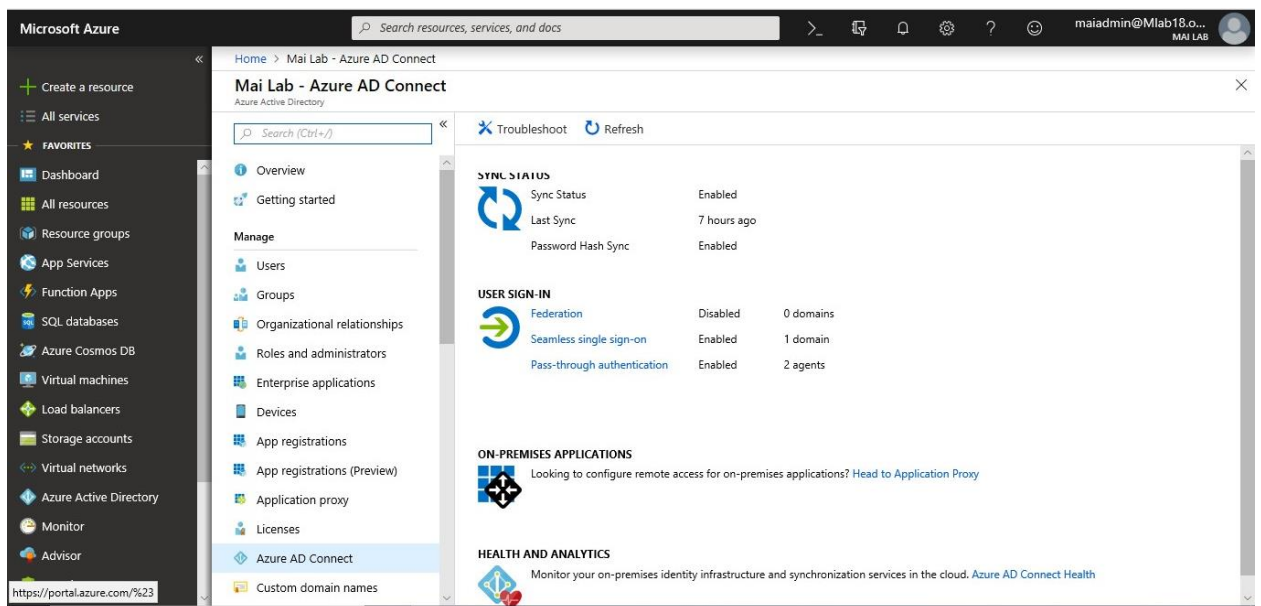
7. Click **Exit**.



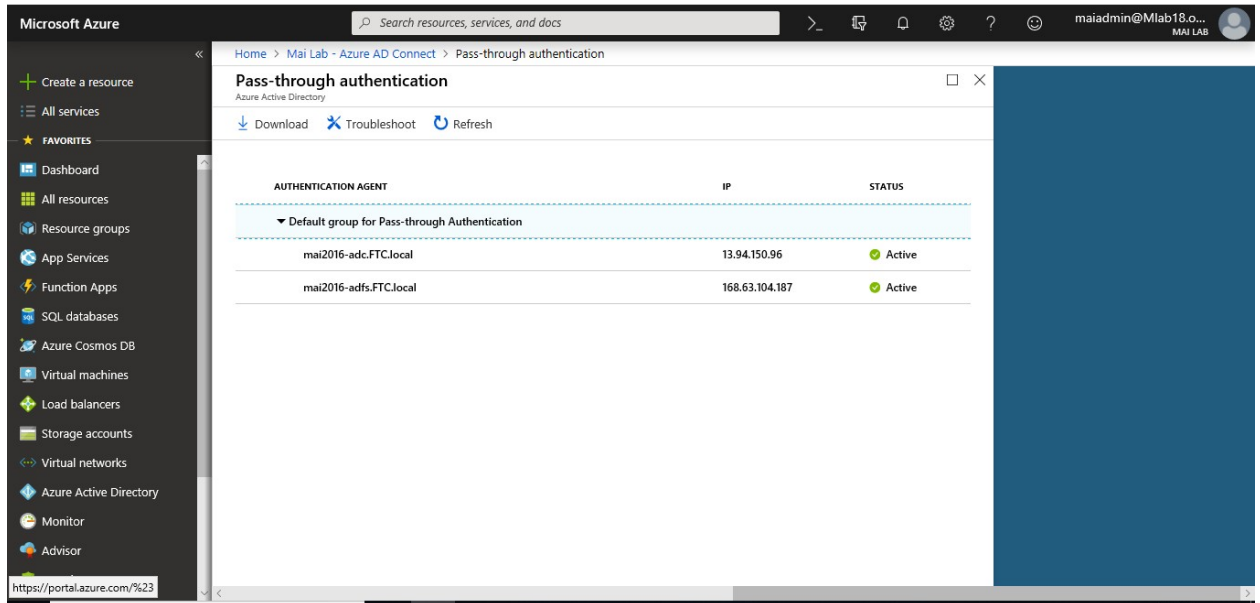
Step 3: Validate PTA

Follow these instructions to verify that you have enabled Pass-through Authentication correctly:

1. Sign in [Azure Portal](#), Select **Azure Active Directory** in the left pane.
2. Select **Azure AD Connect**, verify that the **Pass-through authentication** feature appears as **Enabled**.



3. Select **Pass-through authentication**. The **Pass-through authentication** pane lists the servers where your Authentication Agents are installed.



Note: In case, both PTA servers are down, end user won't be able to login to cloud services because authentication is done directly from On-Premises Active directory through PTA agents.

Chapter 3

Organize Users & Devices in Microsoft Intune

Create Intune Groups to organize Users and Devices

Groups in Intune give you great flexibility for managing your devices and users. You can set up groups to suit your organizational needs (for example, by geographic location, department, or hardware characteristics). You can use groups to perform a wide variety of administrative tasks at scale, from setting policies for a set of users to deploying applications to a set of devices.

You can add the following types of groups:

- **Assigned groups** - Manually add users or devices into a static group
- **Dynamic groups** - (Using Azure Active Directory Premium) Let you dynamically build either user or device groups defined with either simple or advanced rules

Configure Security Groups

In the Microsoft Intune admin portal, you can create, edit, and delete security groups. Security groups are a good resource to use when you populate user groups. You can use security groups as criteria for the organization groups that service administrators use for day-to-day management of Intune, including deploying software or assigning policies.

Security groups can include the following:

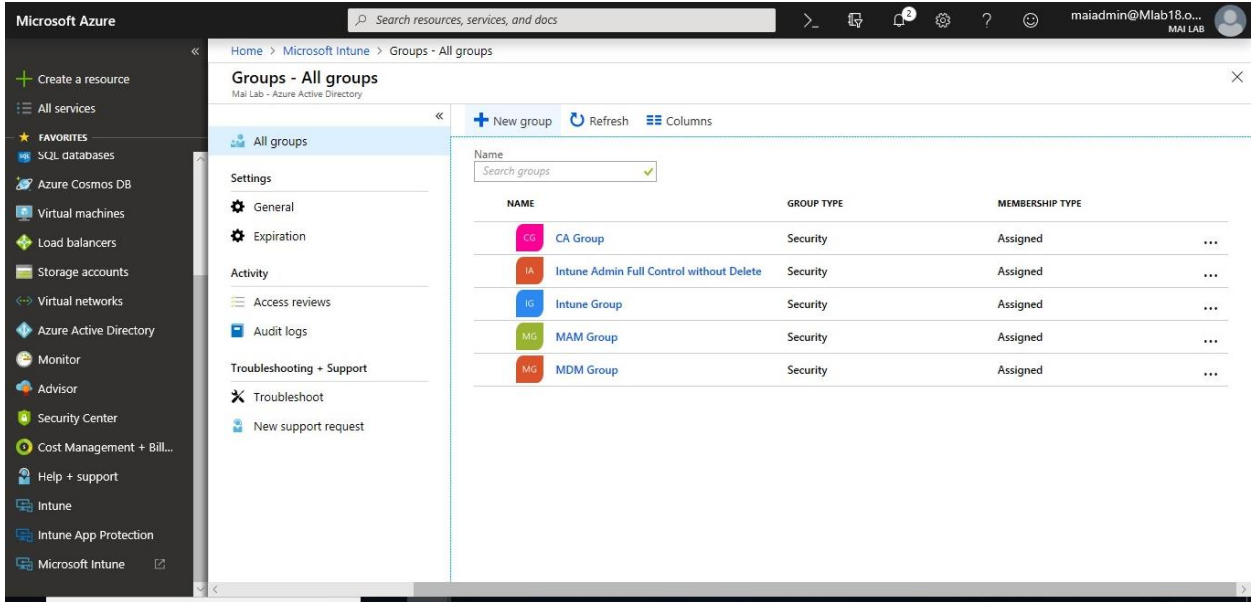
- Users and groups sync from your on-premises Active Directory
- Users and groups add directly in Azure Active Directory through the Office 365 admin center or the Azure portal are available to you to use when you create user groups in Intune.

To Create Assigned Group

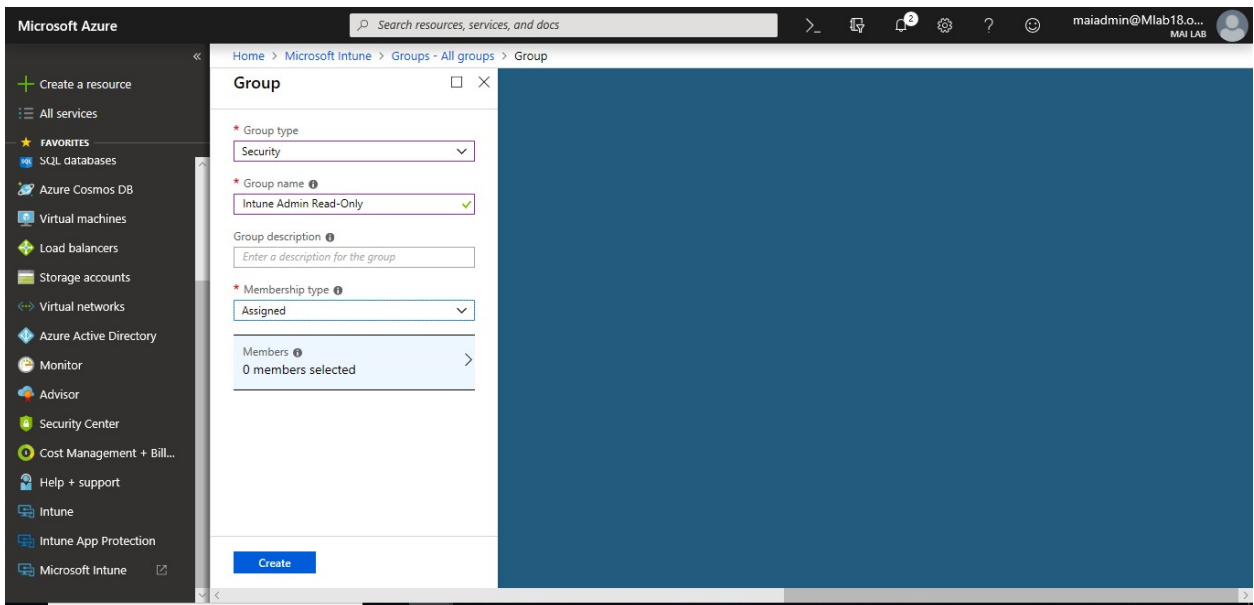
To create Intune groups to organize users and devices, you can follow below steps

1. Sign into the [Azure portal](#). Choose **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. On the **Intune** pane, choose **Groups** and then choose **New group** in the **All groups** pane.

Microsoft Intune step by step on Azure portal

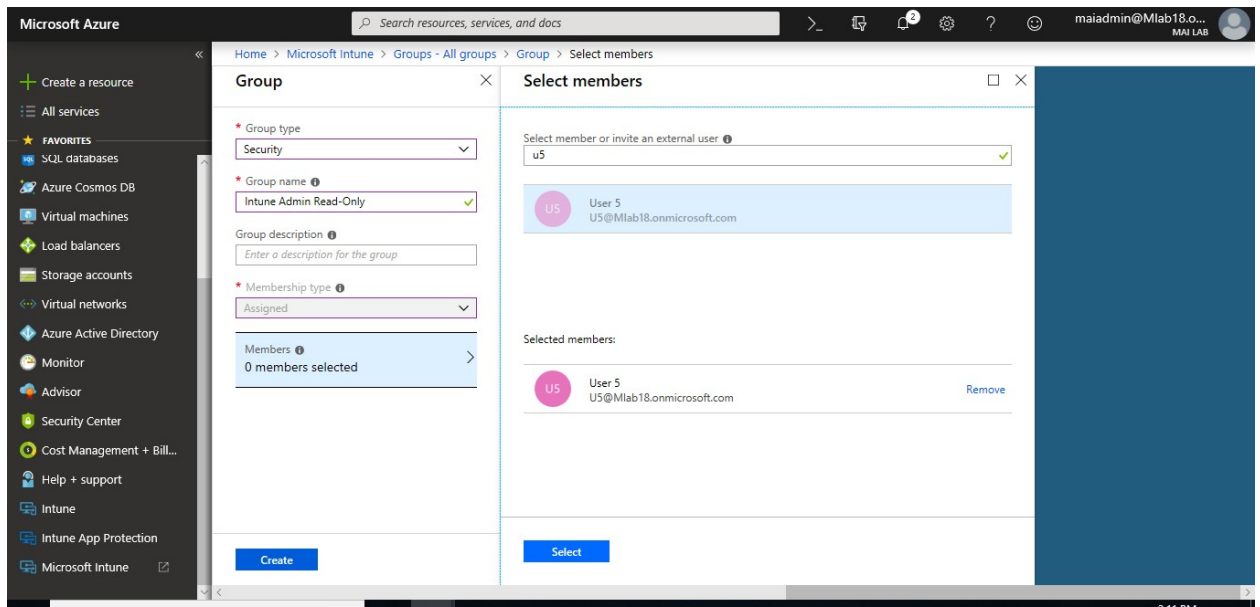


3. For **Group type** “Security”. Type a **Name** and **Description** for the new group.
4. Choose **Membership type**: Assigned

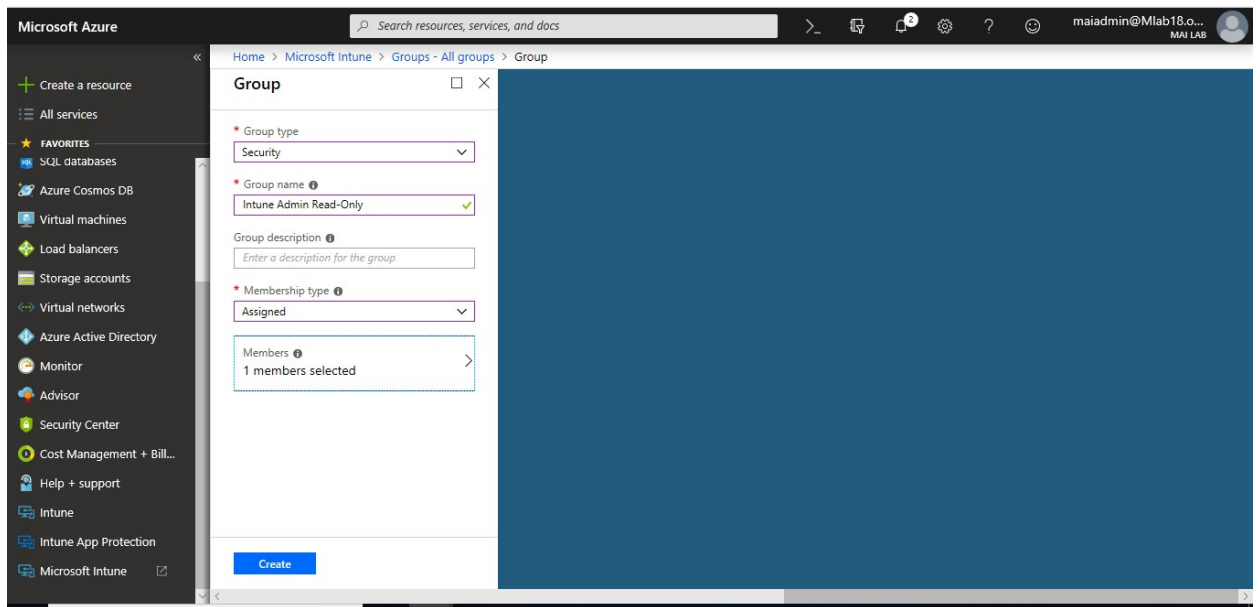


5. Select **Members**, add Users that you want on this group.

Microsoft Intune step by step on Azure portal



6. Choose **Create** to add the new group.

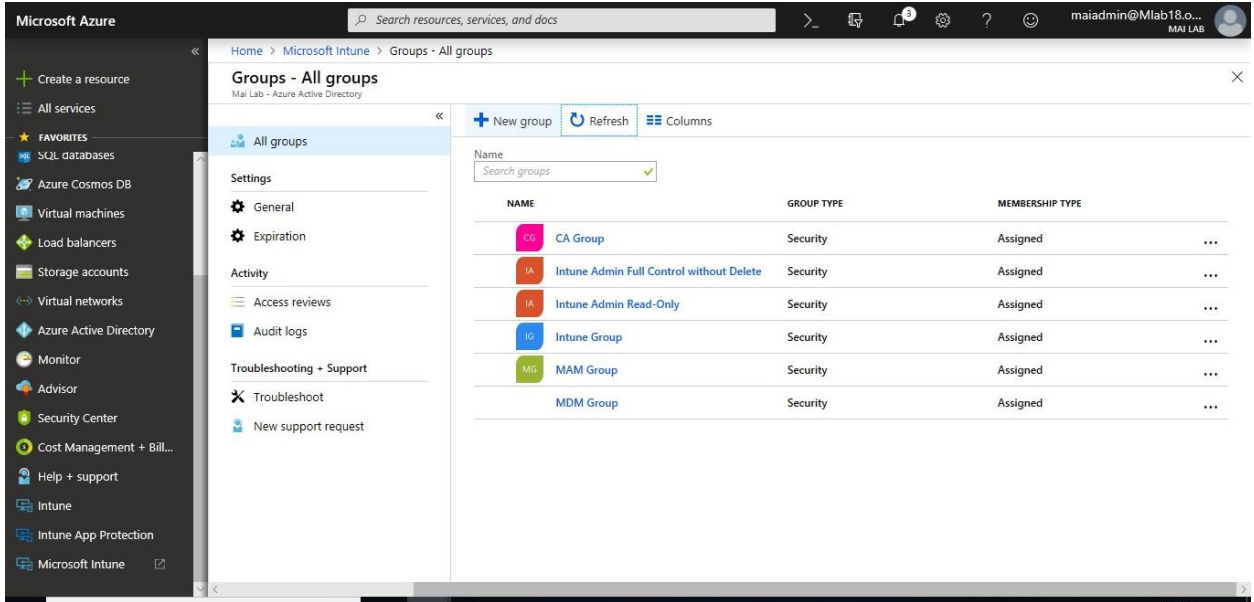


To Create Dynamic User Group

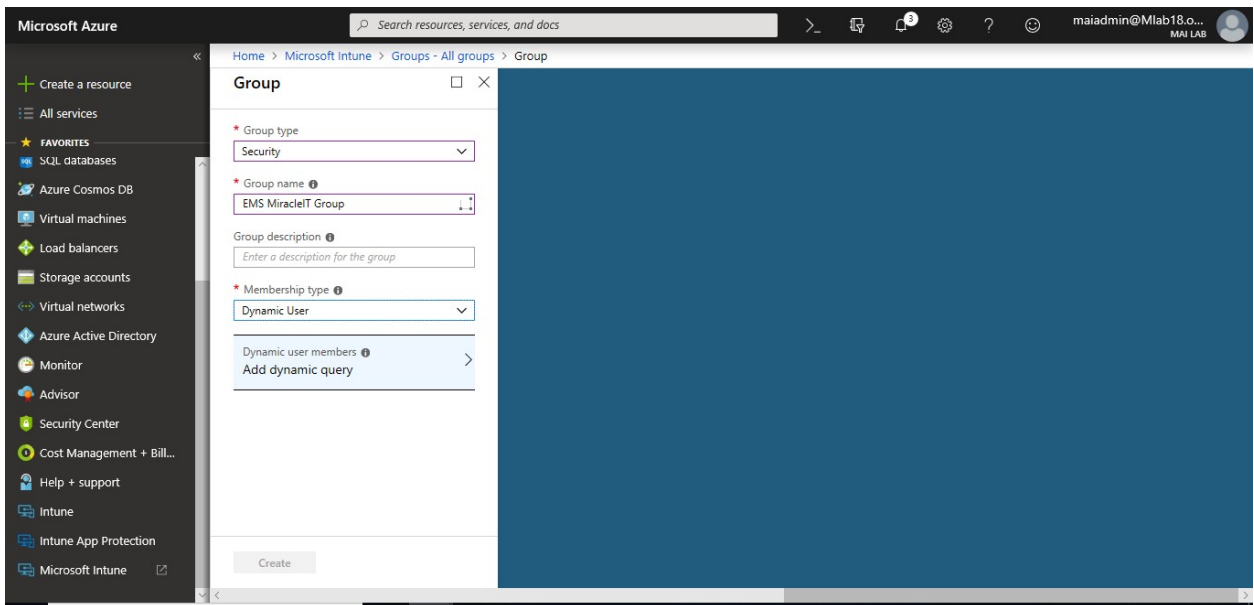
To create dynamic group to organize specific domain users, you can follow below steps

1. Sign into the [Azure portal](#). Choose **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. On the **Intune** pane, choose **Groups** and then choose **New group** in the **All groups** pane.

Microsoft Intune step by step on Azure portal

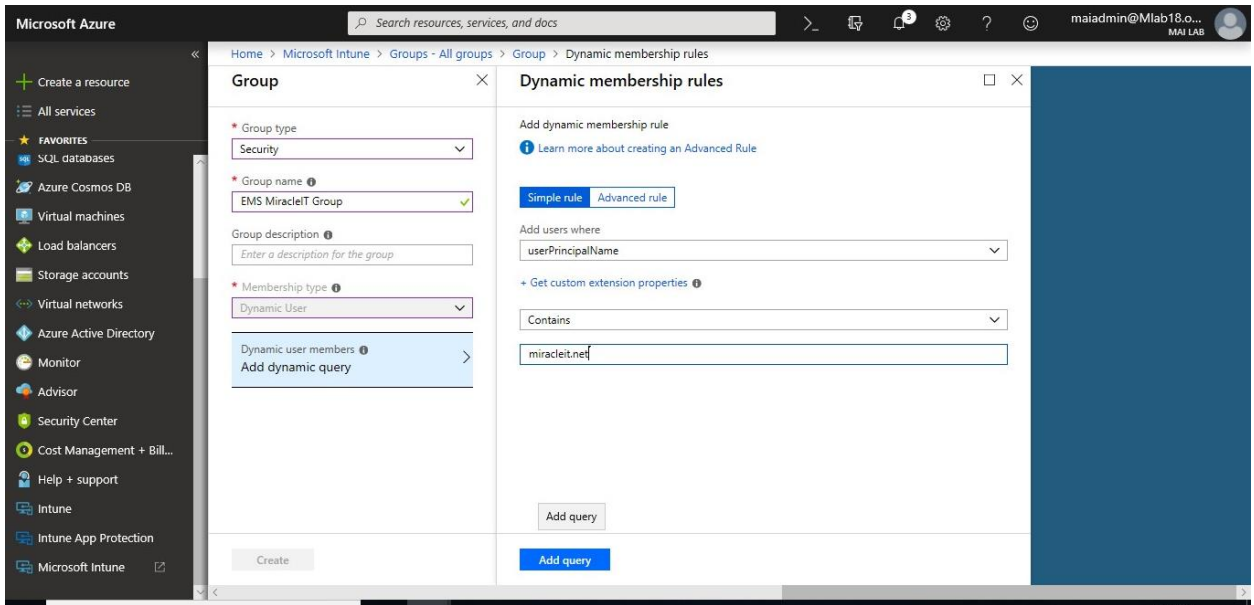


3. For **Group type** “Security”. Type a **Name** and **Description** for the new group.
4. Choose **Membership type**: Dynamic user

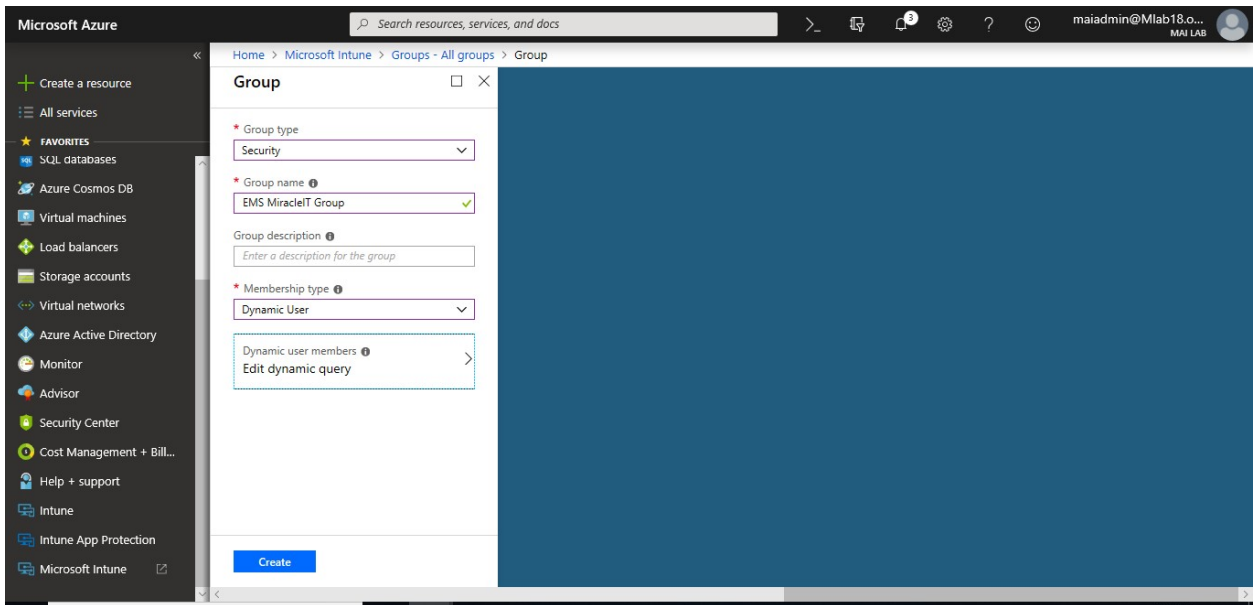


5. Select **Add dynamic query**, add dynamic membership rule that you want. On this lab, we need to add all users for domain miracleit.net.

Microsoft Intune step by step on Azure portal

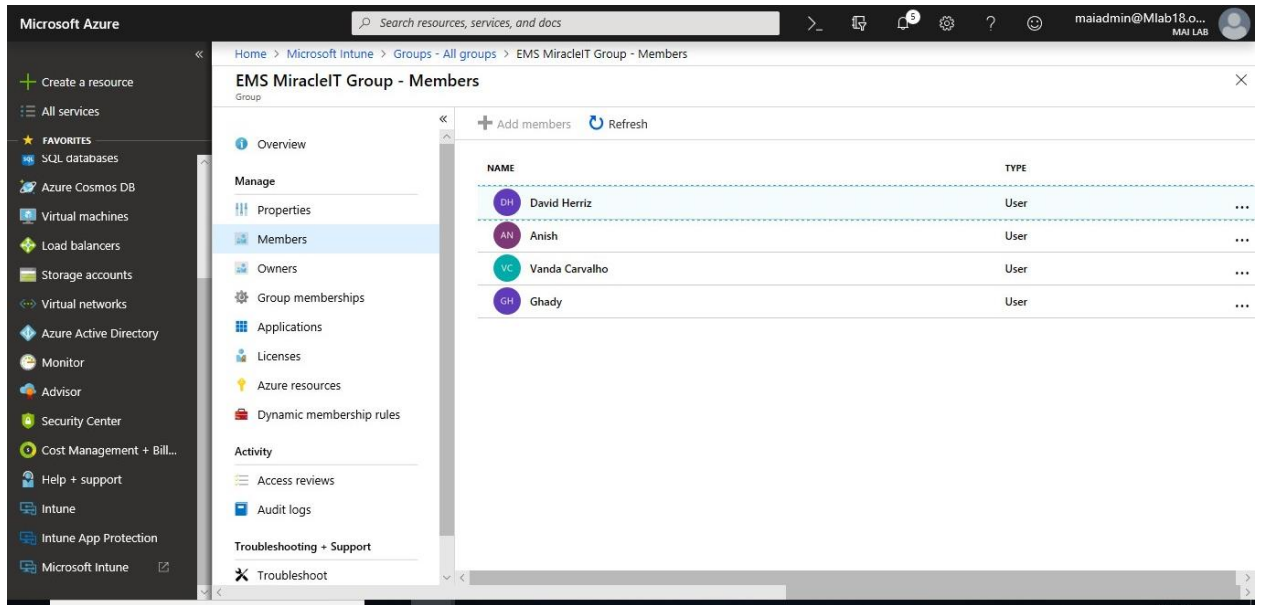


6. Choose Create to add the new group.



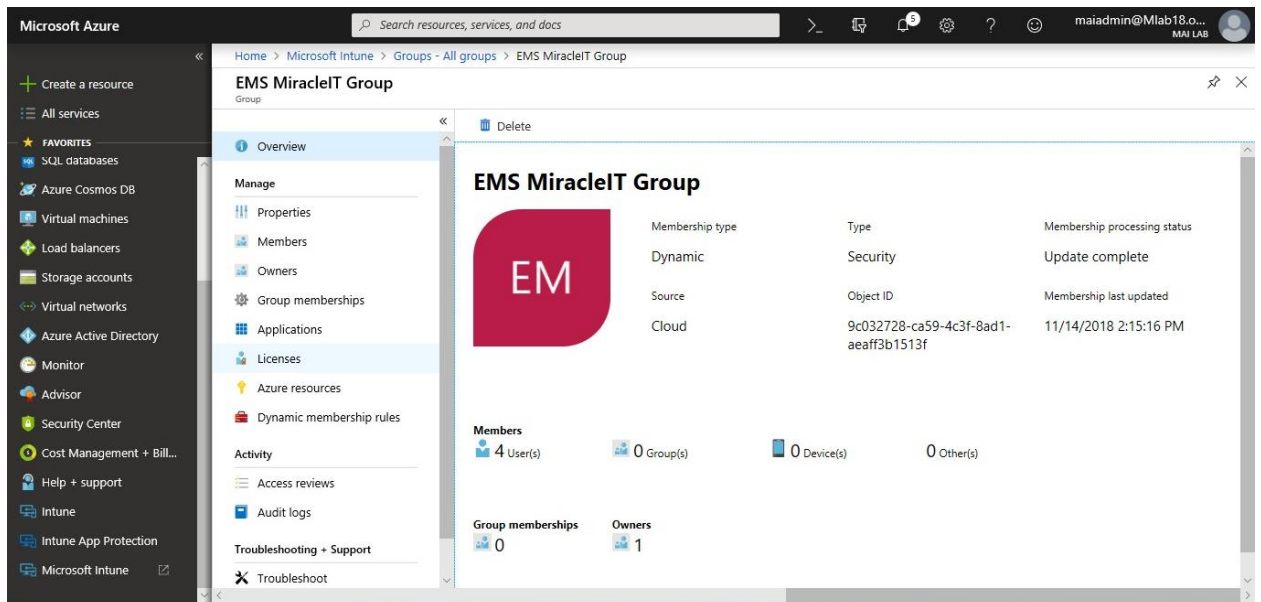
7. After 5-10 min. Members add automatic on this group.

Microsoft Intune step by step on Azure portal



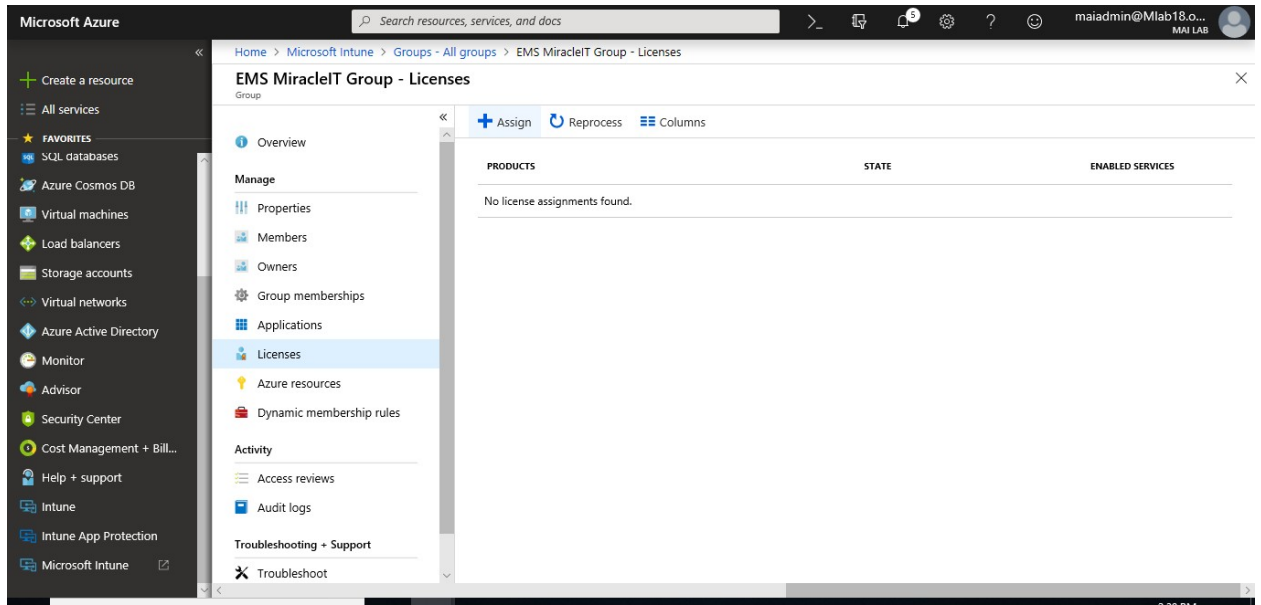
To automatic assign Enterprise Mobility + Security licenses to specific group, you can follow below steps:

1. Sign into the [Azure portal](#). Choose **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. On the **Intune** pane, choose **Groups** and Select group that you want to assign license to it automatic.

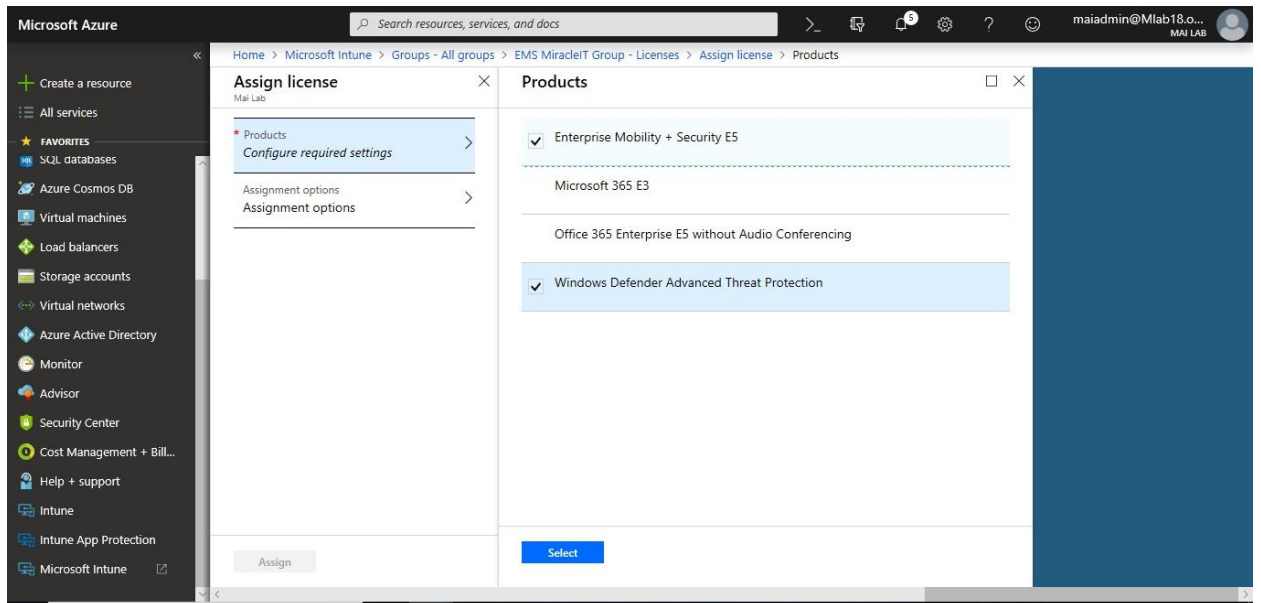


3. Select **licenses** on left pane, then Click **Assign**.

Microsoft Intune step by step on Azure portal



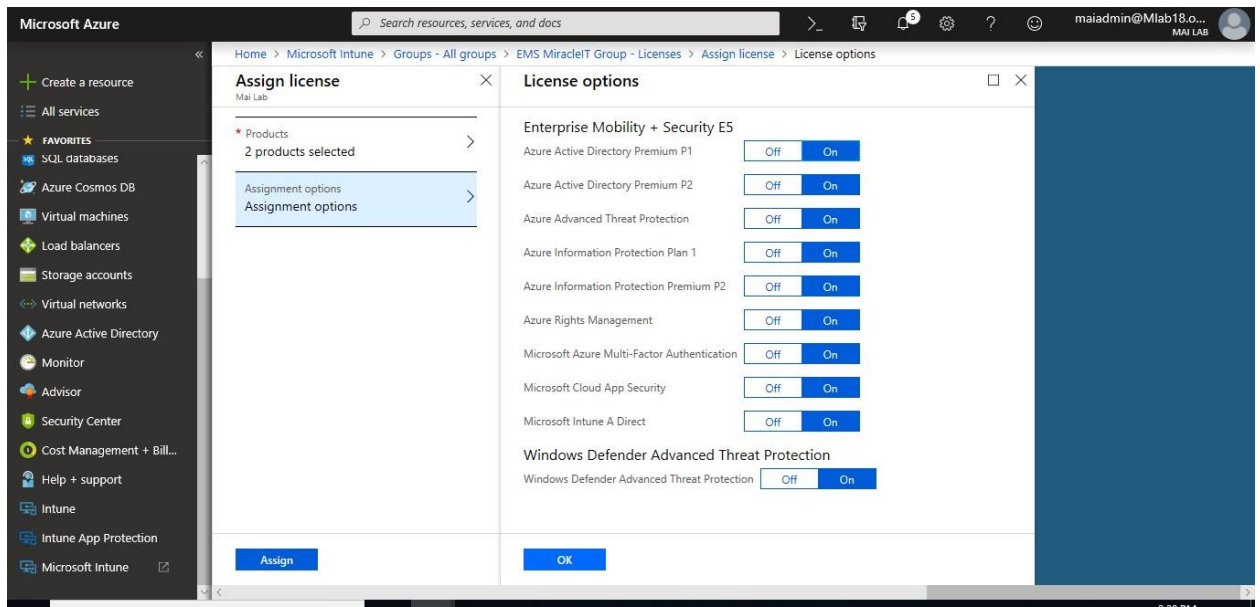
4. Select **Products**, Check on licenses that you want to assign.



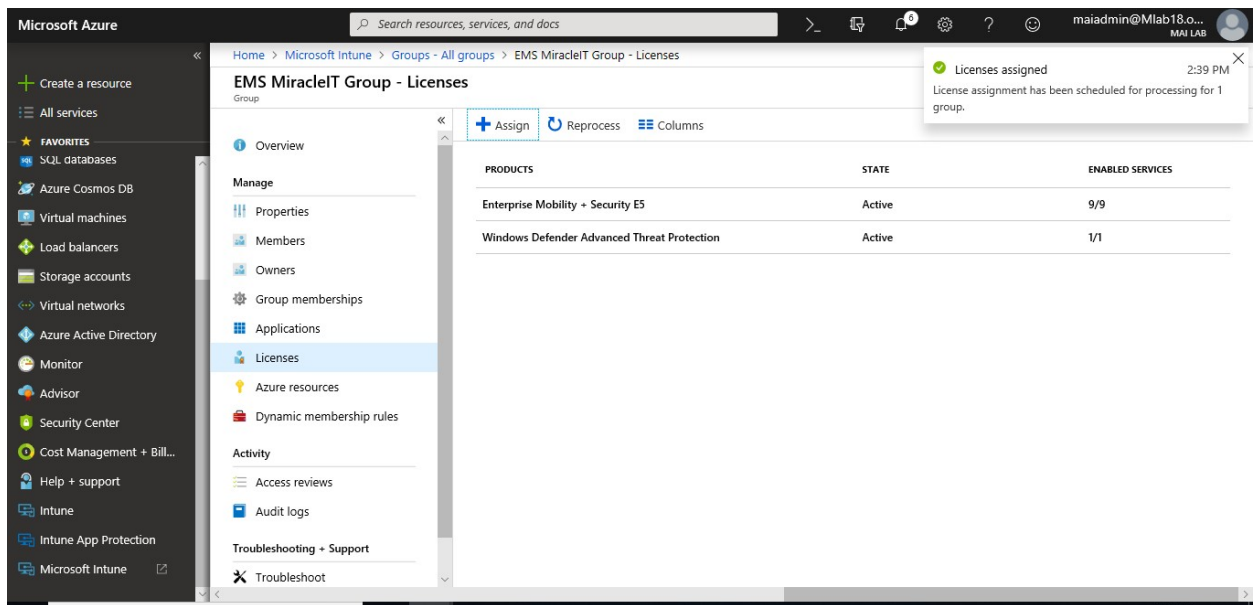
5. Select **Assignment options**, select all licenses option that you want. Turn ON/OFF license options won't affect on the product licenses.

Note: for example, if you turn off license option for Azure AD premium, you won't be able to use it with another user. As **license per user count from product licenses** not from licenses options.

Microsoft Intune step by step on Azure portal



6. Once you click Assign, you will find the product license appear on portal.



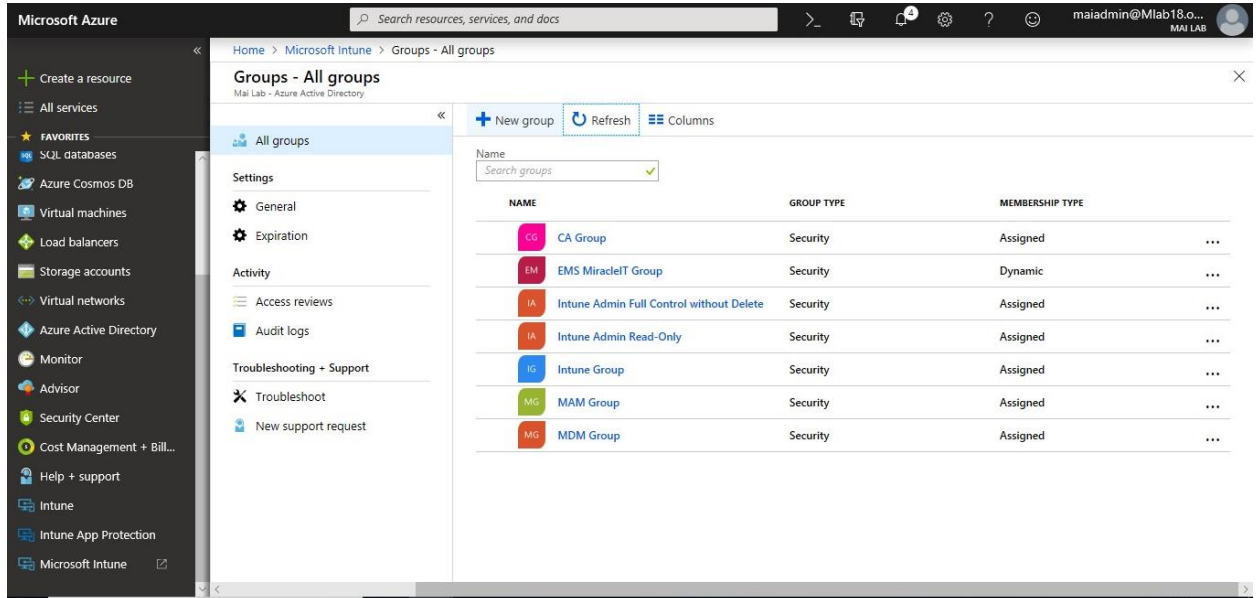
Note: If you assign licenses through group, once you remove this group, the license will be removed. You won't be able to modify license on specific user who is member of this group direct. you need to manage license through this group.

To Create Dynamic Device Group

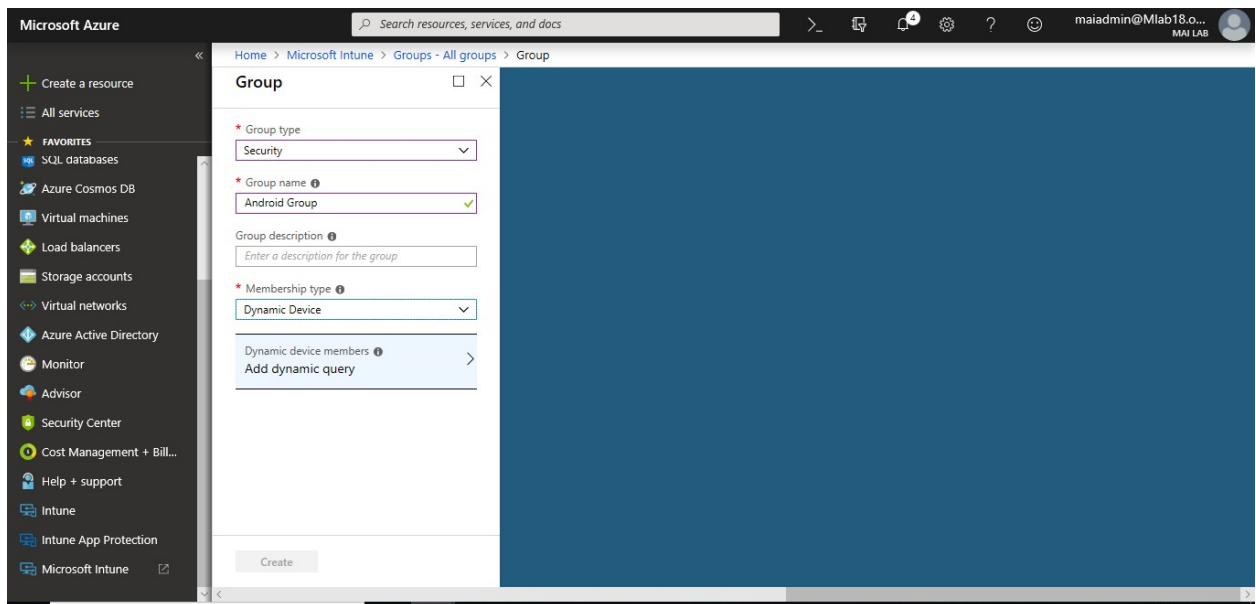
To create dynamic group to organize Android devices, you can follow below steps

1. Sign into the [Azure portal](#). Choose **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.

2. On the **Intune** pane, choose **Groups** and then choose **New group** in the **All groups** pane.

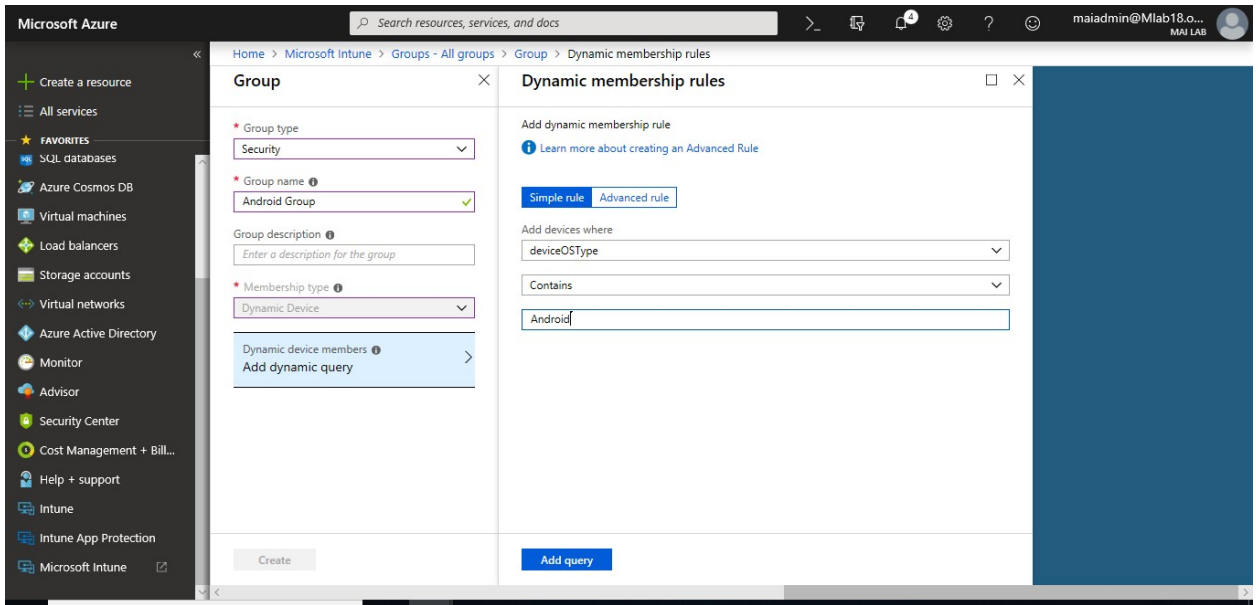


3. For **Group type** “Security”. Type a **Name** and **Description** for the new group.
4. Choose **Membership type**: Dynamic Device

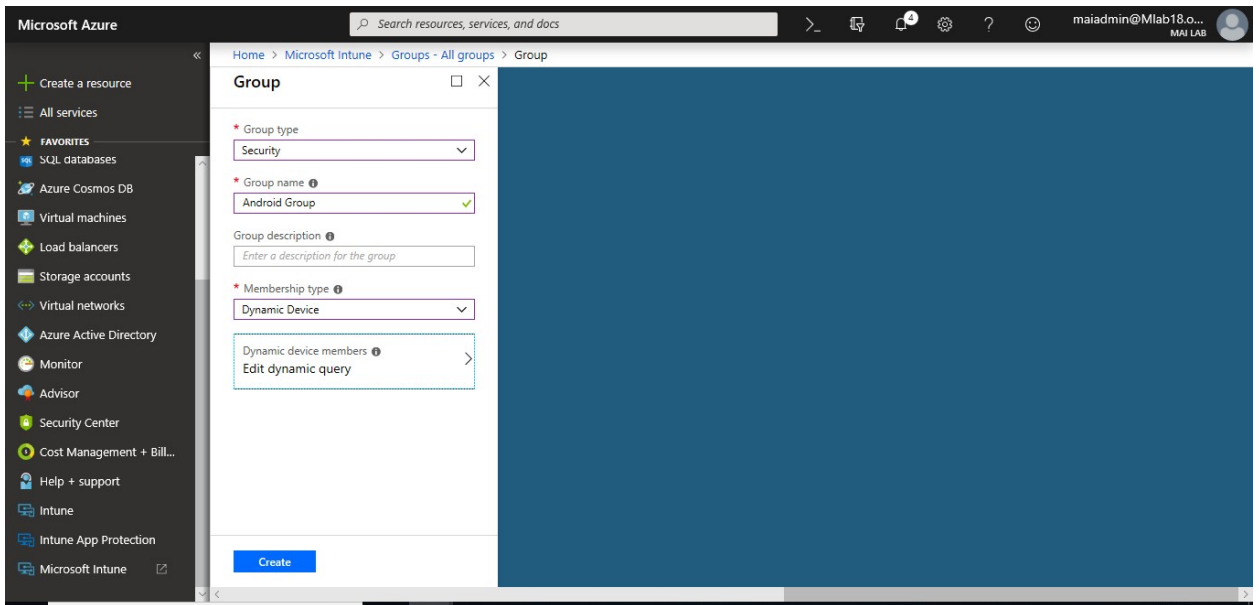


5. Select **Add dynamic query**, add dynamic membership rule that you want. On this lab, we need to add all Android devices.

Microsoft Intune step by step on Azure portal

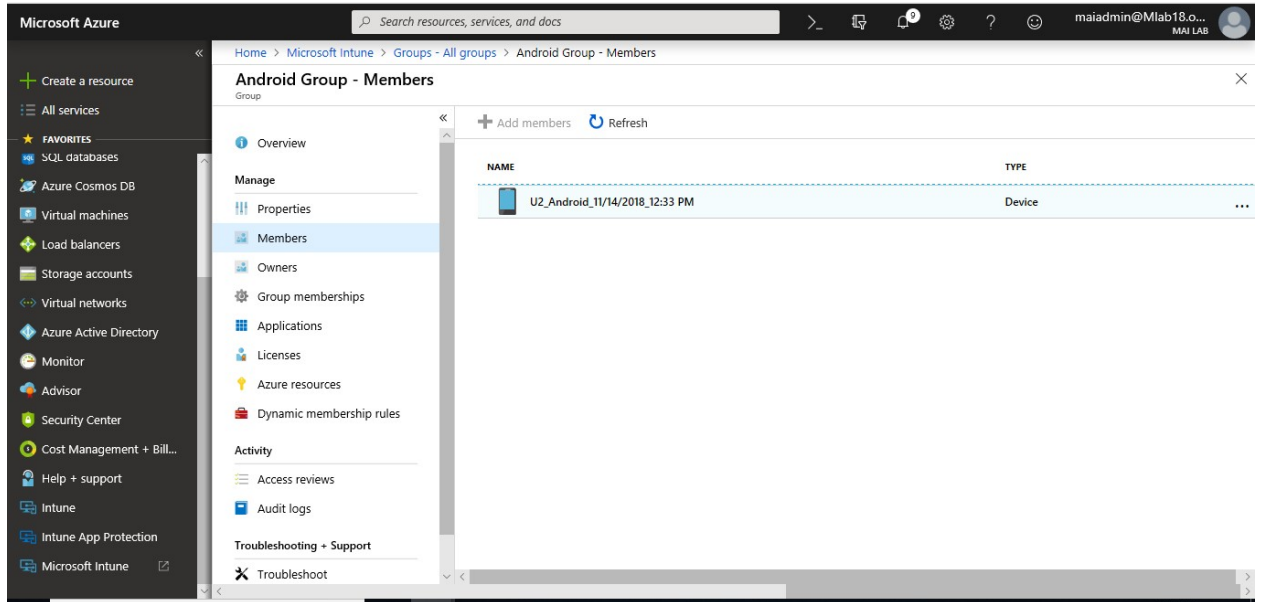


6. Choose Create to add the new group.



7. After 5-10 min. Members add automatic on this group

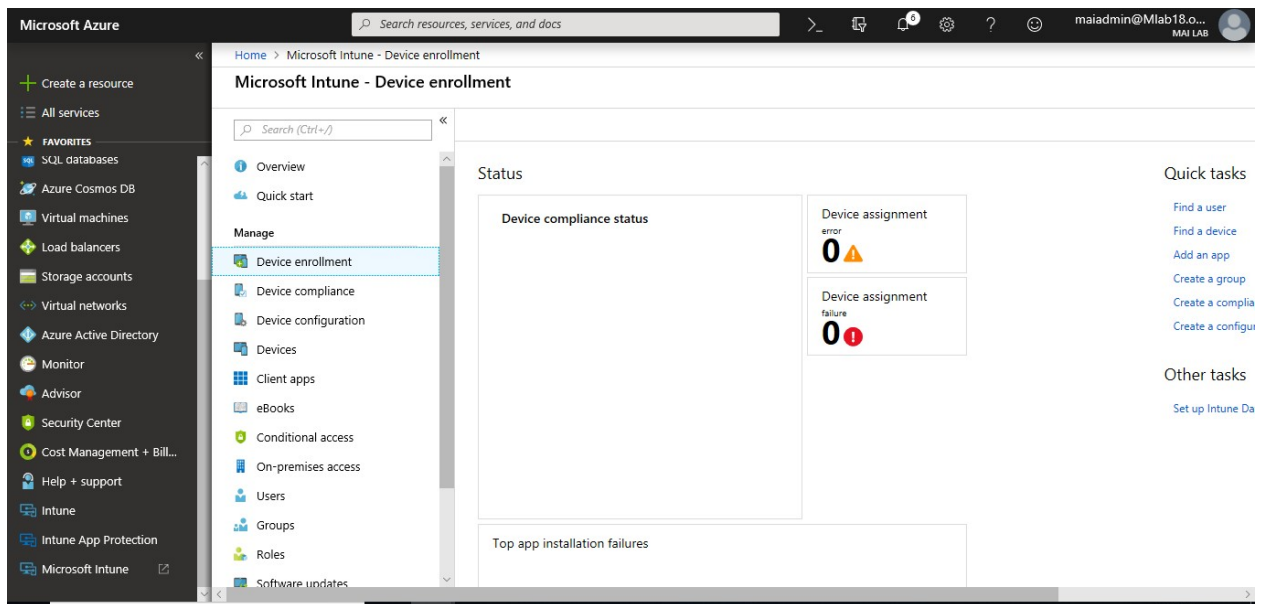
Microsoft Intune step by step on Azure portal



Configure Device Categories

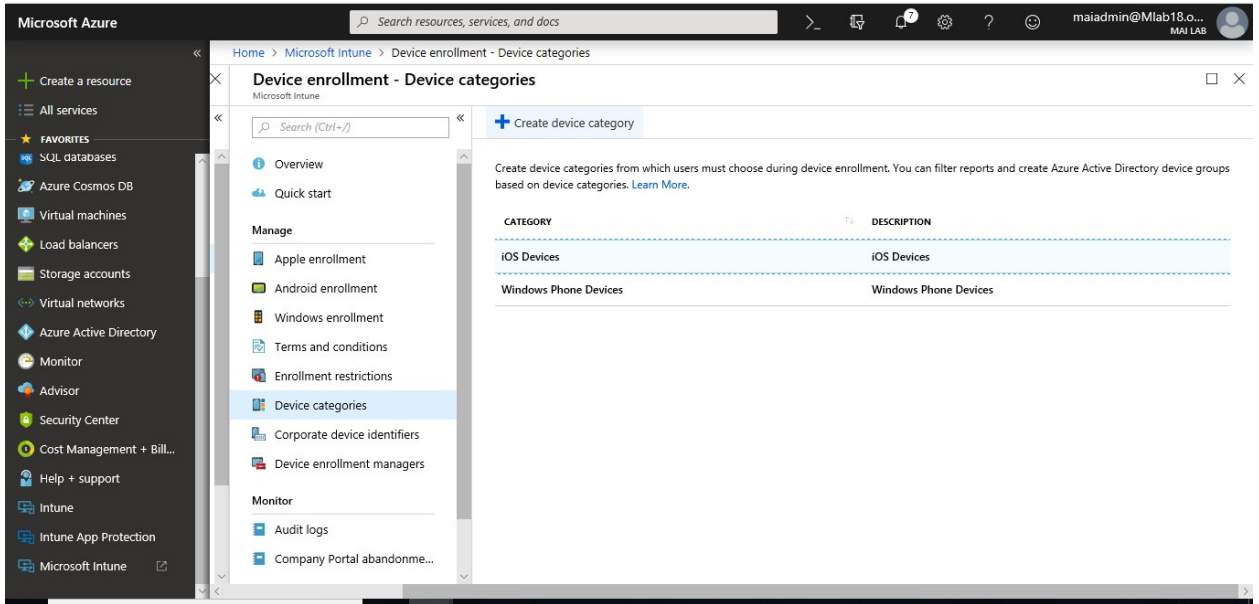
To Create device categories on the Intune blade of the Azure portal, you can follow below steps:

1. Sign into the [Intune portal](#), choose **Device enrollment**.

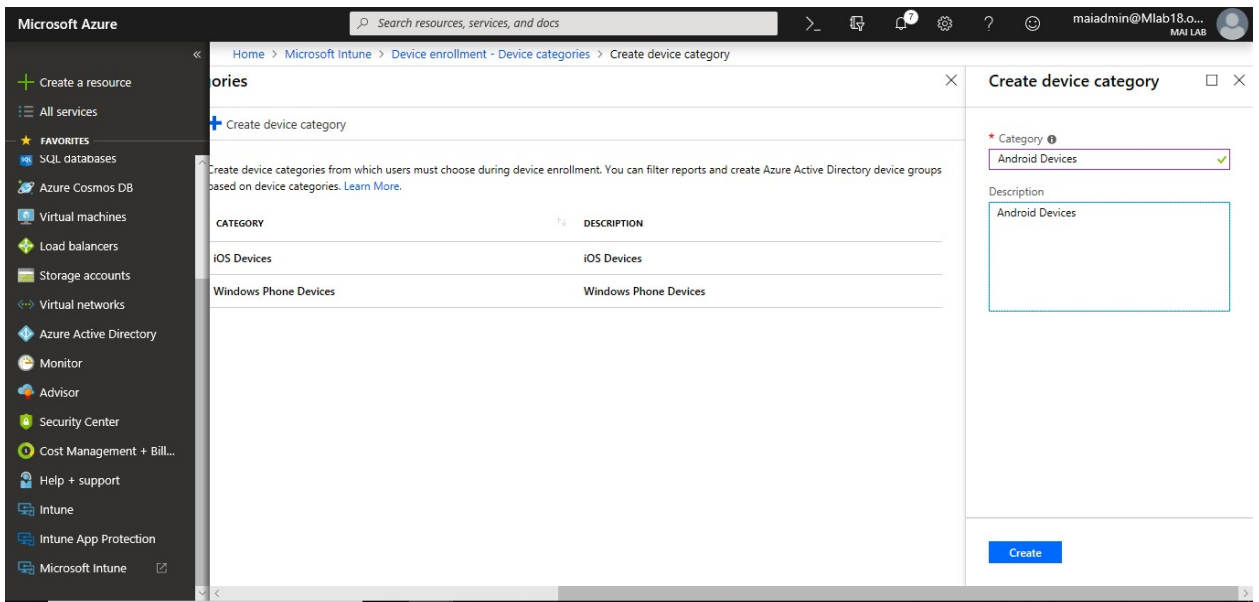


2. On the **Device enrollment** blade, choose **Device categories**.
3. On the **Device categories** page, choose **Create** to add a new category.

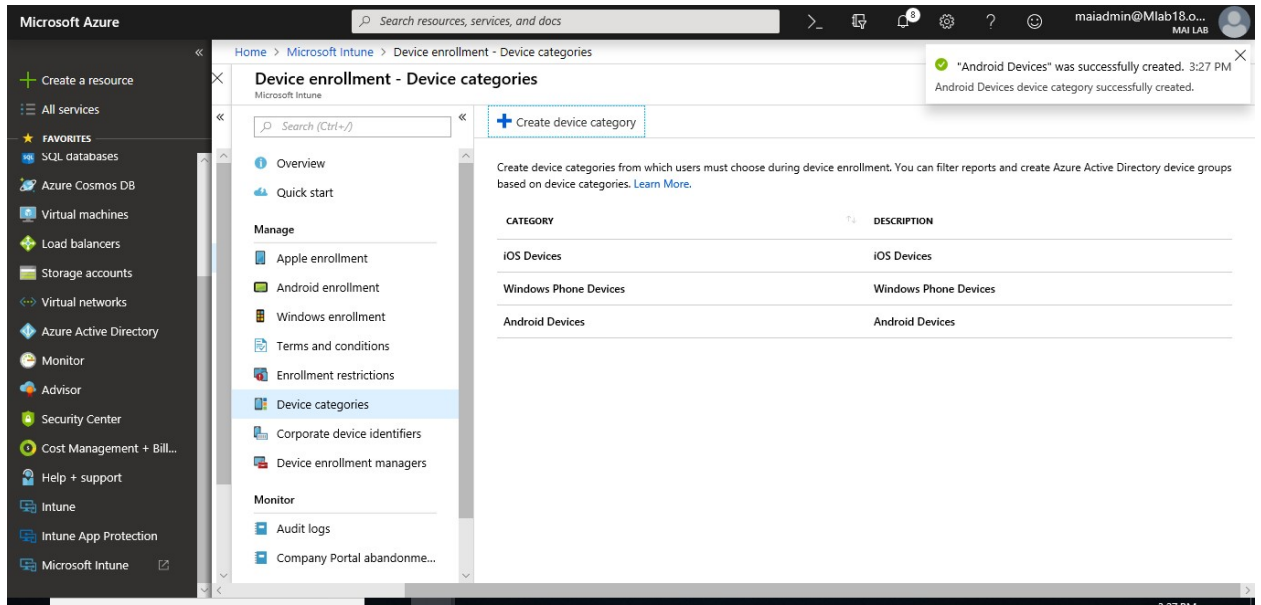
Microsoft Intune step by step on Azure portal



4. On the **Create device category** blade, enter a **Name** for the new category, and an optional **Description**. When you are done, select **Create**.



5. You can see the new category in the list of categories.



Device Enrollment Manager

You can enroll up to 1,000 mobile devices with a single Azure Active Directory account by using a device enrollment manager (DEM) account.

Limitations of devices that are enrolled with a DEM account

DEM user accounts and devices that are enrolled with a DEM user account have the following limitations:

- Wipe can't be done from the Company Portal. Wiping a device enrolled by a DEM user account can be done from the Intune in Azure portal.
- Only the local device appears in the Company Portal app or website.
- DEM user accounts can't use Apple Volume Purchase Program (VPP) apps with Apple VPP user licenses because of per-user Apple ID requirements for app management.
- Devices can install VPP apps if they have Apple VPP device licenses.
- Devices are blocked for Conditional Access with the exception of Windows 10 1803+

Permissions for DEM

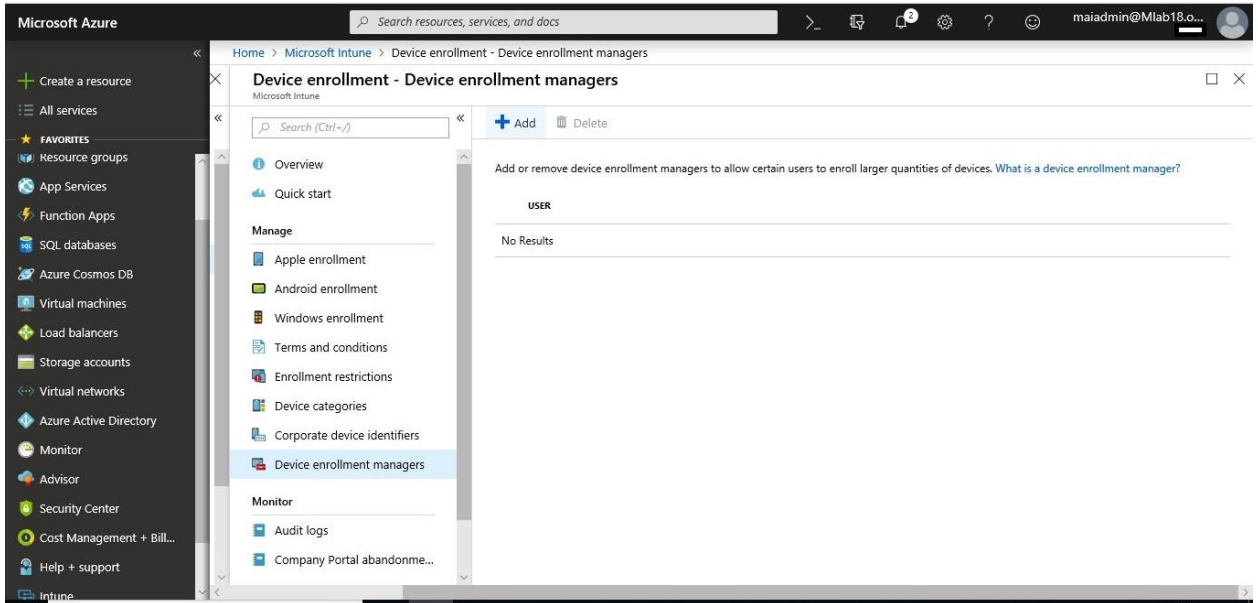
Global Administrator or Intune Service Administrator Azure AD roles are required to

- assign DEM permission to an Azure AD user account
- see all DEM users

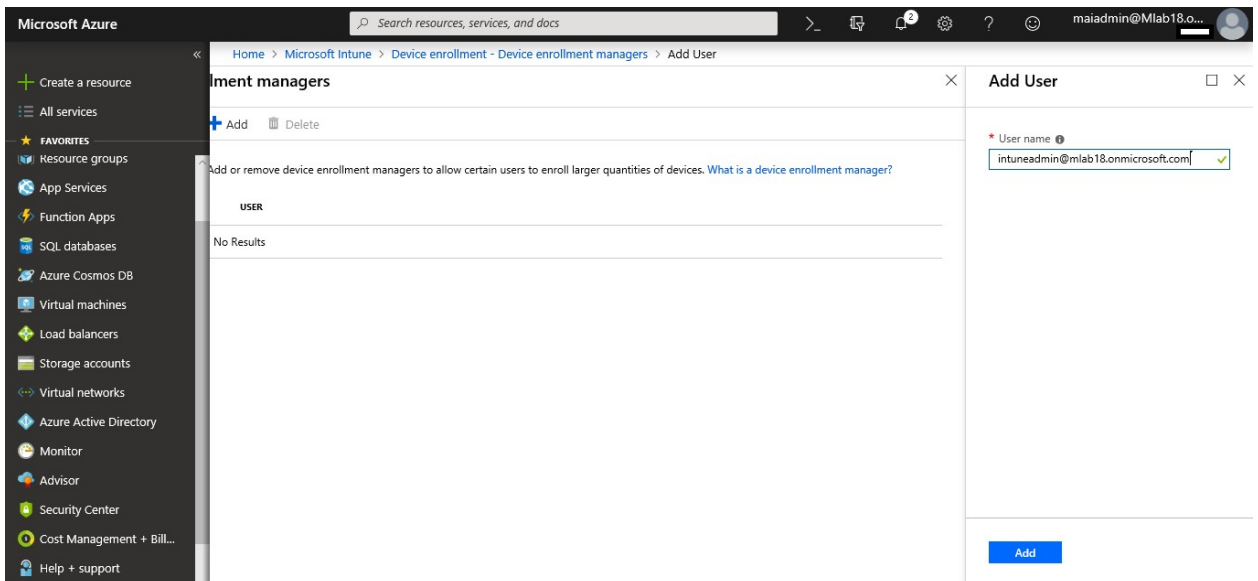
If a user doesn't have the Global Administrator or Intune Service Administrator role assigned to them but has read permissions enabled for the Device Enrollment Managers role assigned to them, they can see only the DEM users they've created.

Assign Device Enrollment Manager to enroll Microsoft Intune

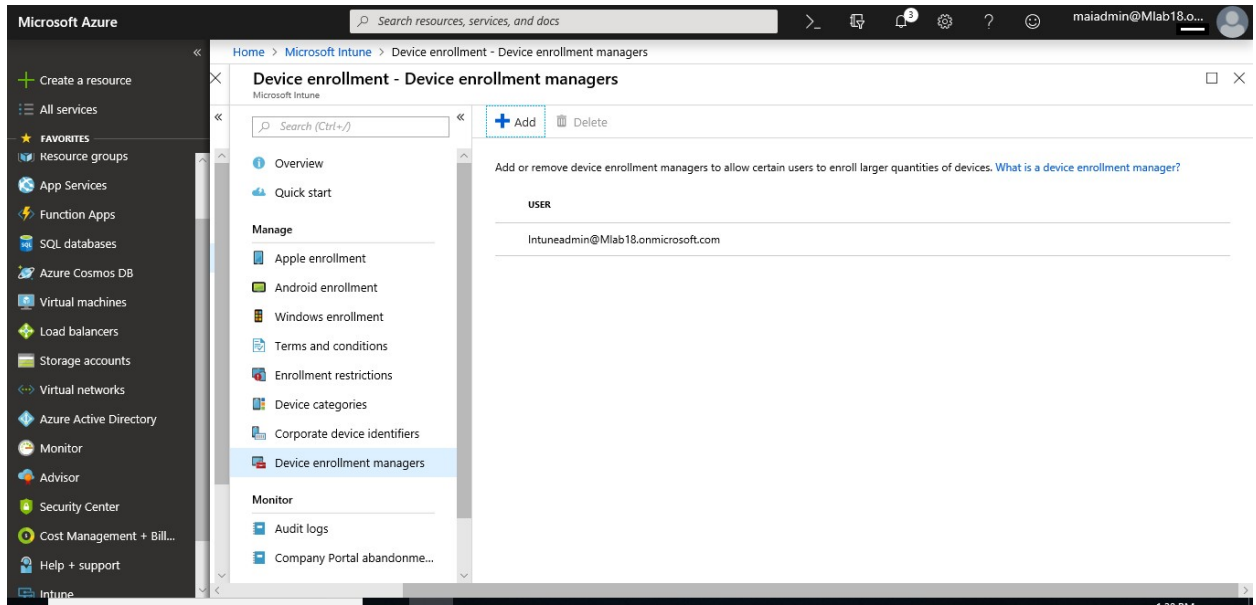
1. Sign into the [Intune portal](#), choose **Device enrollment** > **Device enrollment managers**. Then select **Add**.



2. On the **Add User** blade, enter a user principal name for the DEM user, and select **Add**.



3. The DEM user is added to the list.



Assign Additional Administrators to manage Microsoft Intune

Administrator roles are common between the different Microsoft cloud services although some services might not support some roles. Intune uses the following roles:

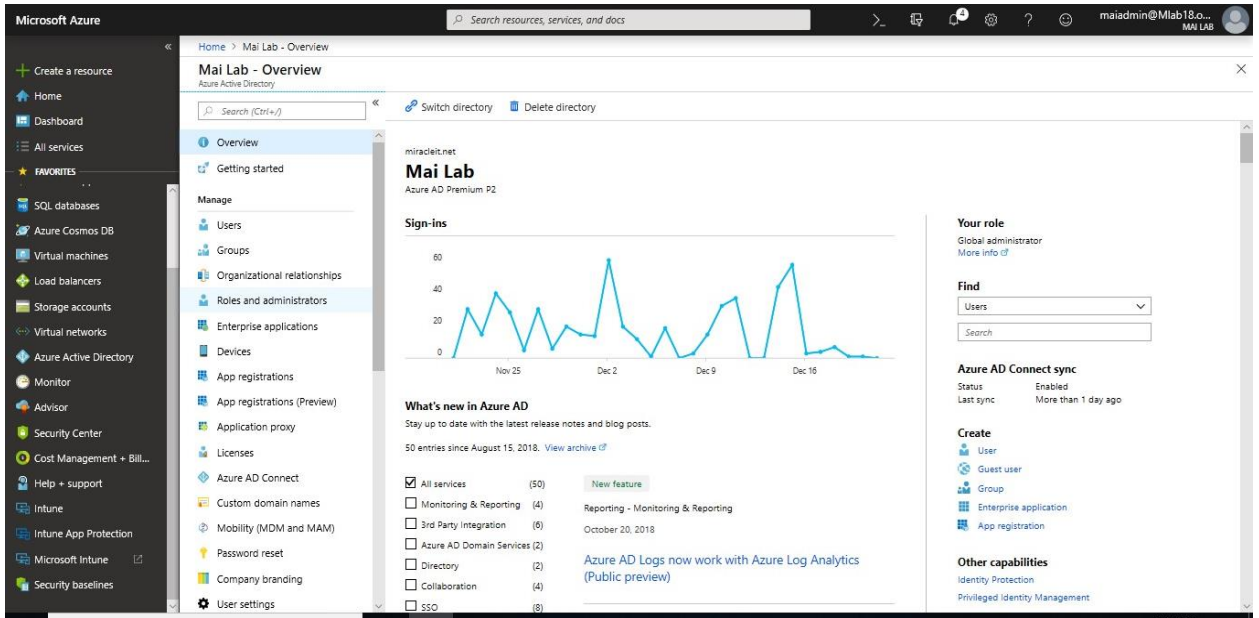
- **Global administrator:** Users with this role have access to all administrative features in Azure AD & all Cloud services.
- **Intune Service administrator:** Users with this role have global permissions within Intune
- **Conditional Access Administrator:** Users with this role only have permissions to view, create, modify, and delete conditional access policies

Note: The Intune Service Administrator role does not provide the ability to manage Azure AD's conditional access settings. Members of Intune roles require an Intune license.

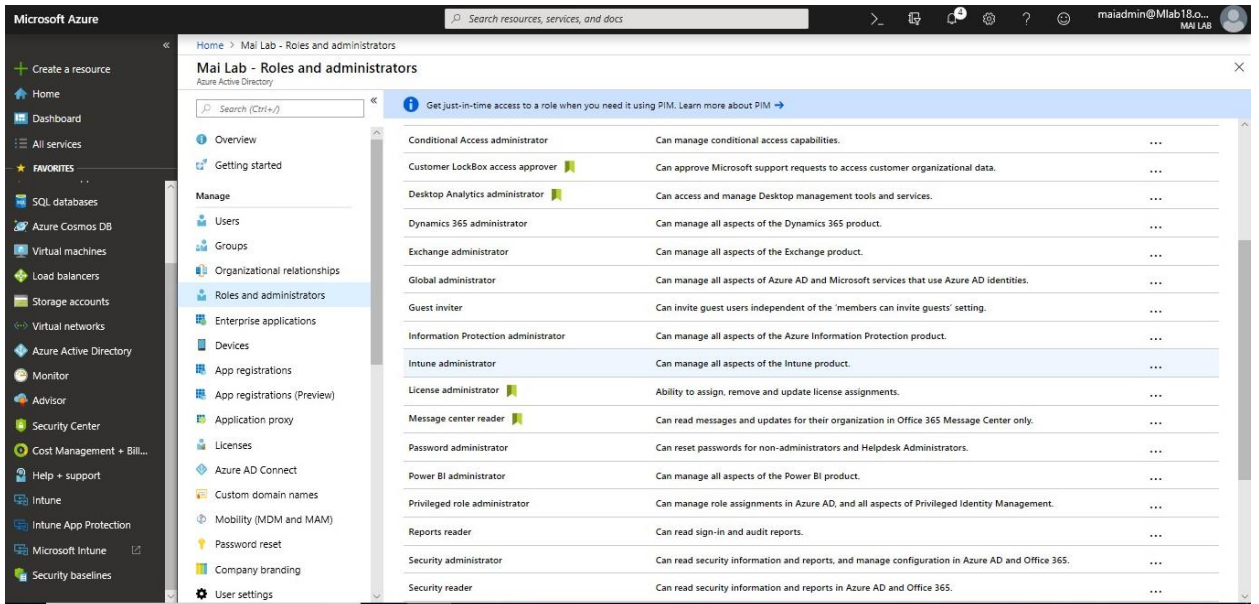
To add user on Intune admin role, you need to follow below steps:

1. Sign in to the [Azure portal](#) using a Global administrator account for the directory. Select **Azure Active Directory**

Microsoft Intune step by step on Azure portal

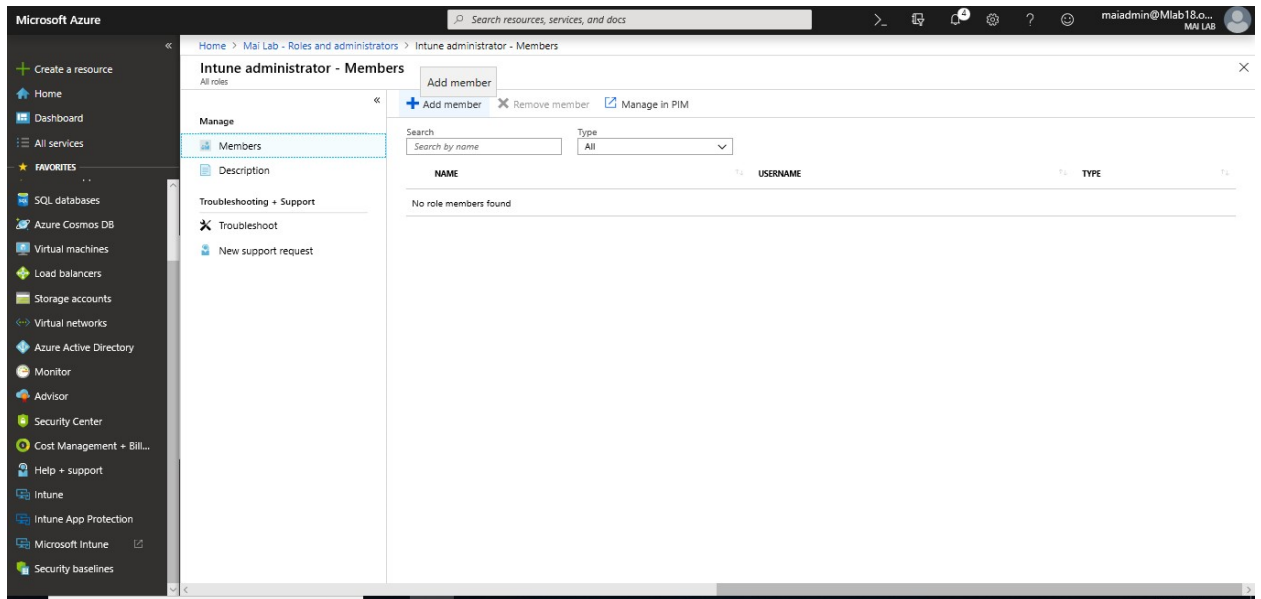


2. Click **Roles and Administrators**, then Select **Intune Administrator**.

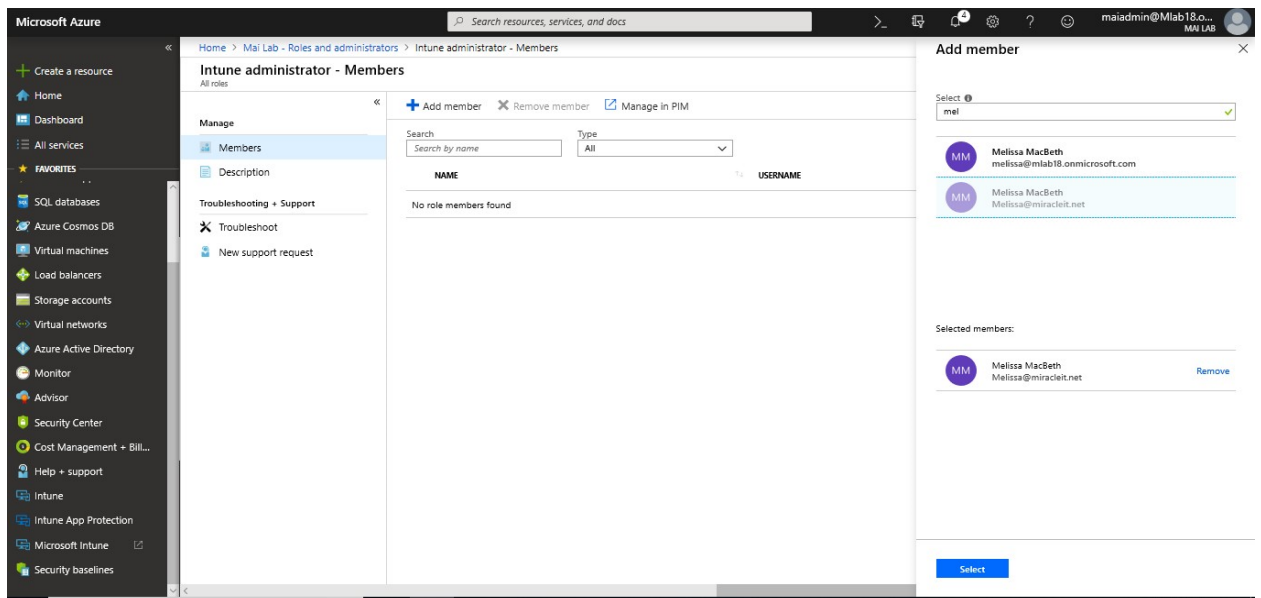


3. On **Intune Administrator** Blade, select **Add member**.

Microsoft Intune step by step on Azure portal



4. Type the user that you want to provide him administrator role for Intune, click **Select**.



5. Now user add to be member for Intune Administrator.

Role-based administration control (RBAC) with Microsoft Intune

RBAC helps you control who can perform various Intune tasks within your organization, and who those tasks apply to. You can either use the built-in roles that cover some common Intune scenarios, or you can create your own roles. A role is defined by:

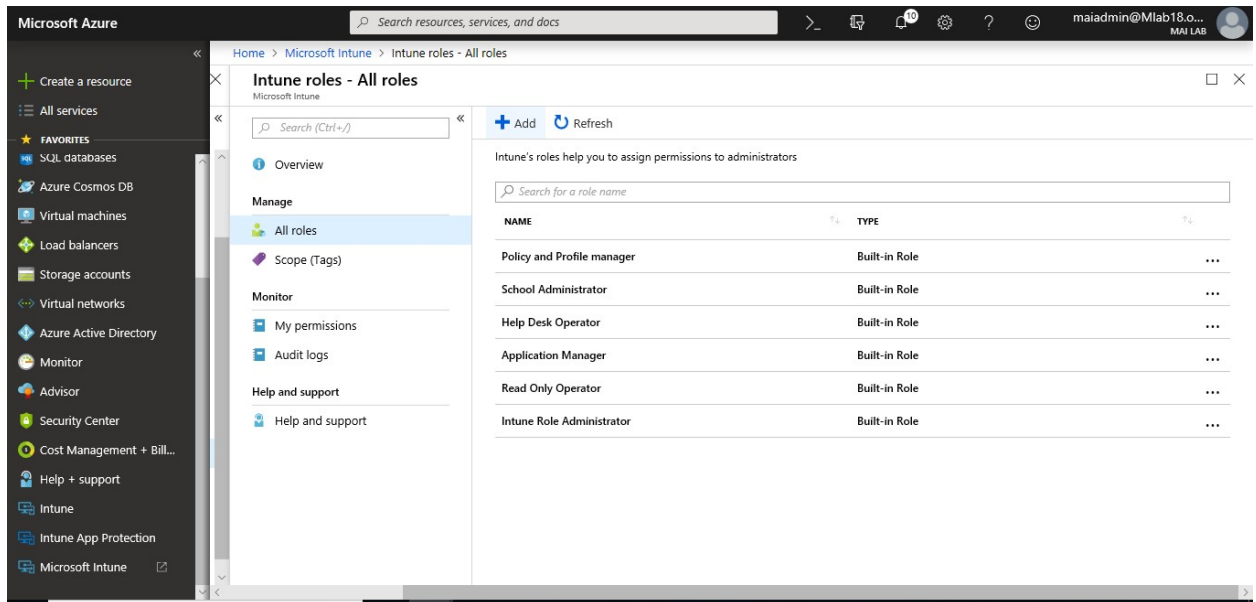
- **Role definition:** The name of a role, the resources it manages, and the permissions granted for each resource.

Microsoft Intune step by step on Azure portal

- **Members:** The user groups that are granted the permissions.
- **Scope:** The user or device groups that the members can manage.
- **Assignment:** When the definition, members, and scope have been configured, the role is assigned.

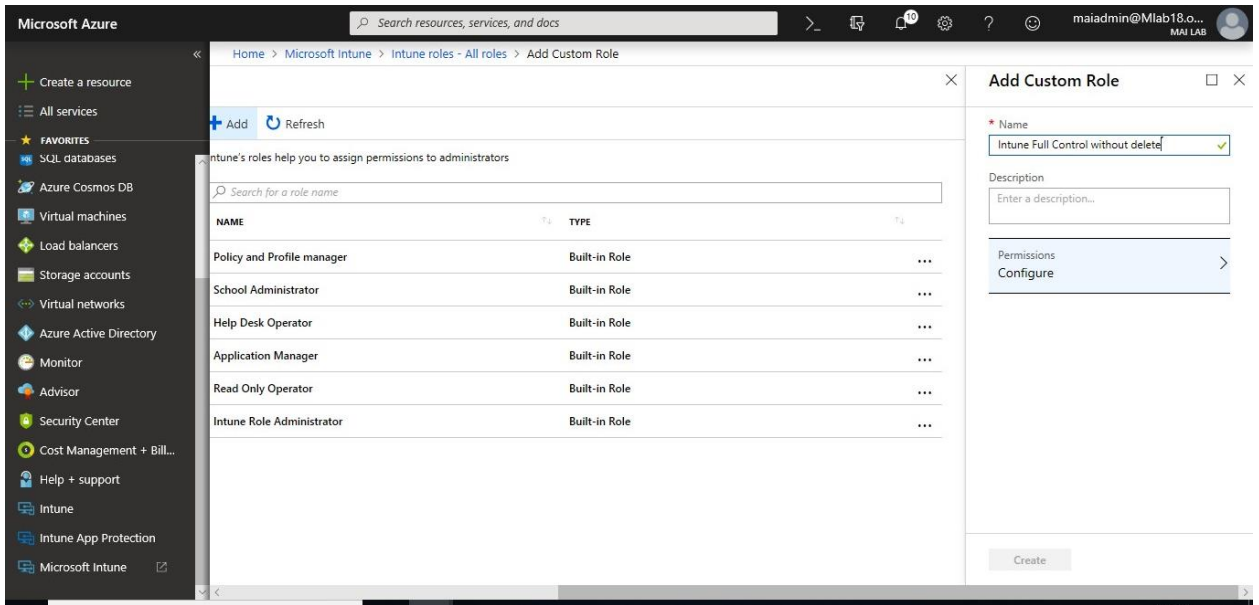
To create a custom role

1. Sign into the [Azure portal](#). Choose **All services** from the left menu, then type **Intune** in the text box filter.
2. Choose **Intune** > **Intune Roles** > **All roles** > **Add**.

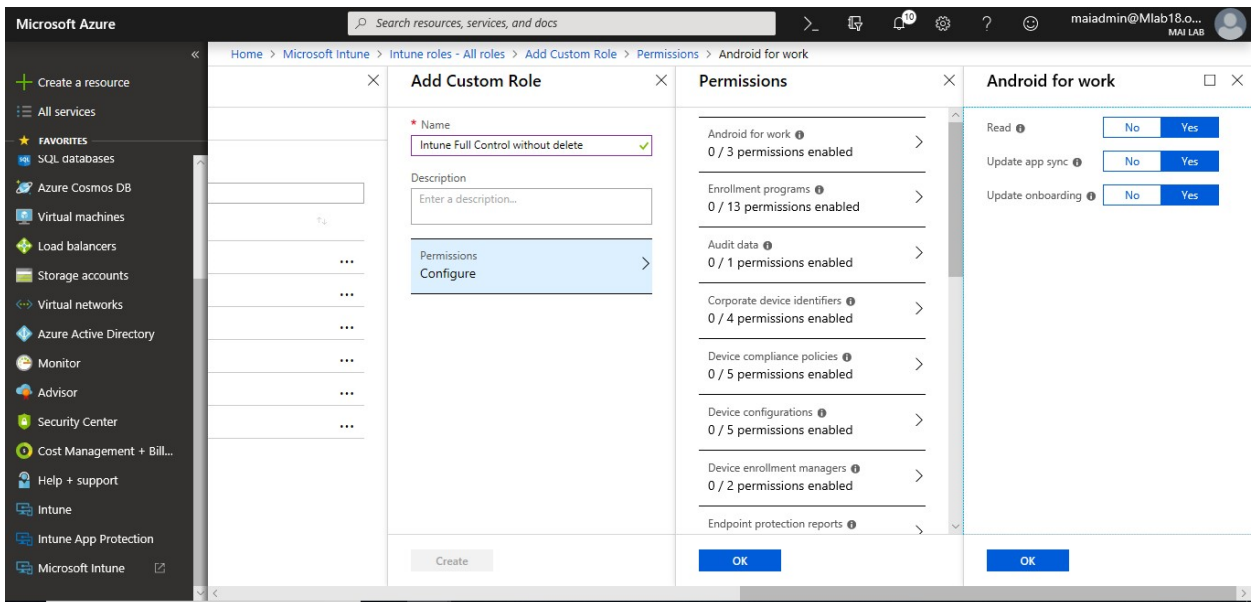


3. On the **Add Custom Role** pane, enter a name and description for the new role, then click **Permissions**.

Microsoft Intune step by step on Azure portal

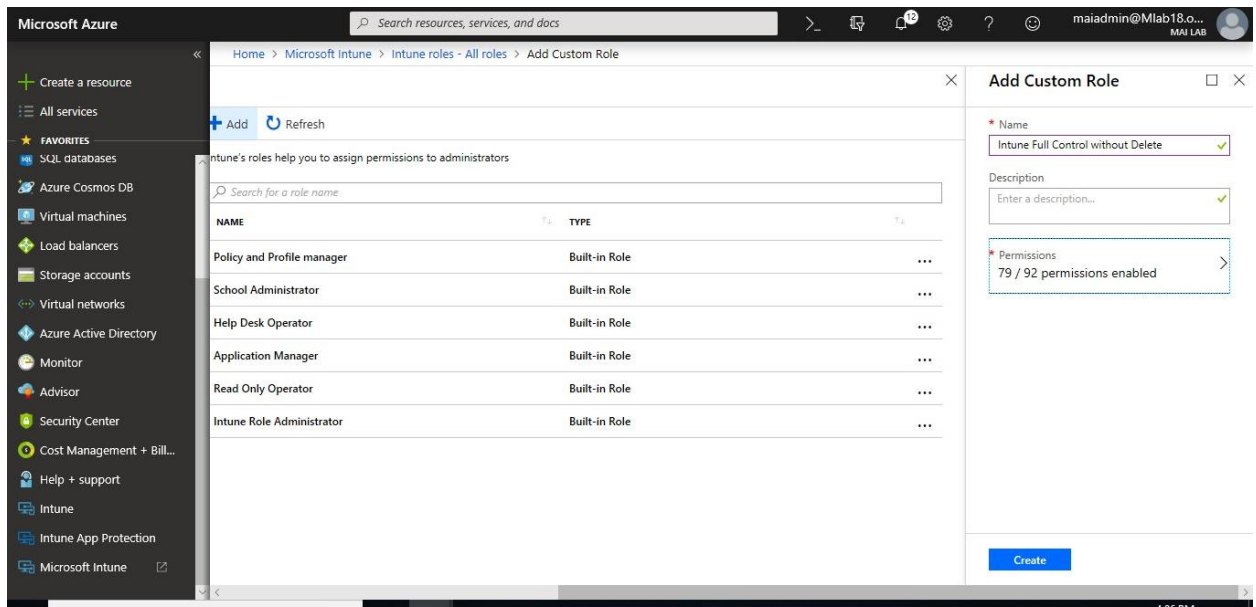


4. On the **Permissions** pane, choose the permissions you want to use with this role.
5. When you are done, choose **OK**.

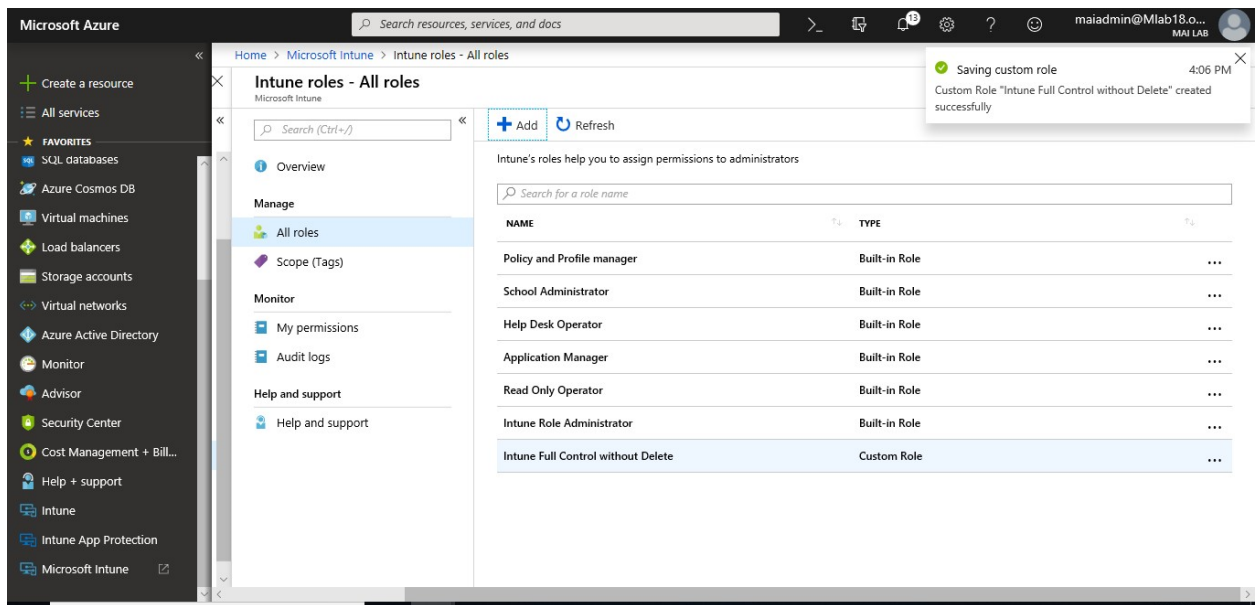


6. On the **Add Custom Role** pane, click **Create**.

Microsoft Intune step by step on Azure portal

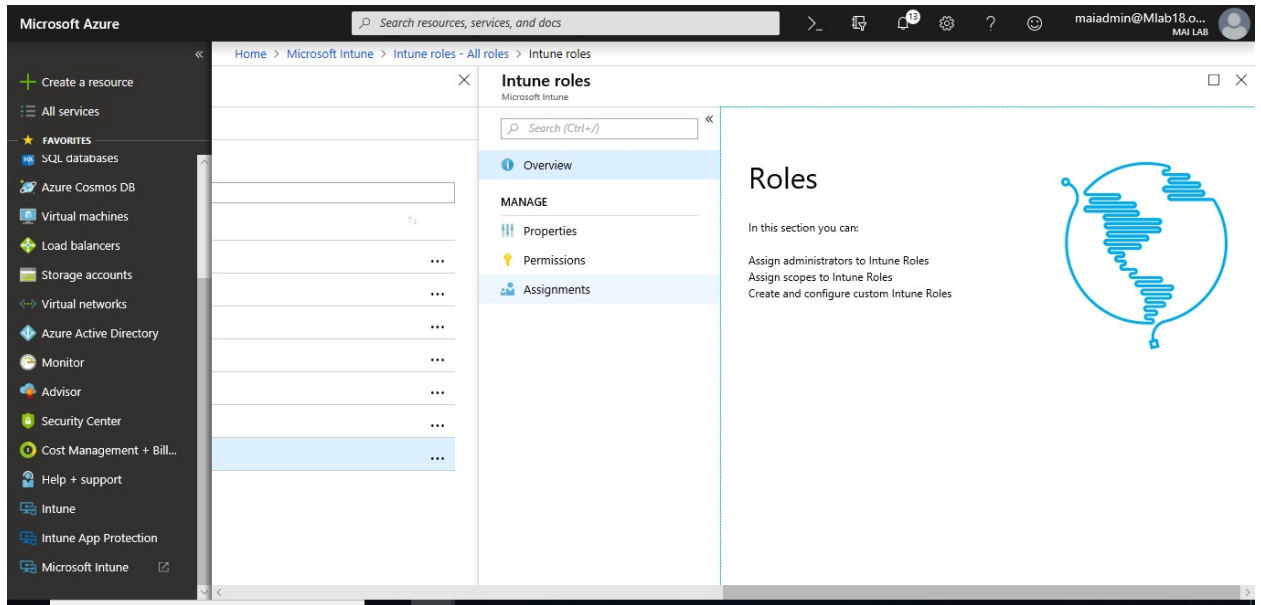


7. The new role is displayed in the list on the **Intune roles - All roles** pane.

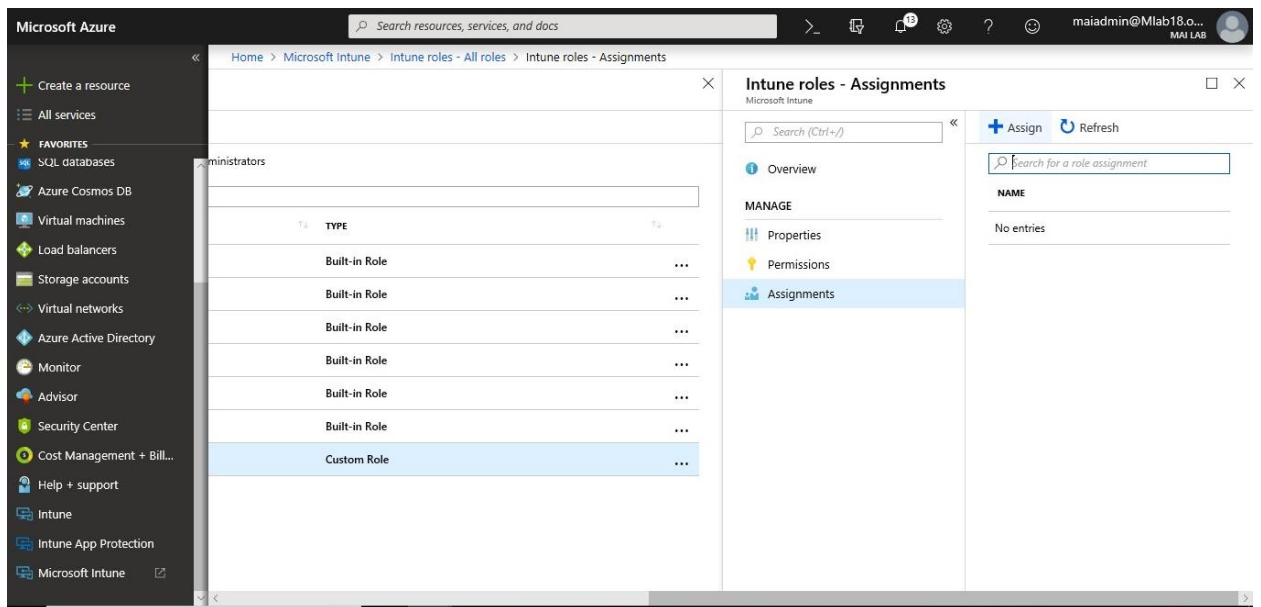


To assign a custom role

1. On the **Intune roles - All roles** pane, choose the custom role you want to assign.
2. On the <role name> - **Overview** pane, choose **Manage**, then **Assignments**.

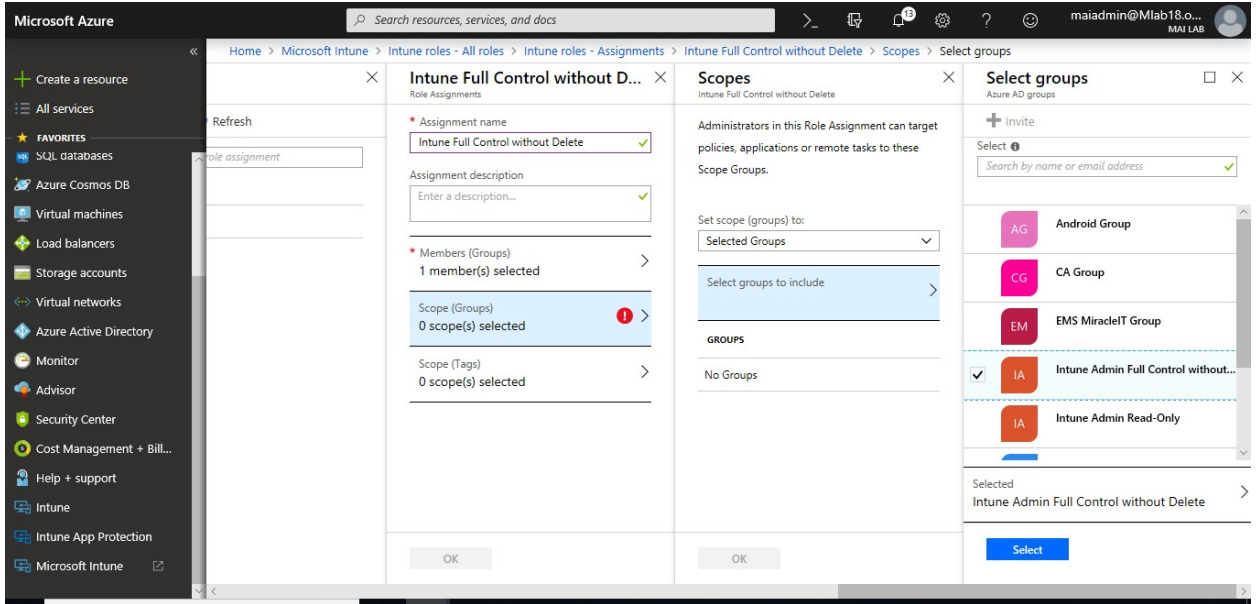


3. On the custom role pane, choose **Assign**.



4. On the **Role Assignments** pane, enter a **Name** and optional **Description** for the assignment, and then choose the following:

- **Members** - Select a group that contains the user you want to give the permissions to.
- **Scope** - Select a group containing the users who the member above will be allowed to manage.



5. When you are done, click **OK**. The new assignment is displayed in the list of assignments.

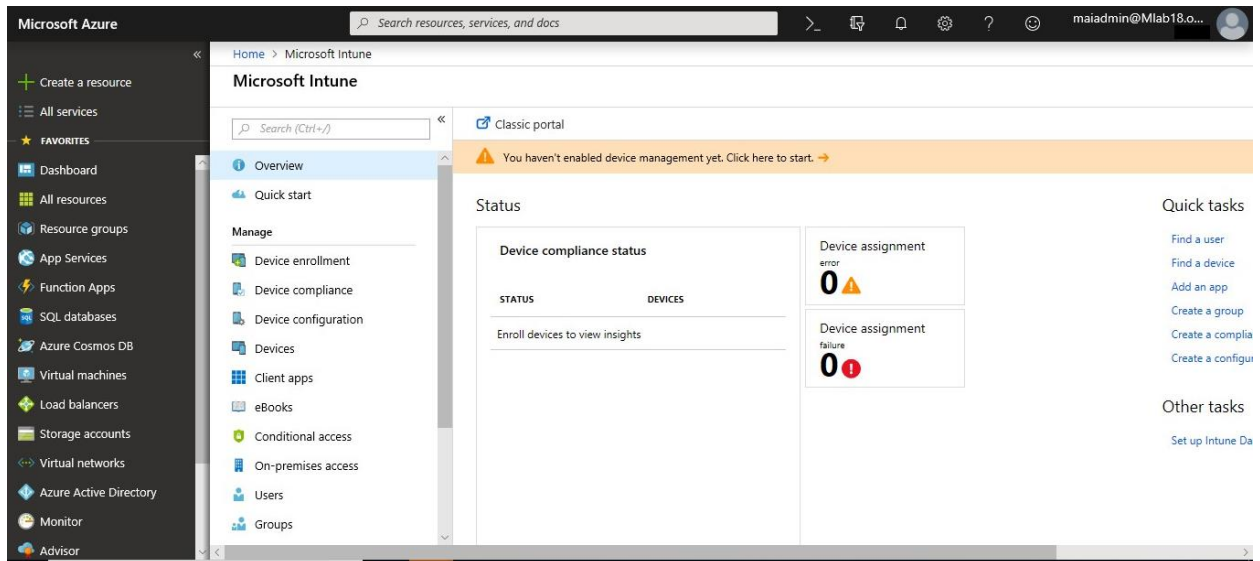
Chapter 4

Mobile Devices Management (MDM) Authority

Set Mobile Device Management Authority

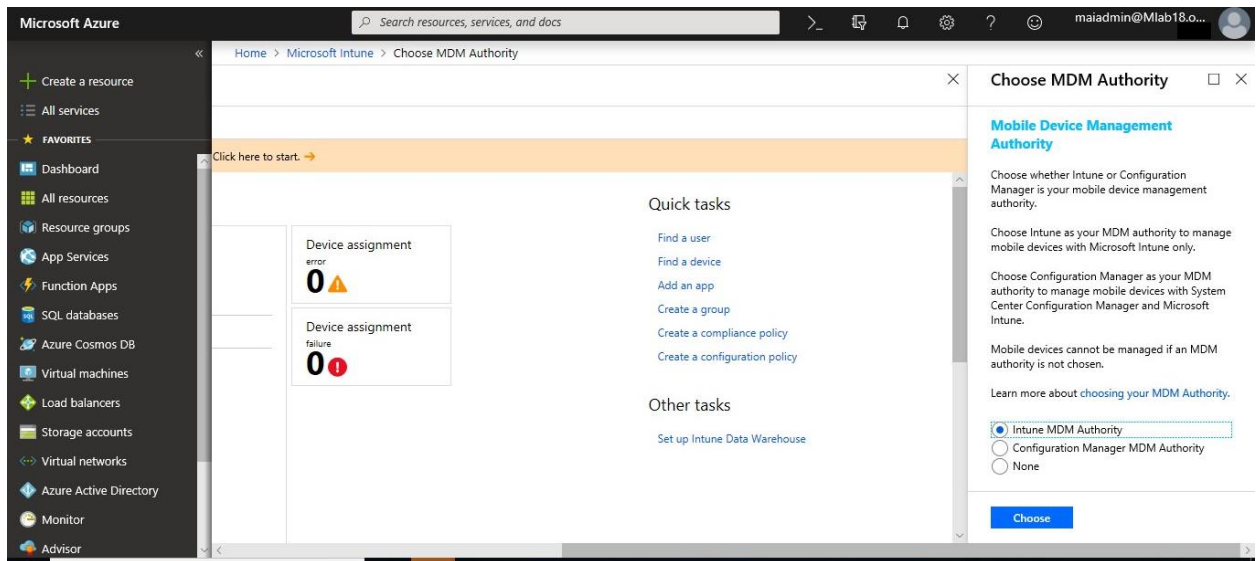
To Set Mobile Device Management Authority, you can follow below steps

1. Sign into the [Azure portal](#). Choose **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. Select the orange banner to open the **Mobile Device Management Authority** setting. The orange banner is only displayed if you haven't yet set the MDM authority.

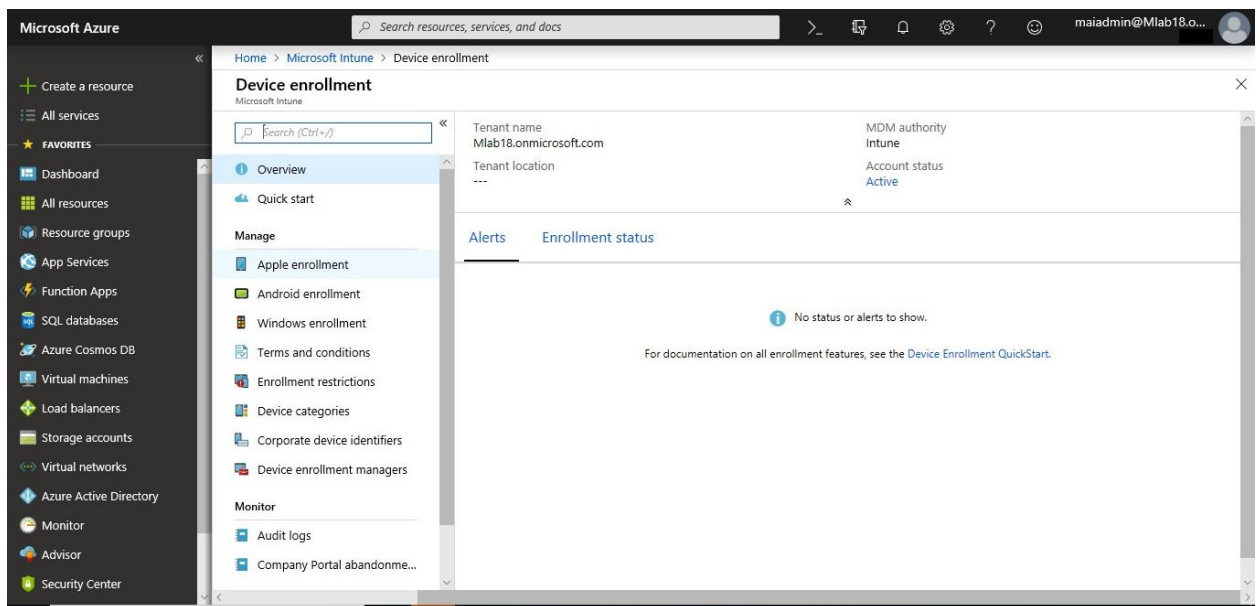


3. Under **Mobile Device Management Authority**, choose your MDM authority from the following options:
 - Intune MDM Authority
 - Configuration Manager MDM Authority
 - None

Microsoft Intune step by step on Azure portal



4. Now MDM Authority be active with Intune.



5. Enable mobile device management for the device platform you want to manage:

- iOS.
- Windows Phone.
- Android: No requirements
- Android Enterprise “Android for work”.

6. Enroll devices:

- Android – Install the Company Portal app from Microsoft Corporation available on [Google Play](#) and sign in with Intune user credentials added above.

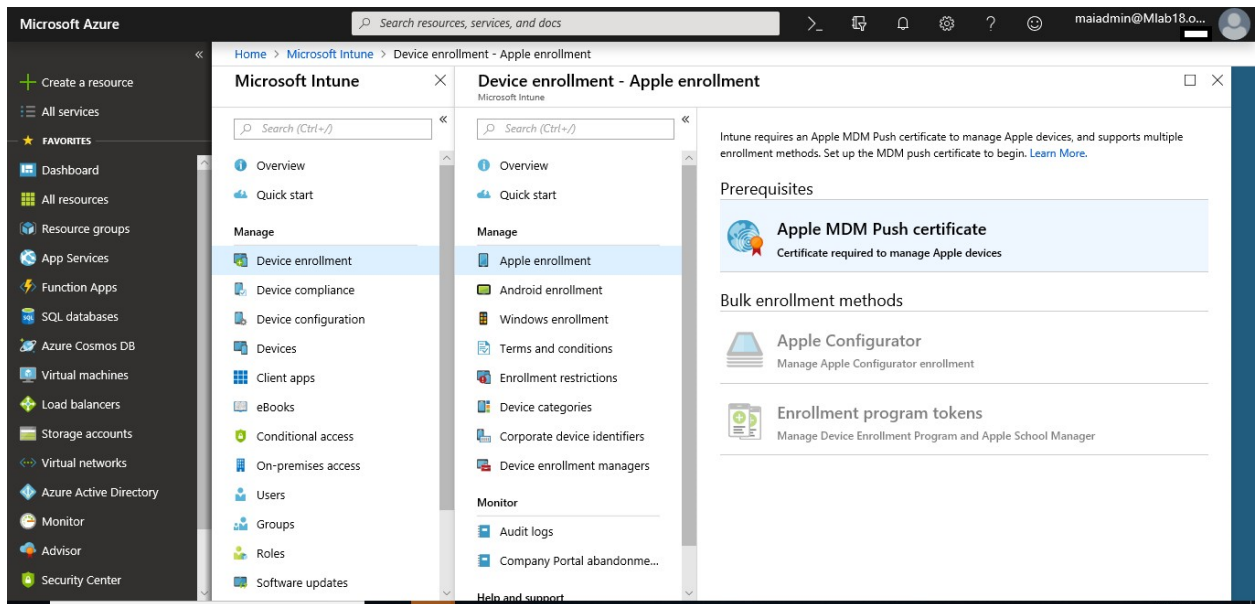
Microsoft Intune step by step on Azure portal

- iOS – Install the Company Portal app from Microsoft Corporation available in the [App Store](#) and sign in with Intune user credentials added above. View Enrolled devices to add your device.
- Windows Phone 8.1 or later - Users install the Company Portal app from Microsoft Corporation available in the [Windows Phone store](#) and sign in with Intune user credentials. View Enrolled devices to add your device.

Prepare for Mobile Device Management Authority “iOS”

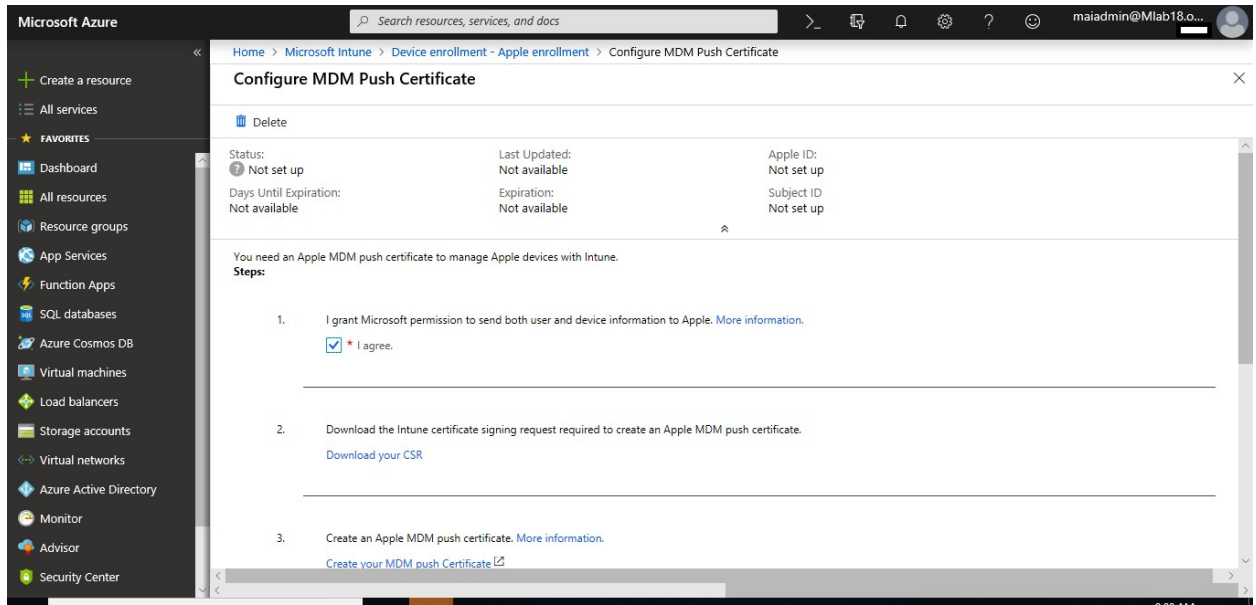
For some type of Mobile Devices, we need to do some preparations before they can be managed like iOS, you need to create and sign an APNs Certificate

1. In the [Azure portal](#), choose **Device enrollment** > **Apple Enrollment** > **Apple MDM Push Certificate**, and then follow these steps in the [Azure portal](#).



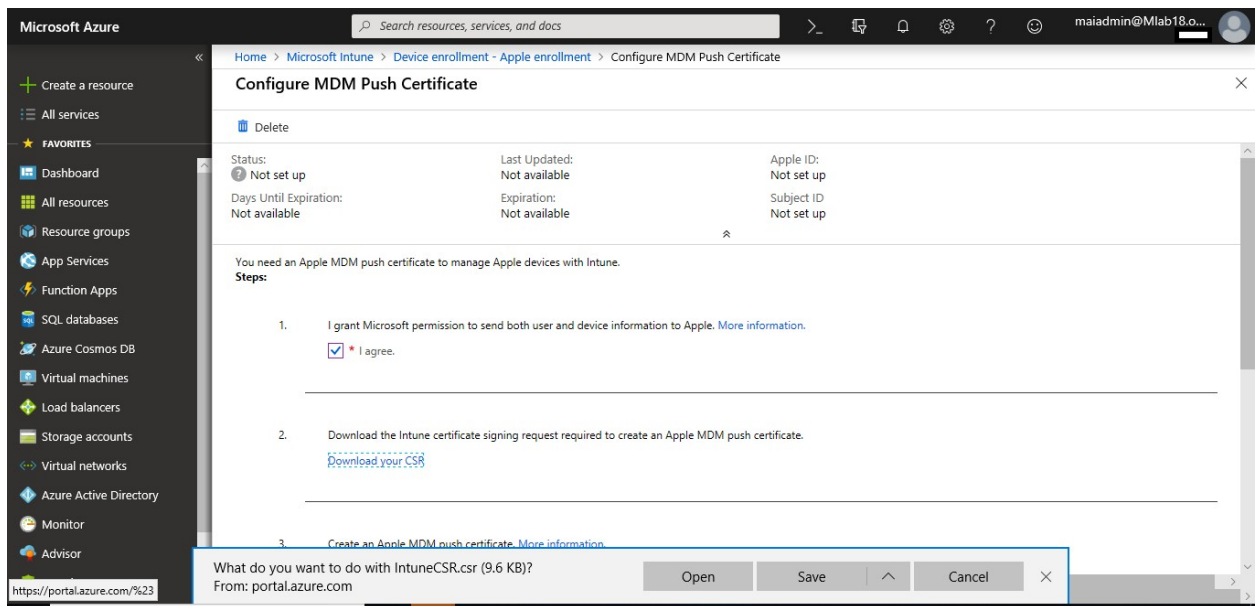
Step 1. Grant Microsoft permission to send user and device information to Apple

2. Select **I agree**. to give Microsoft permission to send data to Apple.



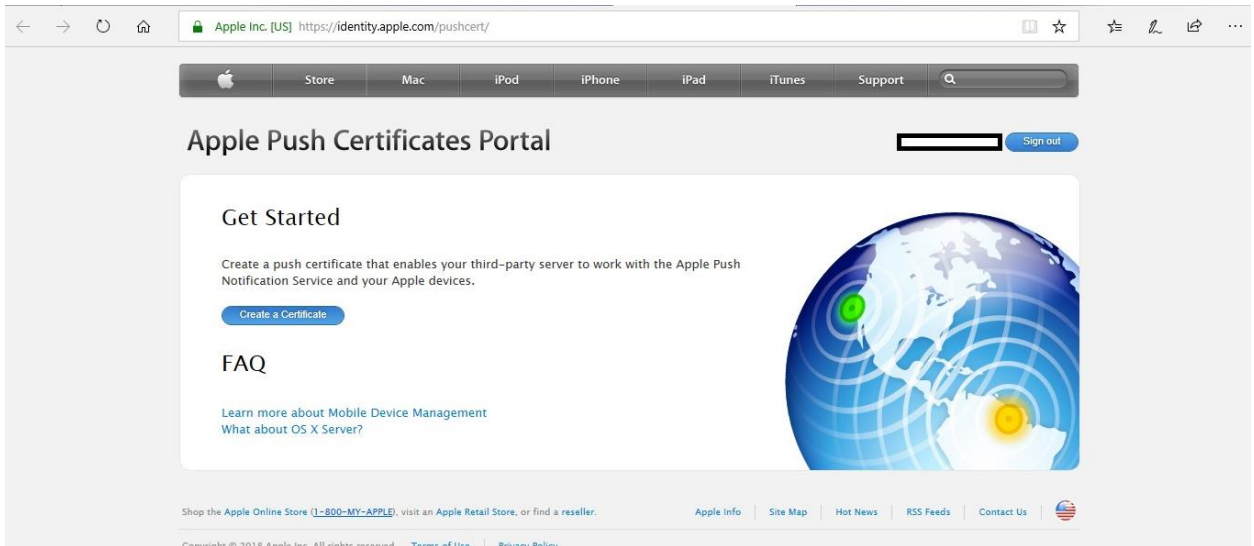
Step 2. Download the Intune certificate signing request required to create an Apple MDM push certificate

3. Select **Download your CSR** to download and save the request file locally. The file is used to request a trust relationship certificate from the Apple Push Certificates Portal.

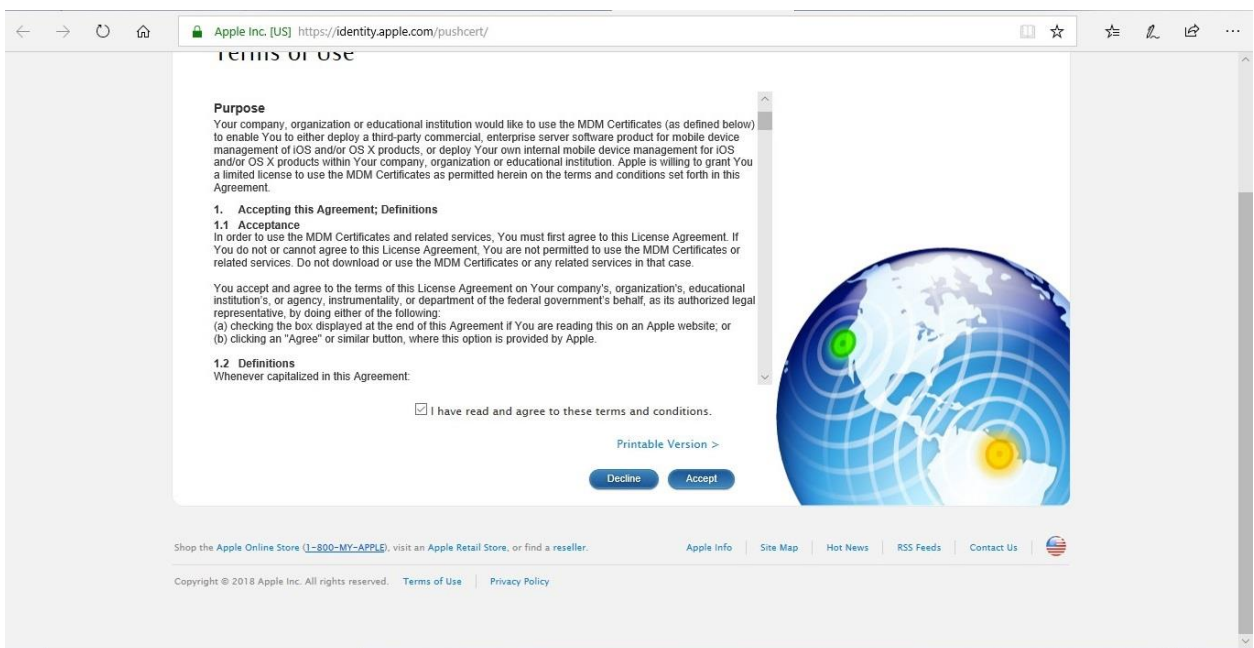


Step 3. Create an Apple MDM push certificate

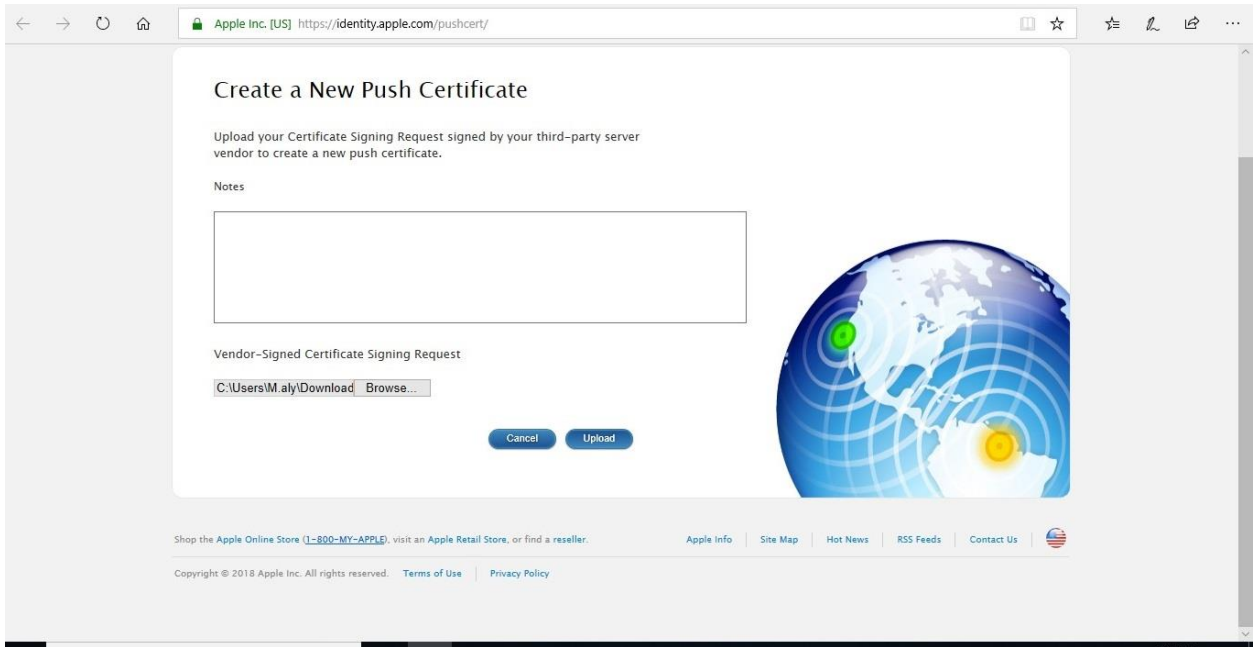
4. Select **Create your MDM push Certificate** to go to the Apple Push Certificates Portal. Sign in with your company Apple ID, and then click **Create a Certificate**.



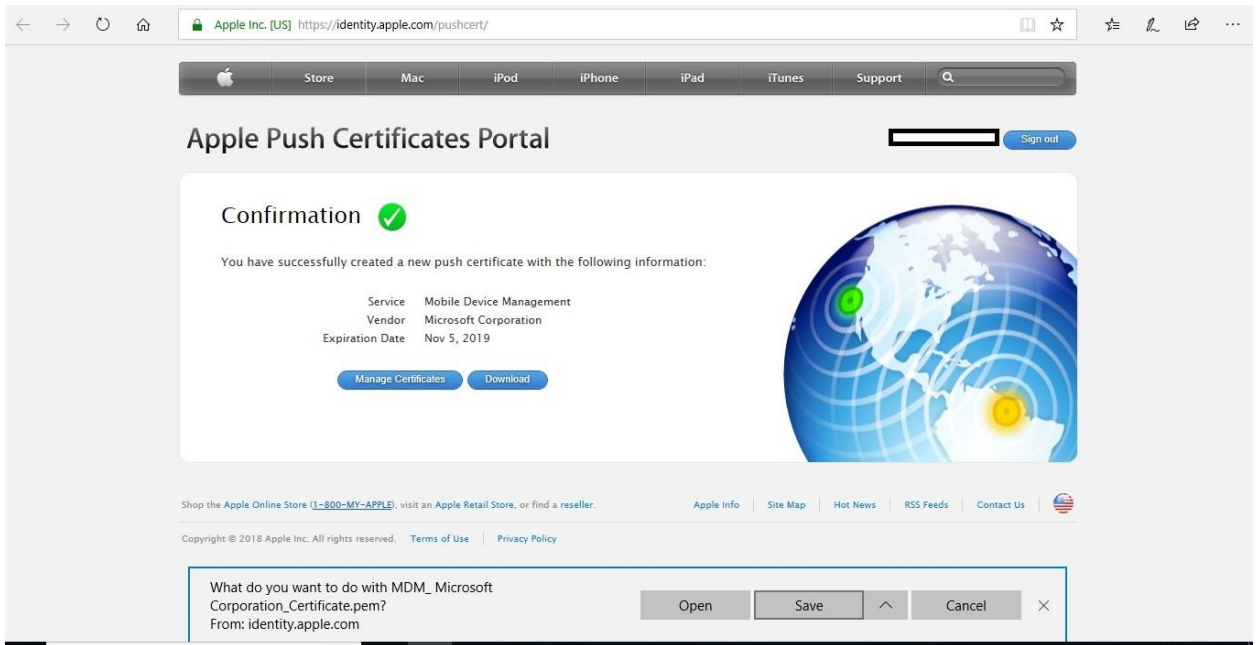
5. On **Terms of Use** Page, check **I have read and agree** and click **Accept**.



6. Select **Choose File** and browse to the certificate signing request file, and then choose **Upload**.



7. On the Confirmation page, choose **Download** to download the certificate (.pem) file, and save the file locally.



Note

The certificate is associated with the Apple ID used to create it. As a best practice, use a **company Apple ID** for management tasks and make sure the mailbox is monitored by more than one person like a **distribution list**. **Never use a personal Apple ID**. To create new Apple ID for your **company distribution list mail**, you can use [this link](#).

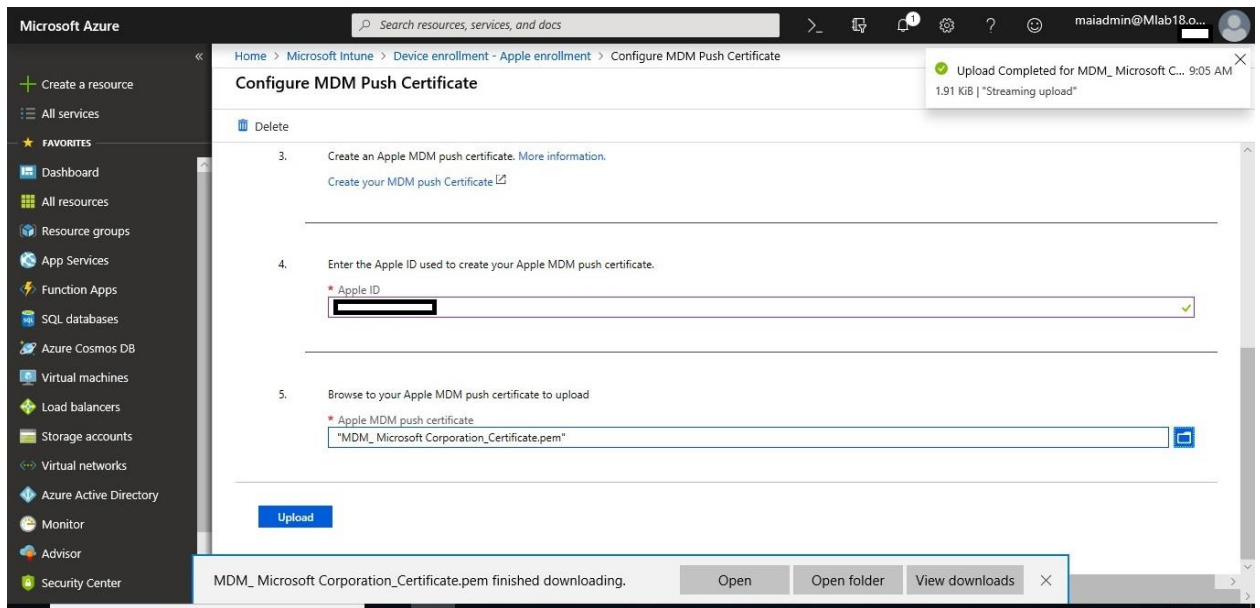
Microsoft Intune step by step on Azure portal

Step 4. Enter the Apple ID used to create your Apple MDM push certificate

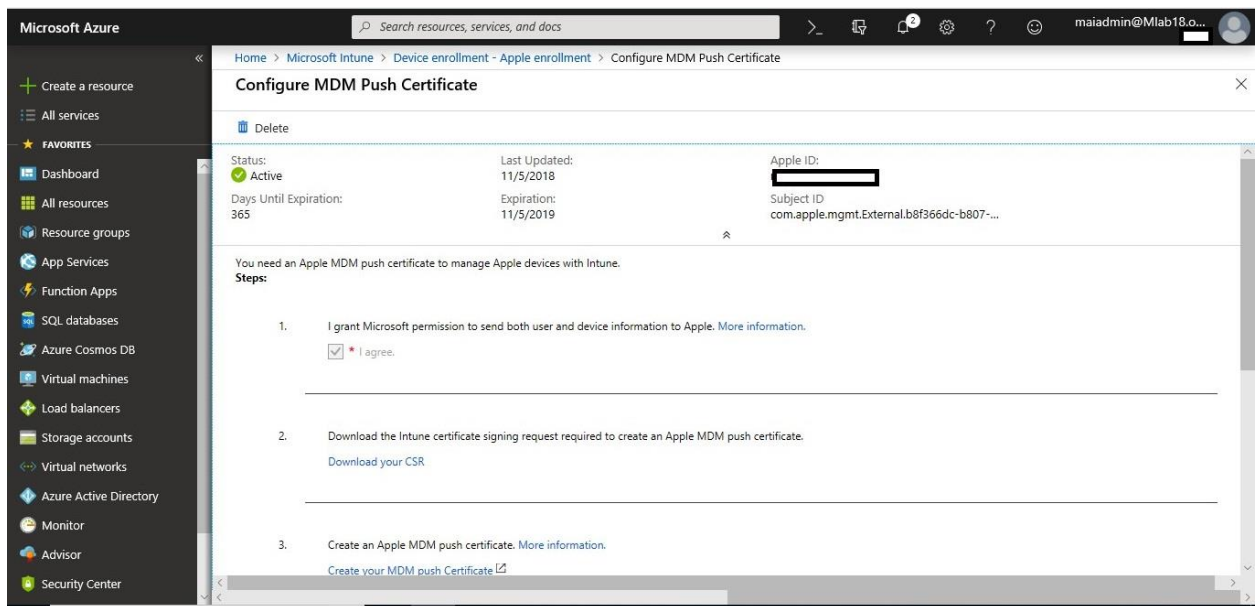
- Record this ID as a reminder for when you need to renew this certificate.

Step 5. Browse to your Apple MDM push certificate to upload

- Go to the certificate (.pem) file, choose **Open**, and then choose **Upload**.



- With the push certificate, Intune can enroll and manage Apple devices.



Prepare for Mobile Device Management Authority “Windows phone & Windows 10 MDM”

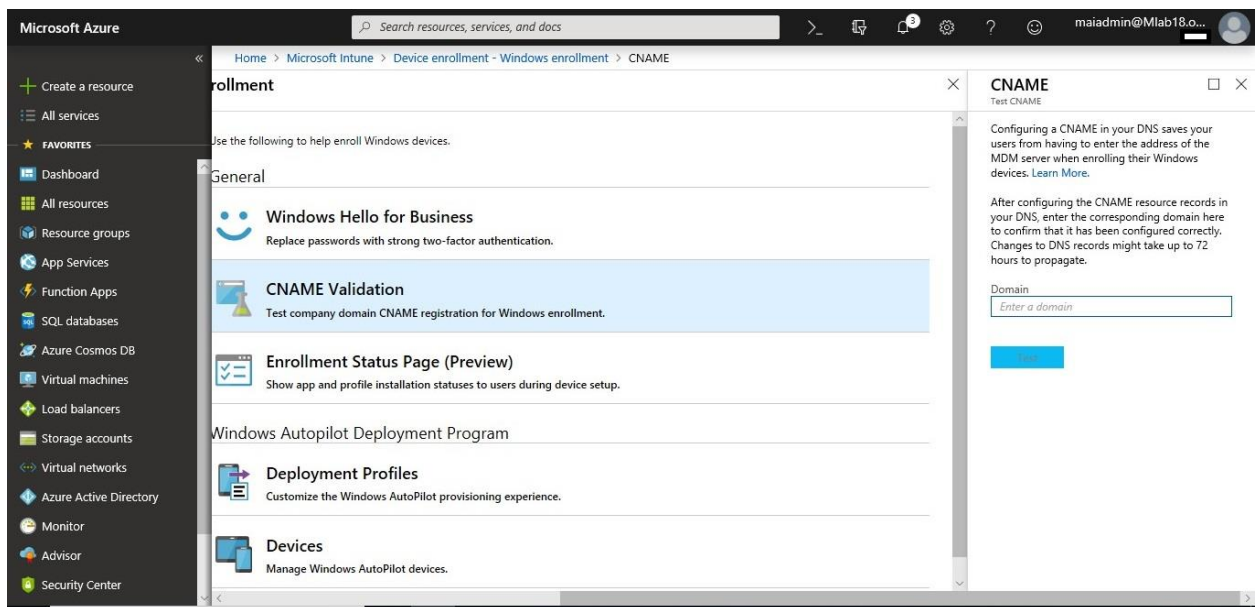
Setup requirements for Windows Phone mobile device management depend upon how you'll manage devices. Setting two CNAMEs in your company's DNS registration makes enrollment easier for users. If your users will download the Company Portal app from the Store, then once you've configured DNS settings, you just need to set up the Company Portal and inform users how to enroll.

Set up Windows Phone Enrollment with Intune

To simplify enrollment, create a domain name server (DNS) alias (CNAME record type) that redirects enrollment requests to Intune servers. Otherwise, users trying to connect to Intune must enter the Intune server name during enrollment.

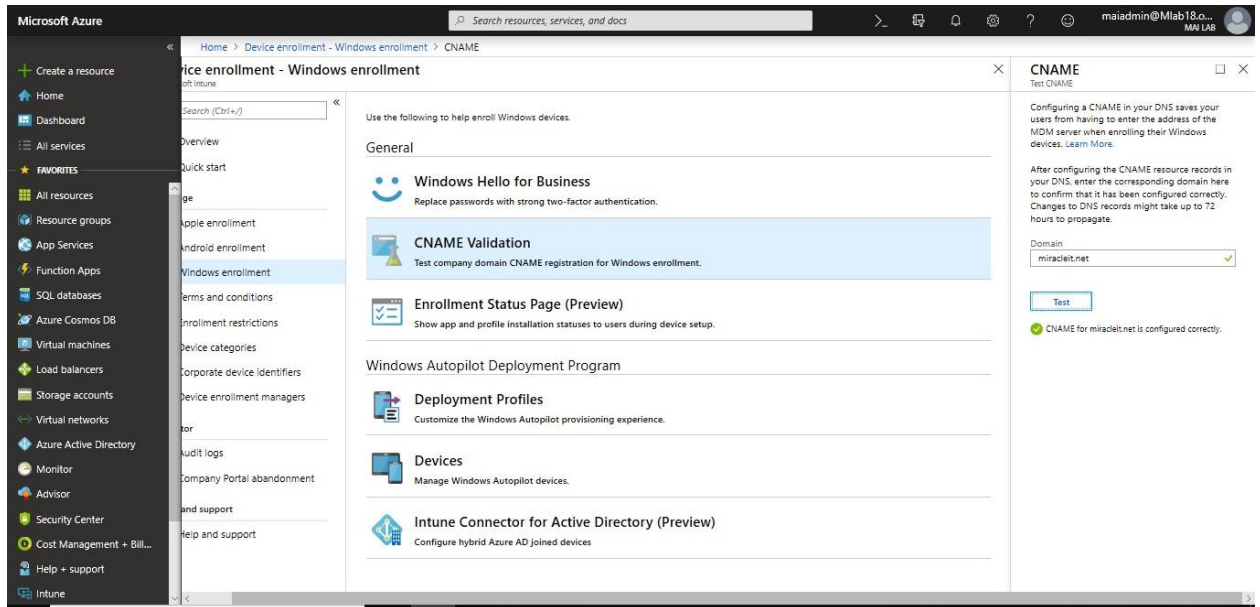
To verify the CNAME Record, you need to follow below steps:

1. Sign in to the [Azure portal](#), and select **Intune > Device enrollment > Windows enrollment > CNAME Validation**.



2. Create CNAME resource records for your company's domain on public DNS. The CNAME resource records must contain the following information:

TYPE	Host Name	Points to	TTL
CNAME	EnterpriseEnrollment.company_domain.com	EnterpriseEnrollment-s.manage.microsoft.com	1 Hour
CNAME	EnterpriseRegistration.company_domain.com	EnterpriseRegistration.windows.net	1 Hour



Prepare for Mobile Device Management Authority “Android”

As an Intune administrator, you can manage the following Android devices:

- Android devices, including Samsung Knox Standard devices.
- Android enterprise devices, including Android work profile devices and Android kiosk devices.

Set up Android Enrollment

By default, Intune allows enrollment of Android and Samsung Knox Standard devices. After fulfilling the prerequisite, admins merely need to [tell their users how to enroll their devices](#).

Set up Android Enterprise “Android for work” Enrollment

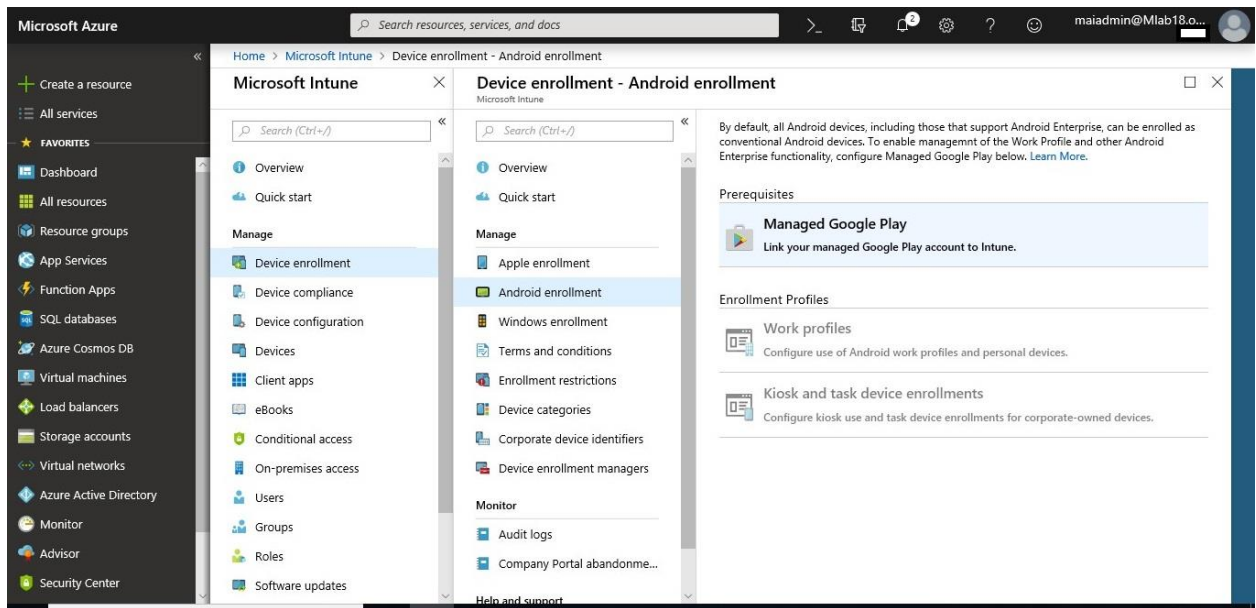
Android enterprise is a set of Android device features and services that separate personal apps and data from a work profile containing work apps and data. Android enterprise devices include work profile devices and kiosk devices.

To set up enrollment for Android enterprise devices, you must first connect Android enterprise to Intune.

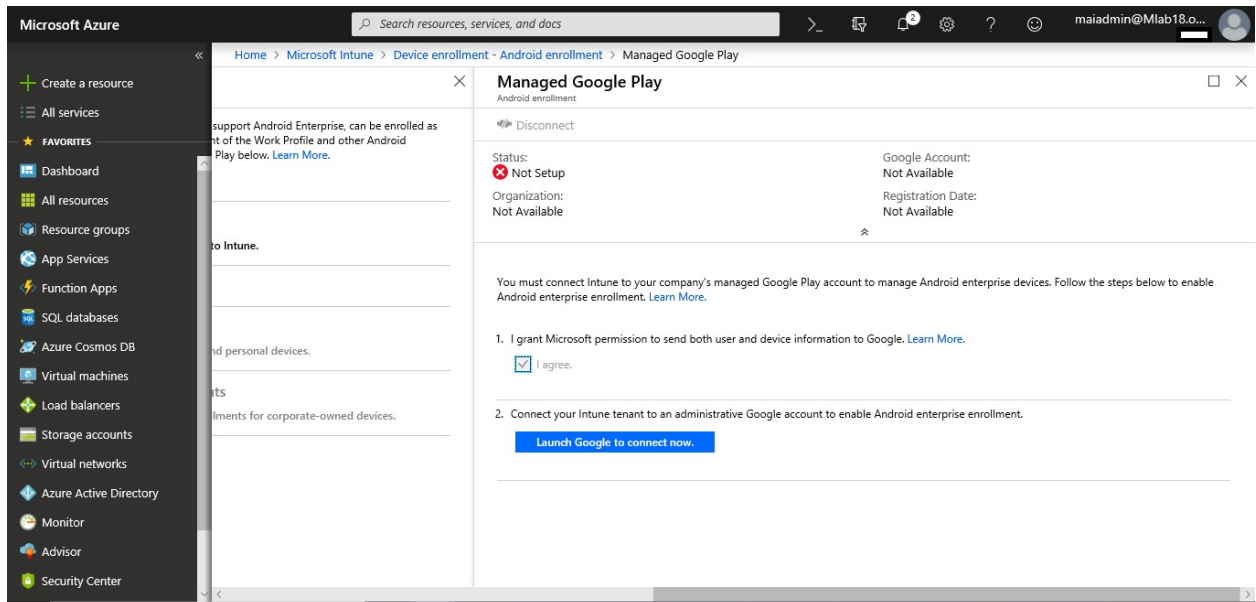
Microsoft Intune step by step on Azure portal

Note: Due to interaction between Google and Microsoft domains, this step may require that you adjust your browser settings. Make sure that "portal.azure.com" and "play.google.com" are in the same security zone in your browser.

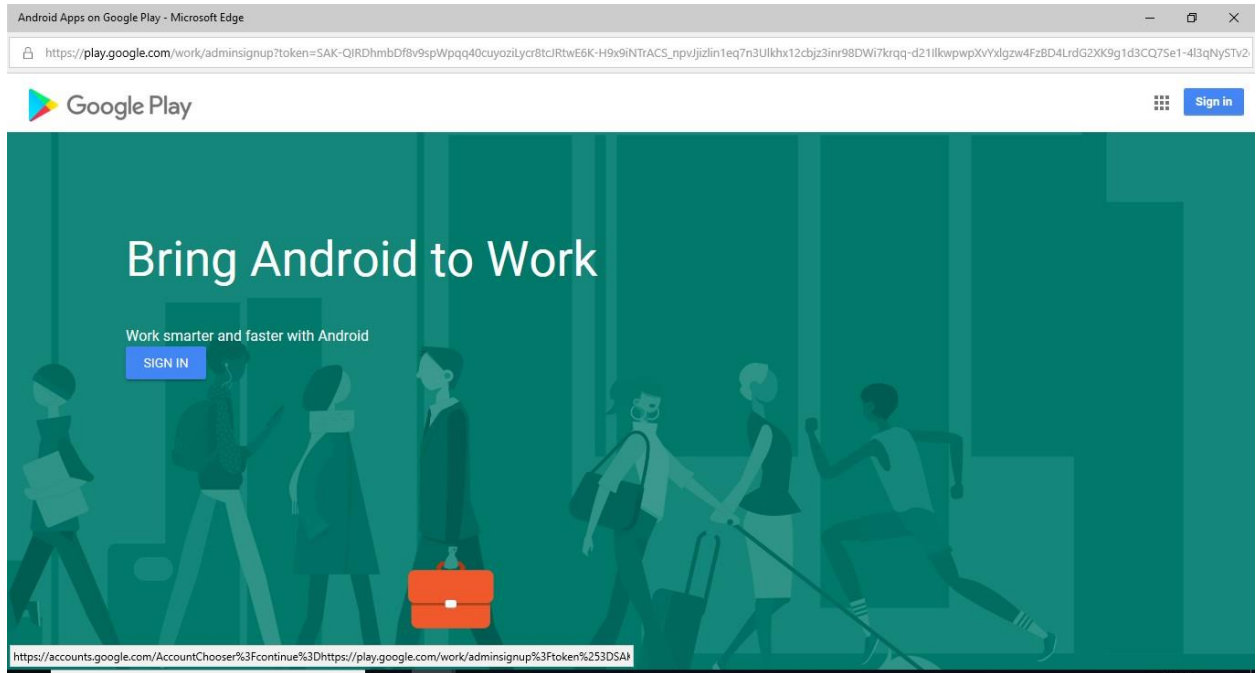
1. Sign in to the [Intune in the Azure portal](#), choose **Device enrollment > Android enrollment > Managed Google Play**. If you are using a custom Intune admin role, access to this requires Organization Read and Update permissions.



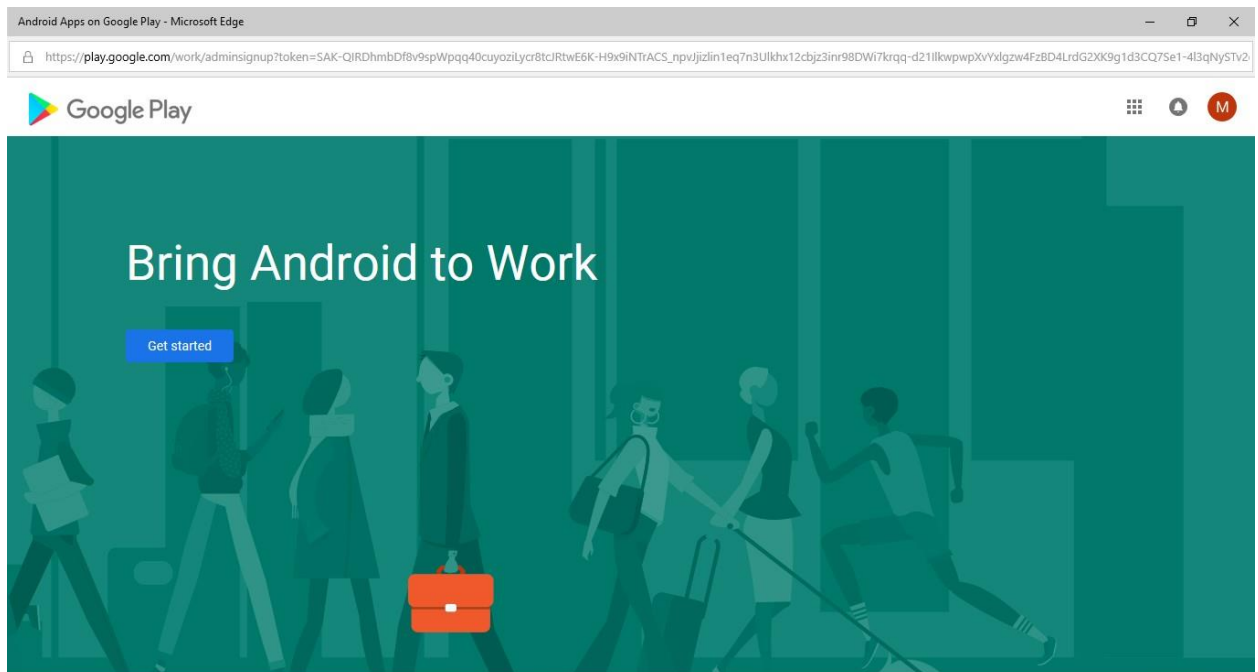
2. Choose **I agree** to grant Microsoft permission to send user and device information to Google.



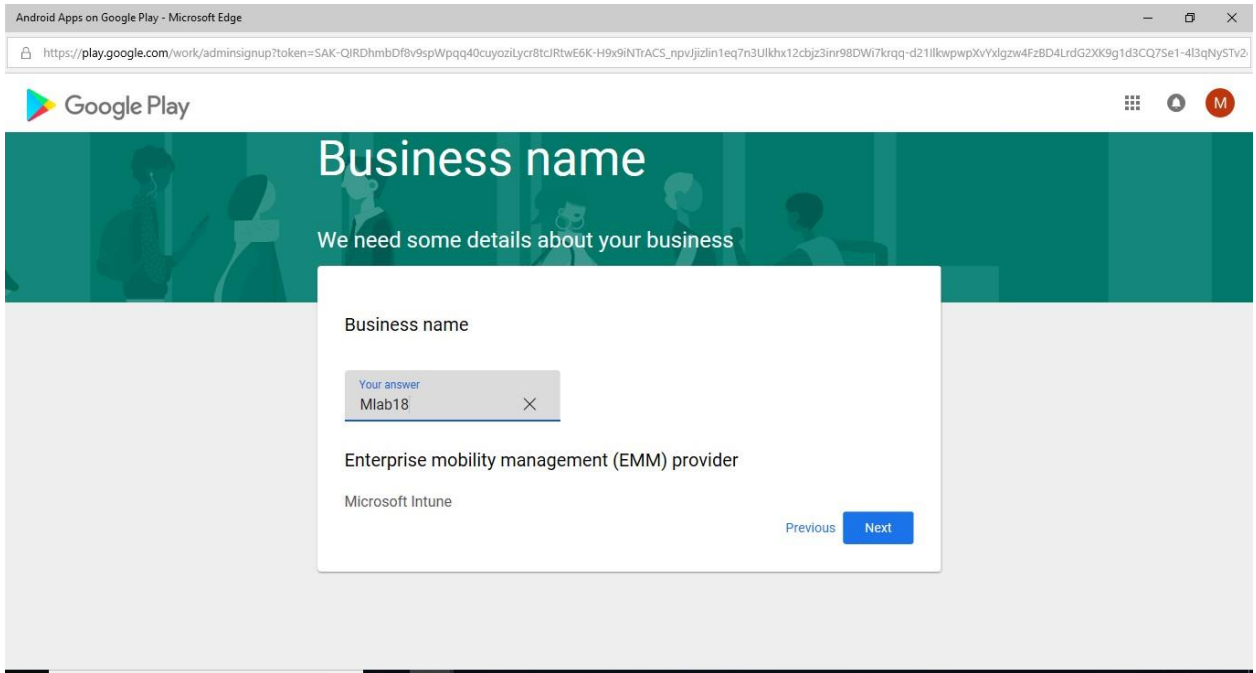
3. Choose **Launch Google to connect now** to open the Managed Google Play website. The website opens on a new tab in your browser.



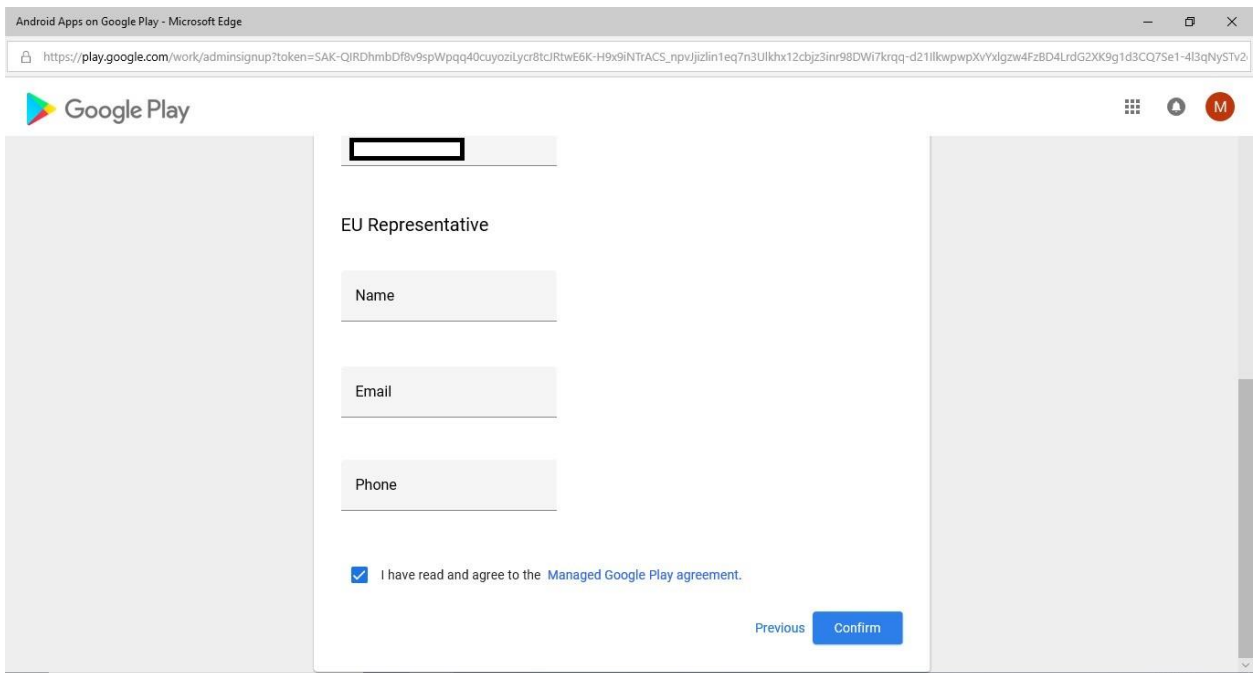
4. On Google's sign in page, enter the Google account that will be associated with all Android enterprise management tasks for this tenant. This is the Google account that your company's IT admins share to manage and publish apps in the Google Play console. You can use an existing Google account or create a new one. The account you choose **must not be associated with a G-Suite domain**.



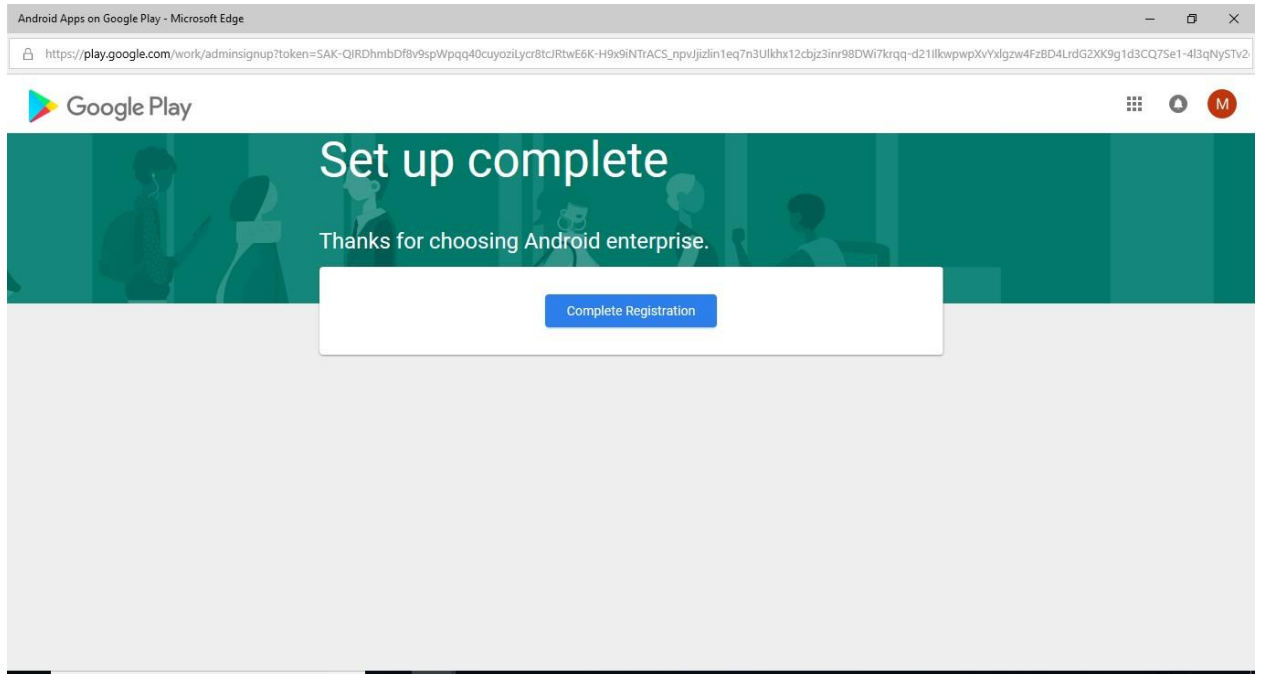
5. Provide your company's name for **Organization name**. For **Enterprise mobility management (EMM) provider**, **Microsoft Intune** should be displayed.



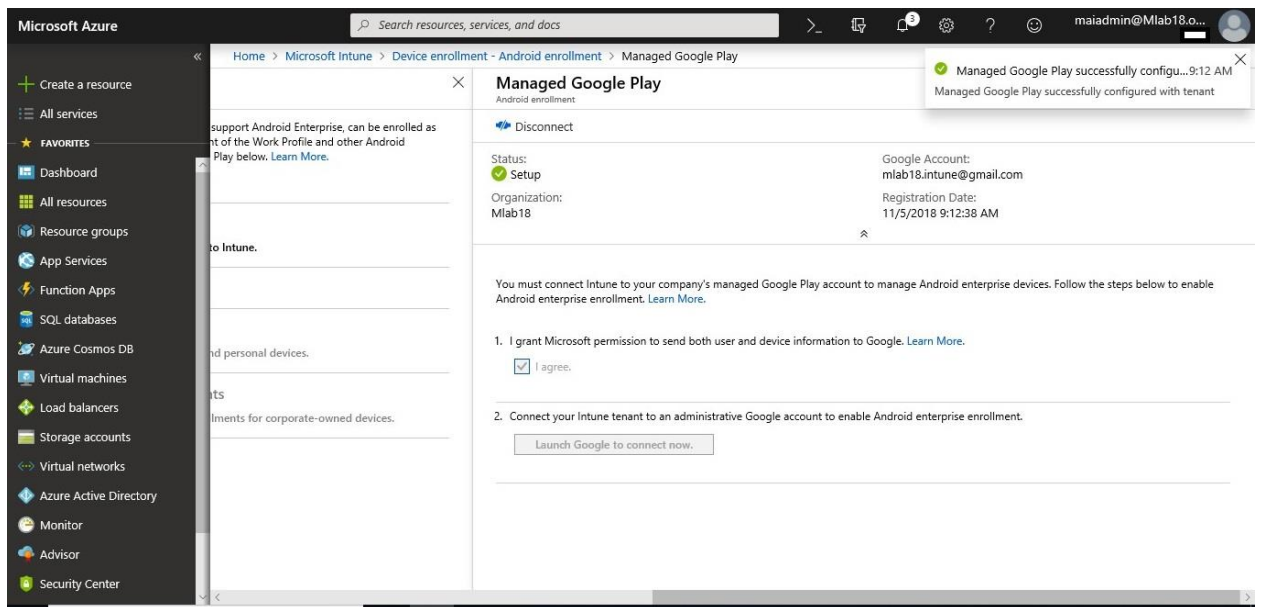
6. Agree to the Android agreement, and then choose **Confirm**. Your request will be processed.



7. Then Click Complete Registration.



11. Now you're ready to manage Android Enterprise devices.



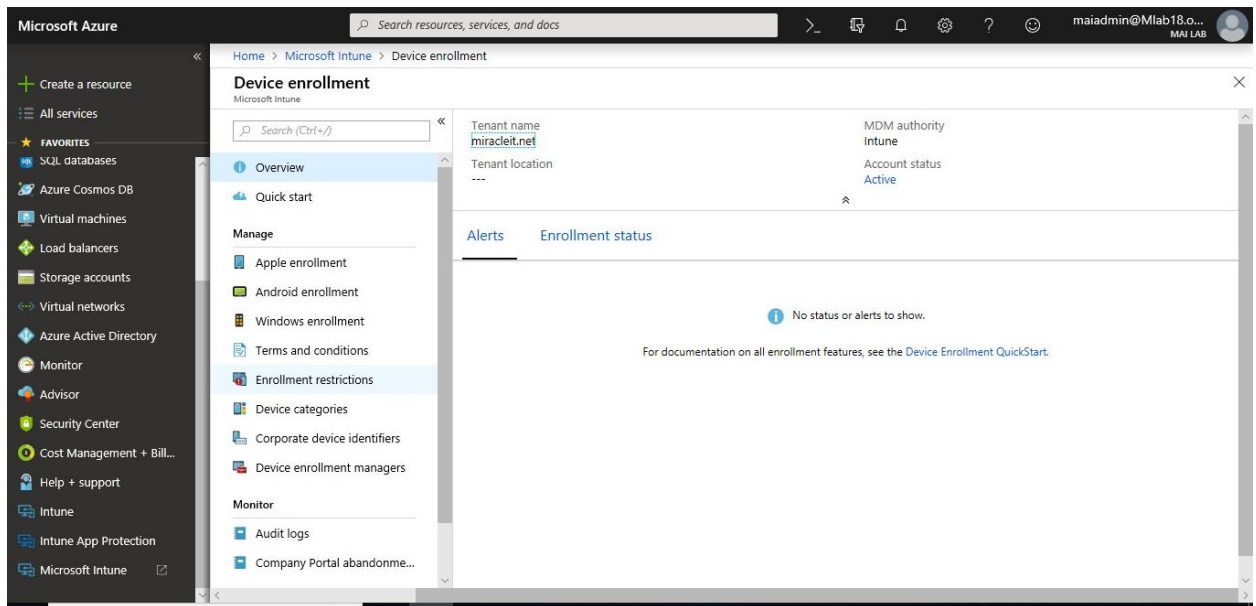
Set Enrollment Restrictions

You can create and manage enrollment restrictions that define the number and types of devices that can enroll into management with Intune. You can create multiple restrictions and apply them to different user groups.

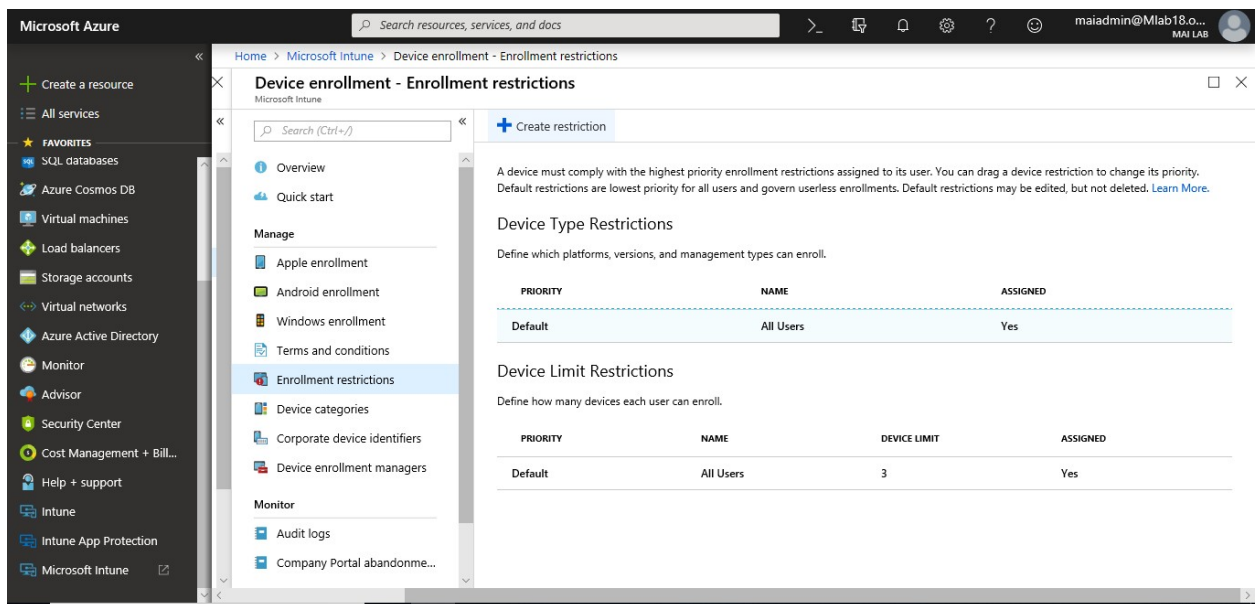
To create an enrollment restriction, you can follow below steps:

Microsoft Intune step by step on Azure portal

1. Sign in to the [Azure portal](#). Select **More Services**, search for **Intune**, and then choose **Intune**.
2. Select **Device enrollment** > **Enrollment restrictions**.

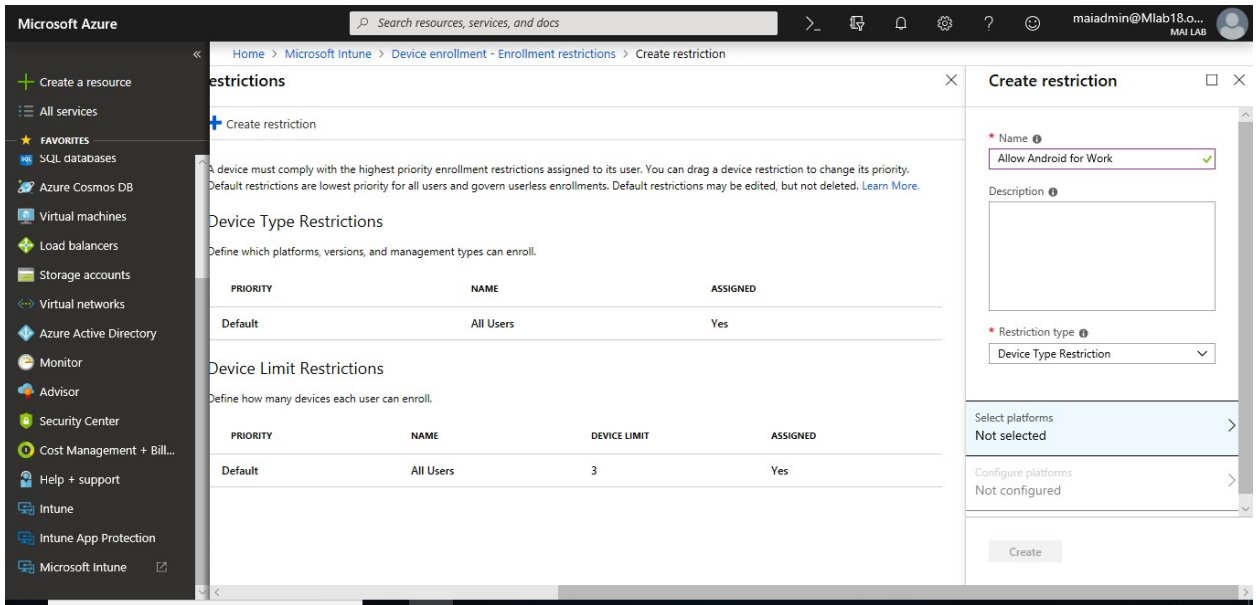


3. Select **Create restriction**.

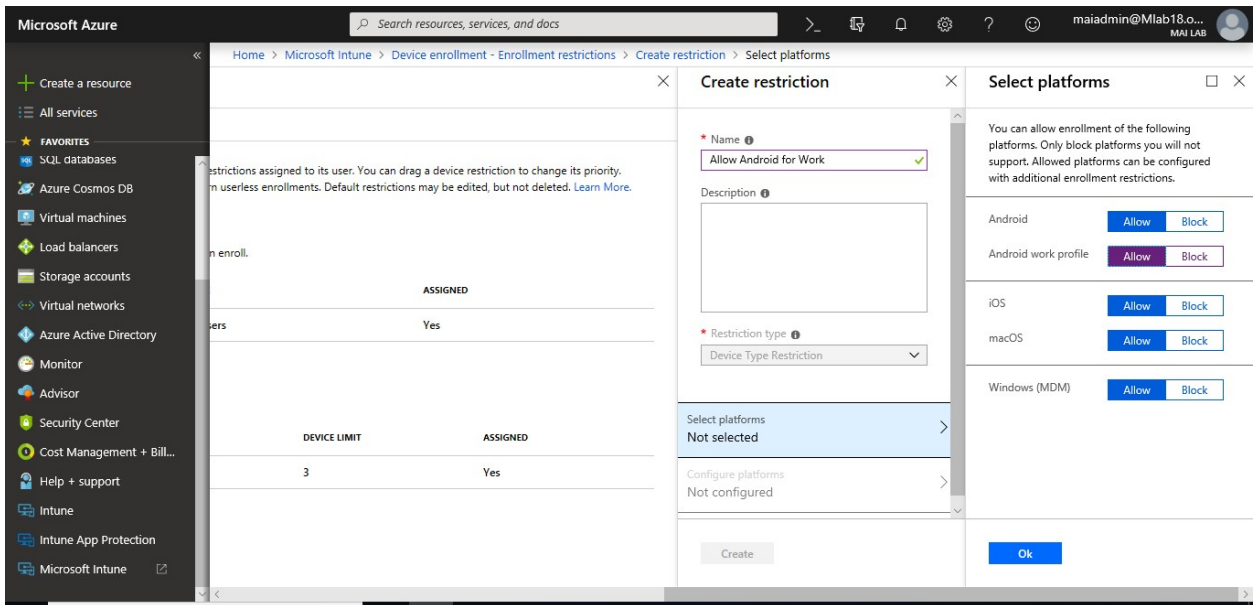


Note: we will **create new restriction** to apply it for **specific group** because if you modify on default, it will be applying for all users.

4. Give the restriction a name and description. Choose a **Restriction type**, Device Type Restriction.

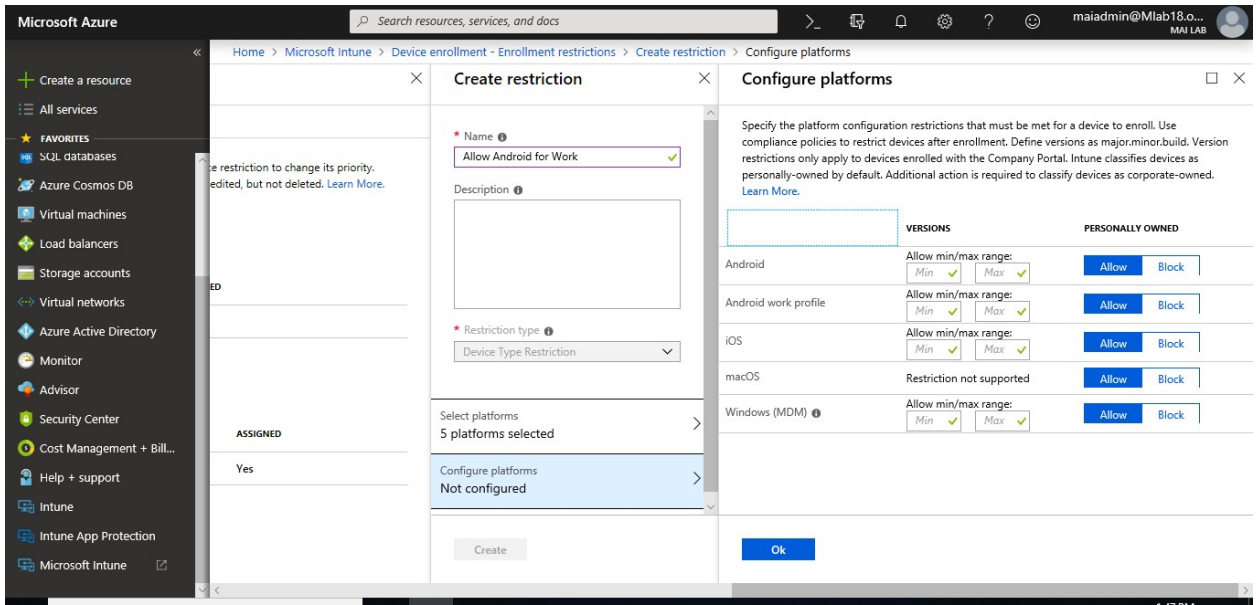


5. For device type restrictions, select **Platforms** to allow or block various platforms.

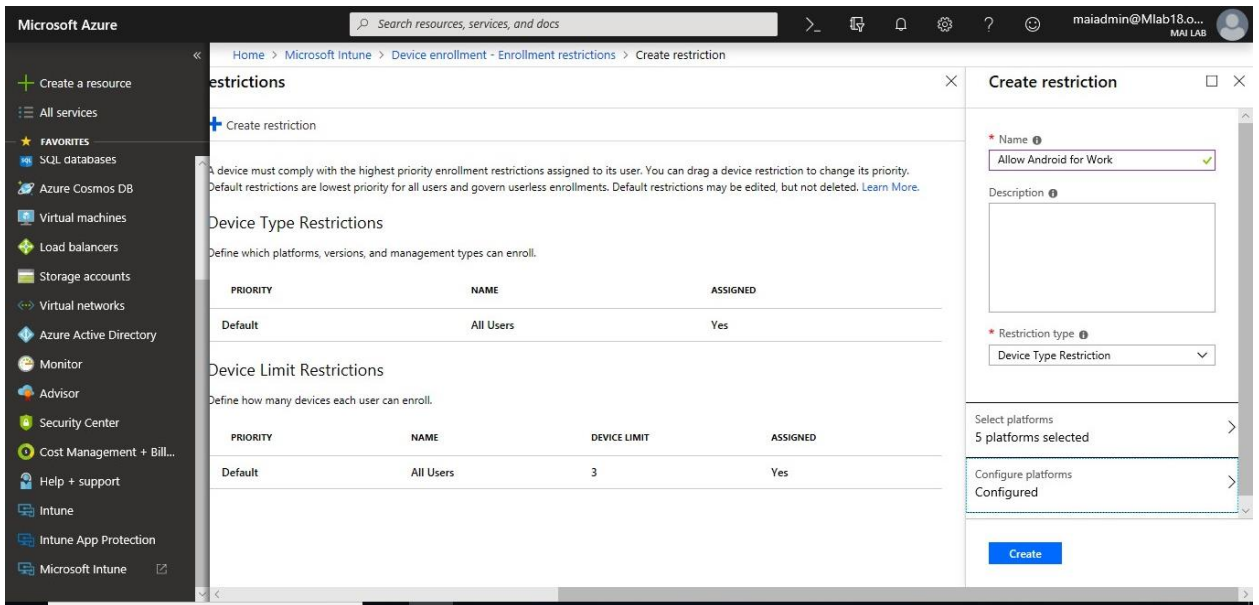


6. For device type restrictions, select **Platform configurations** to allow or block various versions.

Microsoft Intune step by step on Azure portal

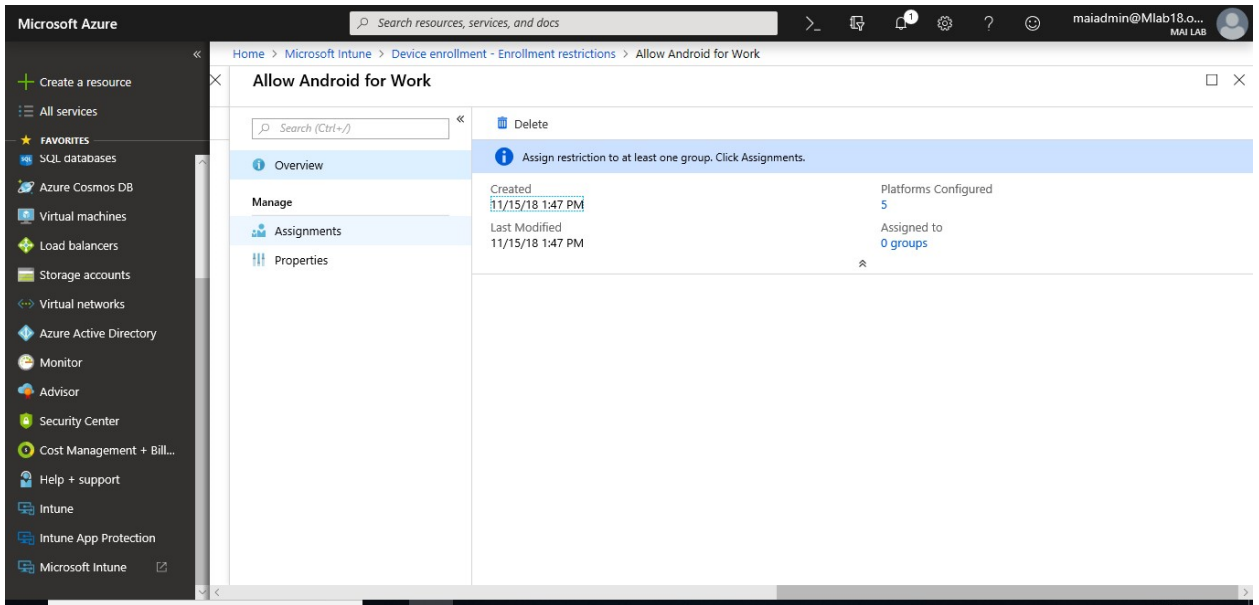


7. On **Create restriction** page, click **Create**.

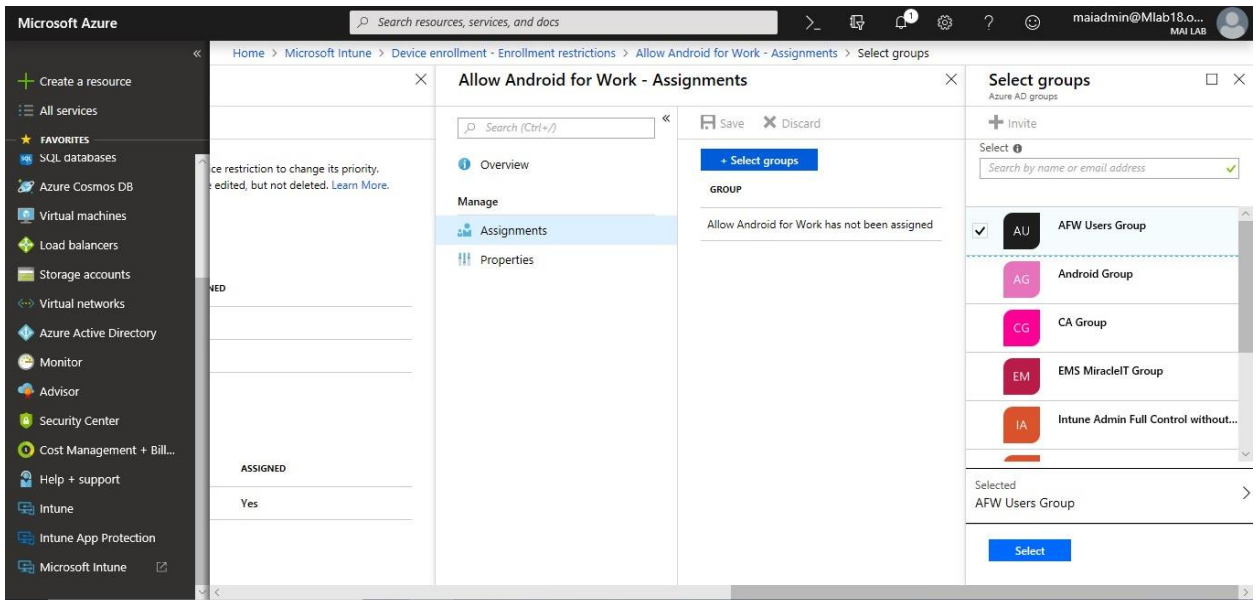


8. Select **Assignments** > + **Select groups**.

Microsoft Intune step by step on Azure portal

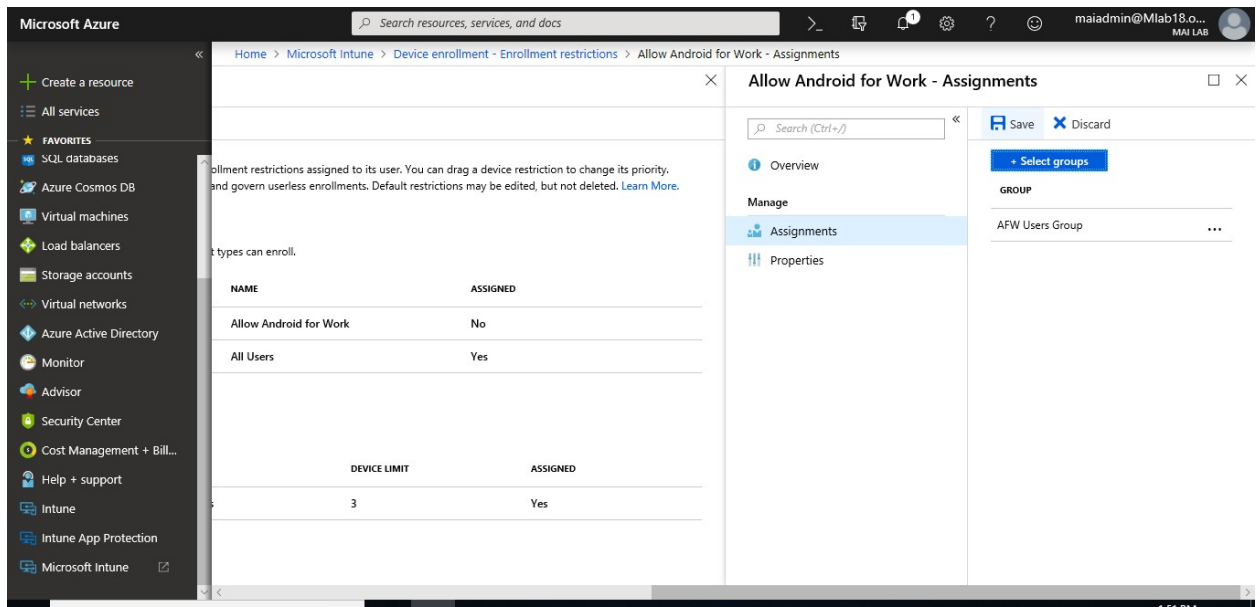


9. Under **Select groups**, select one or more groups, and then choose **Select**. The restriction applies only to groups to which it's assigned. If you don't assign a restriction to at least one group, it won't have any effect.

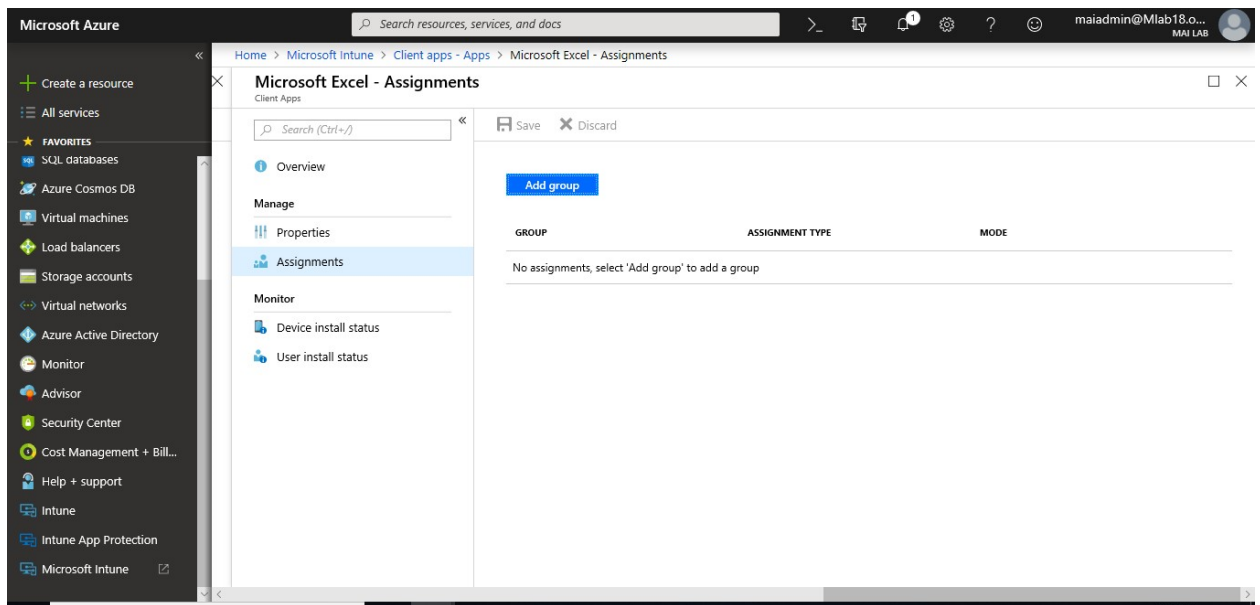


10. Select **Save**.

Microsoft Intune step by step on Azure portal



11. The new restriction is created with a priority just above the default.



Manage your company's terms and conditions for user access

You can require that users accept your company's terms and conditions before using the Company Portal to:

- Enroll devices
- Access resources like company apps and email. Configuration of terms and conditions is optional.

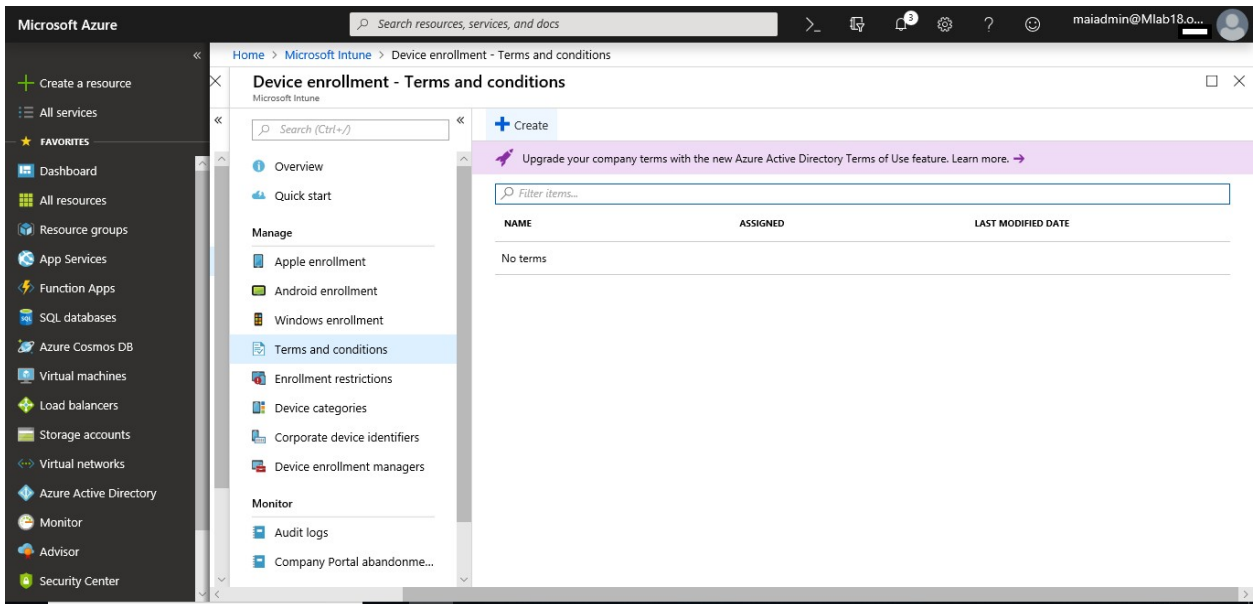
Microsoft Intune step by step on Azure portal

You can create multiple sets of terms and assign them to different groups, such as to support different languages.

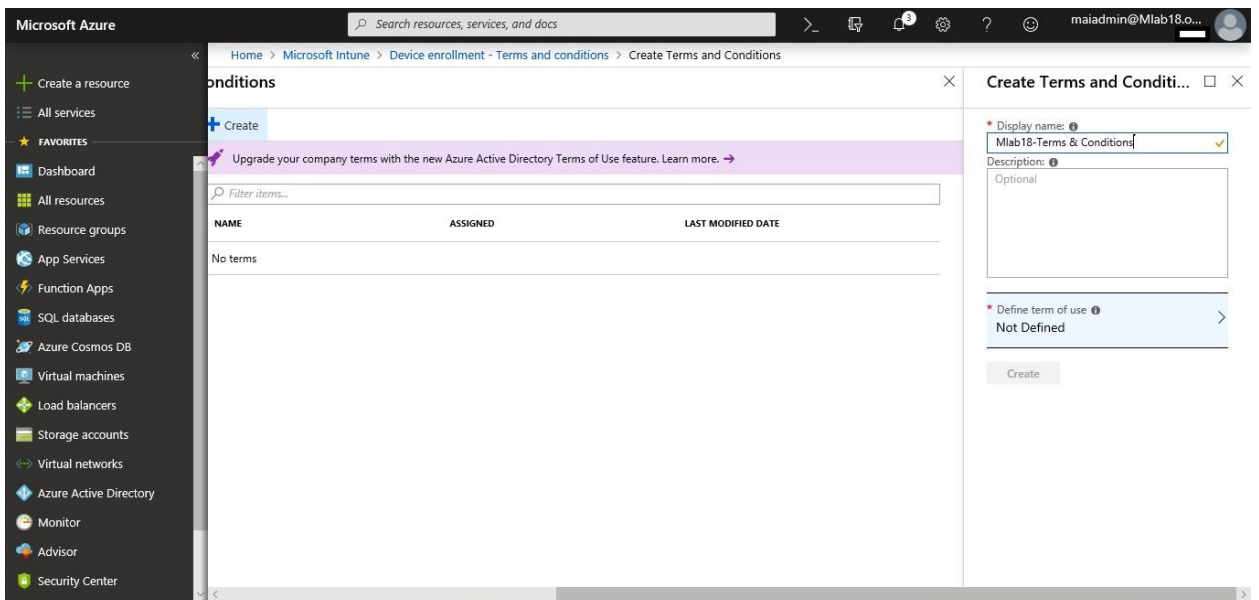
Create Terms and Conditions

Complete these steps to create terms and conditions. The display name and description are for administrative use while terms properties are displayed to users in the Company Portal.

1. Sign into the [Intune portal](#). Choose **Device enrollment** > **Terms and Conditions**. Choose **Create**.



2. On the expanded pane, specify the following information:



Microsoft Intune step by step on Azure portal

3. Choose the arrow next to **Define terms of use** to open the Terms and Conditions pane, and then enter the following information:

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains navigation options like 'Create a resource', 'All services', and 'FAVORITES'. The main area displays the 'Create Terms and Conditions' pane. The 'Create Terms and Conditions' section includes a 'Display name' field with 'Mlab18-Terms & Conditions', a 'Description' field with 'Optional', and a 'Define term of use' dropdown menu set to 'Not Defined'. The 'Terms and Conditions' section includes a 'Title' field with 'Mlab18 Terms', a 'Summary of Terms' field with 'By enrolling your device, you agree to Mlab18 company policies and terms', and a 'Terms and Conditions' text area containing a sample agreement. An 'Ok' button is visible at the bottom of the 'Terms and Conditions' section.

4. Choose **Ok > Create**.

The screenshot shows the Microsoft Azure portal interface after clicking 'Ok > Create'. The left sidebar remains the same. The main area displays the 'Create Terms and Conditions' pane. The 'Terms and Conditions' section is now empty. The 'Create Terms and Conditions' section has a 'Create' button. The 'Create Terms and Conditions' section has a 'Filter items...' field and a table with columns 'NAME', 'ASSIGNED', and 'LAST MODIFIED DATE'. The table is empty, showing 'No terms'.

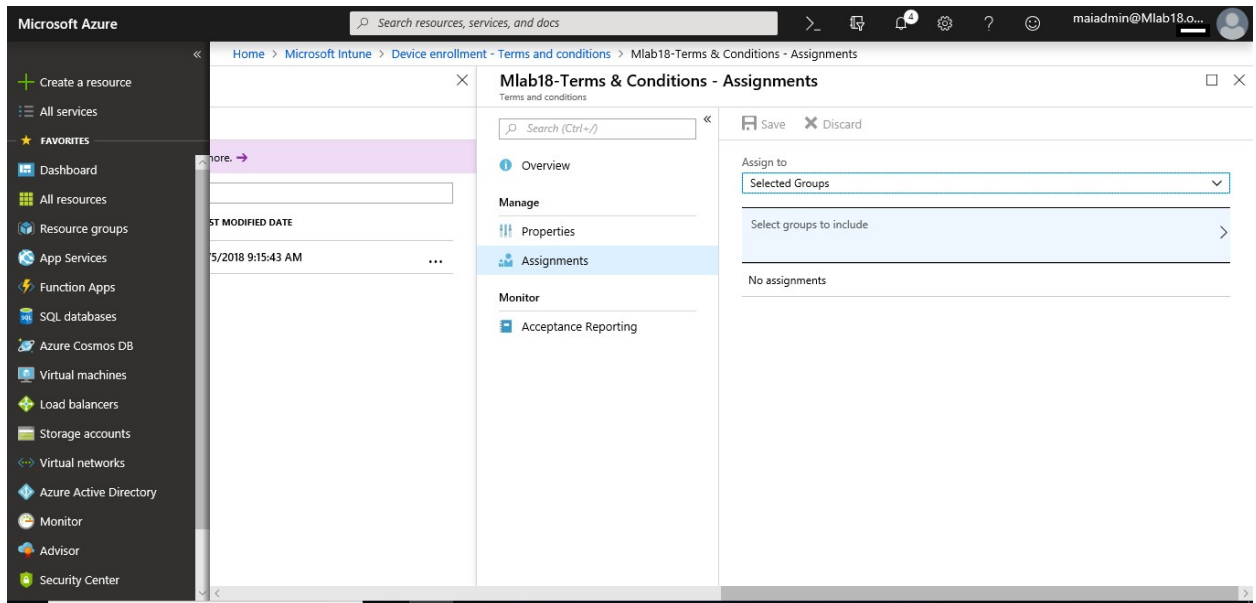
Assign Terms and Conditions

You can assign terms and conditions to groups of users who must accept them before using the Company Portal.

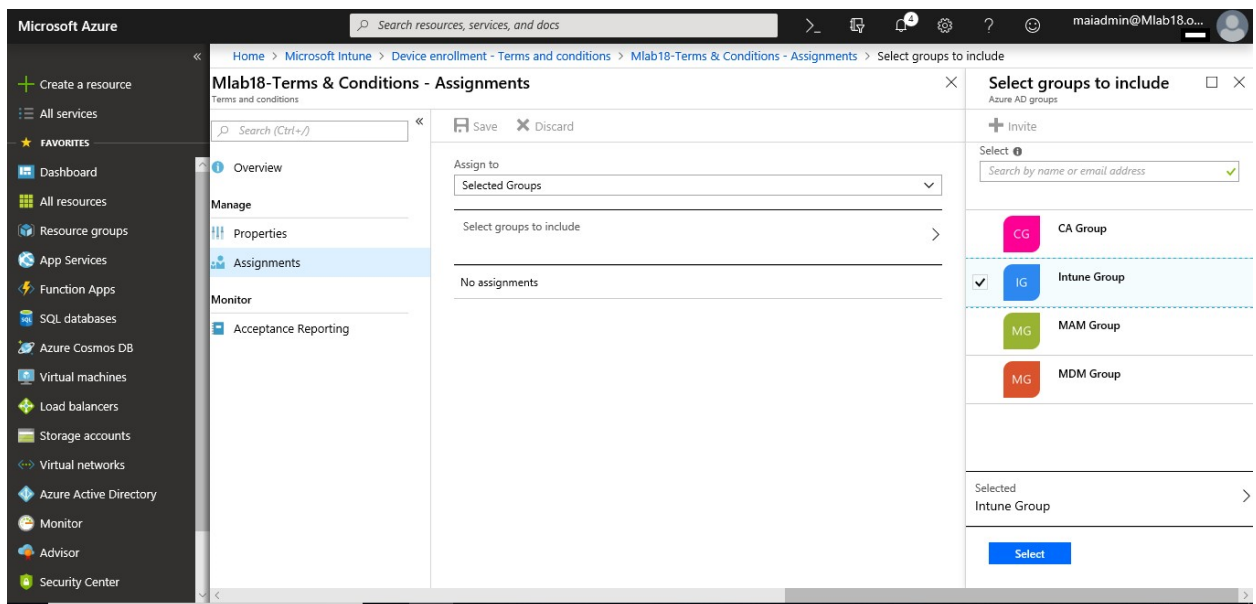
1. In the [Intune portal](#), choose **Device enrollment**, and then choose **Terms and Conditions**.

Microsoft Intune step by step on Azure portal

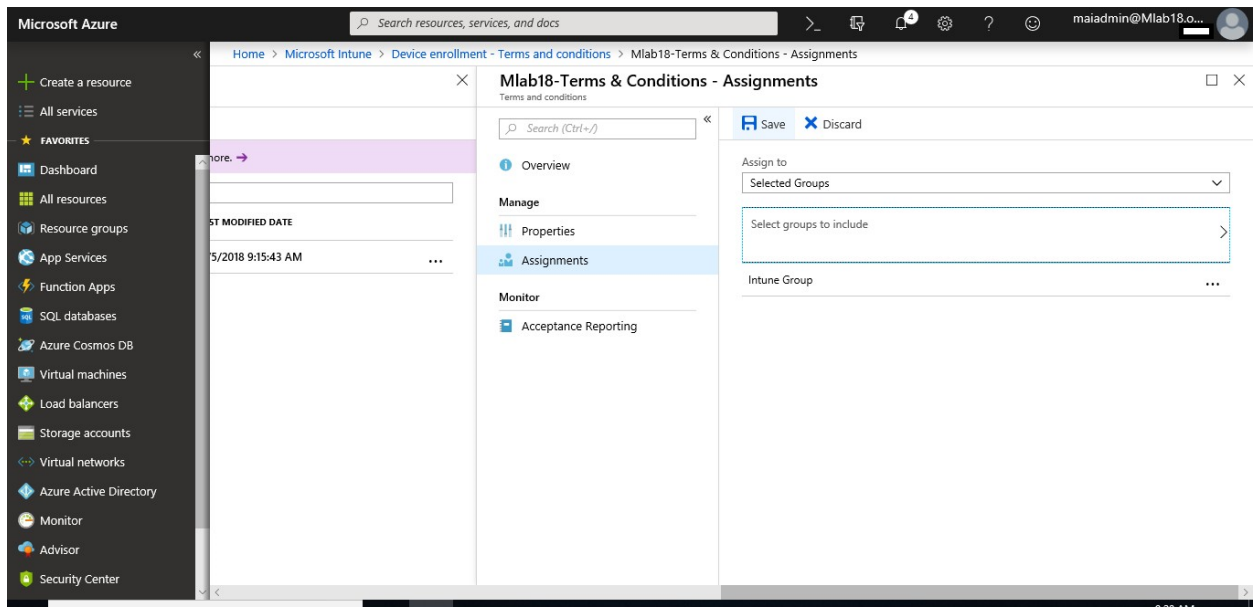
2. In the list of terms and conditions, choose the terms you want to assign > **Manage** > **Assignments**.



3. Choose **Select groups to include** > choose the groups you want to assign the terms > **Select**. Dynamic groups can't be assigned Terms and Conditions.



4. In the **Assigned Groups** pane, choose **Save**.



Identify Devices as Corporate-owned

As an Intune admin, you can identify devices as corporate-owned to refine management and identification. Intune can perform additional management tasks and collect additional information such as the full phone number and an inventory of apps from corporate-owned devices. You can also set device restrictions to block enrollment by devices that aren't corporate-owned.

At the time of enrollment, Intune automatically assigns corporate-owned status to devices that are:

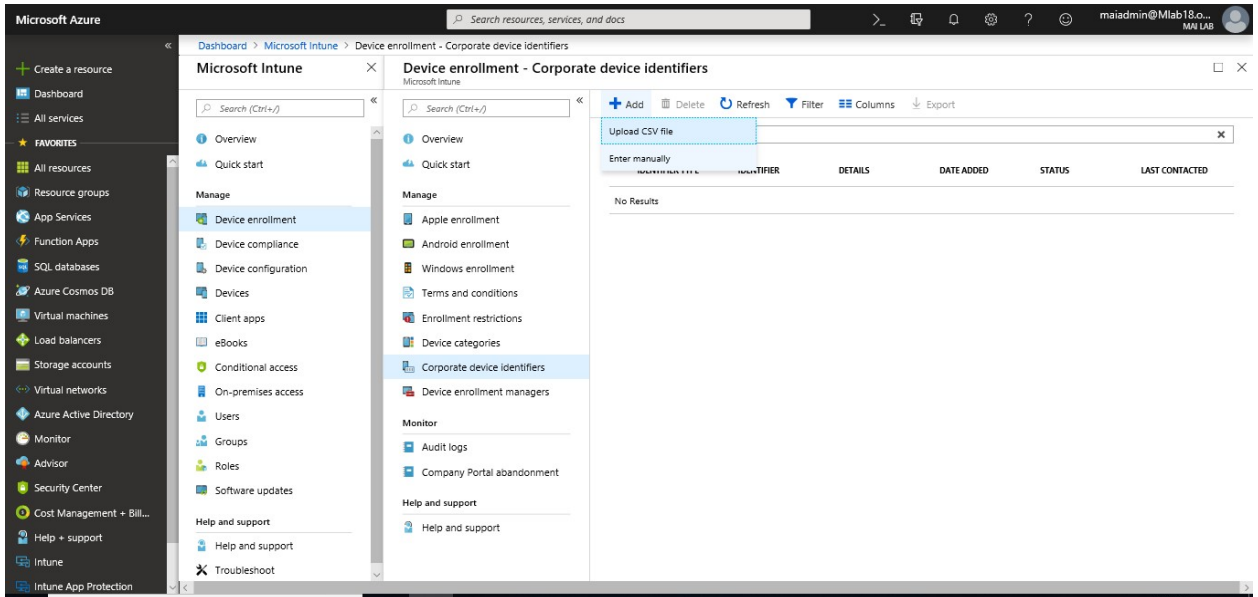
- Enrolled with a [device enrollment manager](#) account (all platforms)
- Enrolled with the Apple Device Enrollment Program, Apple School Manager, or [Apple Configurator](#) (iOS only)
- [Identified as corporate-owned before enrollment](#) with an international mobile equipment identifier (IMEI) numbers (all platforms with IMEI numbers) or serial number (iOS and Android)
- Joined to Azure Active Directory as a Windows 10 Enterprise device
- Set as corporate in the [device's properties list](#). After enrollment, you can change the ownership setting between **Personal** and **Corporate**.

Identify Corporate-owned Devices with IMEI or Serial number

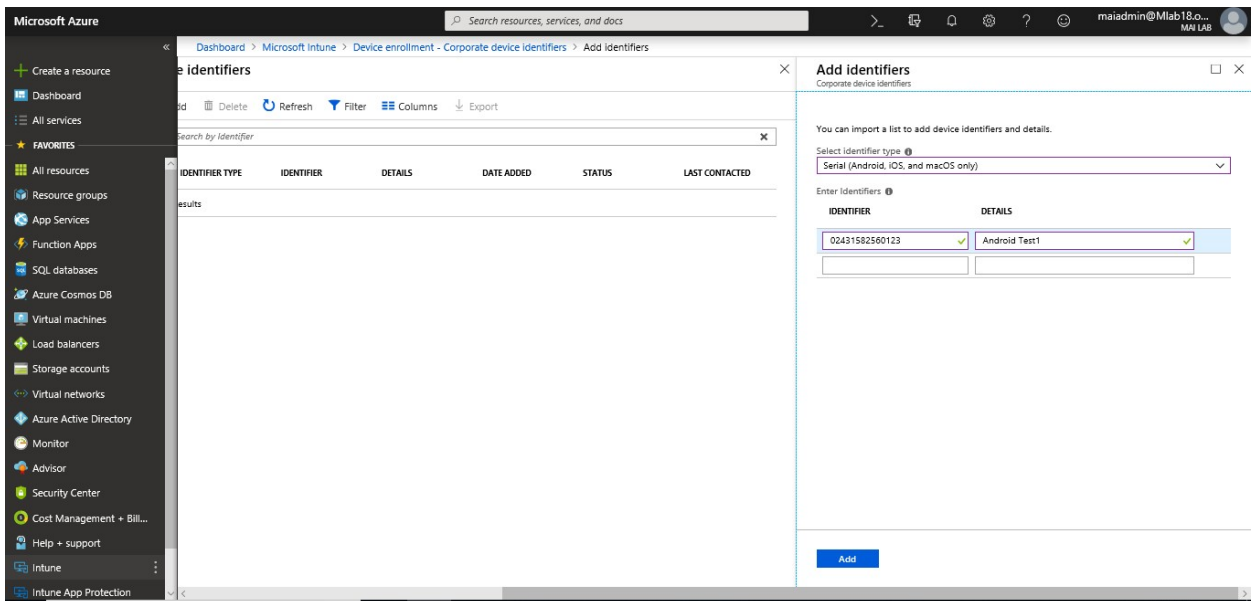
As an Intune admin, you can create and import a comma-separated value (.csv) file that lists IMEI numbers or serial numbers. Intune uses these identifiers to specify device ownership as corporate during device enrollment. You can declare IMEI numbers for all supported platforms. You can only declare serial number for iOS, macOS, and Android devices. Each IMEI or serial number can have details specified in the list for administrative purposes.

Manually Enter Corporate Identifiers

1. In [Intune portal](#), choose **Device enrollment > Corporate device identifiers > Add > Enter manually**.

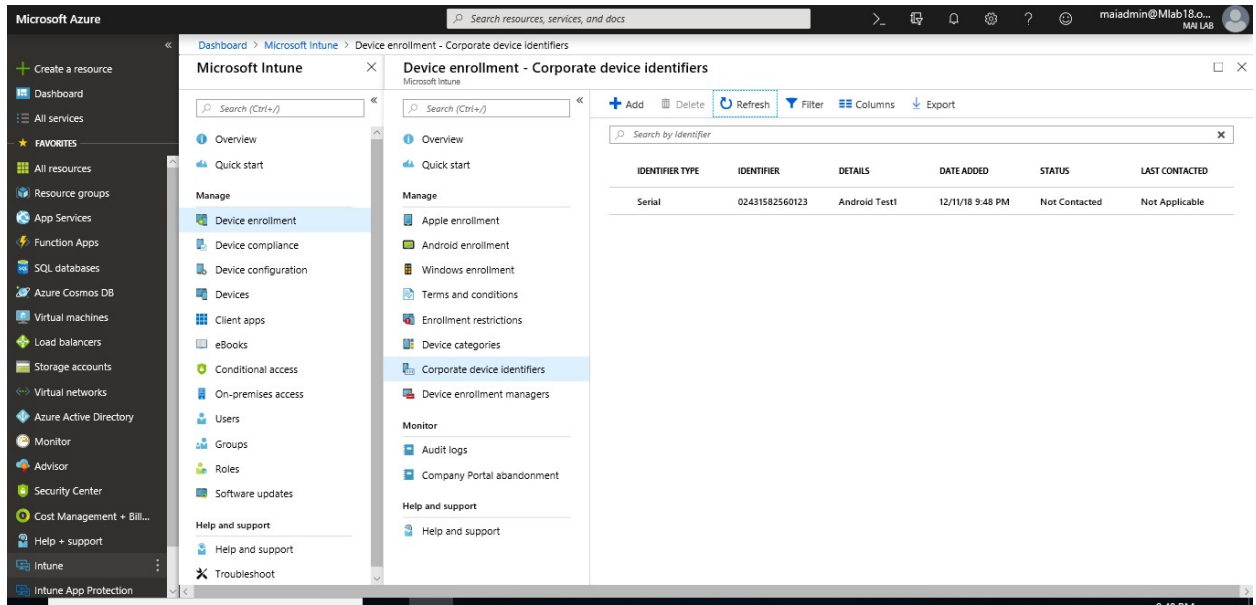


2. In the **Add identifiers** blade, specify the identifier type: **IMEI** or **Serial**.
3. Enter the **Identifier** and **Details** for each identifier you want to add. When you're done entering identifiers, choose **Add**.



4. You can click **Refresh** to see new device identifiers.

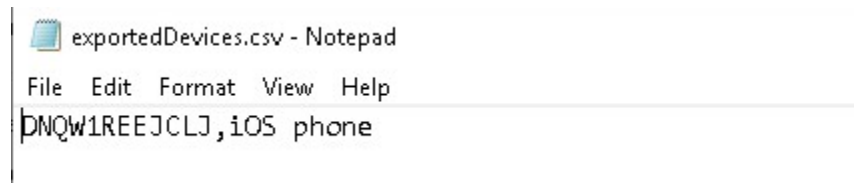
Microsoft Intune step by step on Azure portal



Note: If you entered corporate identifiers that are already in Intune, but have different details, the **Review duplicate identifiers** popup appears. Select the identifiers that you want to overwrite into Intune and choose **Ok** to add the identifiers. For each identifier, only the first duplicate will be compared.

Add Corporate Identifiers by using a .csv file

To create the list, create a two-column, comma-separated value (.csv) list without a header. Add the IMEI or serial numbers in the left column, and the details in the right column. Only one type of ID, IMEI or serial number, can be imported in a single .csv file. Details are limited to 128 characters and are for administrative use only. Details aren't displayed on the device. The current limit is 5,000 rows or 5 MB per .csv file. This will be the **view of csv file** when you **open with notepad**.

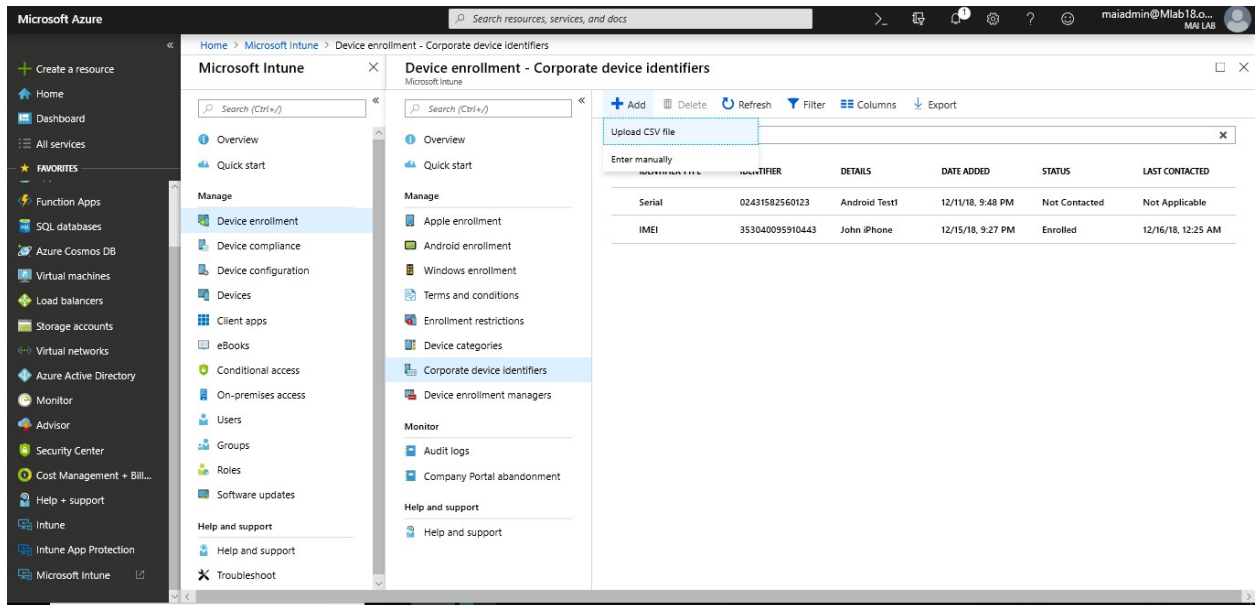


Note: Some Android devices have multiple IMEI numbers. Intune only reads one IMEI number per enrolled device. If you import an IMEI number but it is not the IMEI inventoried by Intune, the device is classified as a personal device instead of a company-owned device. If you import multiple IMEI numbers for a device, uninventoried numbers display **Unknown** for enrollment status.

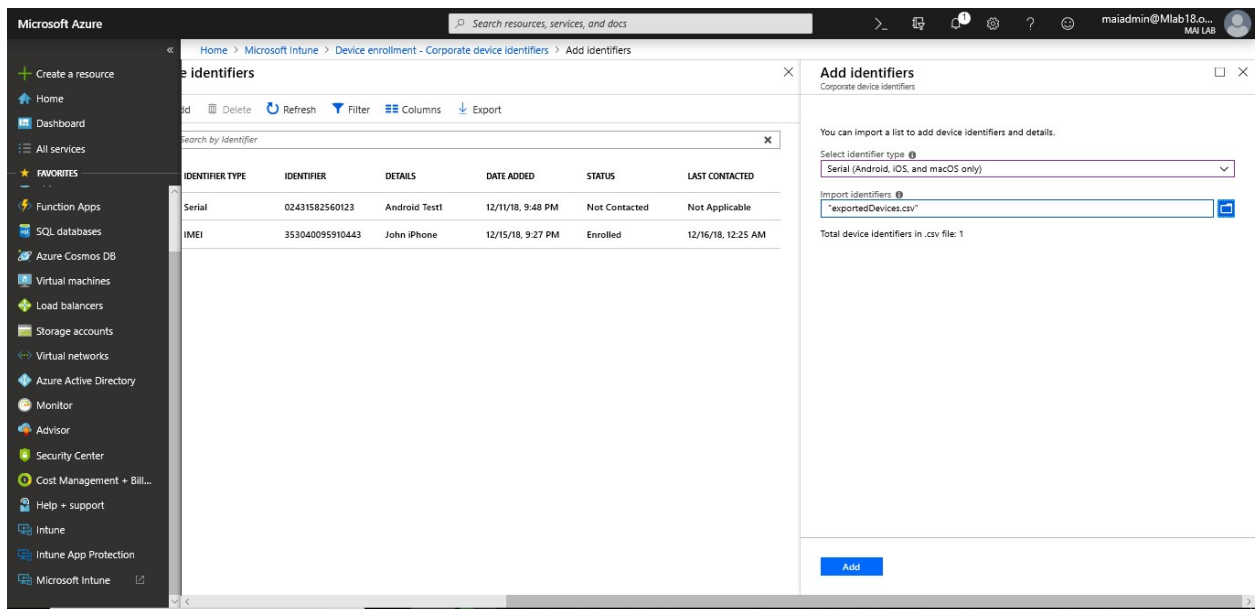
Upload a .csv list of corporate identifiers

Microsoft Intune step by step on Azure portal

1. In [Intune portal](#), choose **Device enrollment** > **Corporate device identifiers** > **Add** > **Upload CSV file**.



2. In the **Add identifiers** blade, specify the identifier type: **IMEI** or **Serial**.
3. Click the folder icon and specify the path to the list you want to import. Navigate to the .csv file and choose **Add**.



Note: If the .csv file contains corporate identifiers that are already in Intune, but have different details, the **Review duplicate identifiers** popup appears. Select the identifiers that you want to overwrite into Intune and choose **Ok** to add the identifiers. For each identifier, only the first duplicate will be compared.

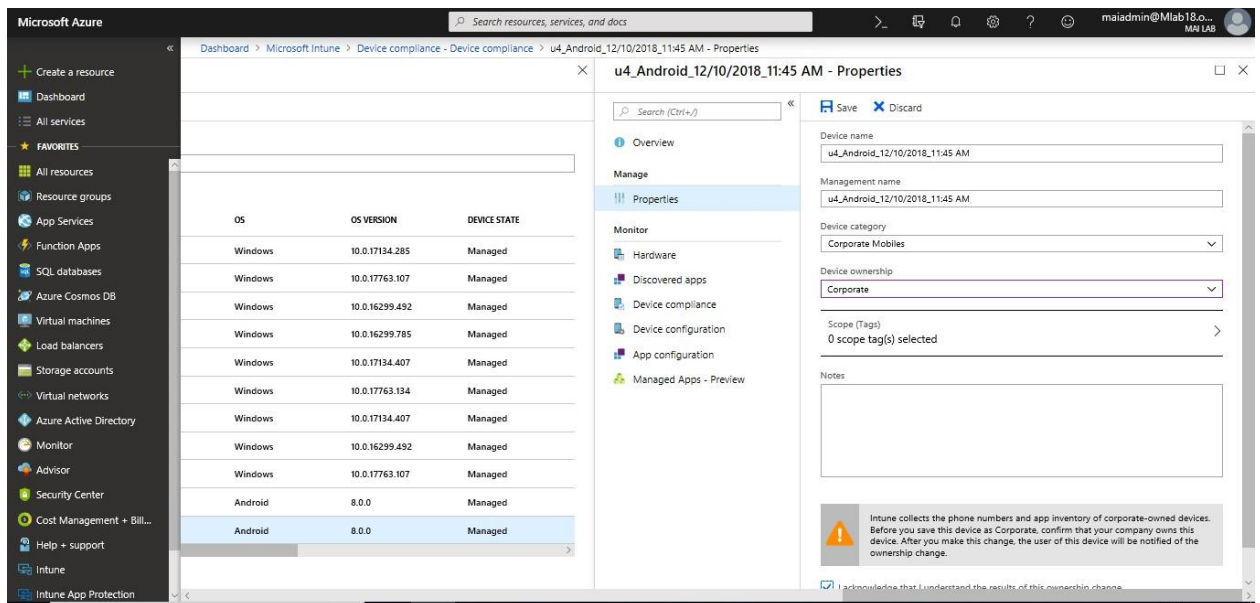
Note: Imported devices are not necessarily enrolled. Devices can have a state of either **Enrolled** or **Not contacted**. **Not contacted** means that the device has never communicated in with the Intune service.

Change Device Ownership

Devices properties display **Ownership** for each device records in Intune. As an admin, you can specify devices as **Personal** or **Corporate**.

To change device ownership:

1. Sign into the [Intune portal](#), go to **Devices** and choose the device that you want.
2. Choose **Properties**.
3. Specify **Device ownership** as **Personal** or **Corporate**. Click **Save**.



Set up iOS device Enrollment with Apple Configurator

Intune supports the enrollment of iOS devices using [Apple Configurator](#) running on a Mac computer. Enrolling with Apple Configurator requires that you USB-connect each iOS device to a Mac computer to set up corporate enrollment. You can enroll devices into Intune with Apple Configurator in two ways:

- **Setup Assistant enrollment** - Wipes the device and prepares it to enroll during Setup Assistant.
- **Direct enrollment** - Does not wipe the device and enrolls the device through iOS settings. This method only supports devices with **no user affinity**.

Apple Configurator enrollment methods can't be used with the [device enrollment manager](#).

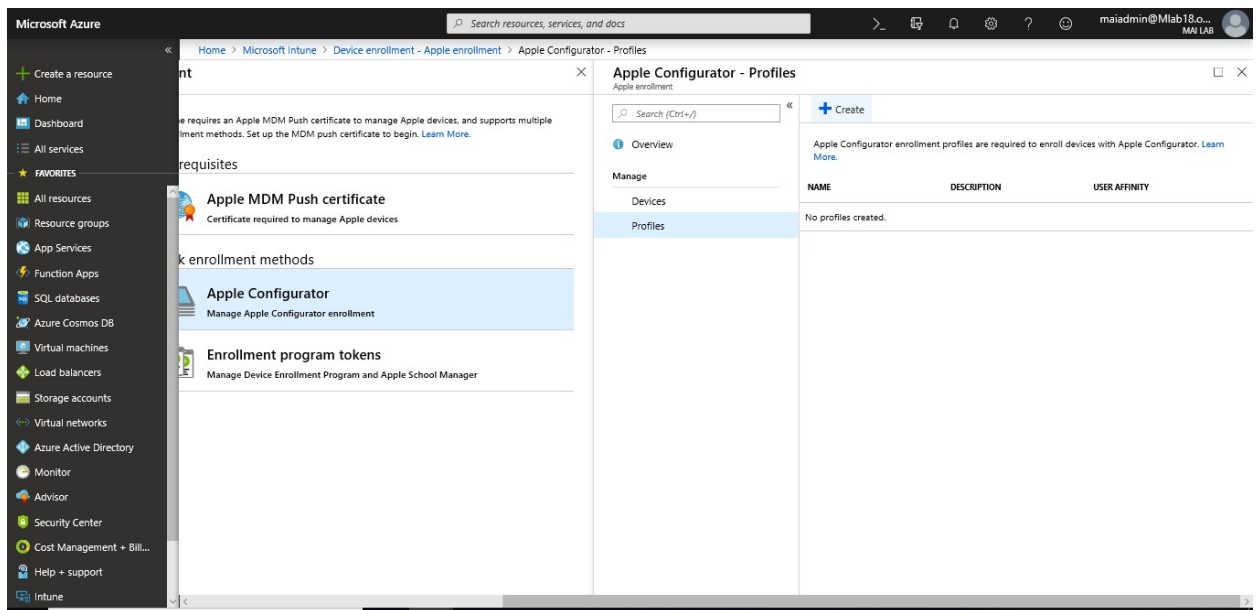
Prerequisites for Apple Configurator

- Physical access to iOS devices
- [Set MDM authority](#)
- [An Apple MDM push certificate](#)
- Device serial numbers (Setup Assistant enrollment only)
- USB connection cables
- MacOS computer running [Apple Configurator 2.0](#)

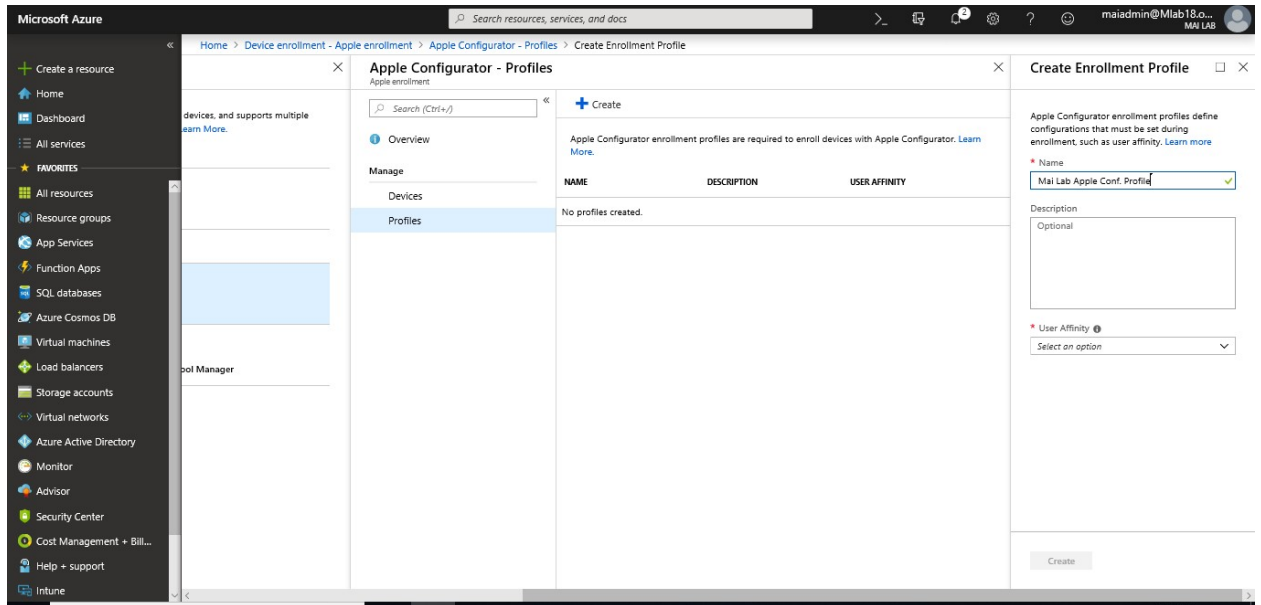
Create an Apple Configurator profile for devices

A device enrollment profile defines the settings applied during enrollment. These settings are applied only once. Follow these steps to create an enrollment profile to enroll iOS devices with Apple Configurator.

1. Sign into the [Intune portal](#), choose **Device enrollment > Apple enrollment > Apple Configurator > Profiles > Create**.

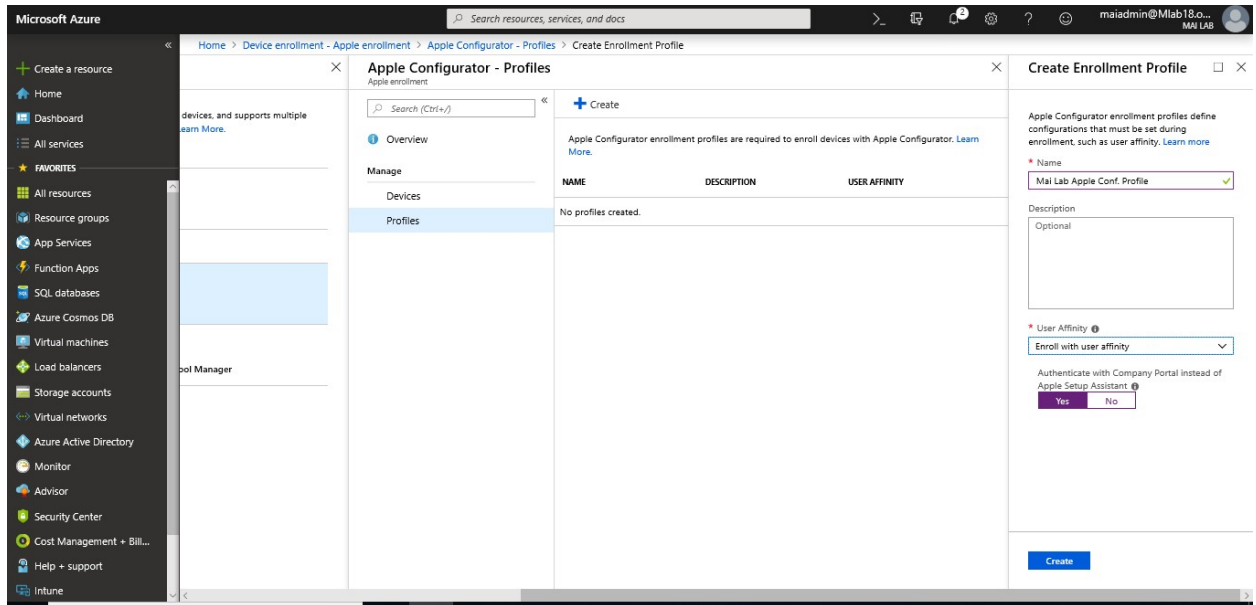


2. Under **Create Enrollment Profile**, type a **Name** and **Description** for the profile for administrative purposes.



Note: Users do not see these details. You can use this Name field to create a dynamic group in Azure Active Directory. Use the profile name to define the enrollmentProfileName parameter to assign devices with this enrollment profile.

3. For **User Affinity**, choose whether devices with this profile must enroll with or without an assigned user.
 - **Enroll with user affinity** - Choose this option for devices that belong to users and that want to use the company portal for services like installing apps. The device must be affiliated with a user with Setup Assistant and can then access company data and email. Only supported for Setup Assistant enrollment. User affinity requires WS-Trust 1.3 Username/Mixed endpoint.
 - **Enroll without User Affinity** - Choose this option for devices unaffiliated with a single user. Use this for devices that perform tasks without accessing local user data. Apps requiring user affiliation (including the Company Portal app used for installing line-of-business apps) won't work. Required for direct enrollment.
4. If you chose **Enroll with User Affinity**, you have the option to let users authenticate with Company Portal instead of the Apple Setup Assistant.



Note: If you want to do any of the following, set **Authenticate with Company Portal instead of Apple Setup Assistant** to **Yes**.

- use multifactor authentication
- prompt users who need to change their password when they first sign in
- prompt users to reset their expired passwords during enrollment

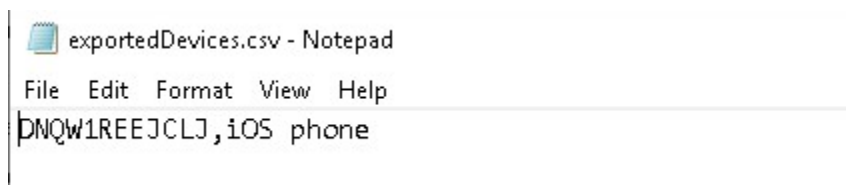
These are not supported when authenticating with Apple Setup Assistant.

5. Choose **Create** to save the profile.

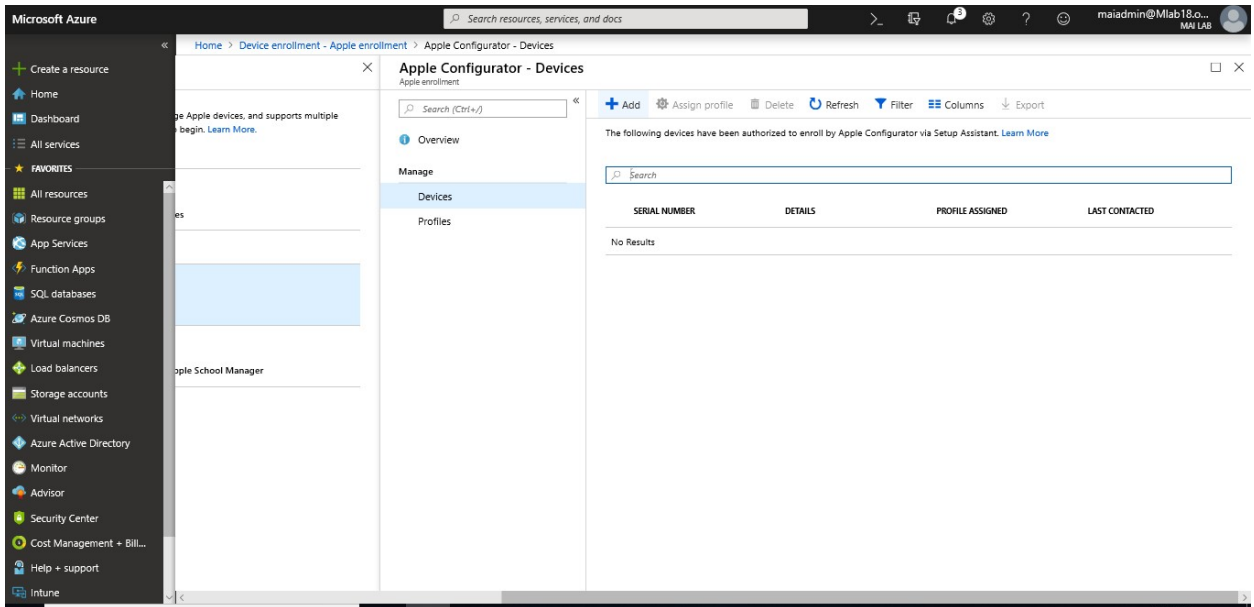
Setup Assistant Enrollment

Step 1: Add Apple Configurator serial numbers

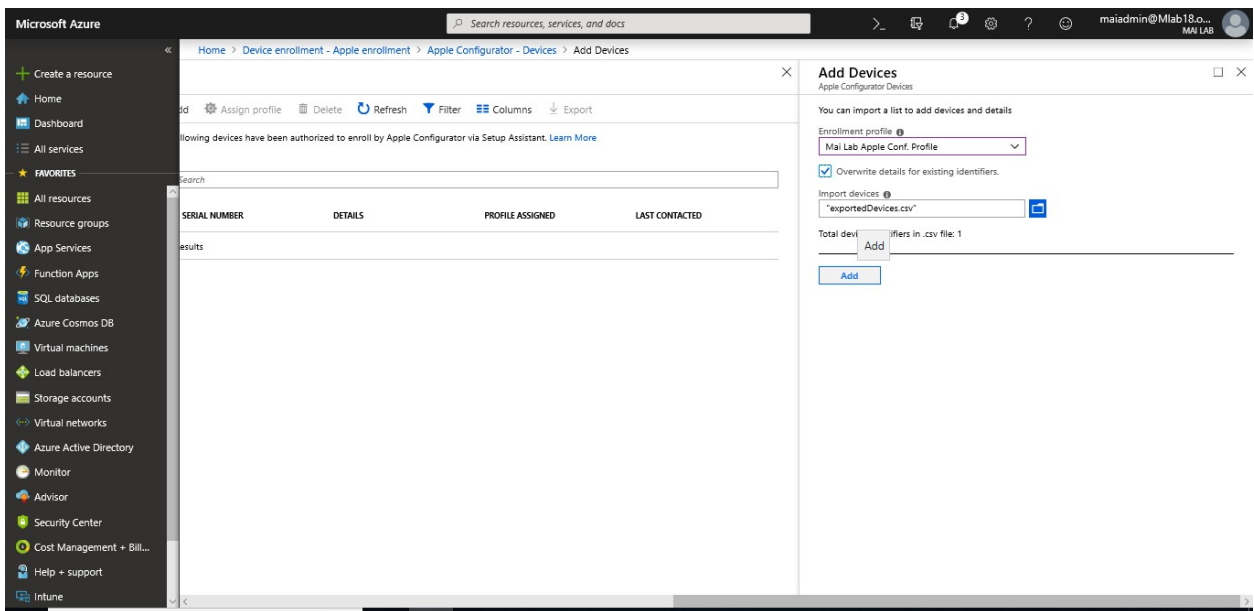
1. Create a two-column, comma-separated value (.csv) list without a header. Add the serial number in the left column, and the details in the right column. The current maximum for the list is 5,000 rows. In a text editor, the .csv list looks like this:



2. In [Intune portal](#), choose **Device enrollment** > **Apple enrollment** > **Apple Configurator** > **Devices** > **Add**.



3. Select an **Enrollment profile** to apply to the serial numbers you're importing. If you want the new serial number details to overwrite any existing details, choose **Overwrite details for existing identifiers**.
4. Under **Import Devices**, browse to the csv file of serial numbers, and select **Add**.

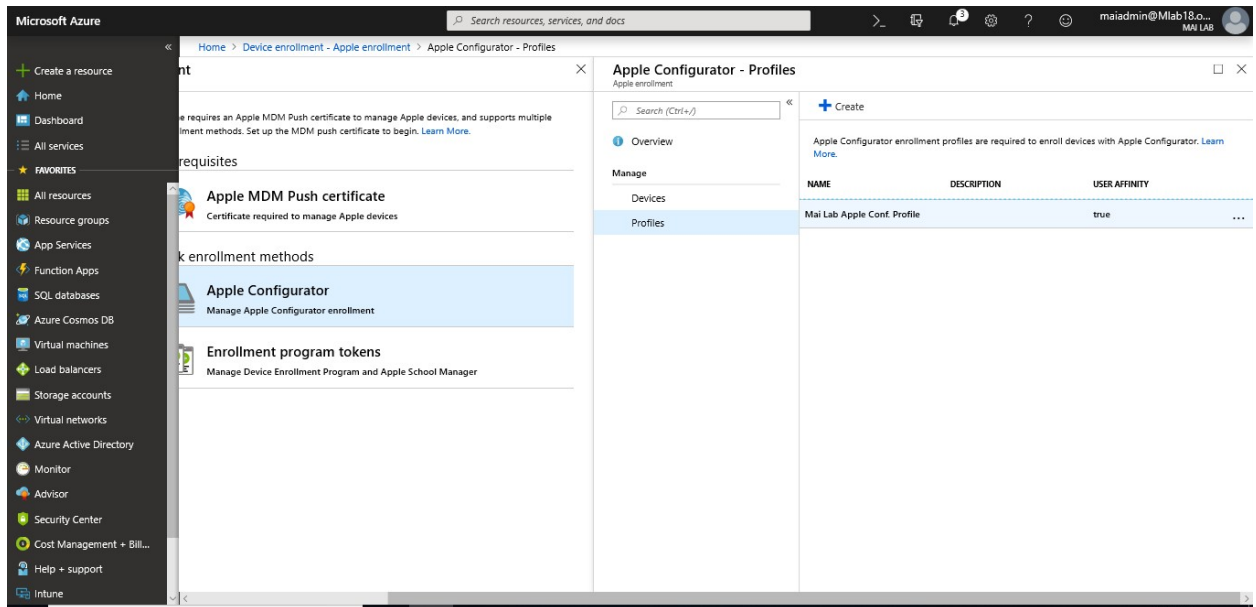


Step 2: Export the profile

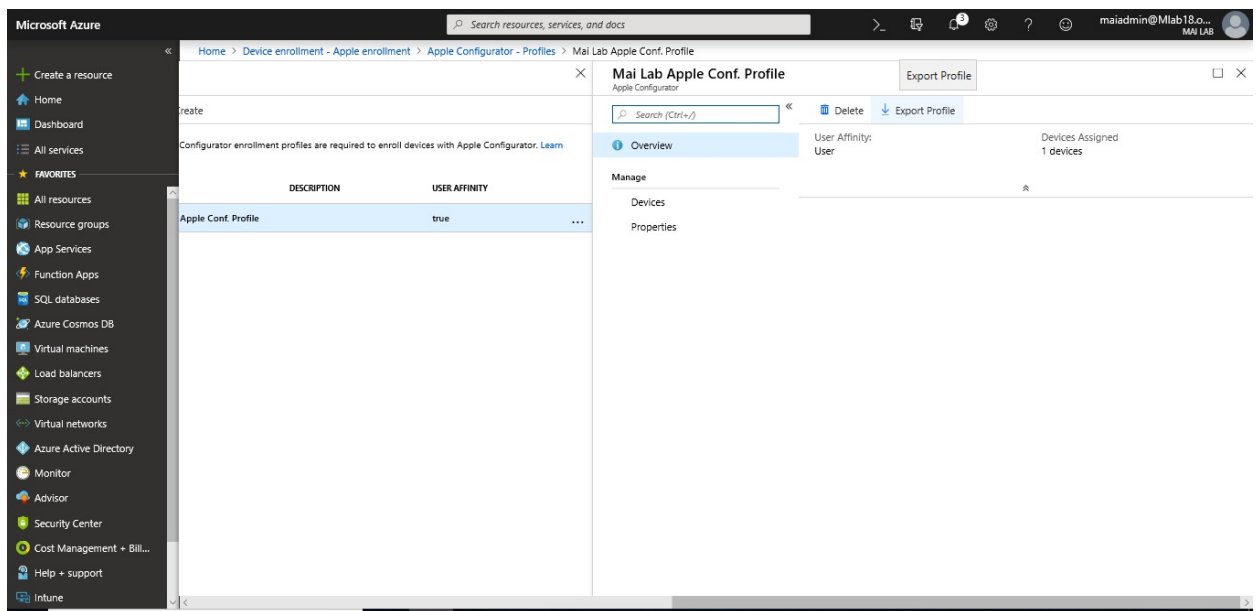
After you create the profile and assign serial numbers, you must export the profile from Intune as a URL. You then import it into Apple Configurator on a Mac for deployment to devices.

Microsoft Intune step by step on Azure portal

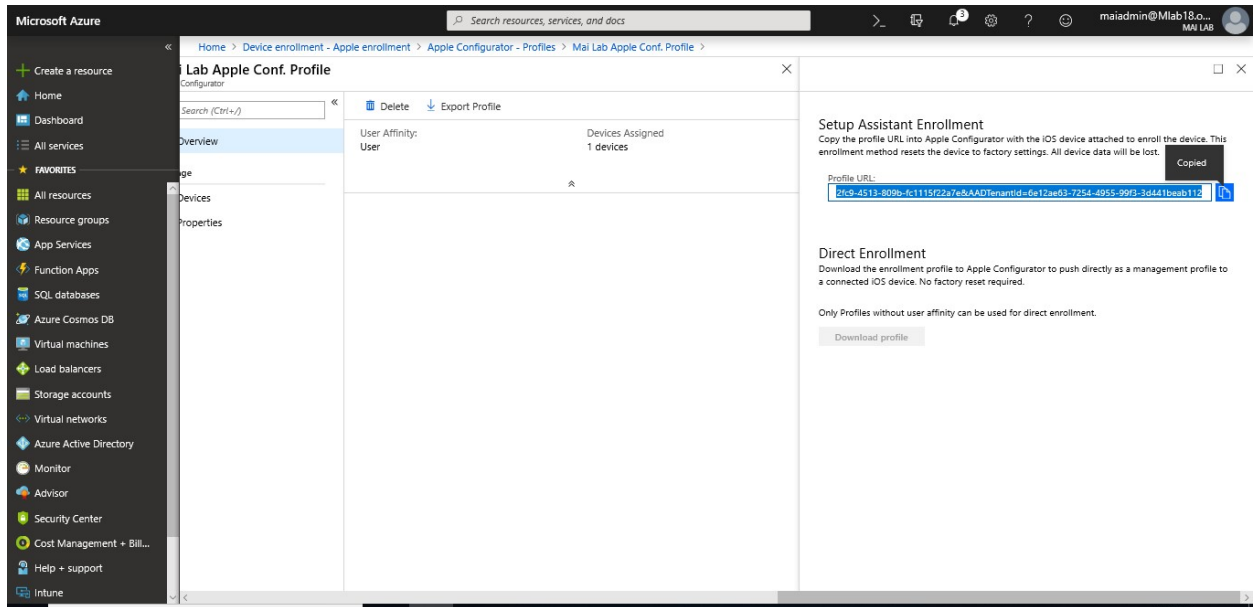
1. In [Intune portal](#), choose **Device enrollment** > **Apple enrollment** > **Apple Configurator** > **Profiles** > choose the profile to export.



2. On the profile, select **Export Profile**.



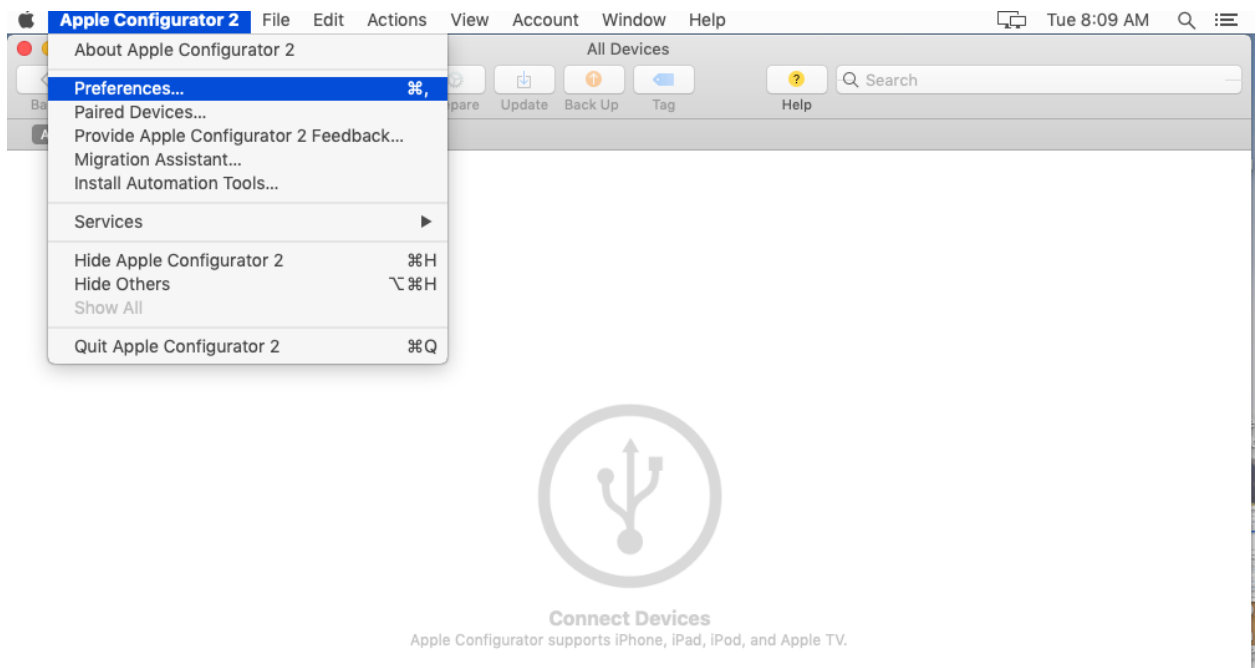
3. Copy the **Profile URL**. You can then add it in Apple Configurator to define the Intune profile used by iOS devices.



4. Next you import this profile to Apple Configurator in the following procedure to define the Intune profile used by iOS devices.

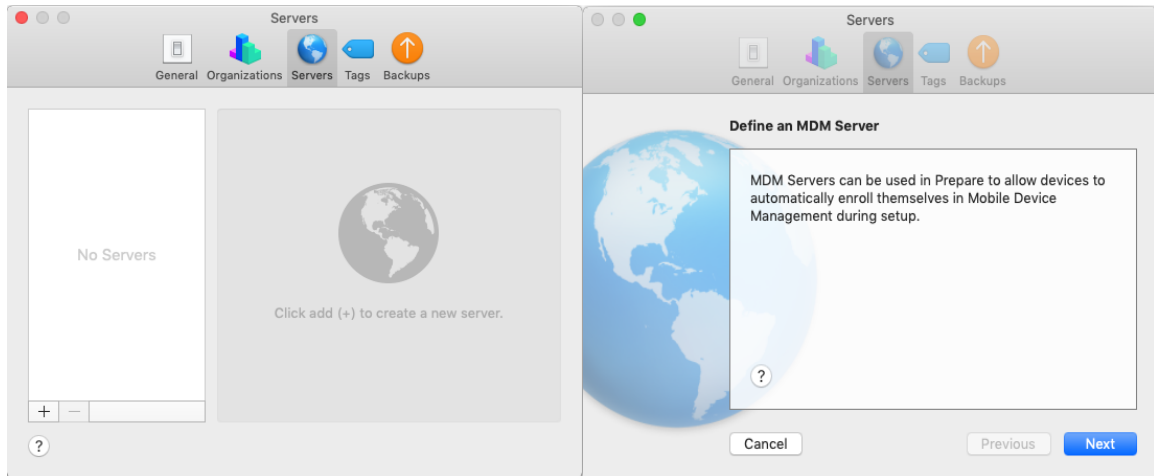
Step 3: Enroll devices with Setup Assistant

1. On a Mac computer, open **Apple Configurator 2**. In the menu bar, choose **Apple Configurator 2**, and then choose **Preferences**.

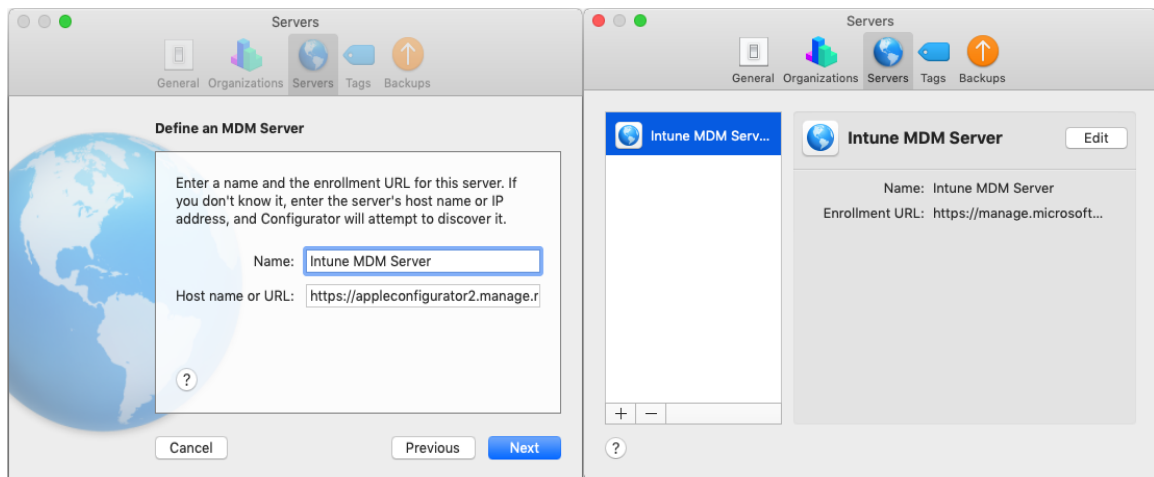


Note: Devices are reset to factory configurations during the enrollment process. As a best practice, reset the device and turn it on. Devices should be at the **Hello** screen when you connect the device.

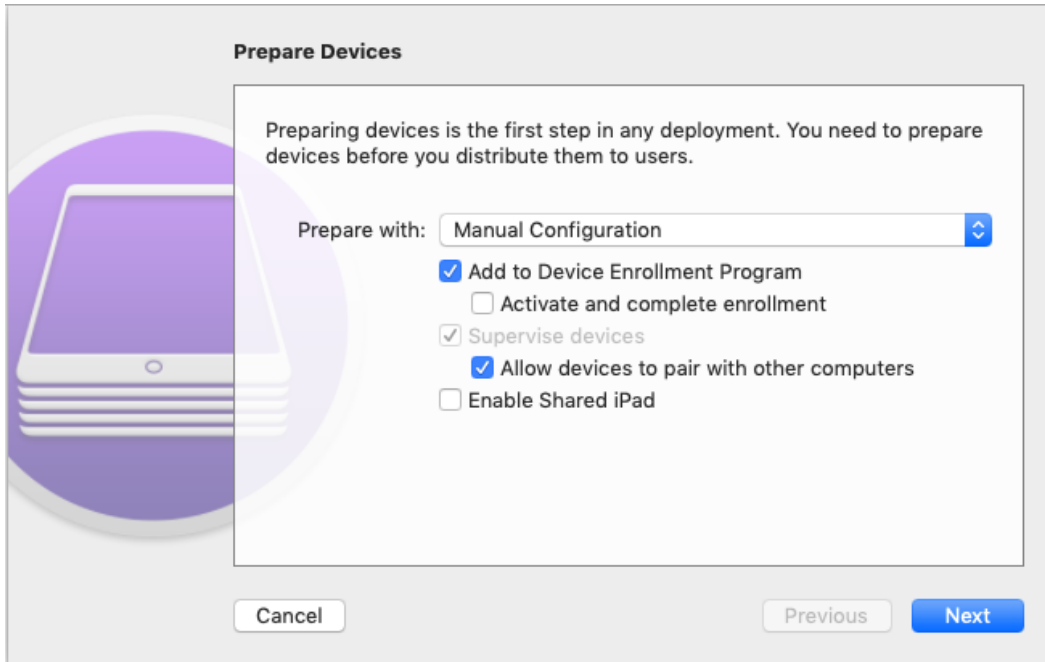
2. In the **preferences** pane, select **Servers** and choose the plus symbol (+) to launch the MDM Server wizard. Choose **Next**.



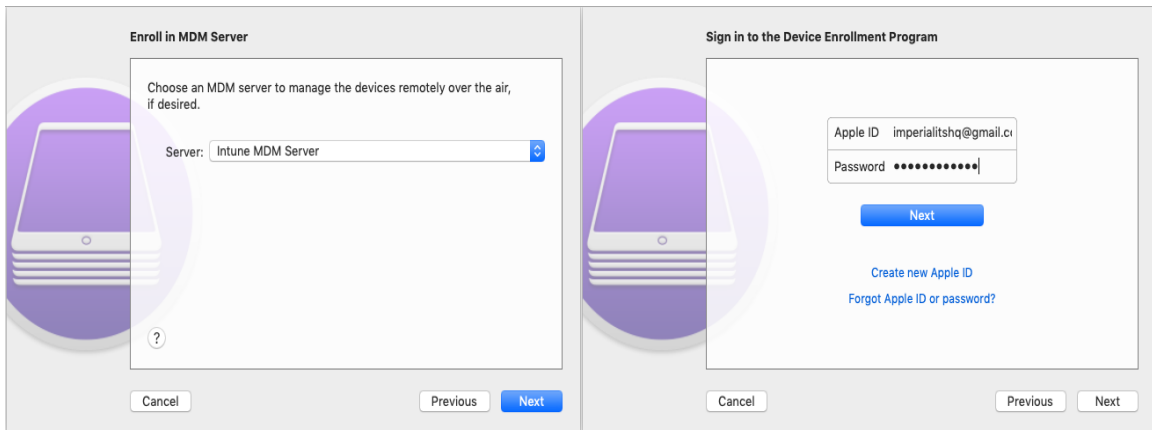
3. Enter the **Host name or URL** and **enrollment URL** for the MDM server under Setup Assistant enrollment for iOS devices with Microsoft Intune. For the Enrollment URL, enter the enrollment profile URL exported from Intune. Choose **Next**. You can safely disregard a warning stating "server URL is not verified." To continue, choose **Next** until the wizard is finished.



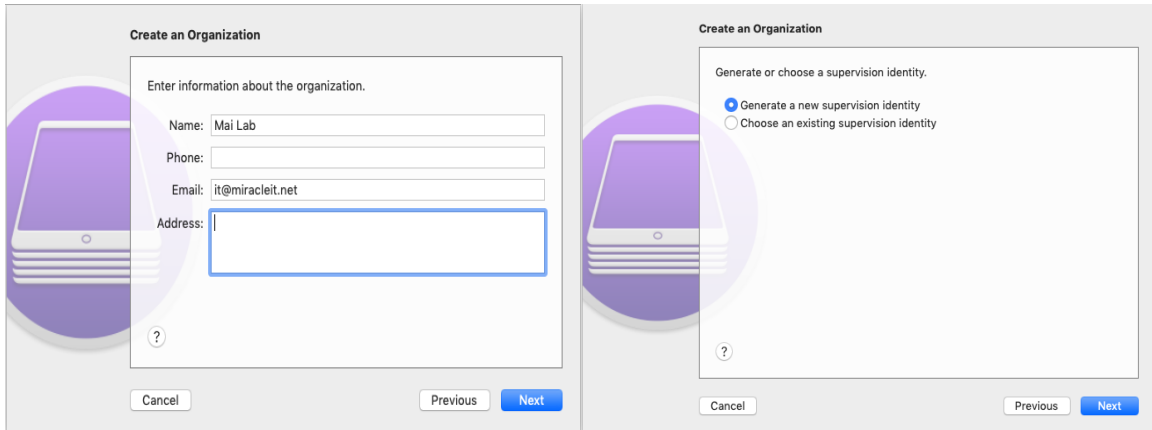
4. Connect the iOS mobile devices to the Mac computer with a USB adapter.
5. Select the iOS devices you want to manage, and then choose **Prepare**. On the **Prepare iOS Device** pane, select **Manual**, and then choose **Next**.



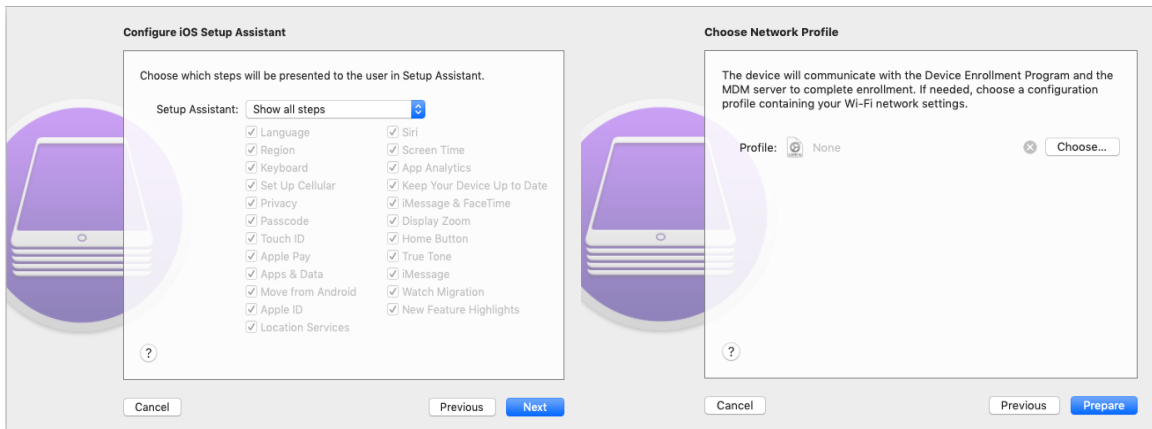
6. On the **Enroll in MDM Server** pane, select the server name you created, and then choose **Next**.



7. On the **Supervise Devices** pane, select the level of supervision, and then choose **Next**.
8. On the **Create an Organization** pane, choose the **Organization** or create a new organization, and then choose **Next**.



9. On the **Configure iOS Setup Assistant** pane, choose the steps to be presented to the user, and then choose **Prepare**. If prompted, authenticate to update trust settings.



10. When the iOS device finishes preparing, disconnect the USB cable.

Step 4: Distribute devices

The devices are now ready for corporate enrollment. Turn off the devices and distribute them to users. When users turn on their devices, Setup Assistant starts.

After users receive their devices, they must complete Setup Assistant. Devices configured with user affinity can install and run the Company Portal app to download apps and manage devices.

Direct Enrollment

When you directly enroll iOS devices with Apple Configurator, you can enroll a device without acquiring the device's serial number. You can also name the device for identification purposes before Intune captures the device name during enrollment. The Company Portal app is not supported for directly enrolled devices. This method does not wipe the device.

Microsoft Intune step by step on Azure portal

Apps requiring user affiliation, including the Company Portal app used for installing line-of-business apps, cannot be installed.

Note: At this method, you need to create profile **Enroll without infinity user** to be able for direct enrollment.

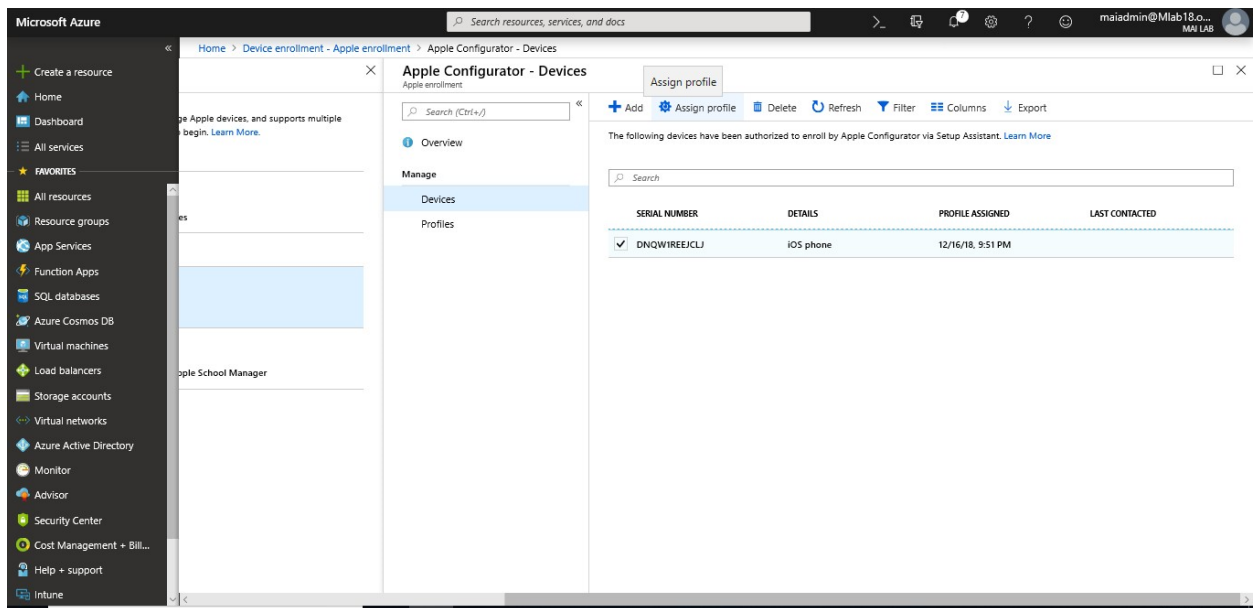
Step 1: Reassign a profile to device serial numbers

You can assign an enrollment profile when you import iOS serial numbers for Apple Configurator enrollment. You can also assign profiles from two places in the Azure portal:

- **Apple Configurator devices**
- **Apple Configurator profiles**

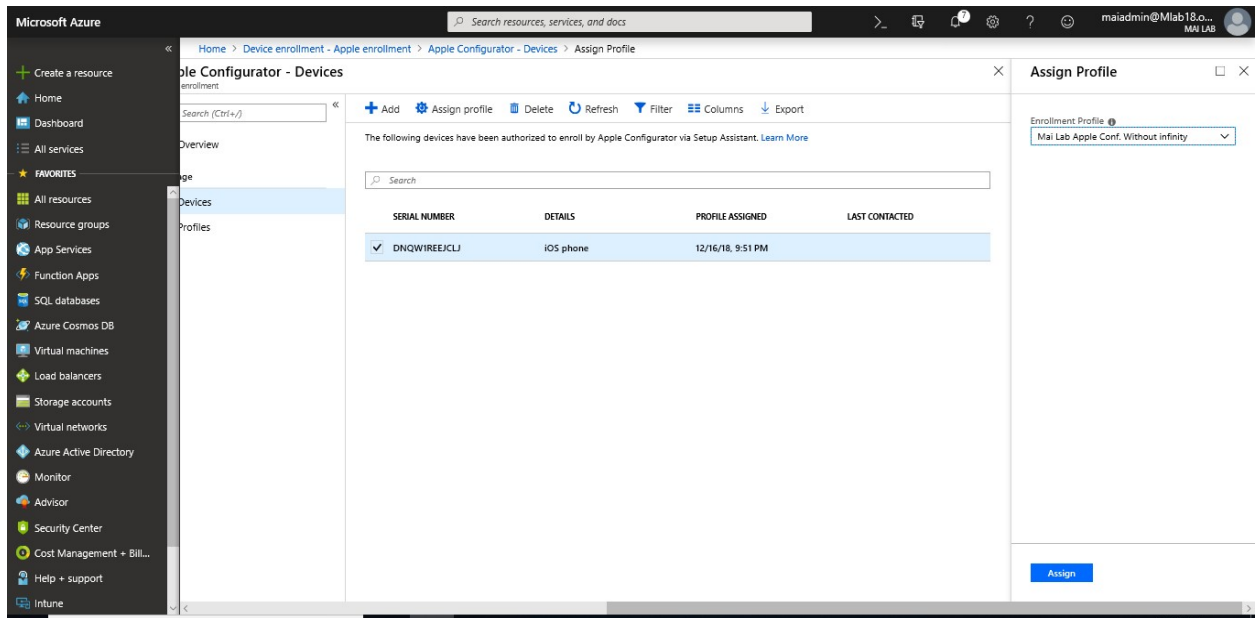
Assign from Apple Configurator devices

1. In [Intune portal](#), choose **Device enrollment > Apple enrollment > Apple Configurator > Devices** > choose the serial numbers > **Assign profile**.



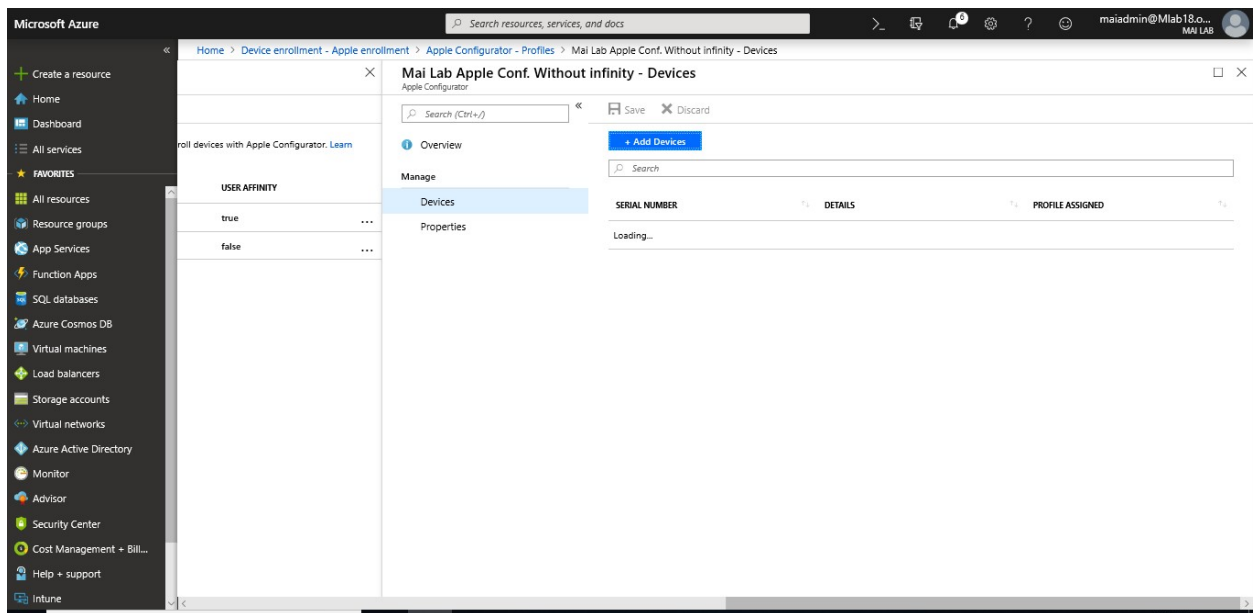
2. Under **Assign Profile**, choose the **New profile** you want to assign, and then choose **Assign**.

Microsoft Intune step by step on Azure portal



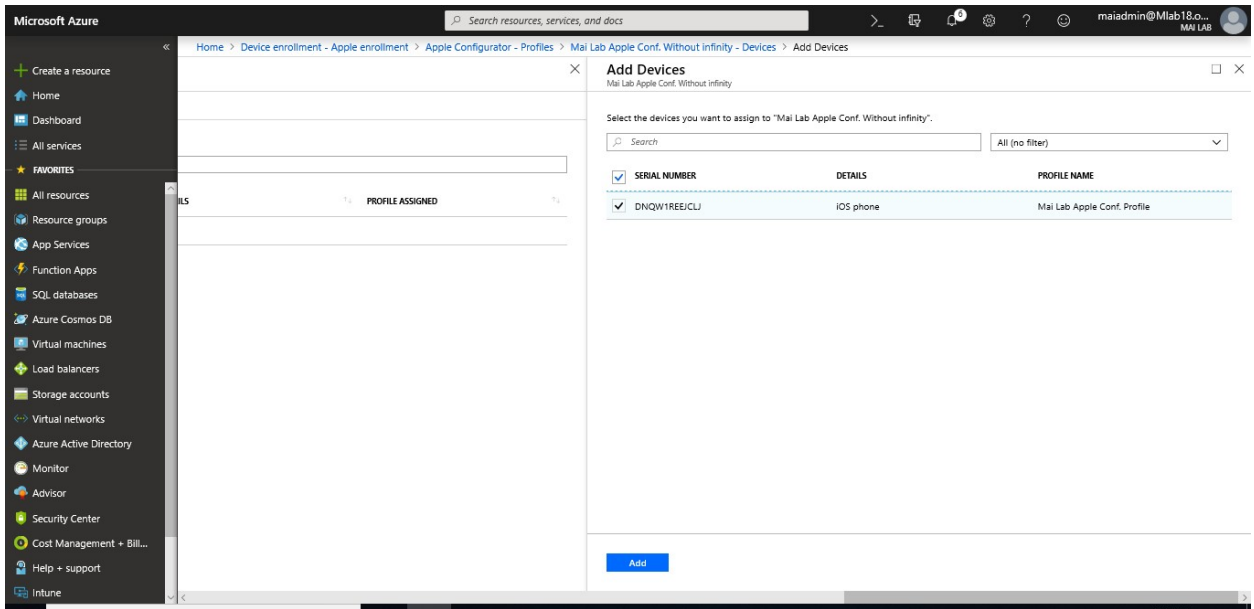
Assign from profiles

1. In [Intune portal](#), choose **Device enrollment** > **Apple enrollment** > **Apple Configurator** > **Profiles** > choose a profile.
2. In the profile, choose **Add Devices**.

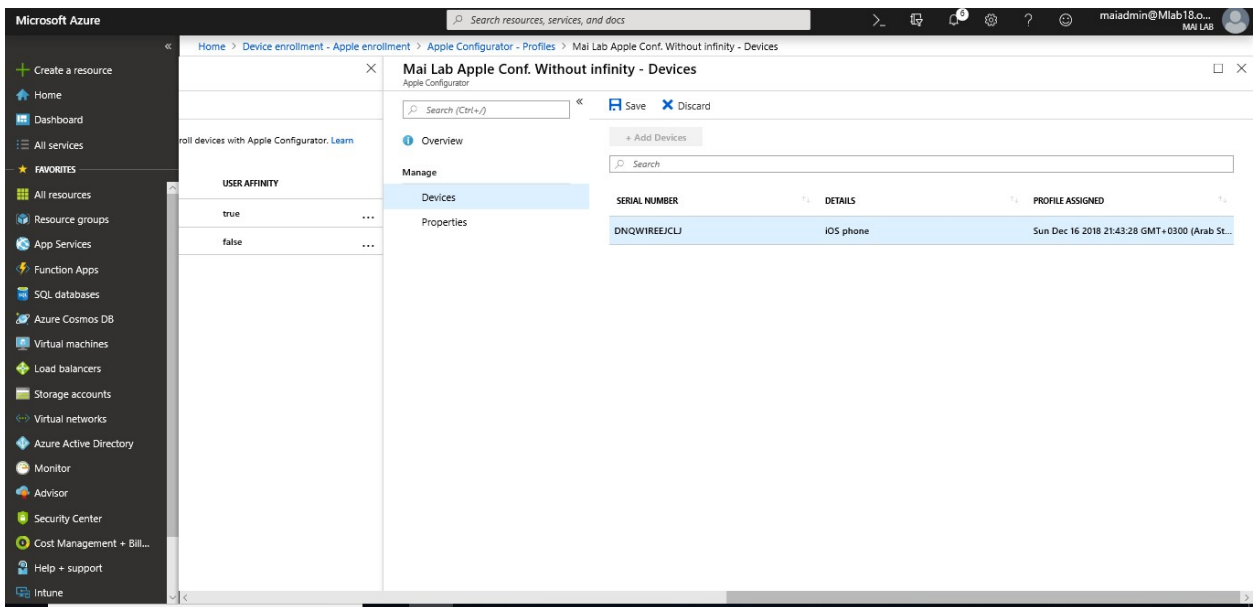


3. Filter to find device serial numbers you want to assign to the profile, select the devices, and then choose **Add**.

Microsoft Intune step by step on Azure portal



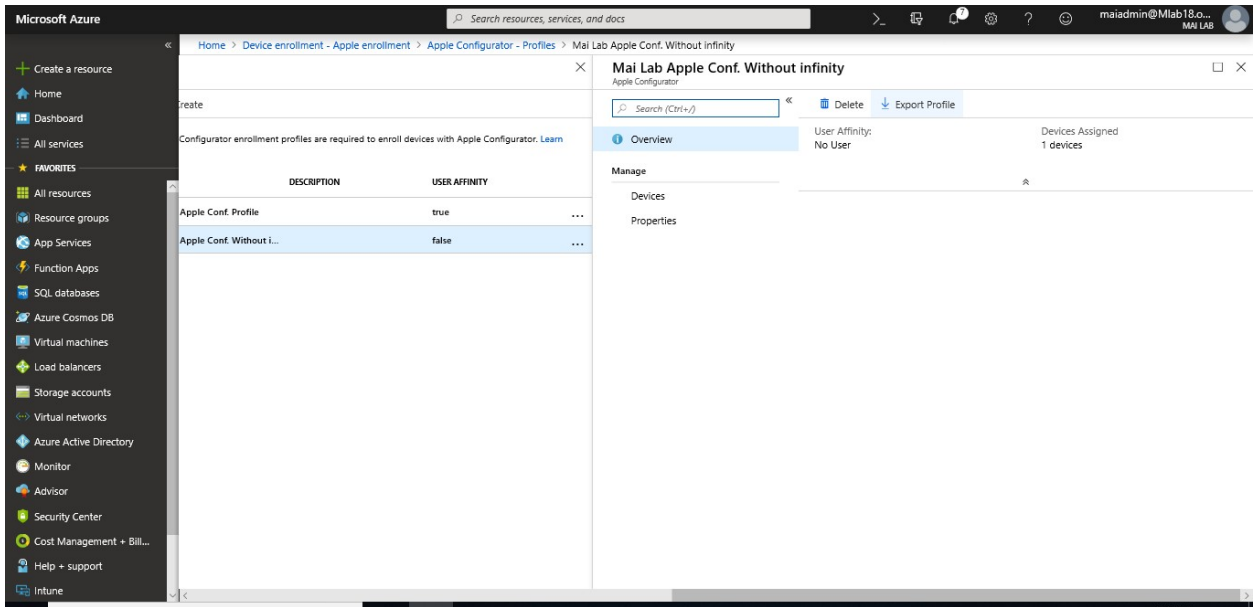
4. Click Save.



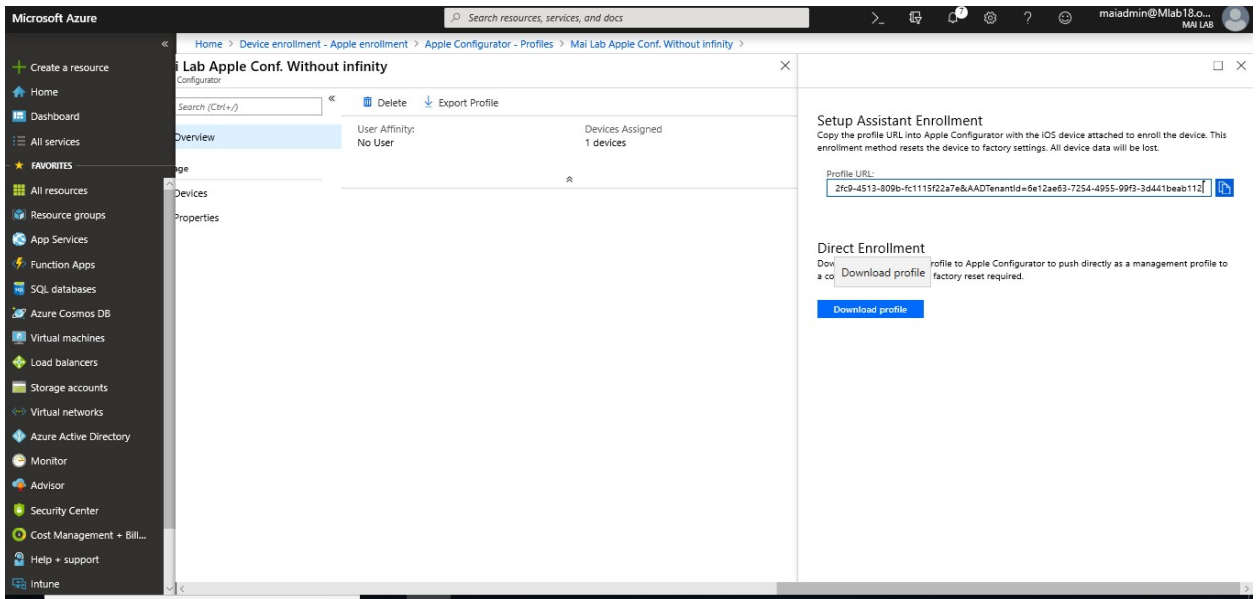
Step 2: Export the profile as .mobileconfig to iOS devices

1. In [Intune portal](#), choose **Device enrollment > Apple enrollment > Apple Configurator > Profiles** > choose the profile to export > **Export Profile**.

Microsoft Intune step by step on Azure portal



2. Under **Direct enrollment**, choose **Download profile**, and save the file.



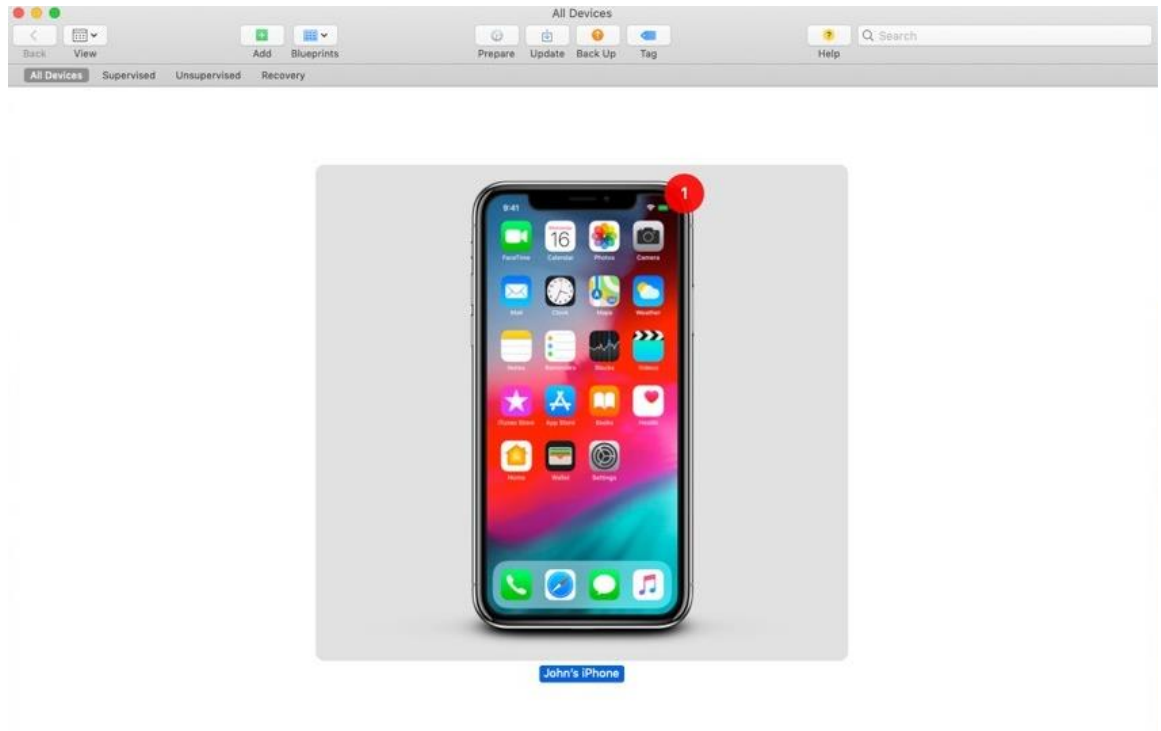
Note: An enrollment profile file is only valid for two weeks at which time you must re-create it.

Step 3: Enroll device directly

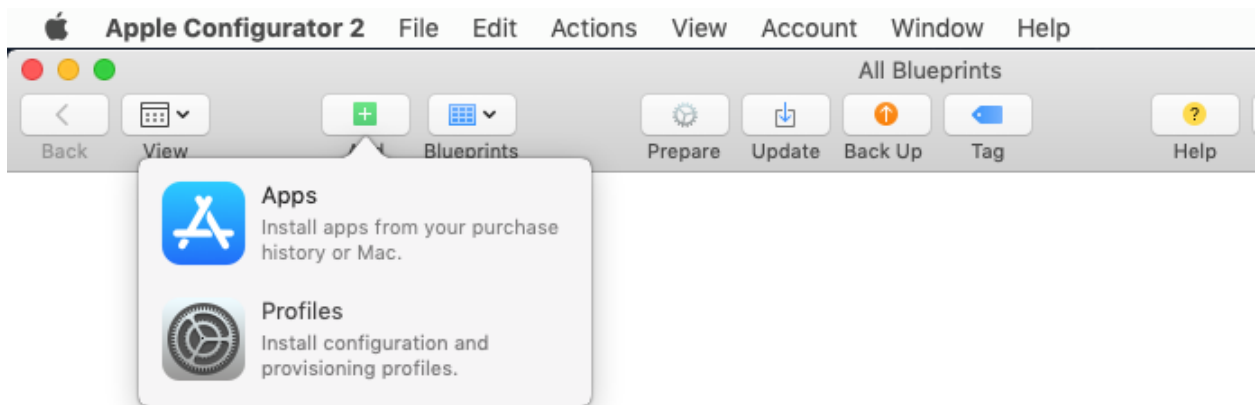
1. Transfer the file to a Mac computer running [Apple Configurator](#) to push directly as a management profile to iOS devices.
2. Prepare the device with Apple Configurator by using the following steps:
 - a) On a Mac computer, open **Apple Configurator 2.0**.

Microsoft Intune step by step on Azure portal

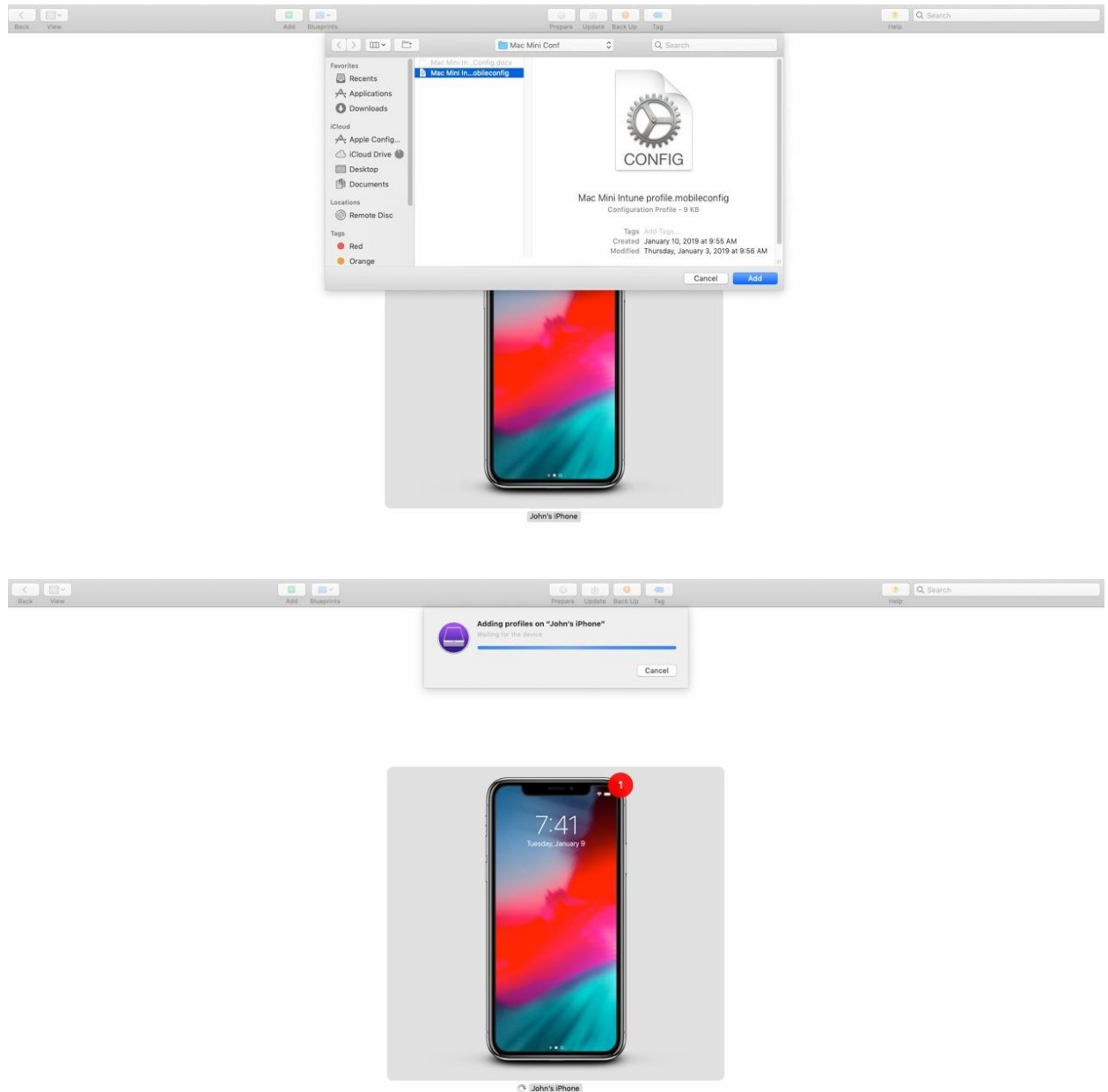
- b) Connect the iOS device to the Mac computer with a USB cord. Close Photos, iTunes, and other apps that open for the device when the device is detected.



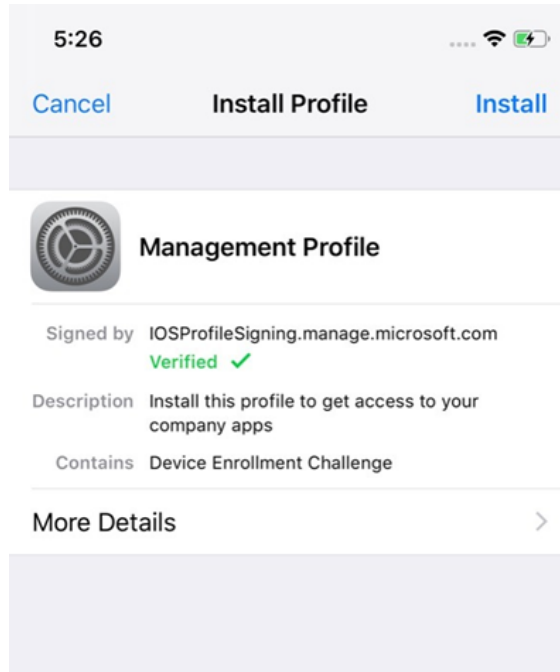
- c) In Apple Configurator, choose the connected iOS device, and then choose the **Add** button. Options that can be added to the device appear in the drop-down list. Choose **Profiles**.



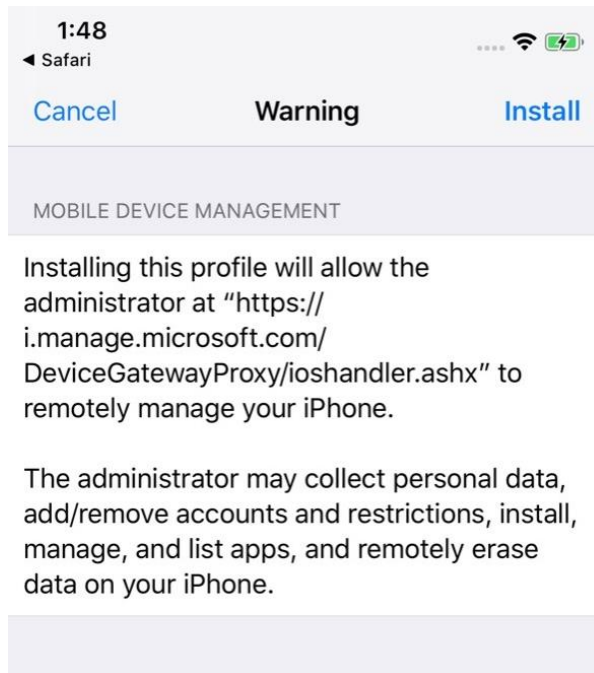
- d) Use the file picker to select the .mobileconfig file that you exported from Intune, and then choose **Add**. The profile is added to the device. If the device is Unsupervised, the installation requires acceptance on the device.



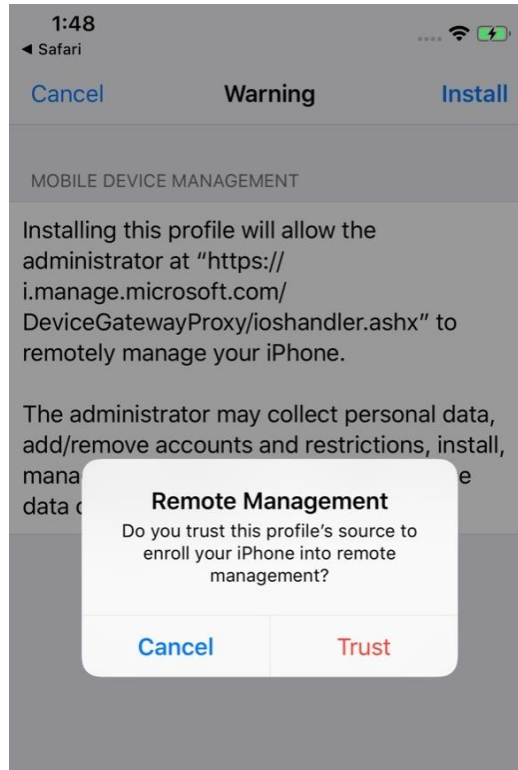
3. Use the following steps to install the profile on the iOS device. The device must have already completed the Setup Assistant and be ready to use. If enrollment entails app deployments, the device should have an Apple ID set up because the app deployment requires that you have an Apple ID signed in for the App Store.
 - a) Unlock the iOS device.
 - b) In the **Install profile** dialog box for **Management profile**, choose **Install**.



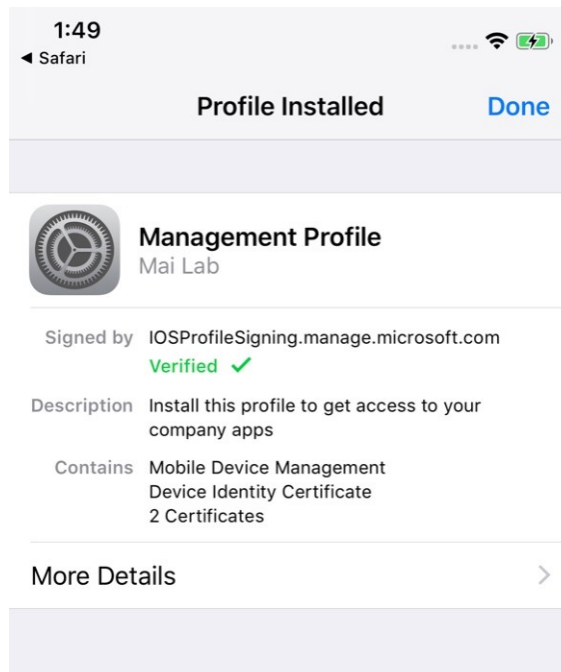
- c) Provide the Device Passcode or Apple ID, if necessary.
- d) Accept the **Warning** and choose **Install**.



- e) Accept the **Remote Warning** and choose **Trust**.



f) When the **Profile Installed** box confirms the profile as Installed, choose **Done**.



4. On the iOS device, open **Settings** and go to **General > Device Management > Management Profile**. Confirm that the profile installation is listed and check the iOS

policy restrictions and installed apps. Policy restrictions and apps might take up to 10 minutes to appear on the device.



5. Distribute devices. The iOS device is now enrolled in Intune and managed.

Intune Company Portal Branding

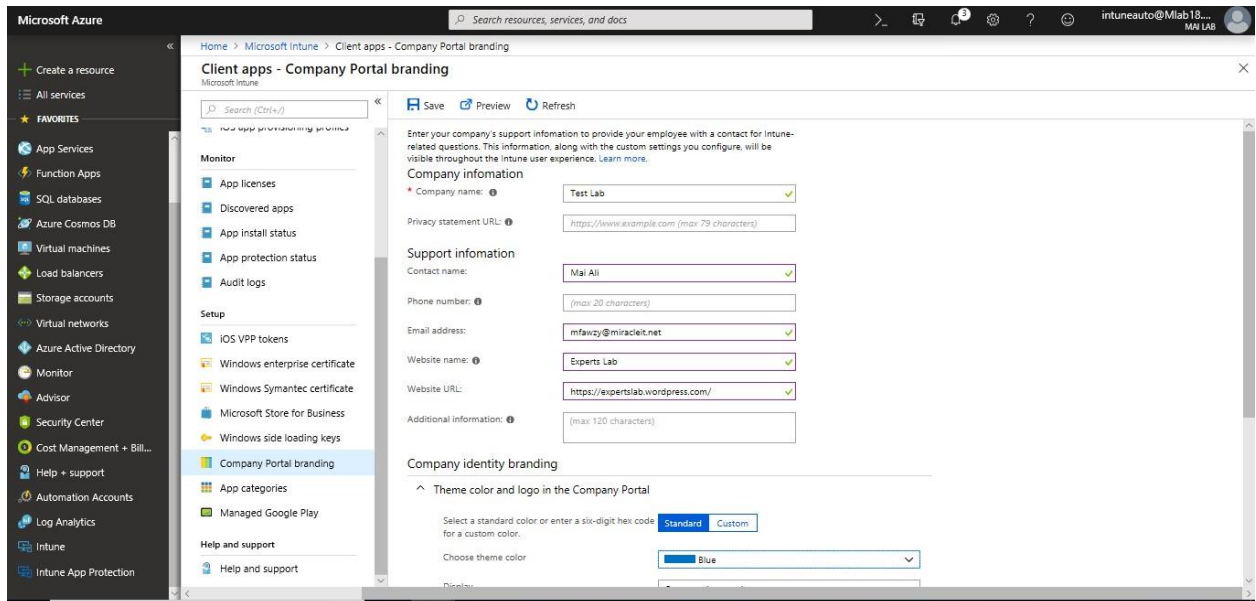
The Microsoft Intune company portal is where users access company data and can do common tasks like enrolling devices, installing apps, and locating information for assistance from your IT department.

Note: When you customize the Company Portal, the configurations apply to both the Company Portal website and Company Portal apps. Users must have an Intune license assigned to access the Company Portal.

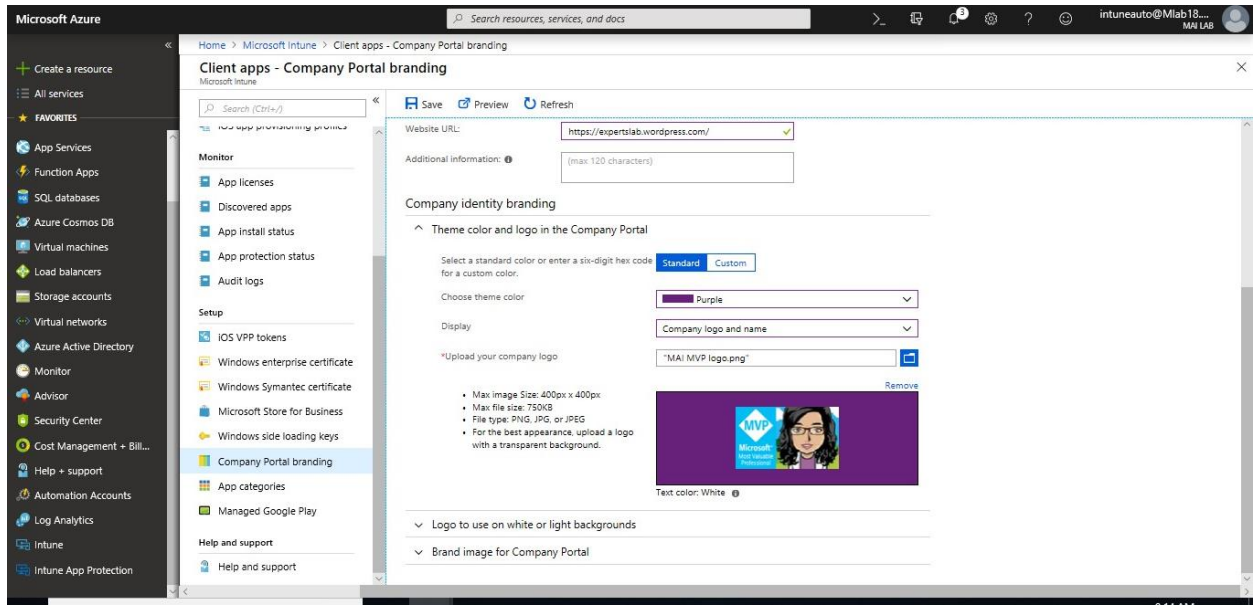
To Configure Company Portal branding, you need to follow below steps:

1. Sign into the [Intune in Azure portal](#). Click **Client Apps** and then click **Company Portal branding**. Enter your company's support information to provide your employee with a contact for Intune-related questions.:
 - **Company Name** – Name of the company portal with max length of 40.
 - **Company privacy statement URL** – URL that specifies company privacy terms.
 - **IT department contact name** – Contact name of IT department with max length of 40.
 - **IT department phone number** – Phone number of IT dept.
 - **IT department email address** – Specify email address of IT dept.
 - **Support website name** – The name of the support website for display.

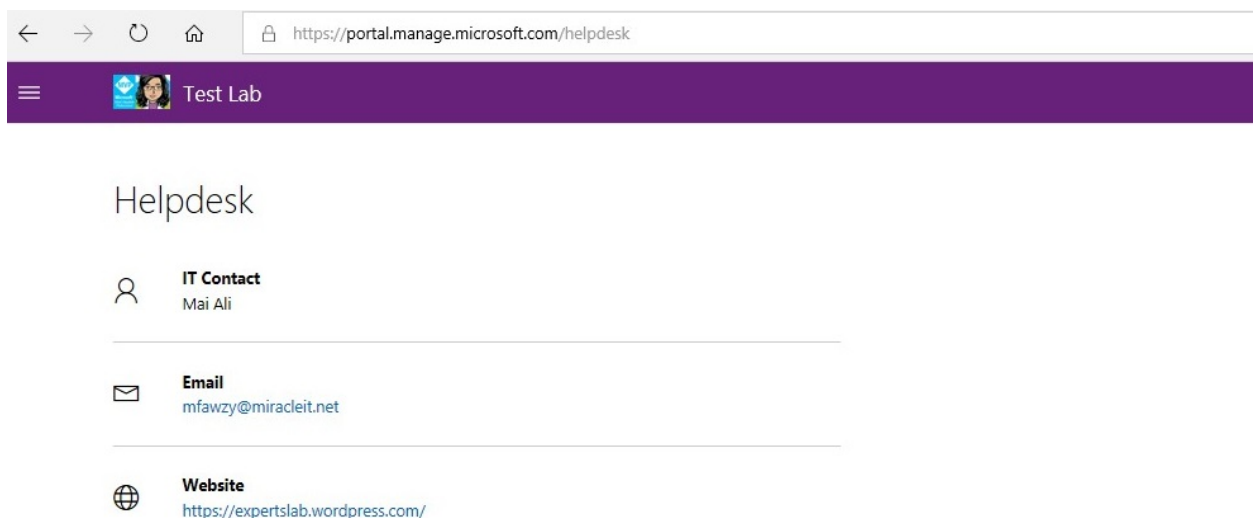
- **Support website URL** – Allows users to use the support website for help.
- **Additional information** – Some more info in case if you want to display on Contact IT page.



2. On **Company identity branding** tab, you can customize your Company Portal with your company logo, company name, theme color and background.
3. On **Theme color and logo in the Company Portal** tab, select a standard color or enter a six-digit hex code for a custom color and upload company logo.
 - **Select a standard color or enter a six-digit hex code:** Choose **Standard** to visually select a color. Choose **Custom** to select a specific color based on a hex code value.
 - **Choose theme color:** Select a theme color to apply to the Company Portal. You can choose from a standard color or enter a specific hex code.
 - **Display:** Select whether to display the **Company logo and name**, the **Company logo only**, or the **Company name only**.
 - **Upload your company logo:** You can upload your company logo to show in your Company Portal. Note the text color is automatically chosen to provide the highest level of contrast. For the best appearance, upload a logo with a transparent background.



4. On **Logo to use on white or light backgrounds** tab, choose a logo that will look best on white or light backgrounds. **Upload your company logo:** This option is available if you have chosen to show the company logo. For the best appearance, upload a logo with a transparent background.
5. On **Brand image for Company Portal** tab, display a brand image that reflects your company brand. **Upload your company logo:** This option is available to allow you to display a background image on the user's profile page in the Company Portal app.
6. Click **Save**. After you save your changes, you can choose **Preview your settings** in the Intune Web Portal at the top of the blade to see how your configurations will look.



Note: When you click on preview, you will only be able to preview brand image on an iOS device.

Chapter 5

Protect Mobile Devices Using Microsoft Intune “MDM”

Microsoft Intune helps you protect the devices you manage, and the data stored on those devices. Mobile device management (MDM) takes a full-device approach to securing and controlling smartphones and tablets. IT can secure access to the device by requiring the use of a passcode and keep sensitive data out of the wrong hands by remotely wiping a lost device, include the ability to enforce policies, track inventory and perform real-time monitoring and pushing App.

Device configuration

Intune configuration policies help you protect and configure devices by controlling a multitude of settings and features. For example:

- You can restrict use of hardware features on the device such as the camera, or Bluetooth.
- You can configure compliant and noncompliant apps. You'll get an alert if a noncompliant app is installed (and some platforms can actually block the install).

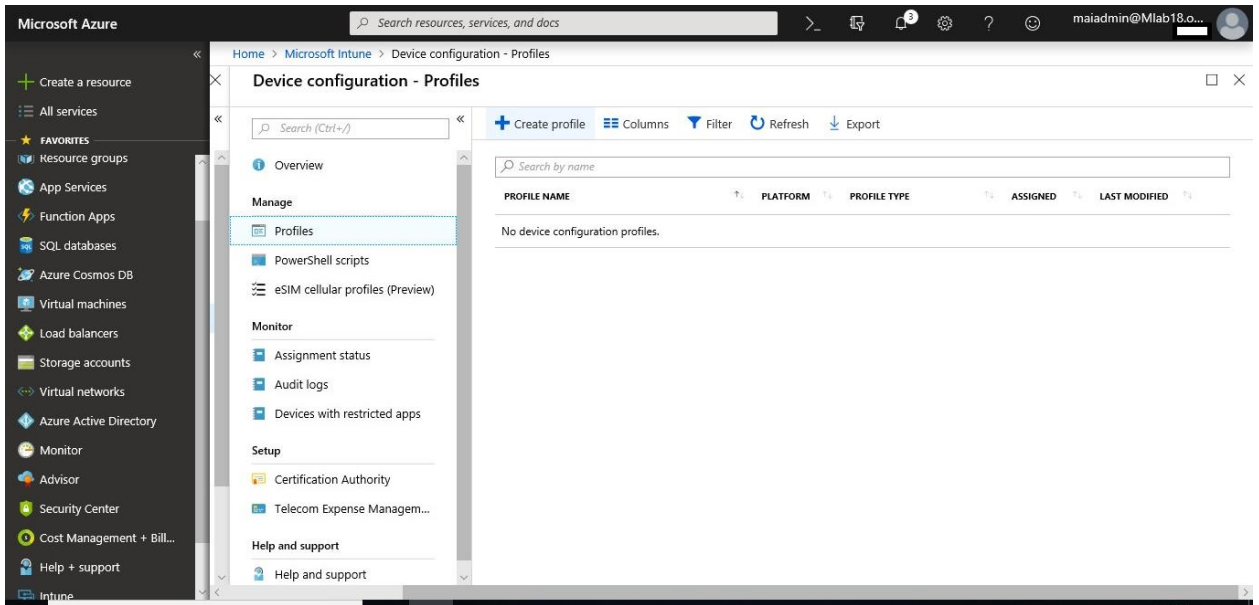
Device Restriction Policy

Device restrictions let you control a wide range of settings and features you manage across a range of categories such as:

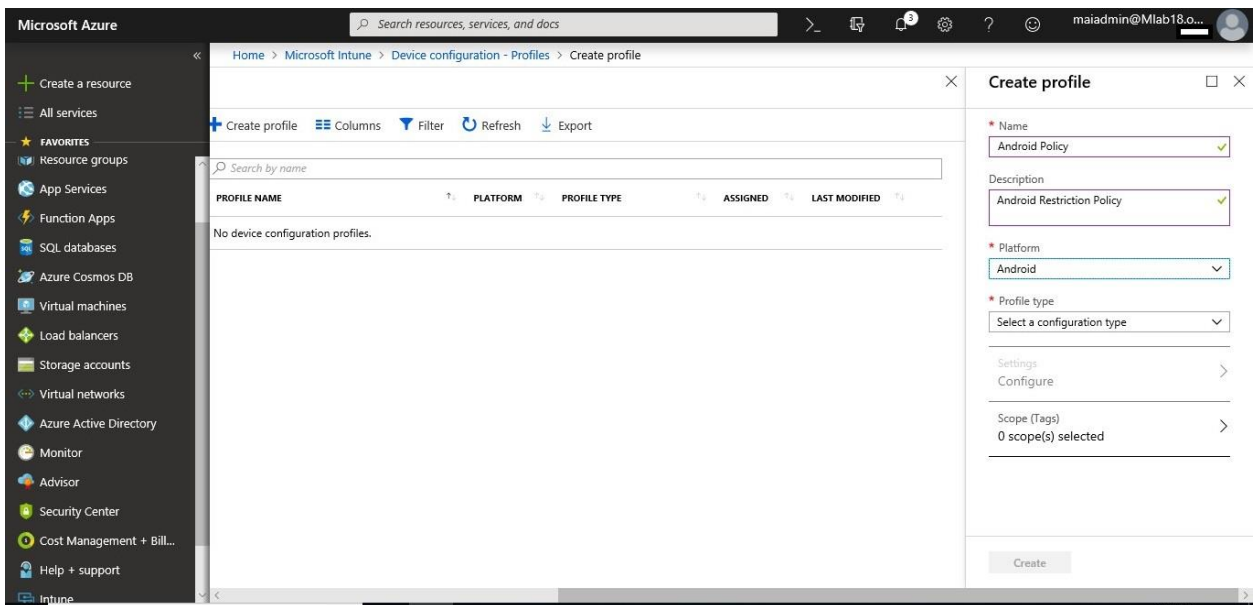
- Security
- Browser
- Hardware
- Data sharing settings

To create and deploy a device restriction policy, you can follow below steps:

1. Sign in to the [Azure portal](#).
2. Select **All services**, filter on **Intune**, and select **Microsoft Intune**.
3. Select **Device configuration** > **Profiles** > **Create profile**.

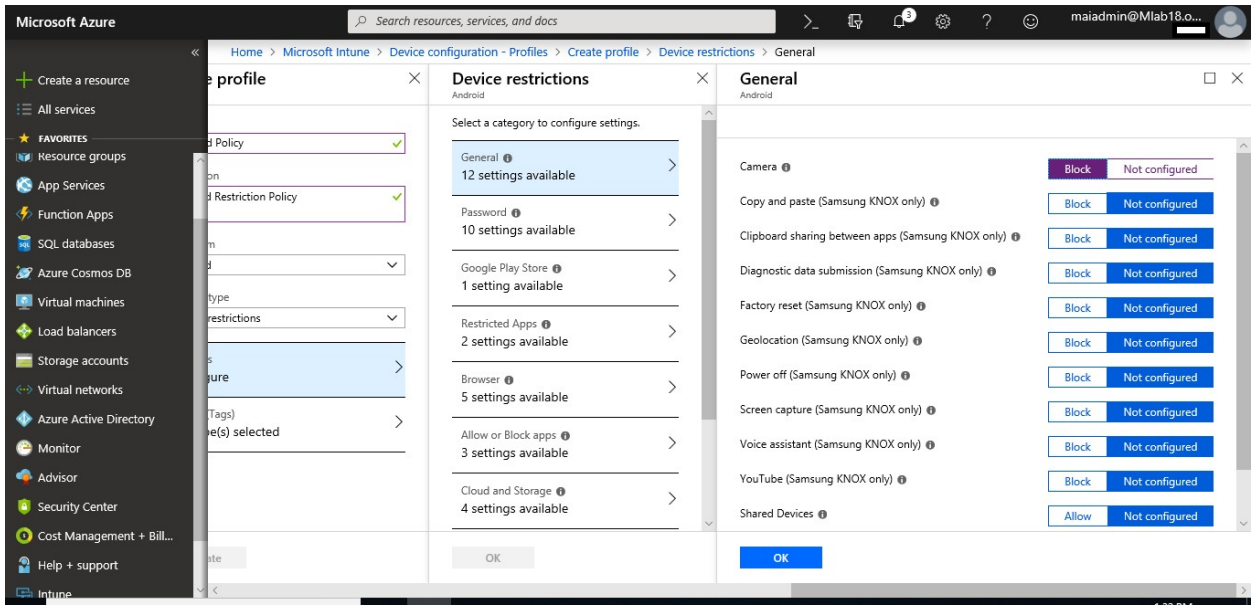


4. Enter a **Name** and **Description** for the device restriction profile.

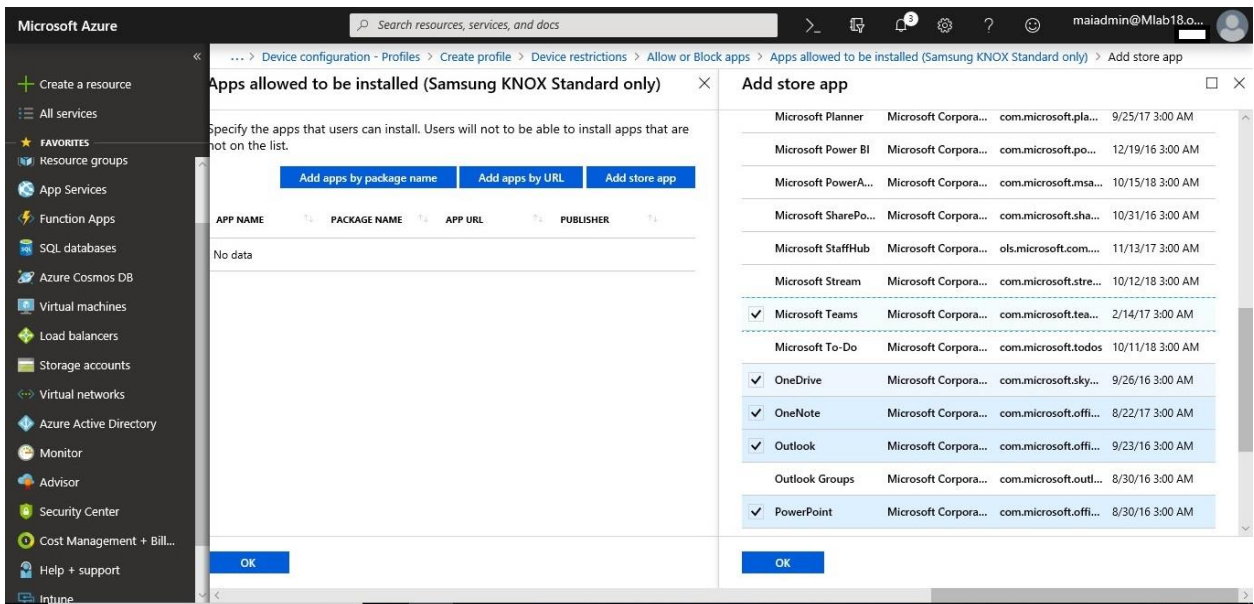


5. From the **Platform** drop-down list, select the device platform to which you want to apply custom settings.
6. From the **Profile type** drop-down list, choose **Device restrictions**. If you want to create a device restrictions profile for Windows 10 Team devices like a Surface Hub, choose **Device restrictions (Windows 10 Team)**.
7. Depending on the platform you chose, the settings you can configure are different. Go to one of the following topics for detailed settings for each platform: In my lab, I choose Android, and want to block camera

Microsoft Intune step by step on Azure portal



8. Select for Samsung Knox, Allow or Block App. Block Facebook & Hidden WhatsApp. Allow Microsoft product “Word, Excel & Outlook”.



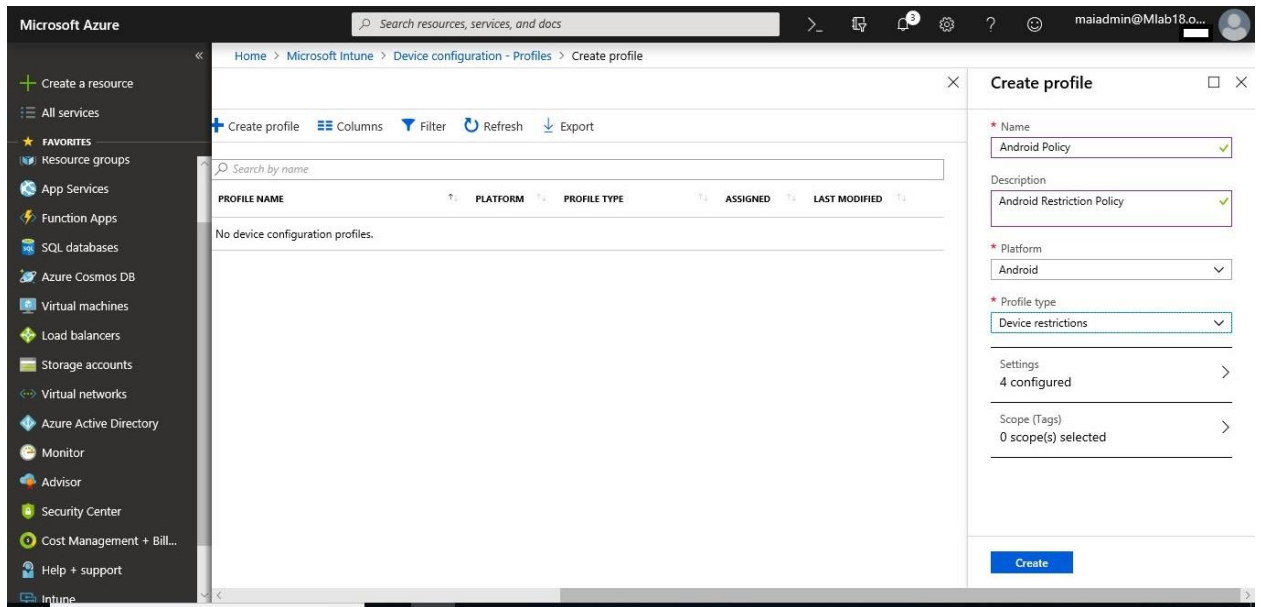
Microsoft Intune step by step on Azure portal

The screenshot shows the Microsoft Azure portal interface. The breadcrumb navigation is: Home > Device configuration - Profiles > Create profile > Device restrictions > Allow or Block apps > Apps blocked from launching (Samsung KNOX Standard only) > Add apps by URL. The main panel is titled 'Apps blocked from launching (Samsung KNOX Standard only)'. It contains a table with columns: APP NAME, PACKAGE NAME, APP URL, and PUBLISHER. The table is currently empty with the text 'No data'. To the right, there is a form titled 'Add apps by URL' with two fields: 'App Name' (set to 'Facebook') and 'URL' (set to 'https://play.google.com/store/apps/details?id=com.facebook.katana&hl=en'). There are 'OK' buttons at the bottom of both the table and the form.

The screenshot shows the Microsoft Azure portal interface. The breadcrumb navigation is: Home > Microsoft Intune > Device configuration - Profiles > Create profile > Device restrictions > Allow or Block apps > Apps hidden from user (Samsung KNOX Standard only). The main panel is titled 'Allow or Block apps'. It contains three sections: 'Apps allowed to be installed (Samsung KNOX Standard only)' with '1 setting available', 'Apps blocked from launching (Samsung KNOX Standard only)' with '1 setting available', and 'Apps hidden from user (Samsung KNOX Standard only)' with '1 setting available'. To the right, there is a form titled 'Apps hidden from user (Samsung KNOX Standard only)'. It contains a table with columns: APP NAME, PACKAGE NAME, APP URL, and PUBLISHER. The table has one row with 'WhatsApp' in both the APP NAME and PACKAGE NAME columns. There are 'OK' buttons at the bottom of both the main panel and the form.

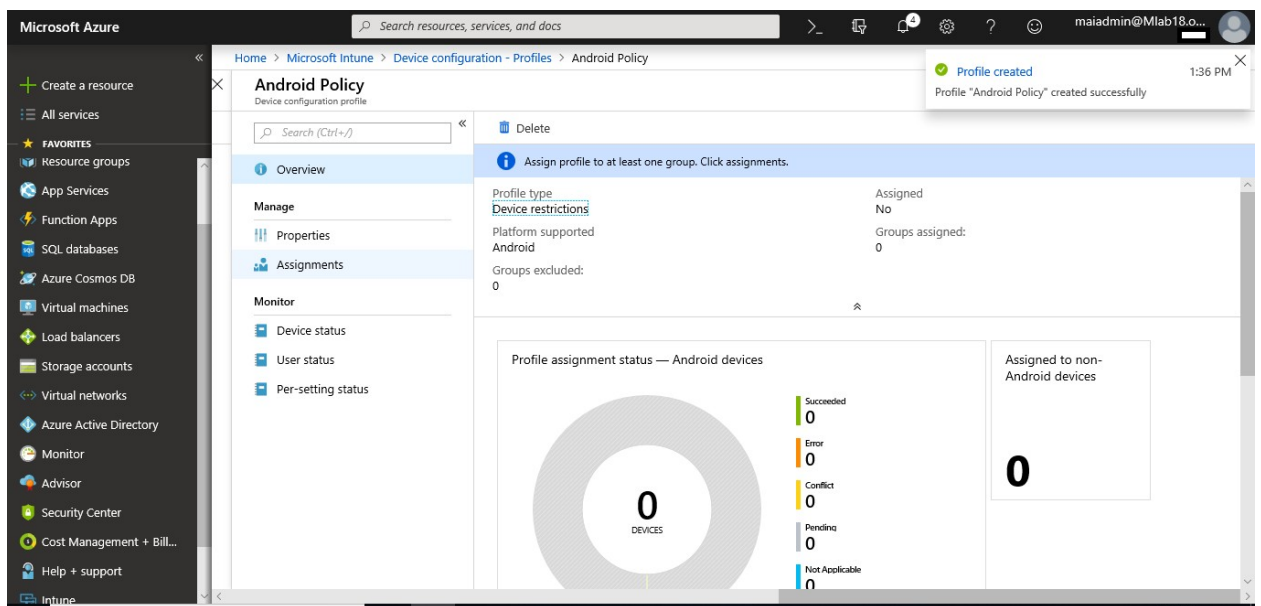
9. When you're done, go back to the **Create profile** page, and click **Create**.

Microsoft Intune step by step on Azure portal



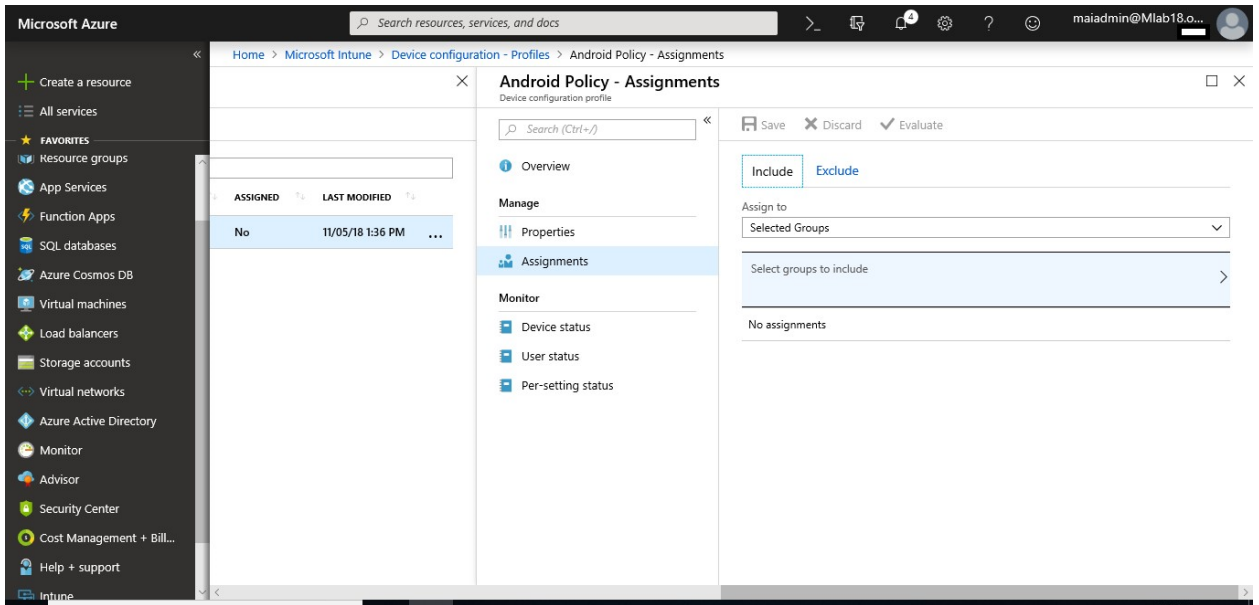
To assign Device Restriction Policy

1. In the [Azure portal](#), select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device Configuration > Policies** > select your device restriction policy.

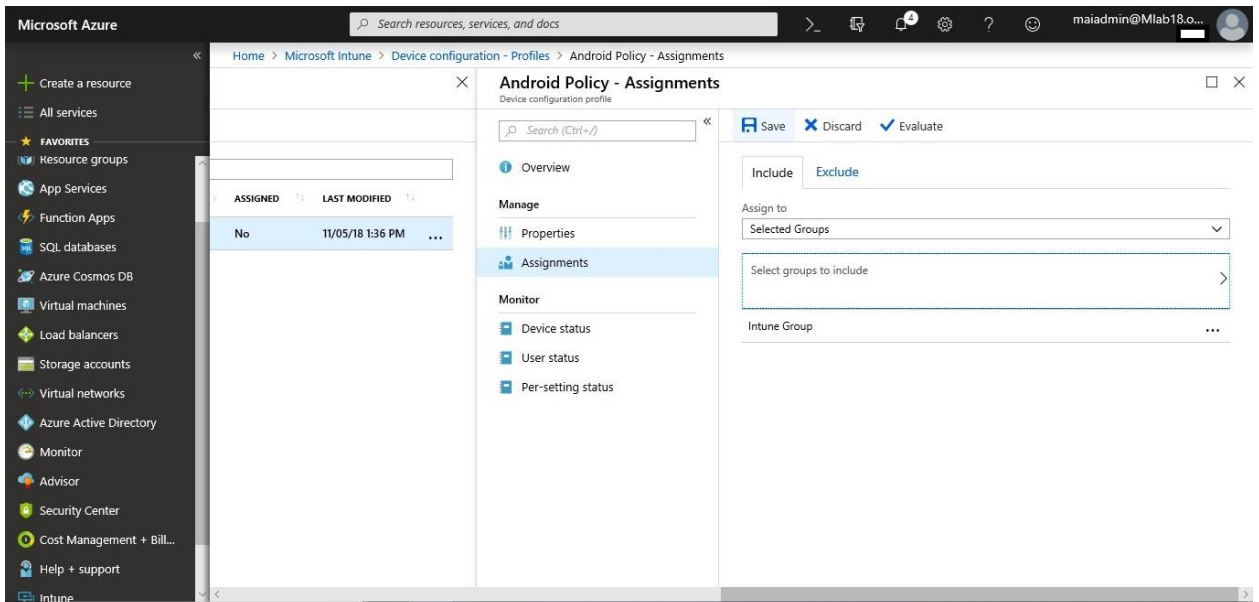


3. Select **Assignments**.

Microsoft Intune step by step on Azure portal



4. Include or exclude your Azure AD groups to assign them the policy.
5. To deploy the policy to the groups, select **Save**. The user devices targeted by the policy are evaluated for compliance.



Custom Device Settings

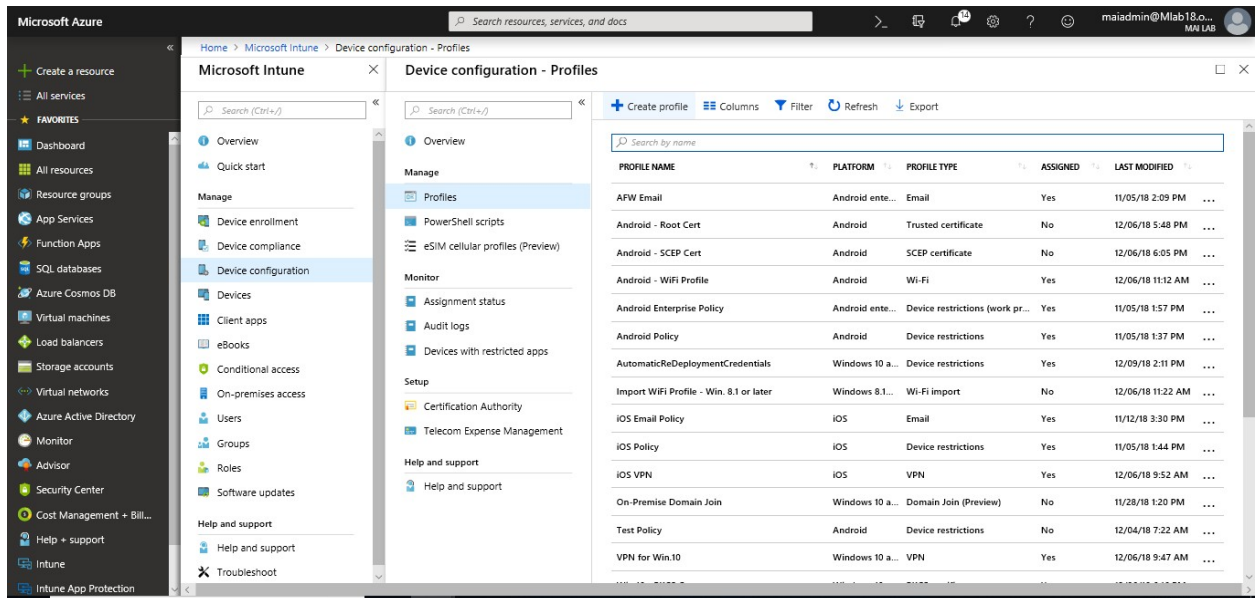
Microsoft Intune includes many built-in settings to control different features on a device. You can also create custom profiles. Custom profiles are great when you want to use device settings and features that aren't built in to Intune. These profiles include features and settings for you to control on devices in your organization. For example, you can create a custom profile that sets the same feature for every iOS device.

Custom Profile for Android

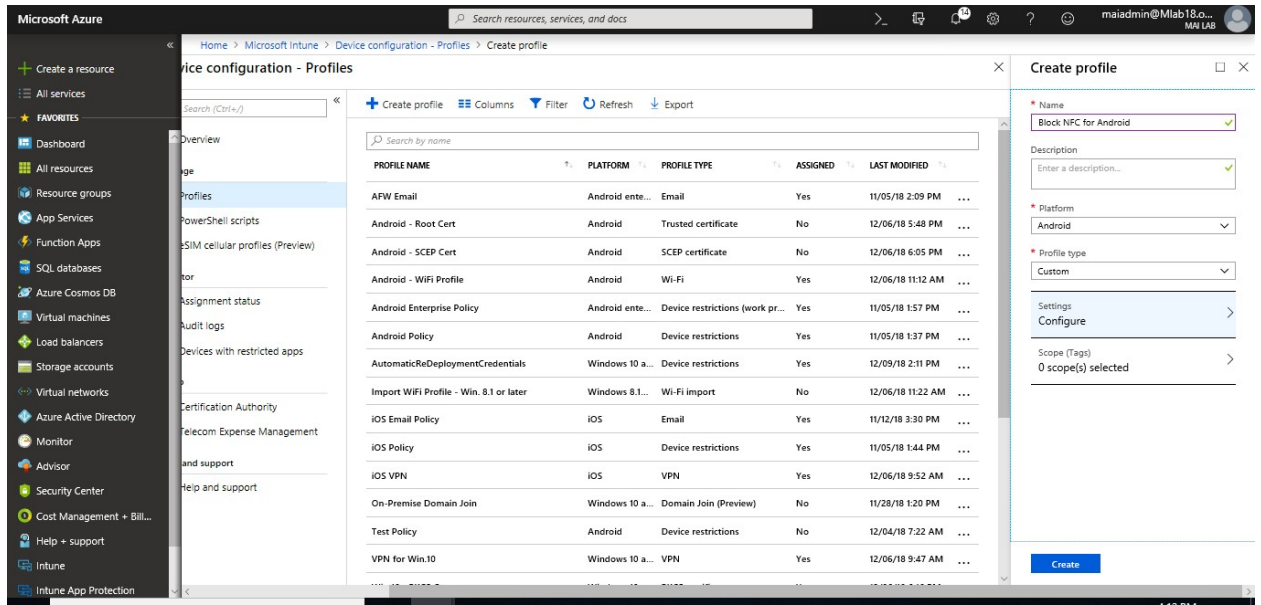
Android custom profiles use Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings to configure different features on Android devices. These settings are typically used by mobile device manufacturers to control these features.

To create a custom Android profile, you need to follow below steps:

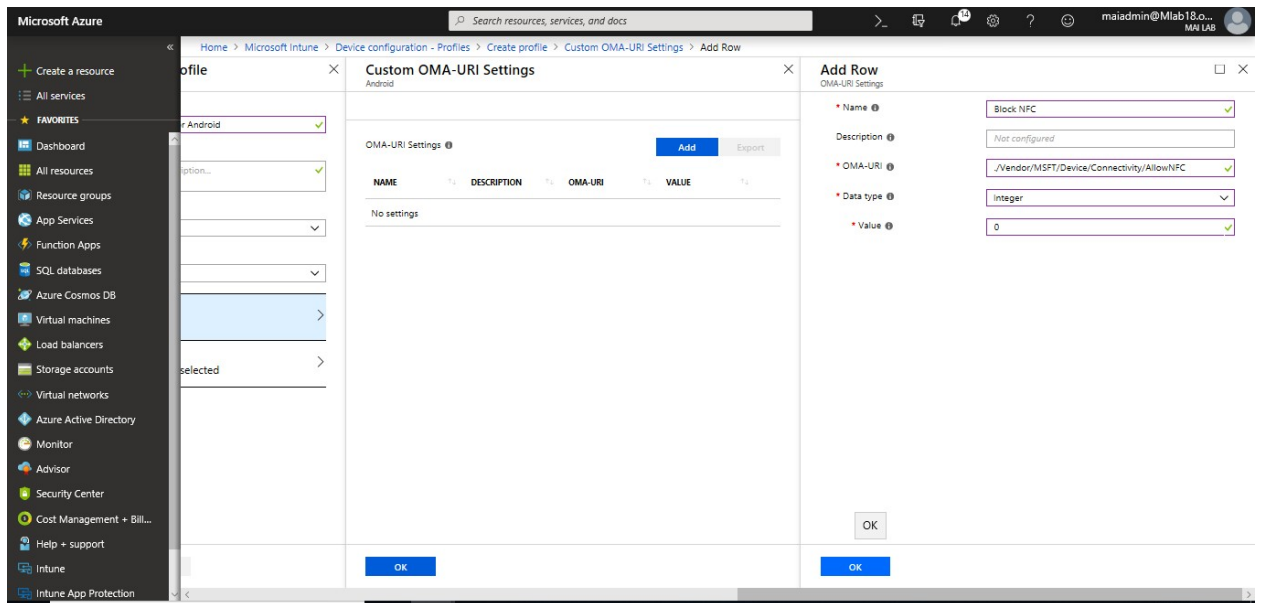
1. In the [Azure portal](#), select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device configuration > Profiles > Create profile**.



3. Enter the following settings:
 1. **Name:** Enter a name for the profile, such as android custom profile.
 2. **Description:** Enter a description for the profile.
 3. **Platform:** Choose **Android**.
 4. **Profile type:** Choose **Custom**.

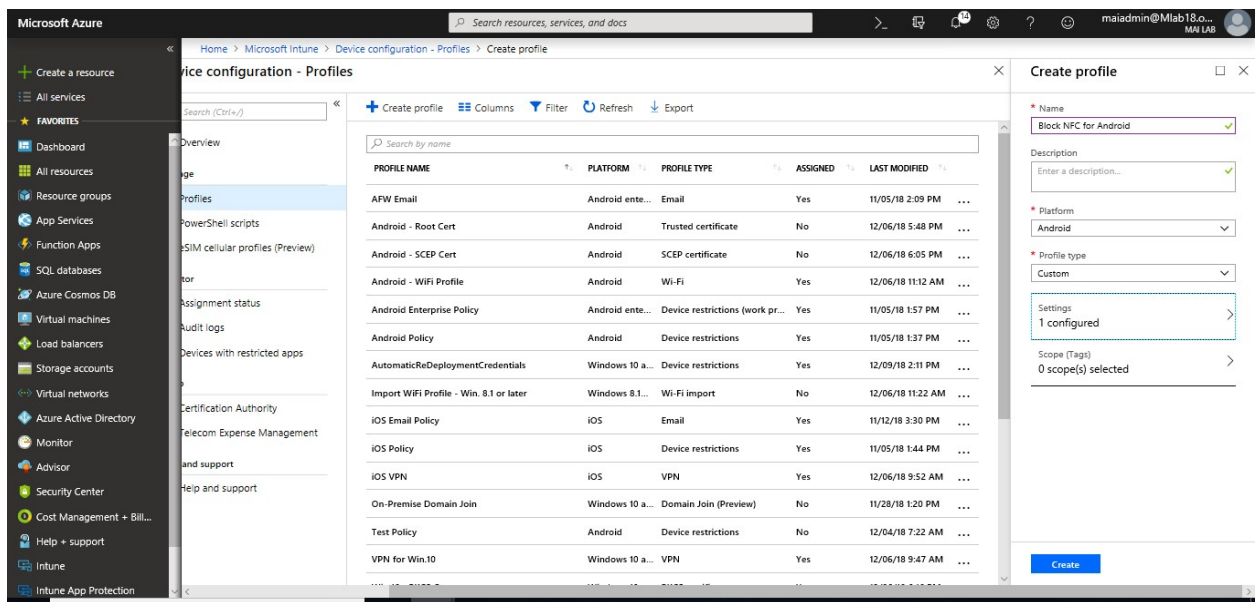


4. In **Custom OMA-URI Settings**, select **Add**. Enter the following settings:
 - a) **Name:** Enter a unique name for the OMA-URI setting so you can easily find it. **“Block NFC”**
 - b) **Description:** Enter a description that gives an overview of the setting, and any other important details.
 - c) **OMA-URI:** Enter the OMA-URI you want to use as a setting. **“./Vendor/MSFT/Device/Connectivity/AllowNFC”**
 - d) **Data type:** Choose the data type you'll use for this OMA-URI setting. Your options: **Integer**
 - e) **Value:** Enter the data value you want to associate with the OMA-URI you entered. The value depends on the data type you selected. **“0”**

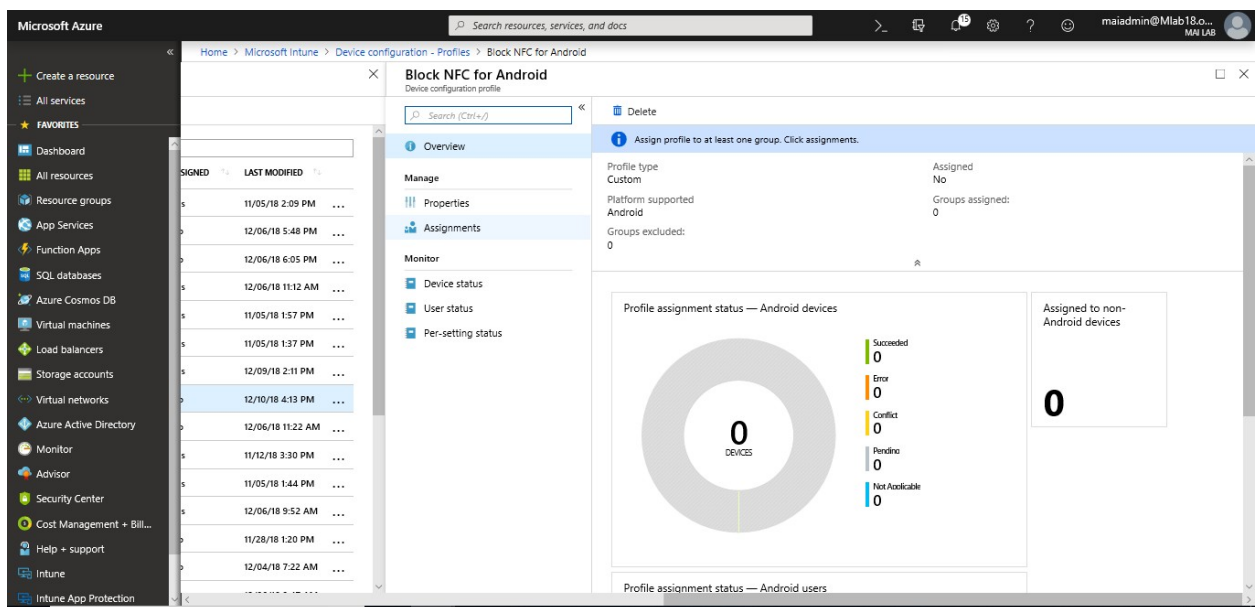


Note: The above configured policy will be applied on **Samsung Knox** not Android Standard. After you add some settings, you can select **Export**. **Export** creates a list of all the values you added in a comma-separated values (.csv) file.

5. Select **OK** to save your changes. Continue to add more settings as needed.
6. When finished, choose **OK > Create** to create the Intune profile. When complete, your profile is shown in the **Device configuration - Profiles** list.

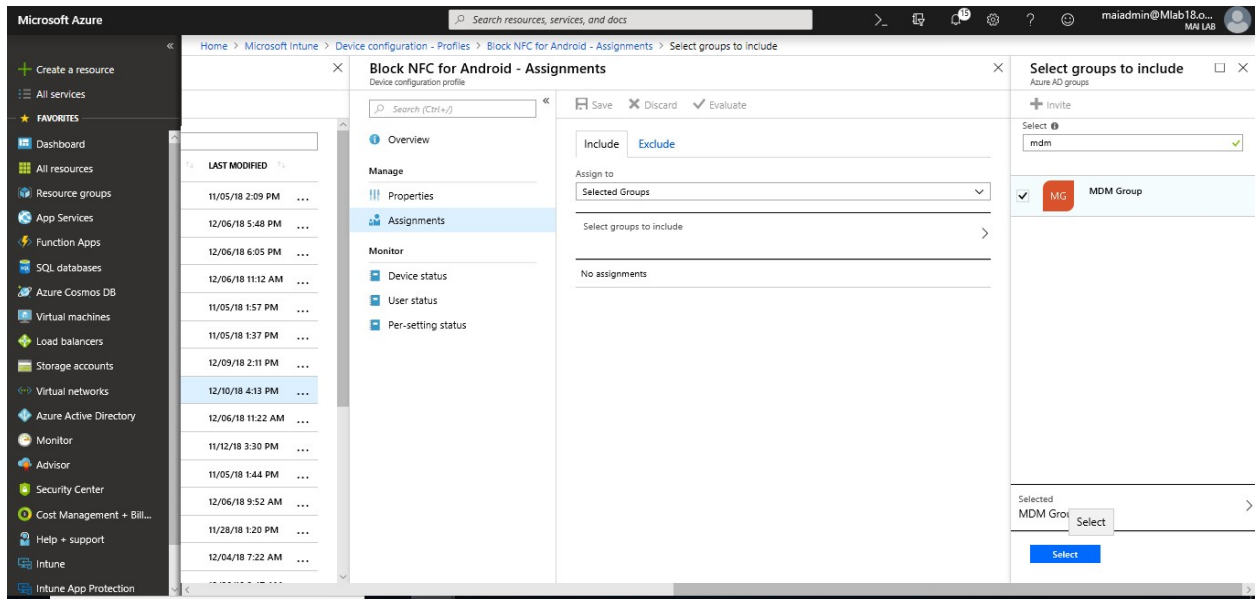


7. In the list of profiles, select the profile you want to assign, and then select **Assignments**.

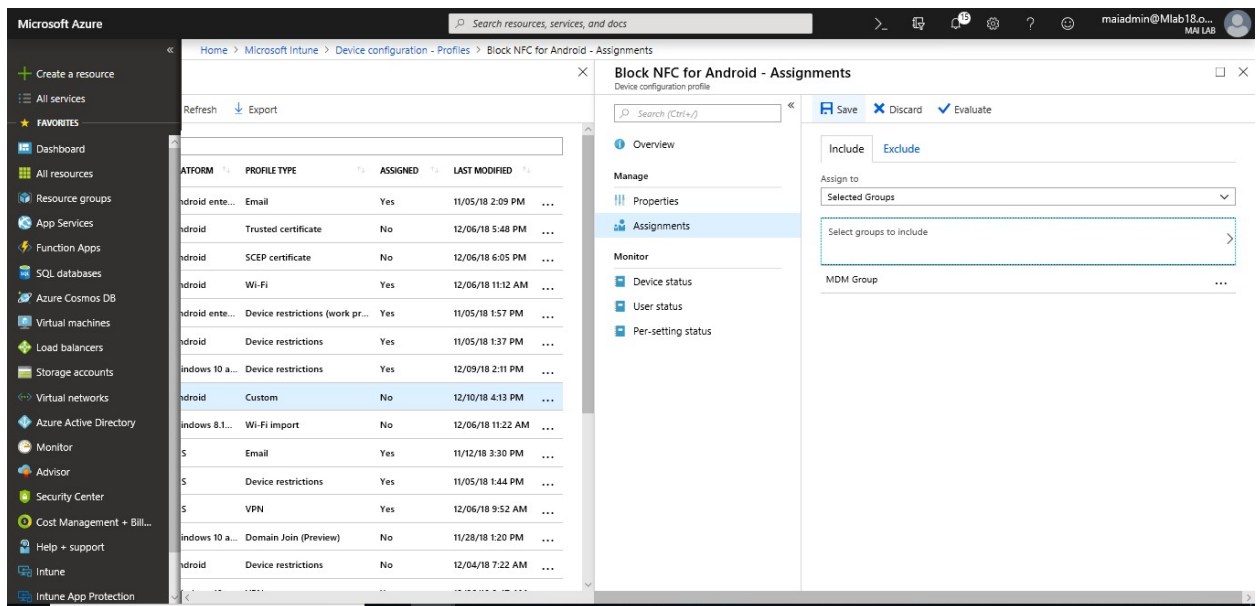


8. Choose to **Include** groups or **Exclude** groups, and then select groups.

Microsoft Intune step by step on Azure portal



9. When you are done, select **Save**.



Custom Profile for iOS Devices

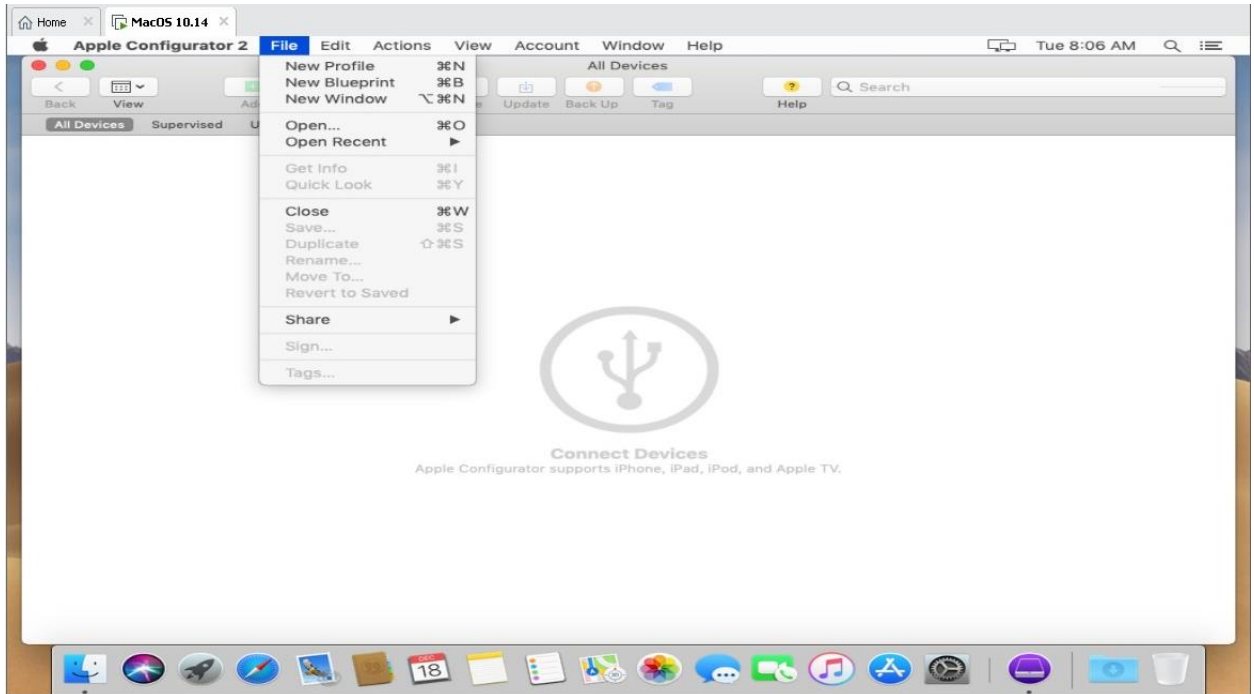
When using iOS devices, there are two ways to get custom settings into Intune:

- Apple Configurator
- Apple Profile Manager

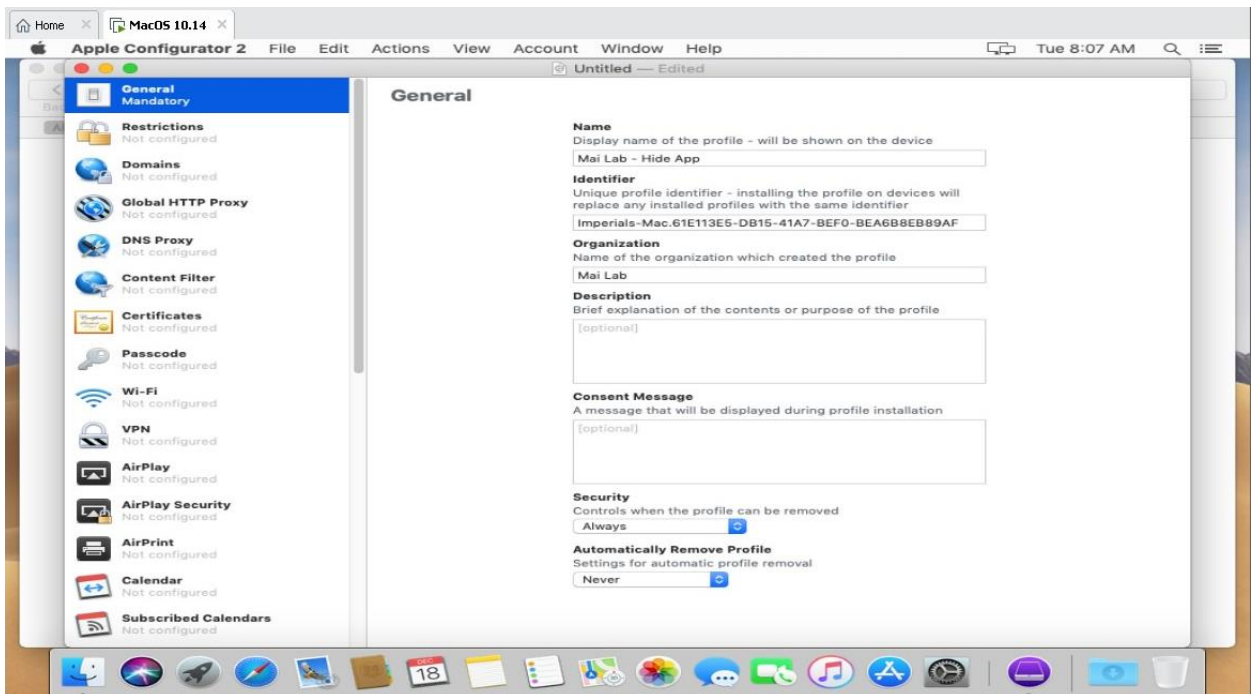
You can use these tools to export settings to a configuration profile. In Intune, you import this file, and then assign the profile to your iOS users and devices. Once assigned, the settings are distributed, and create a baseline or standard for iOS in your organization.

To create and export profiles in Apple Configurator, you need to follow below steps:

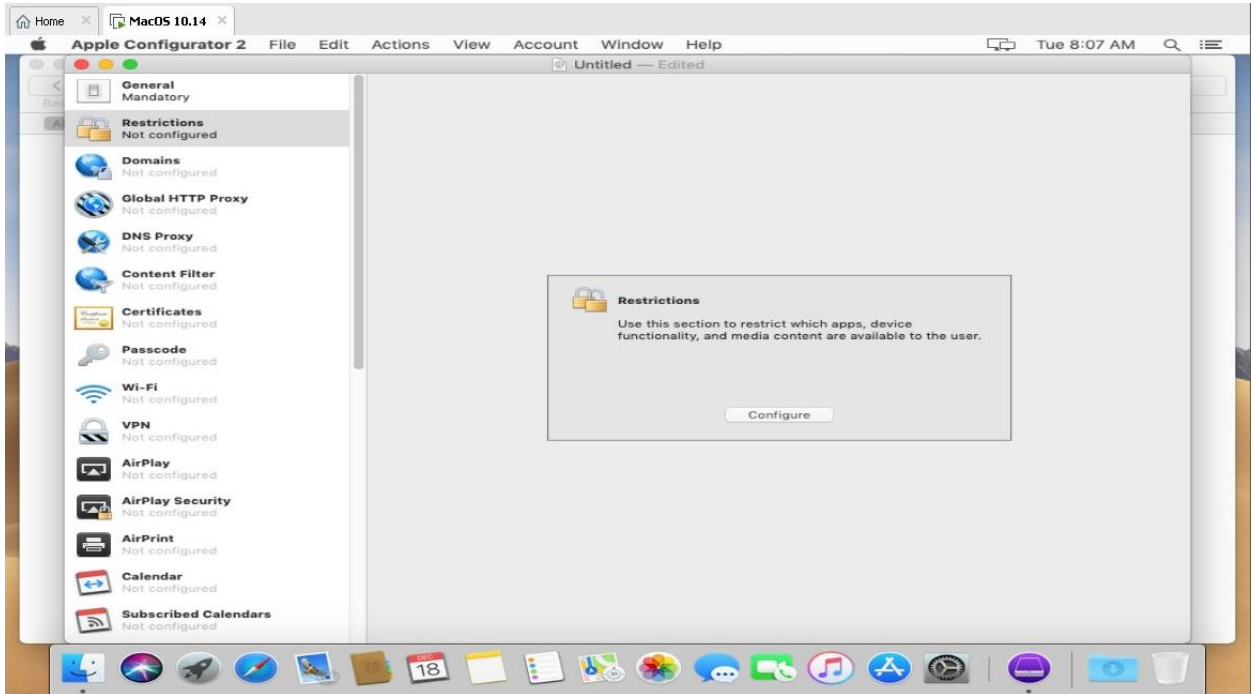
1. Launch **Apple Configurator 2** on MacOS.
2. On the toolbar, open the **File** menu and select **New Profile**.



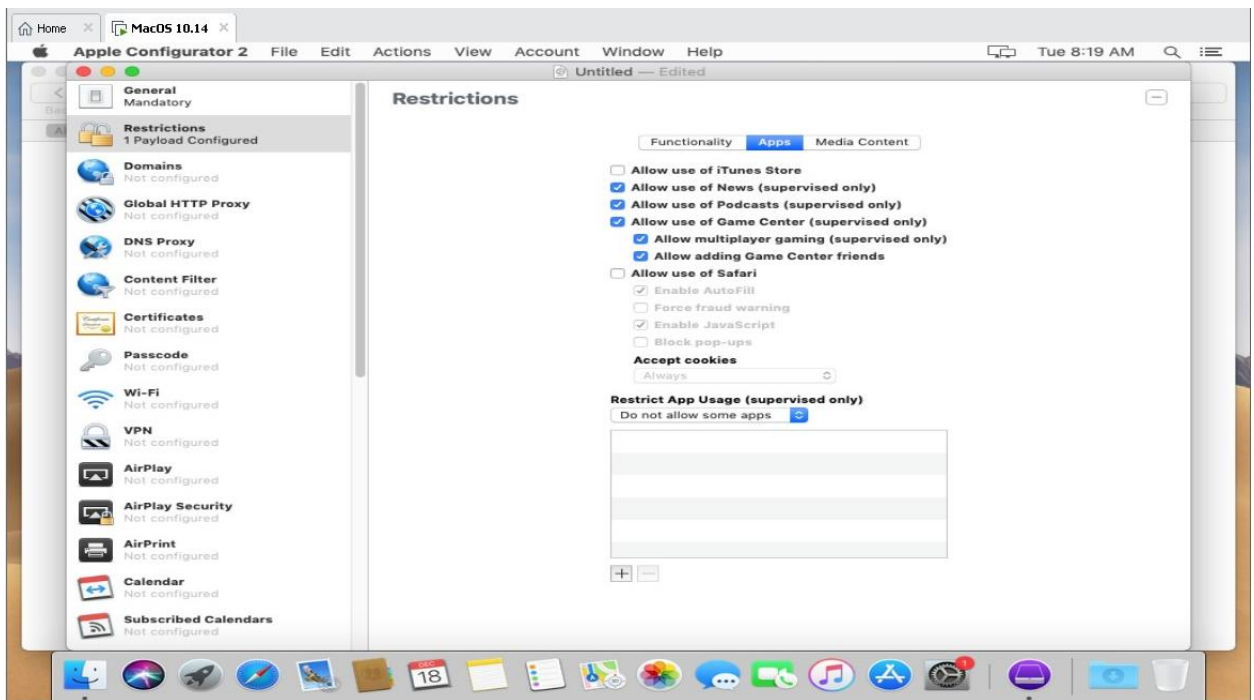
3. On **General** tab, Enter Name of Profile.



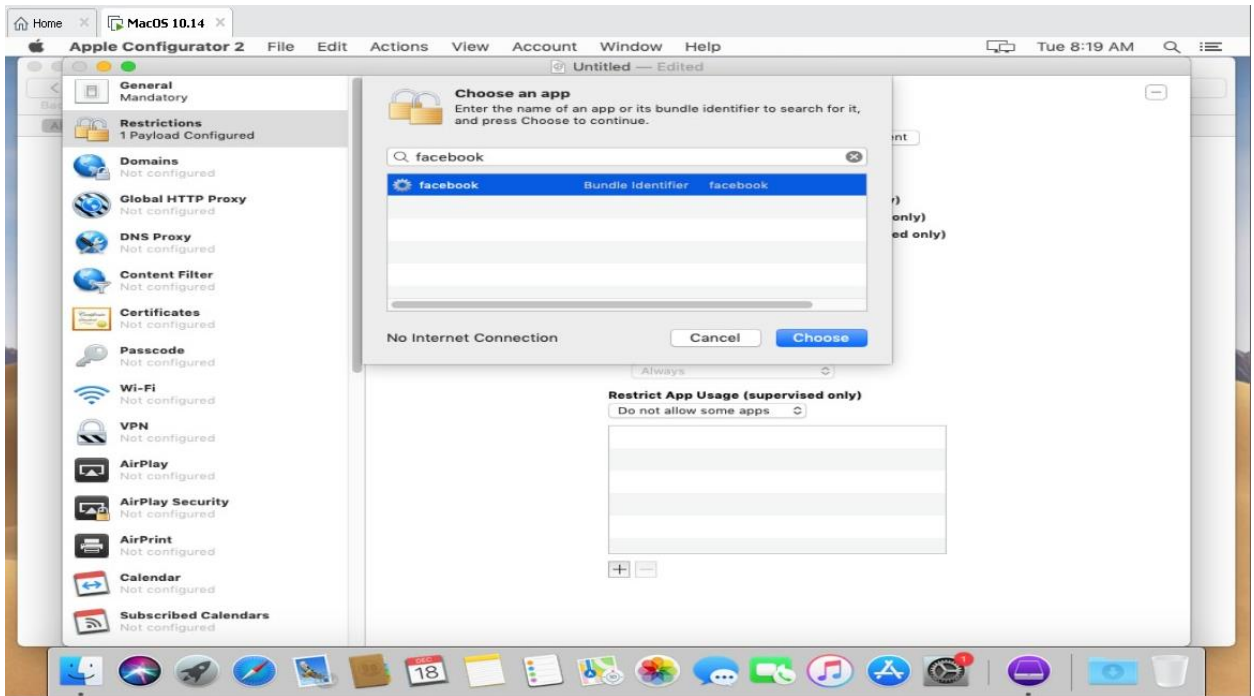
4. Configure the intended settings to be applied. (e.g. **Restriction Policy** on App).



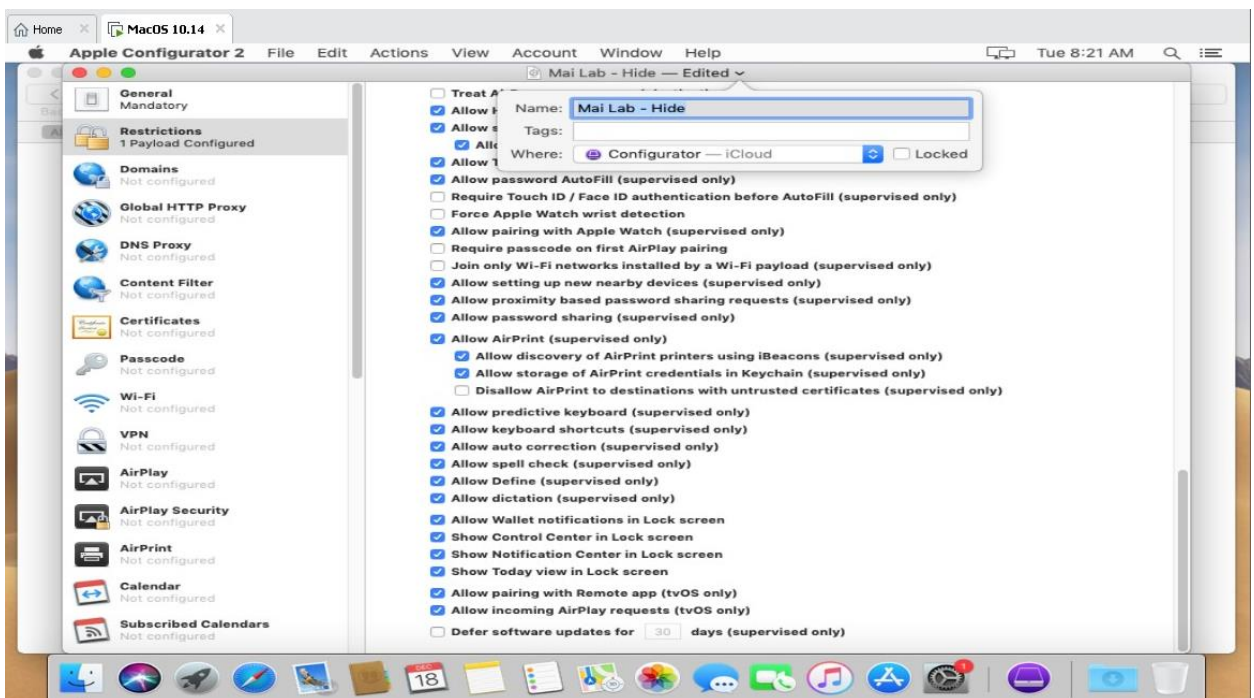
5. On Configure Restriction on App, select restriction that you want e.g. block use iTunes store & block use of safari



6. You can restrict App usage, select **Do not allow some apps** and click + to add some app

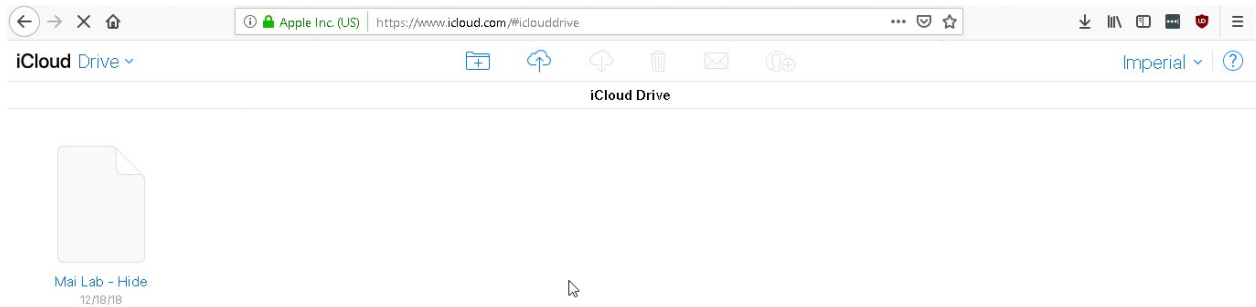


7. After configuring settings as needed, save the profile (a **.mobileconfig** file) to a local directory or on iCloud



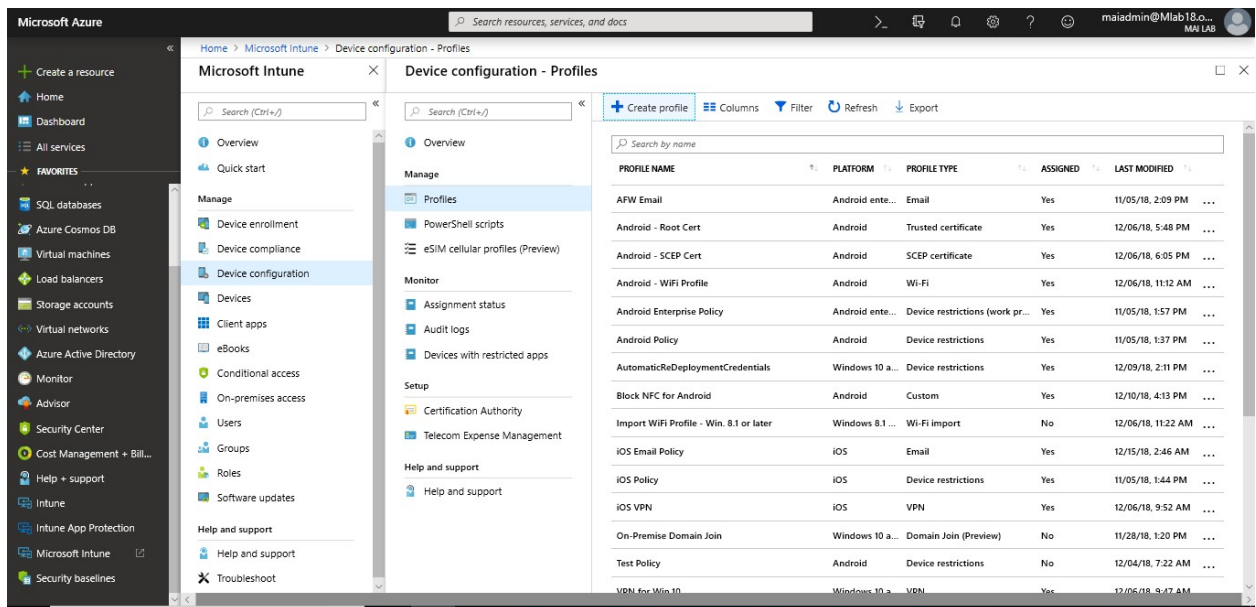
8. Once this profile is created, you can download it from iCloud or copy it from local directory.

Microsoft Intune step by step on Azure portal

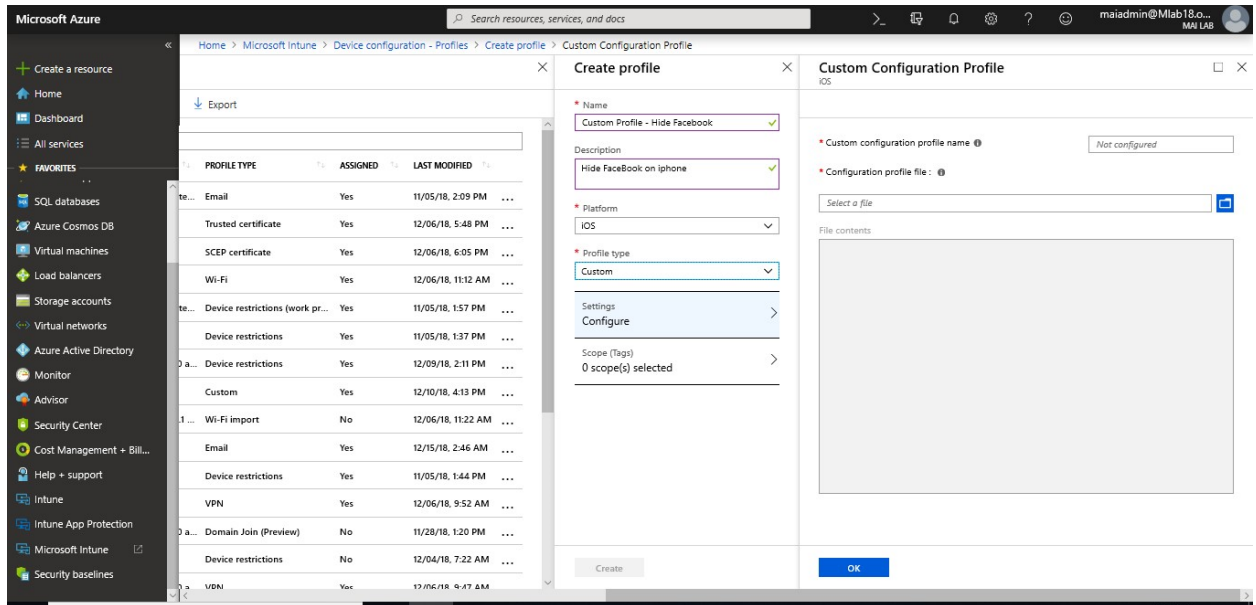


To create a custom iOS profile, you need to follow below steps:

1. In the [Azure portal](#), select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device configuration** > **Profiles** > **Create profile**.

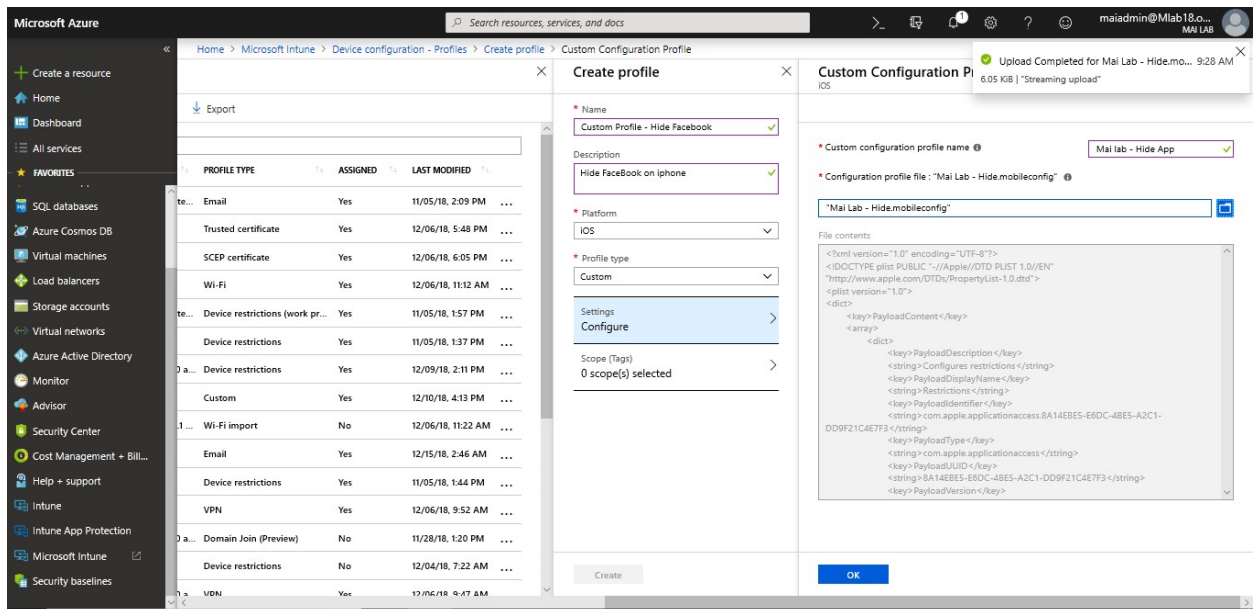


3. Enter the following settings:
 - **Name:** Enter a name for the profile, such as ios custom profile.
 - **Description:** Enter a description for the profile.
 - **Platform:** Choose **iOS**.
 - **Profile type:** Choose **Custom**.



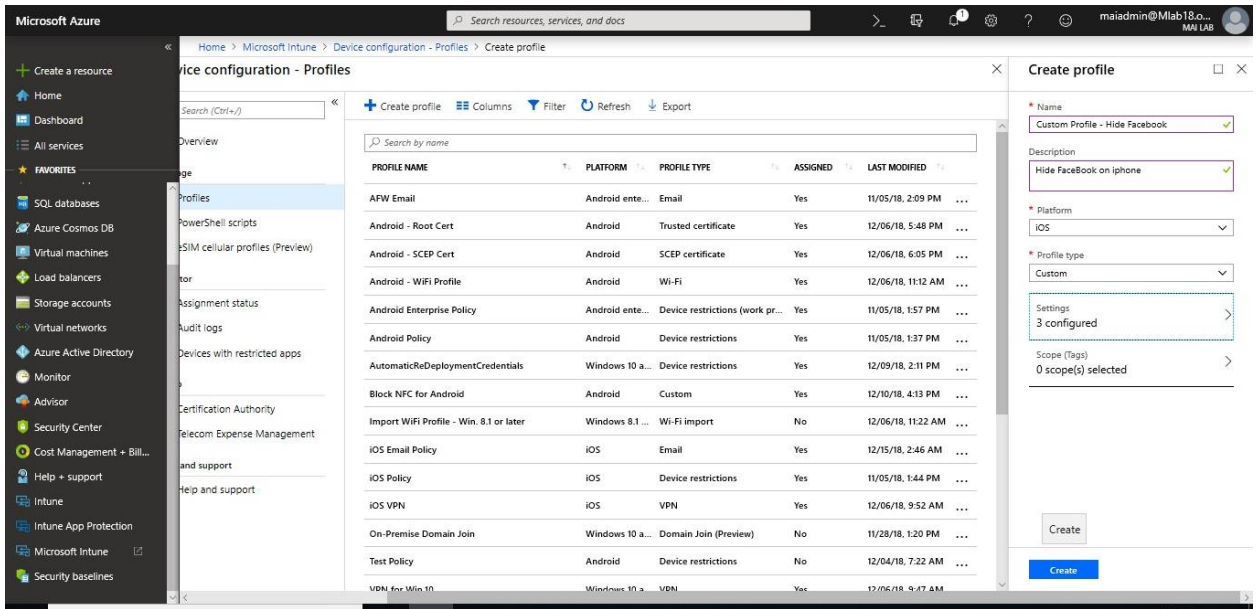
4. In **Custom configuration**, enter the following settings:

- **Custom configuration profile name:** Enter a name for the policy. This name is shown on the device, and in the Intune status.
- **Configuration profile file:** Browse to the configuration profile you created using the Apple Configurator or Apple Profile Manager. The file you imported is shown in the **File contents** area.

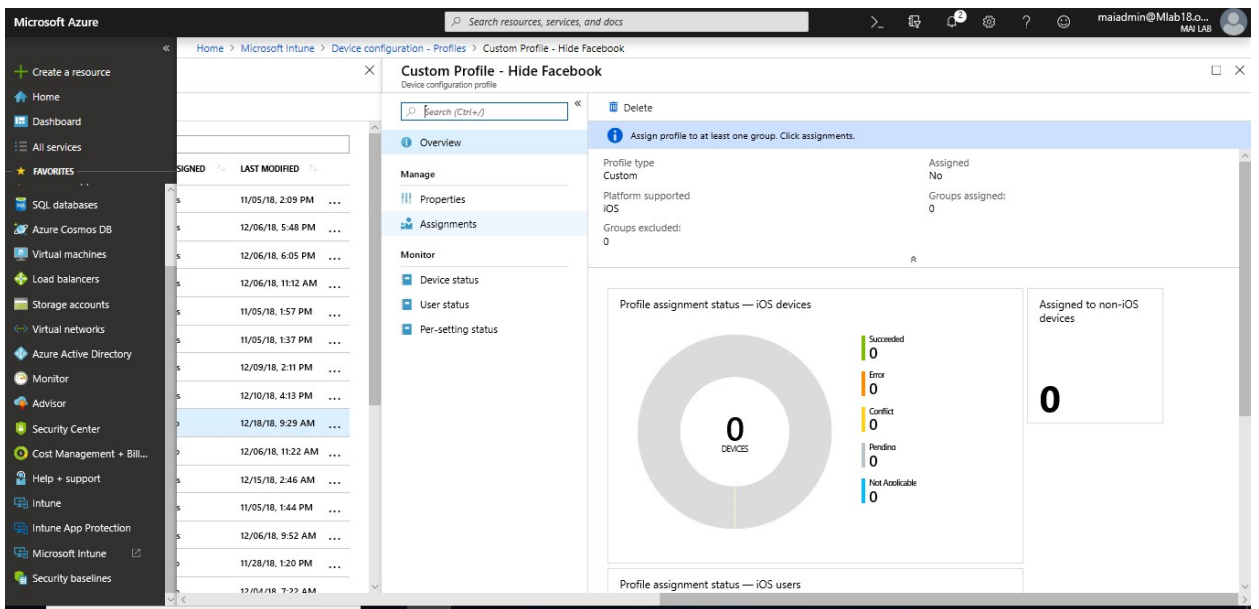


5. Select **OK > Create** to create the Intune profile. When complete, your profile is shown in the **Device configuration - Profiles** list.

Microsoft Intune step by step on Azure portal

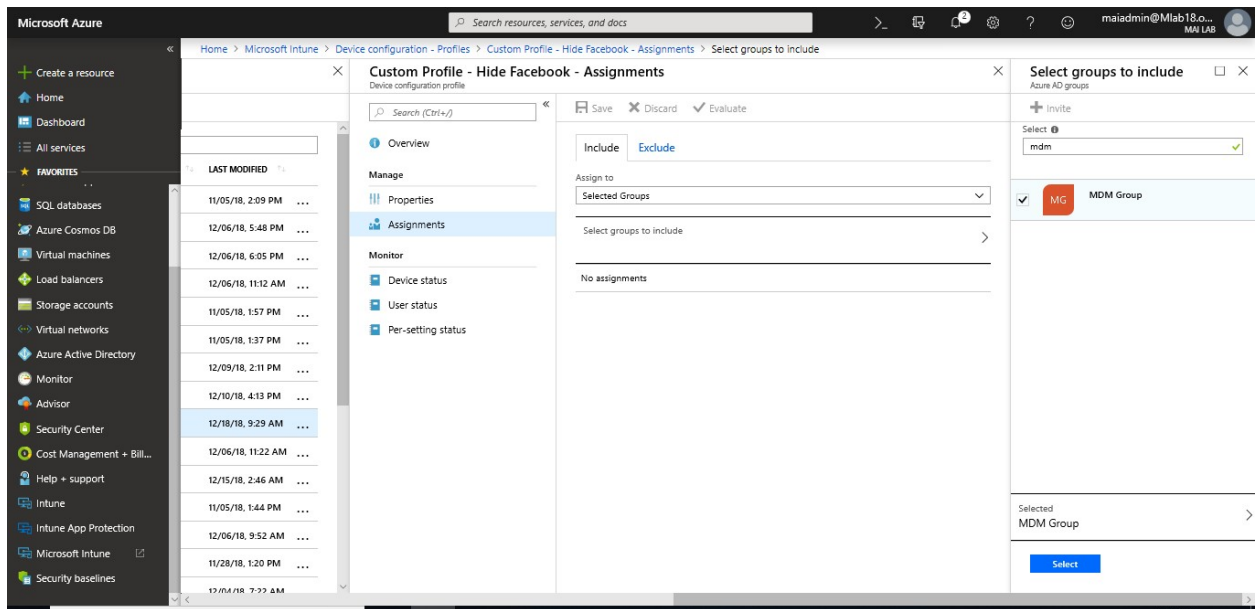


6. In the list of profiles, select the profile you want to assign, and then select **Assignments**.

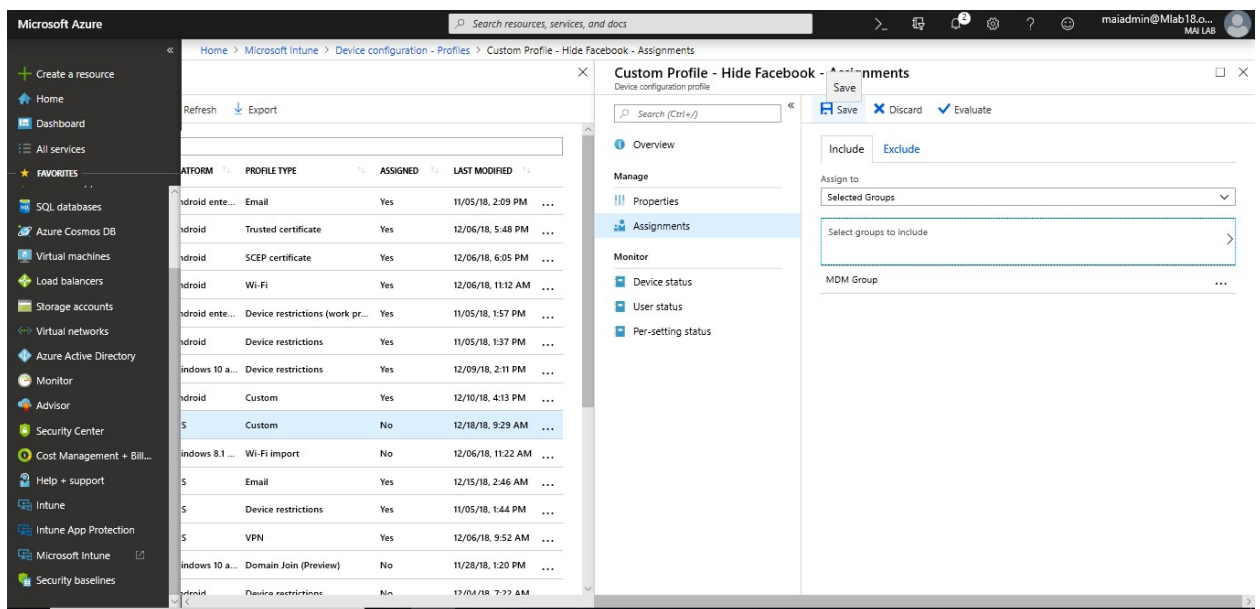


7. Choose to **Include** groups or **Exclude** groups, and then select groups.

Microsoft Intune step by step on Azure portal



8. When you are done, select **Save**.



Compliance Policies in Microsoft Intune

Define the rules and settings that a device must comply with in order to be considered compliant by conditional access policies. You can also use compliance policies to monitor and remediate compliant issues with devices independently of conditional access.

These rules include:

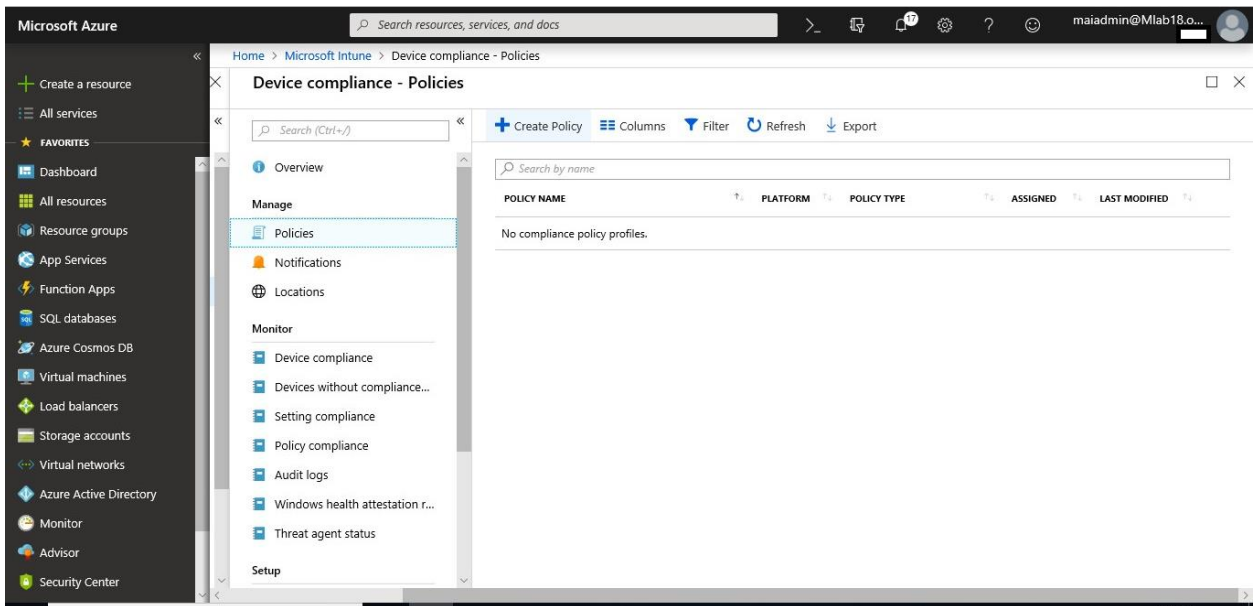
- PIN and passwords
- Encryption

Microsoft Intune step by step on Azure portal

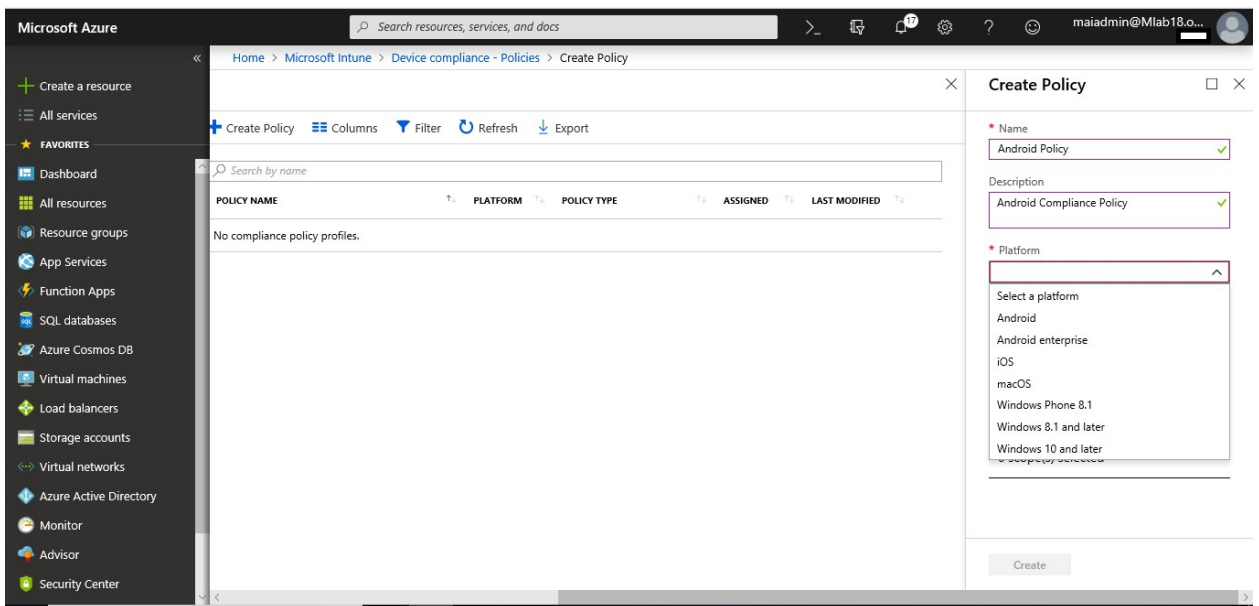
- Whether the device is jailbroken or rooted
- Whether email on the device is managed by an Intune policy

To create Device Compliance policy, you need to follow below steps:

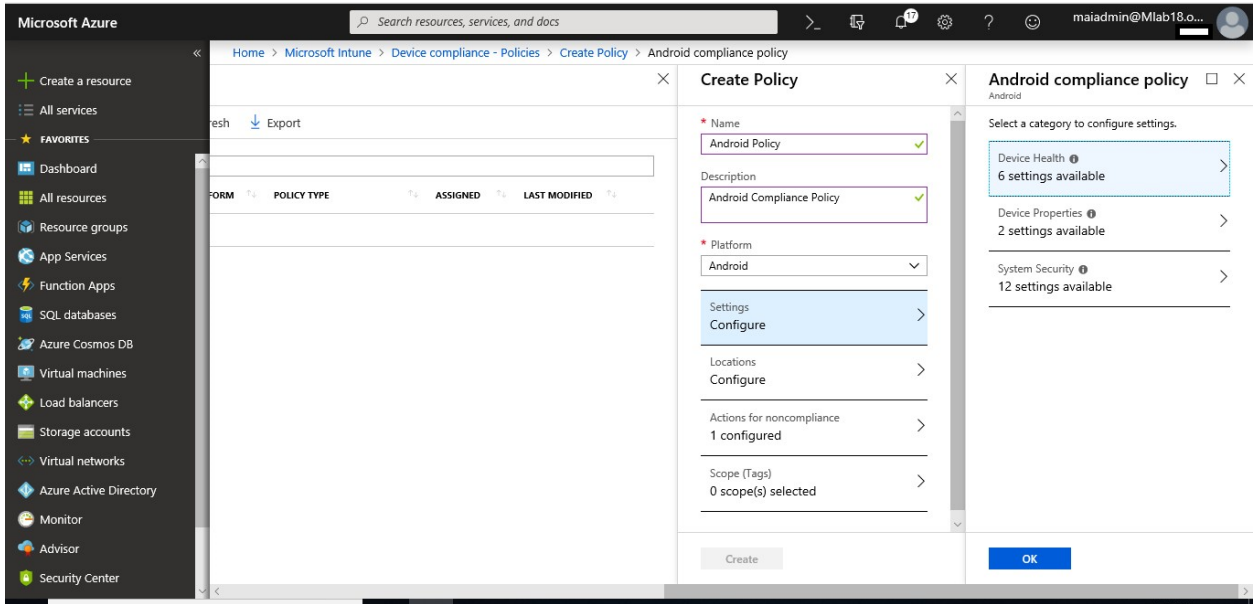
1. In the [Azure portal](#), select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device compliance** > **Policies** > **Create Policy**



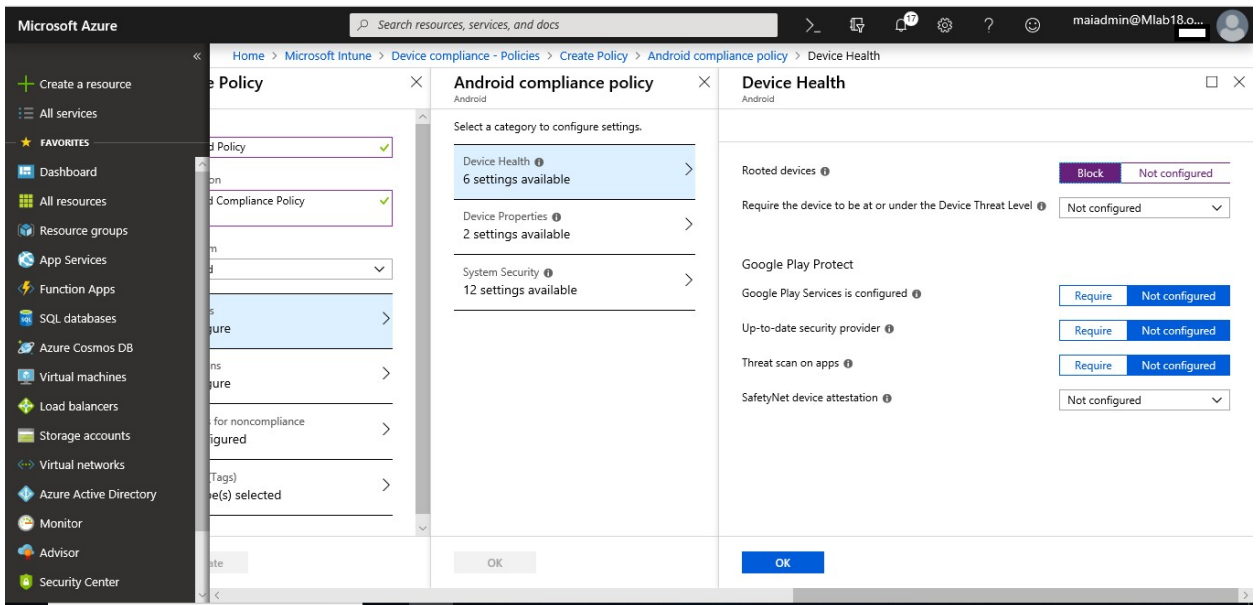
3. Enter a **Name** and **Description**.



4. For **Platform**, select **Android**.

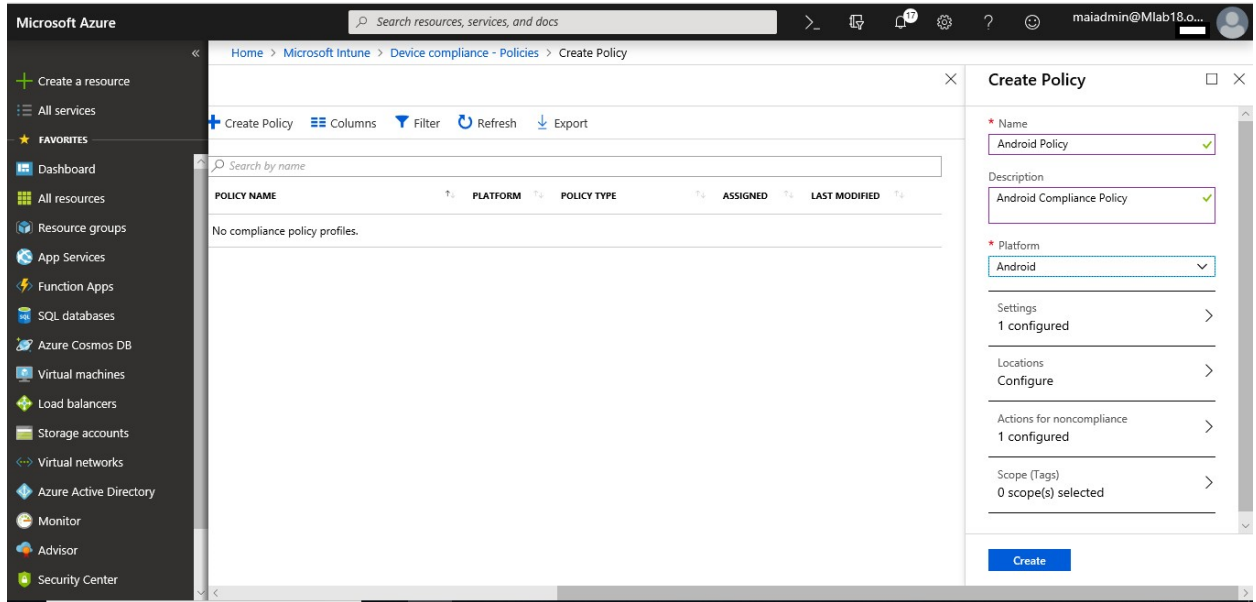


5. Choose **Settings Configure**. Enter the **Device Health**, **Device Properties**, and **System Security** settings. e.g., Block root Devices.



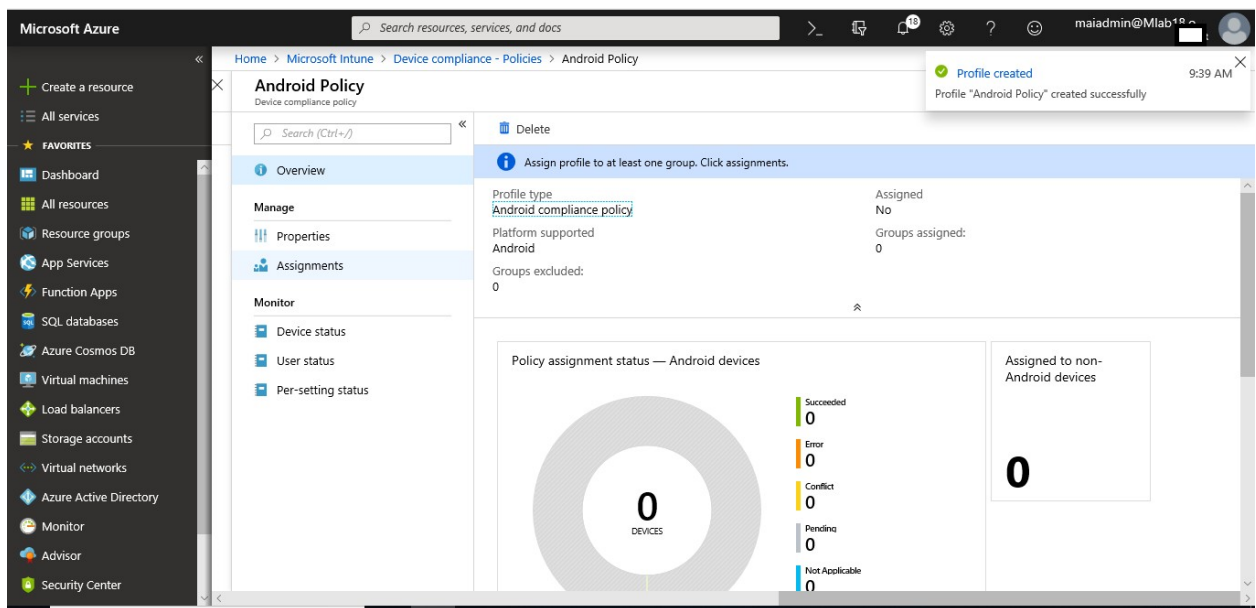
6. Click **Create**.

Microsoft Intune step by step on Azure portal



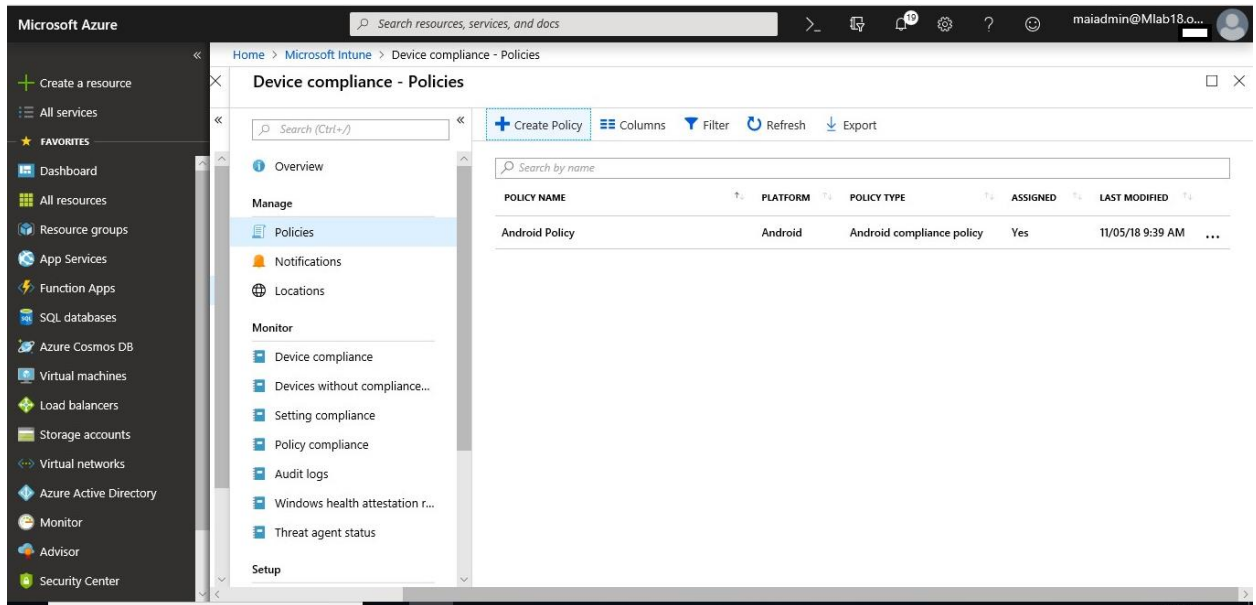
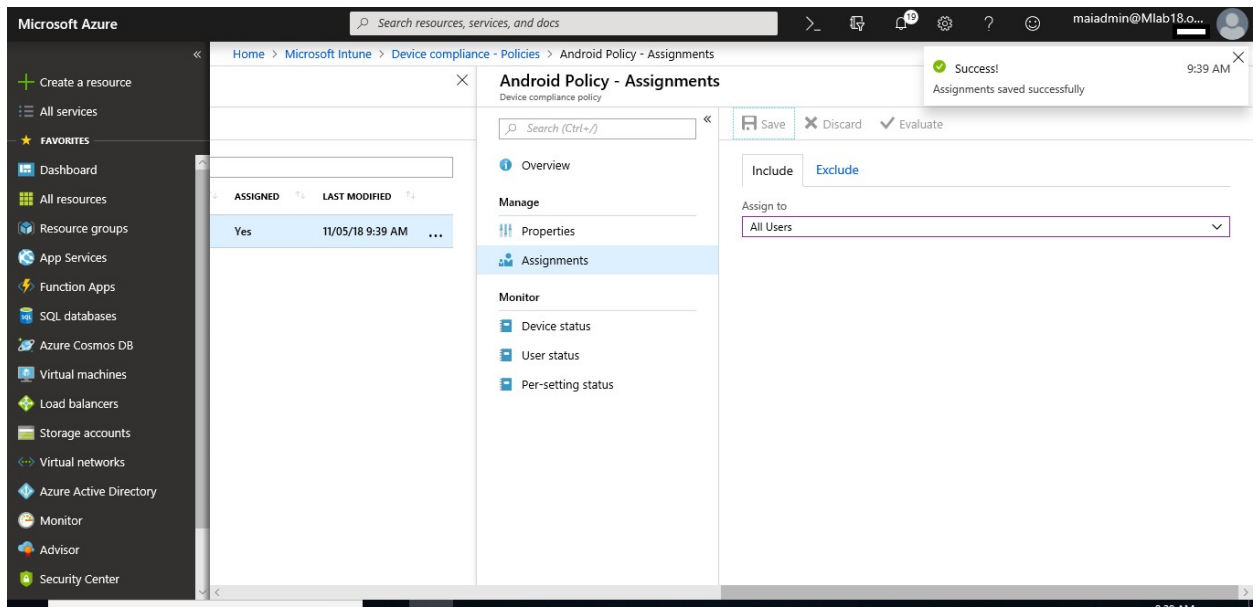
To Assign Compliance Policy on specific group, you need to follow below steps:

1. Choose a policy that you've configured. Existing policies are in **Device compliance > Policies**.



2. Choose the policy and choose **Assignments**. You can include or exclude Azure Active Directory (AD) security groups.
3. Choose **Selected groups** to see your Azure AD security groups. Select the user groups you want this policy to apply and choose **Save** to deploy the policy to users.

Microsoft Intune step by step on Azure portal



Automate email and add actions for noncompliant devices

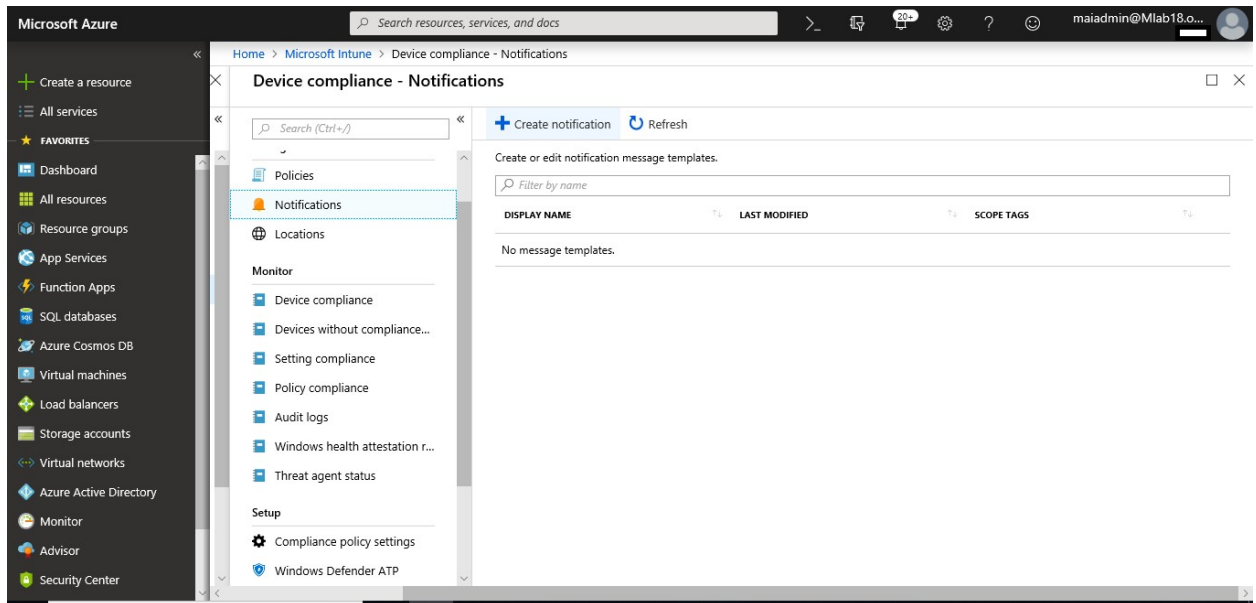
By default, when Intune detects a device that isn't compliant, Intune immediately marks the device as noncompliant. Azure Active Directory (AD) conditional access then blocks the device. When a device is not compliant, **actions for noncompliance** also gives you flexibility to decide what to do.

Create a notification message template

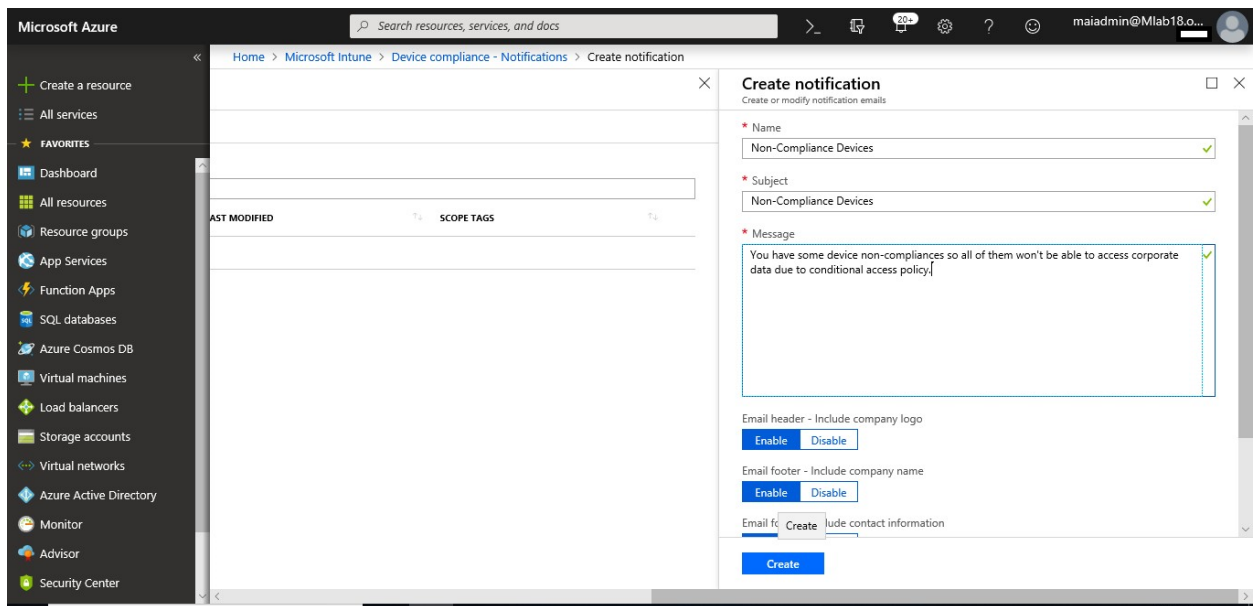
To send email to your users, create a notification message template. When a device is noncompliant, the details you enter in the template is shown in the email sent to your users.

Microsoft Intune step by step on Azure portal

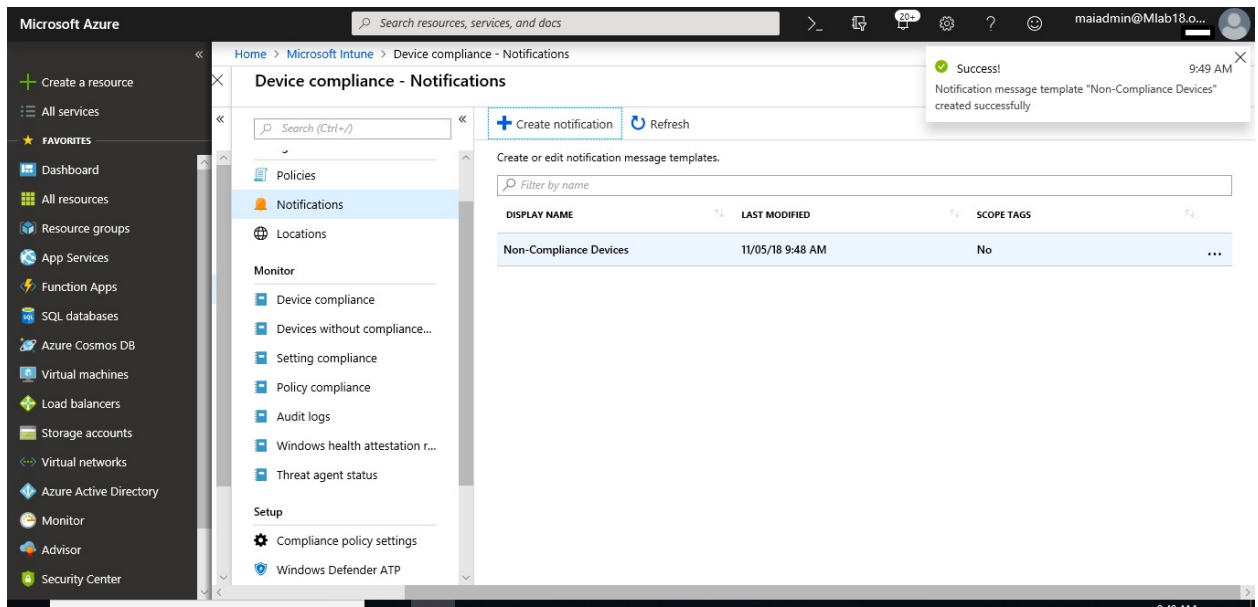
1. In the [Azure portal](#), select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device compliance** > **Notifications**.



3. Select **Create notification**. Enter the following information:



4. Once you're done adding the information, choose **Create**.

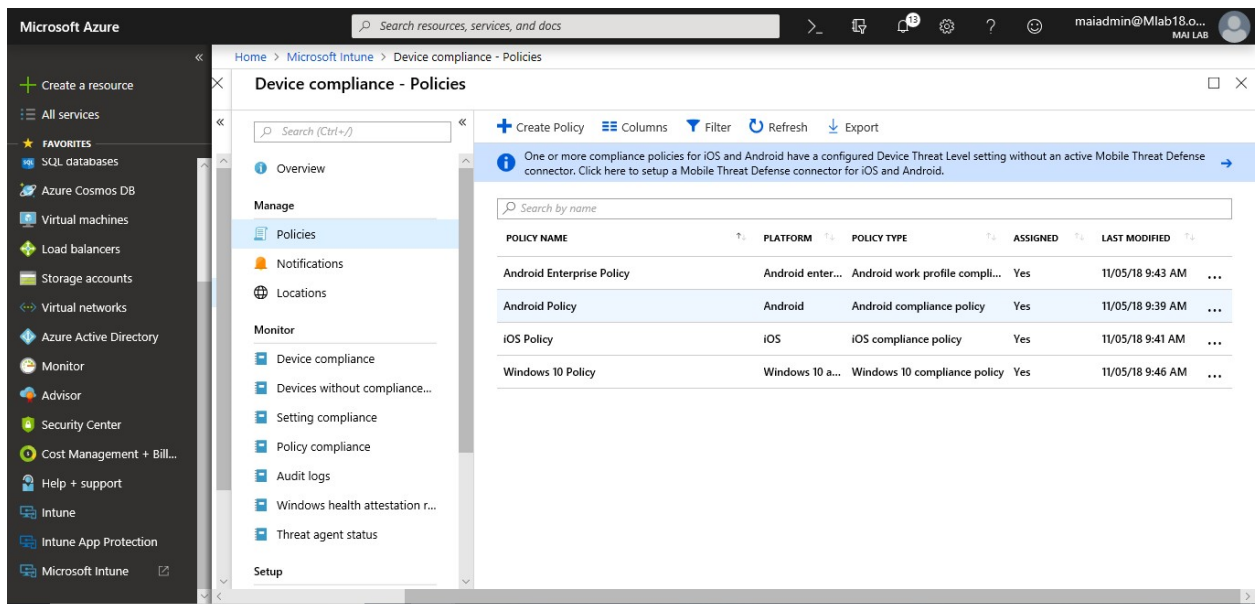


Add actions for noncompliance

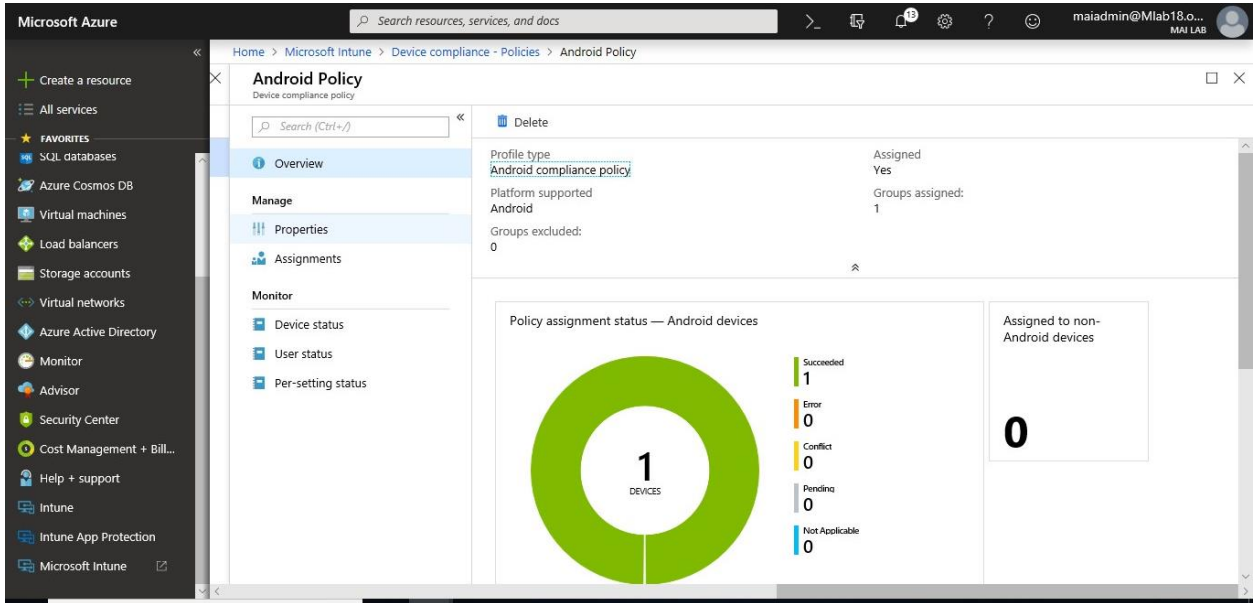
When you create a device compliance policy, Intune automatically creates an action for noncompliance. When a device isn't meeting your compliance policy, this action marks the device as not compliant. You can customize how long the device is marked as not compliant. This action can't be removed.

You can also add another action when you create a compliance policy or update an existing policy.

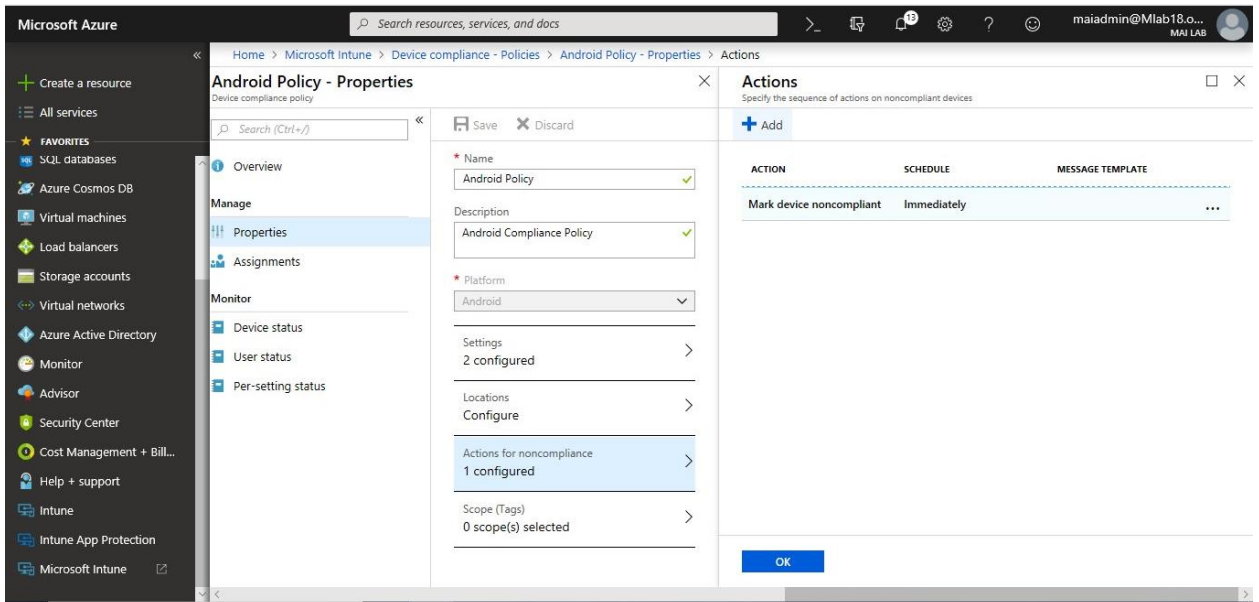
1. In the [Azure portal](#), open **Microsoft Intune > Device compliance**.



2. Select **Policies**, choose one of your policies, and then select **Properties**.

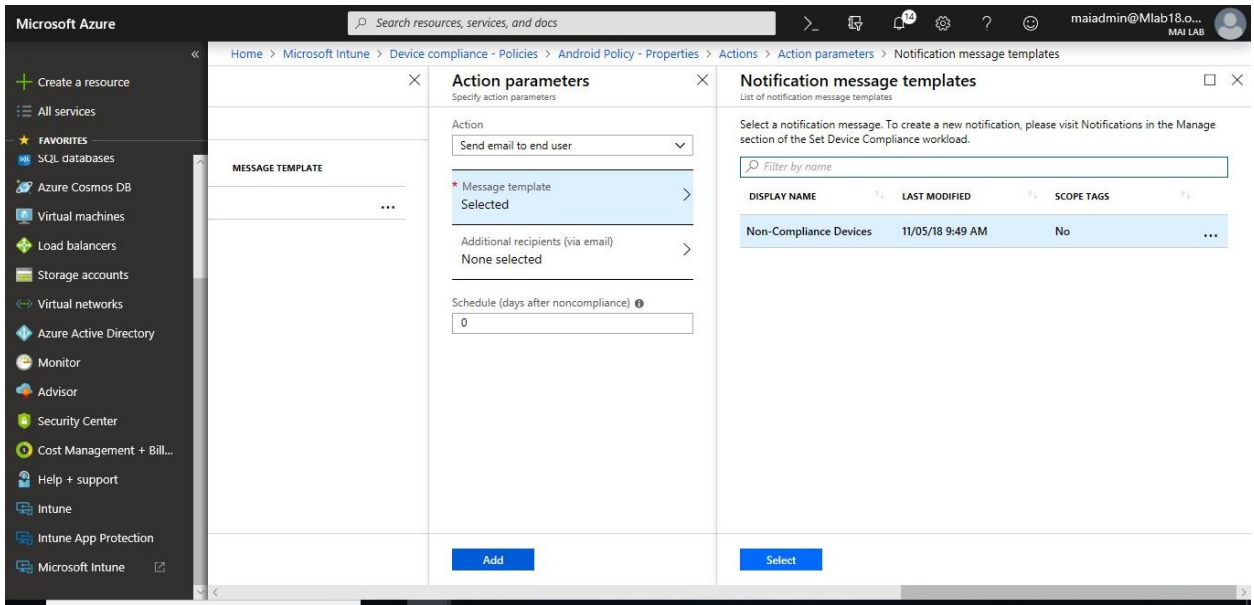


3. Select **Actions for noncompliance** > **Add**.

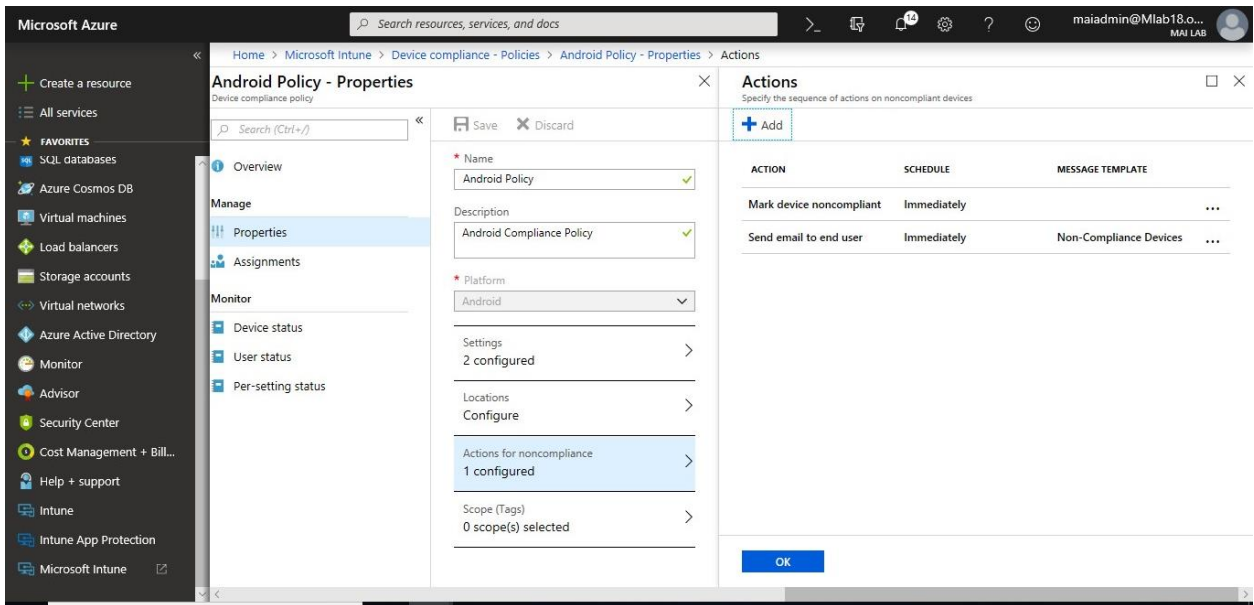


4. Select **your Action**: Send email to end user.

Microsoft Intune step by step on Azure portal



5. When finished, select **Add** > **OK** to save your changes.



Conditional Access policies in Microsoft Intune

Use the Microsoft Intune conditional access policies for Exchange to manage access to Exchange email based on conditions you specify.

You can manage access to:

- Microsoft Exchange On-premises
- Microsoft Exchange Online, SharePoint Online, Skype Online, OneDrive & Teams

Note: You must apply compliance policy on same users that you apply conditional access to them. You will need license Azure AD premium to apply conditional access policy.

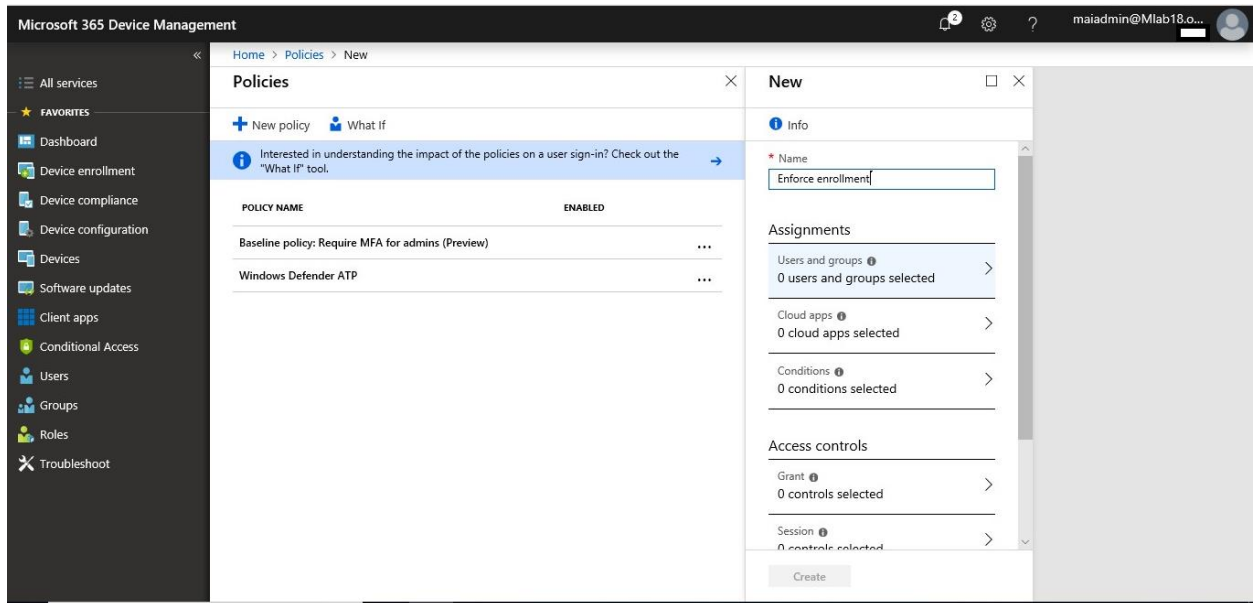
Conditional Access Policy on Exchange Online, SharePoint Online & OneDrive

Configure the policy to require that only managed and compliant devices can access SharePoint Online, OneDrive & Exchange Online. This policy will be stored in Azure Active Directory.

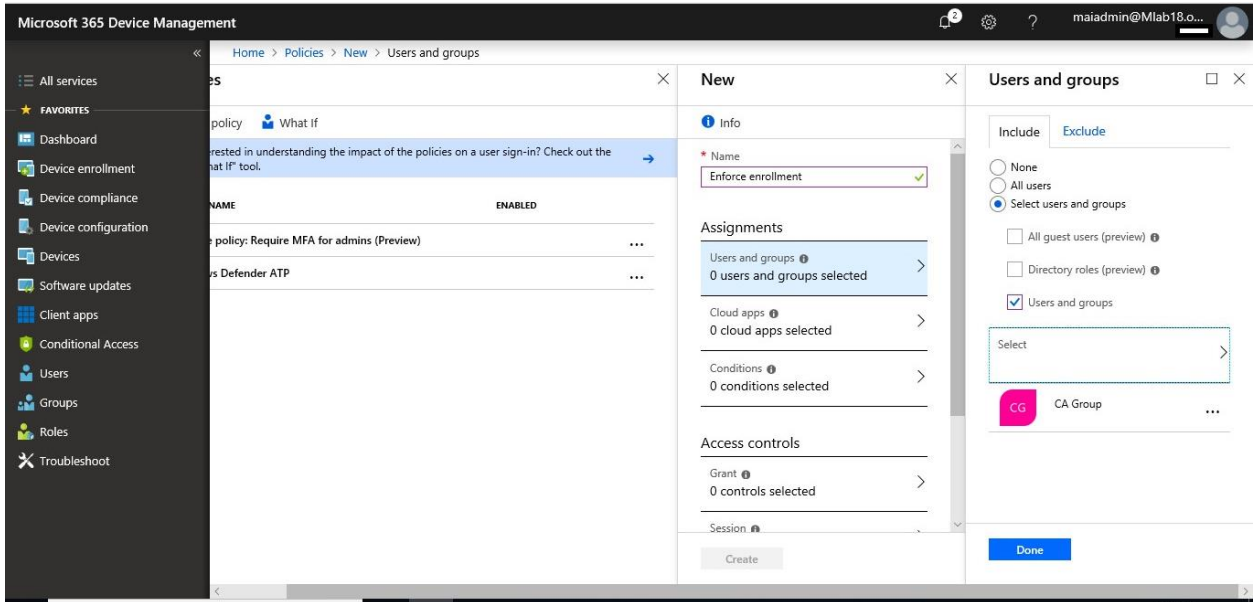
To Create Conditional Access Policy on EXO & SPO, you can follow below steps

The conditional access policy blocks access to resources *if* the device is noncompliant. So, if a device not access compliant, you can block to corporate resources, such as SharePoint or Exchange Online.

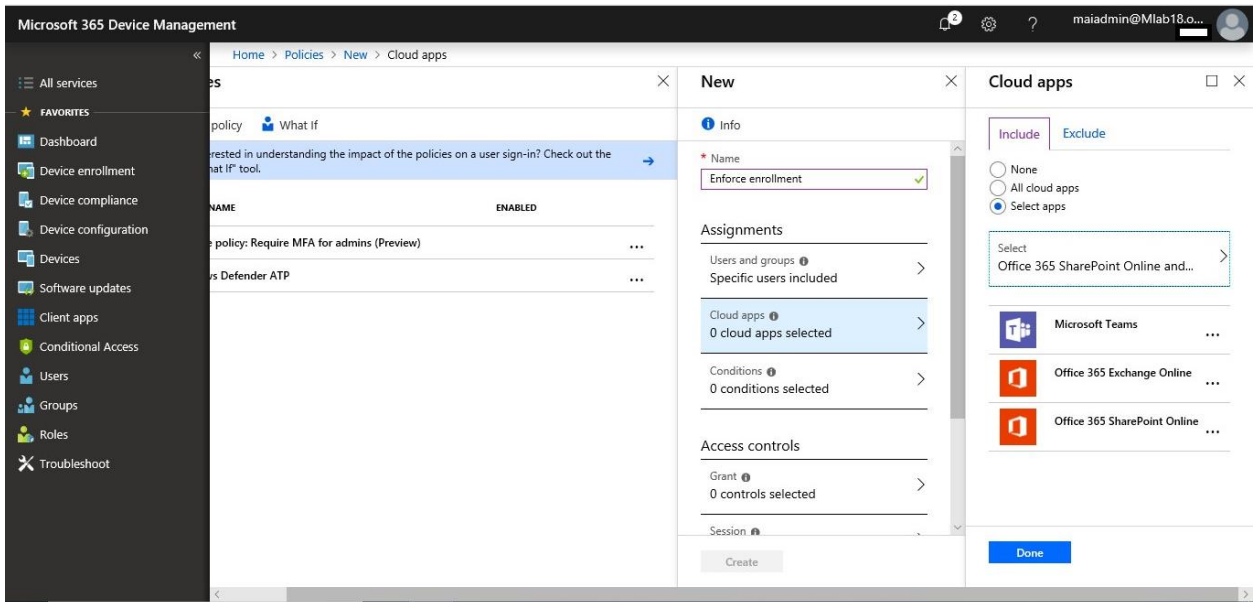
1. In the [Azure portal](#), open **Microsoft Intune > Conditional access > New policy**.



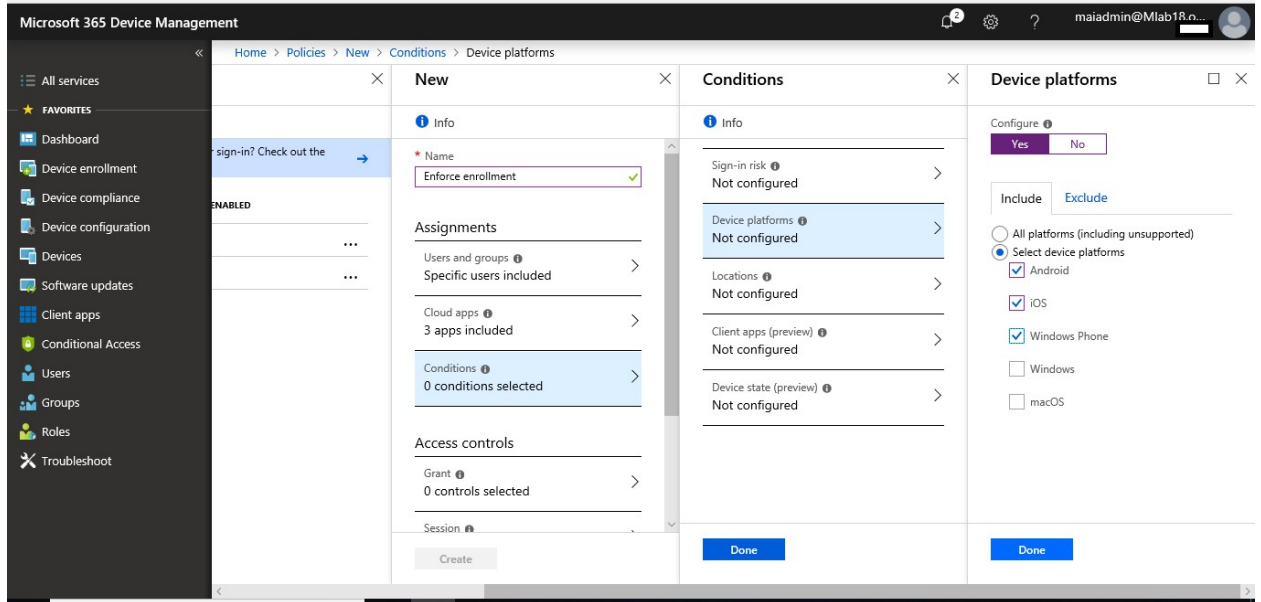
2. Enter a policy **Name** and select **Users and groups**. Use the Include or Exclude options to add your groups for the policy and select **Done**.



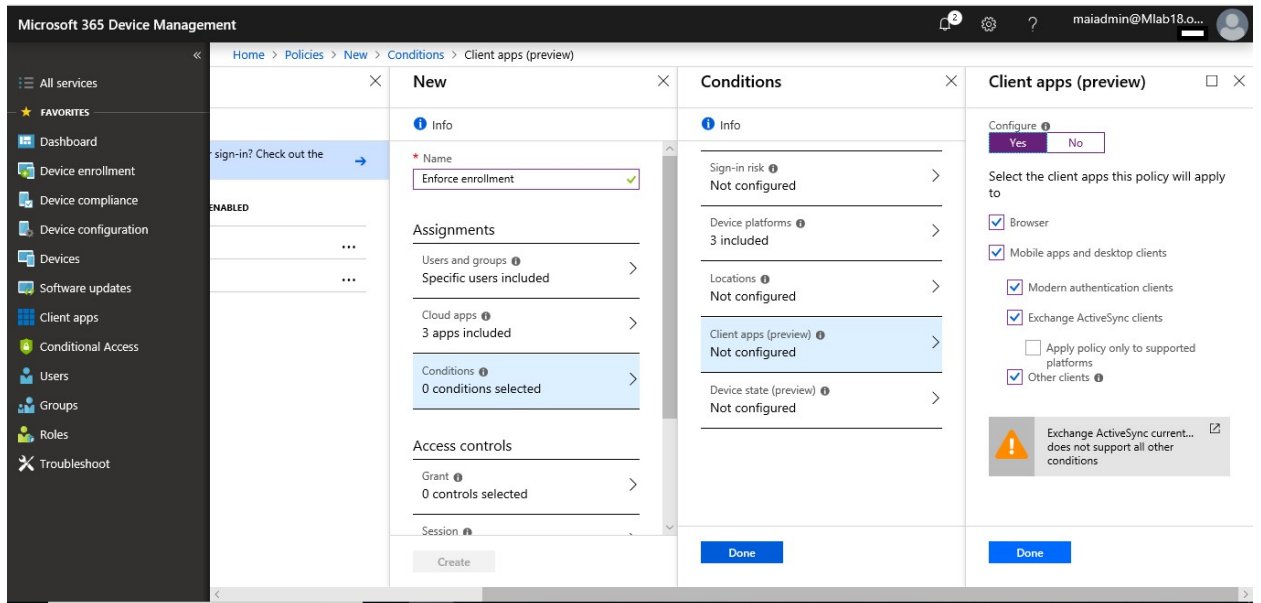
3. Select **Cloud apps** and choose which apps to protect. For example, choose **Select apps**, and select **Teams**, **Office 365 SharePoint Online** and **Office 365 Exchange Online**. Select **Done** to save your changes.



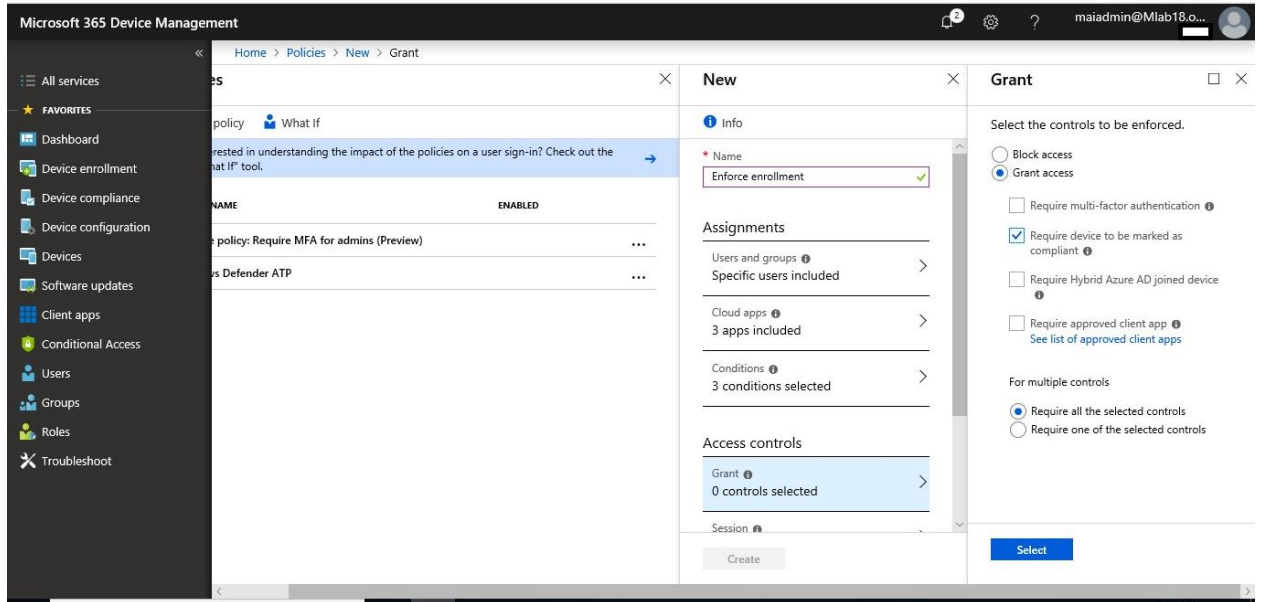
4. Select **Conditions** > **Devices Platform** to apply policy “All Mobile Devices only”



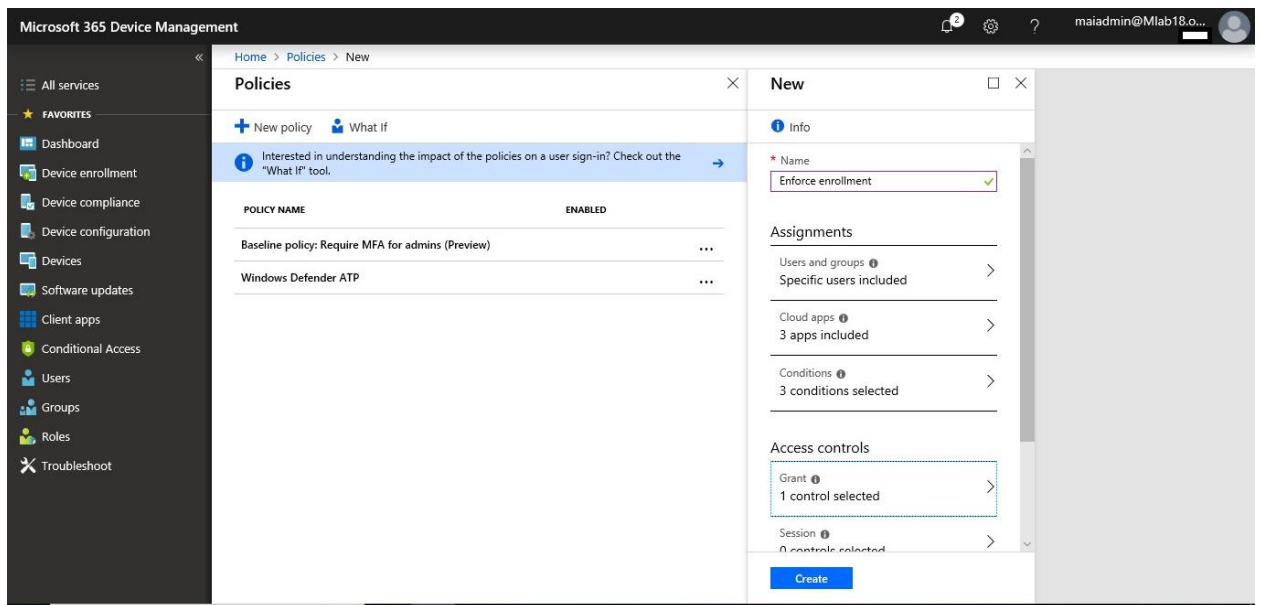
5. Select **Conditions** > **Client apps** to apply the policy to apps and browsers. For example, select **Yes**, and then enable **Browser** and **Mobile apps and desktop clients**. Select **Done** to save your changes.



6. Select **Grant** to apply conditional access based on device compliance. For example, select **Grant access** > **Require device to be marked as compliant**. Choose **Select** to save your changes.



7. Select **Enable policy**, and then **Create** to save your changes.

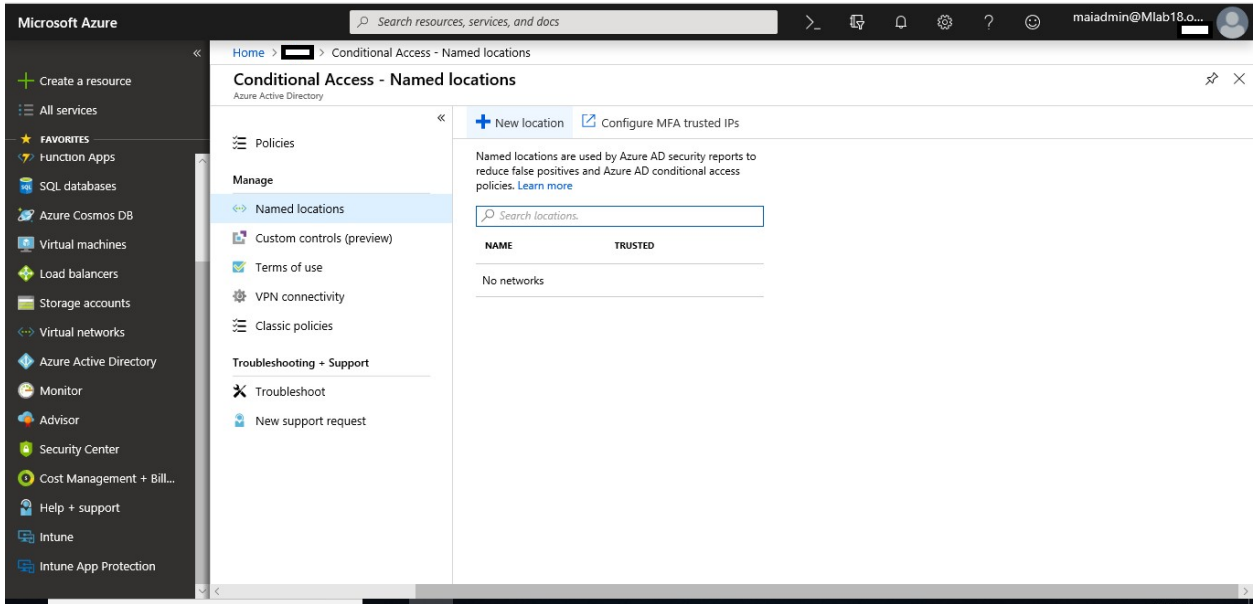


Conditional Access Policy on Cloud Apps from Specific Location

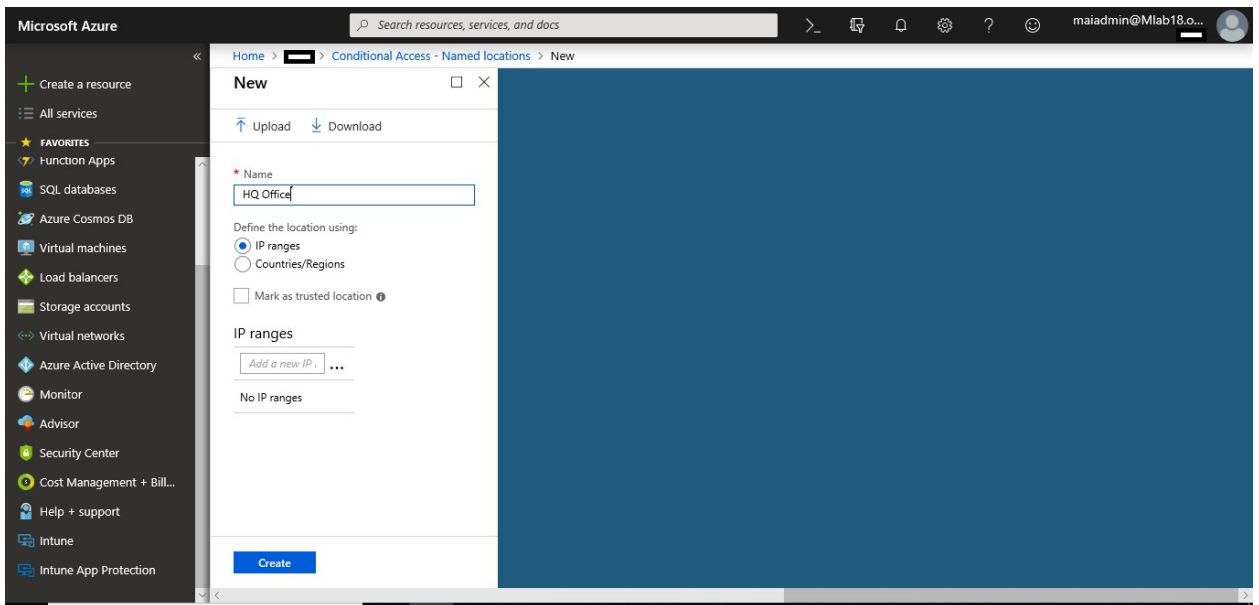
Configure the policy to require MFA to access any cloud app” EXO, SPO, OneDrive” outside Organization. This policy will be stored in Azure Active Directory.

1. In the [Azure portal](#), open **Azure Active Directory** > **Conditional access** > **Named Location**.

Microsoft Intune step by step on Azure portal

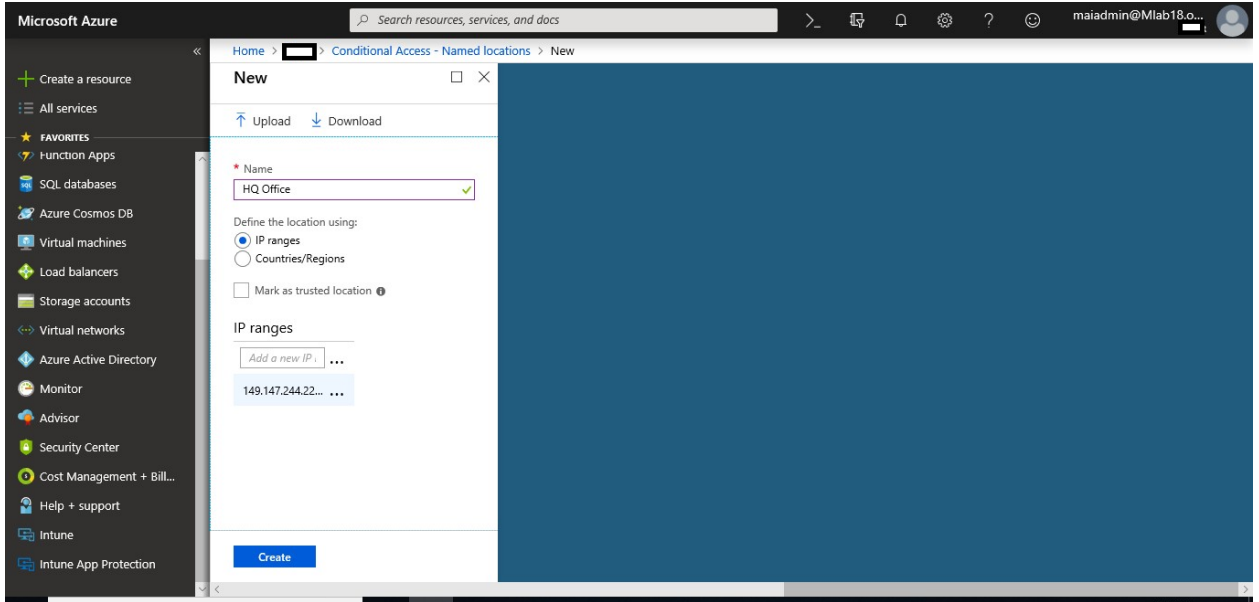


2. Select **New Location** and select **IP Range**. Type **public IP** addresses for your organization.

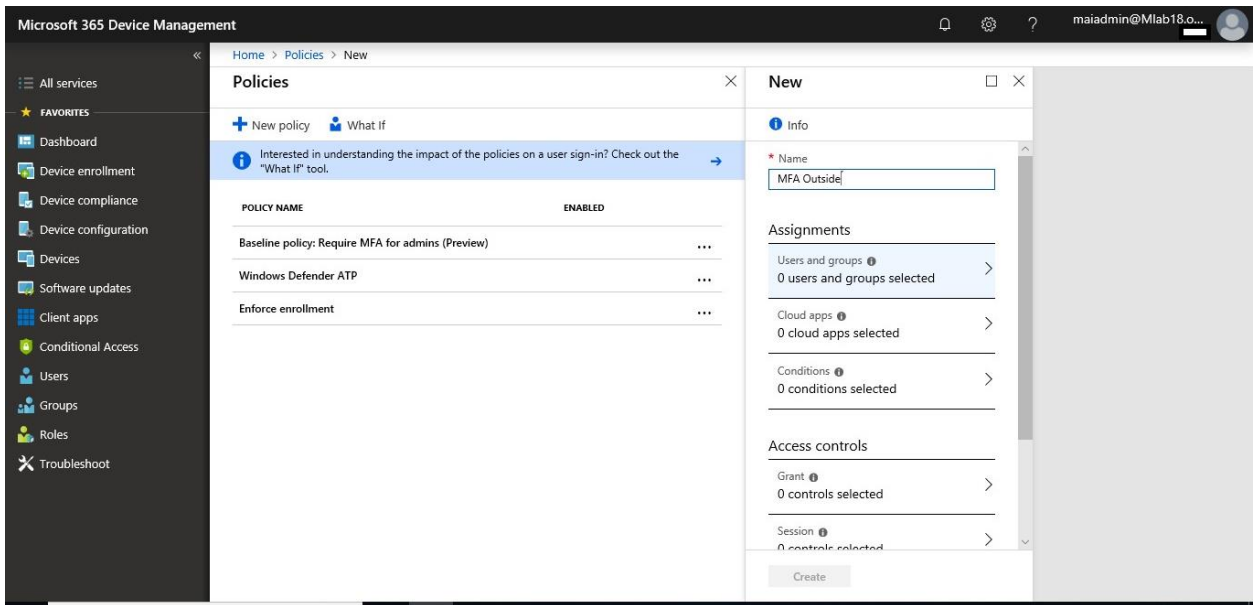


3. Select **Mark as trusted location**, then click **Create**.

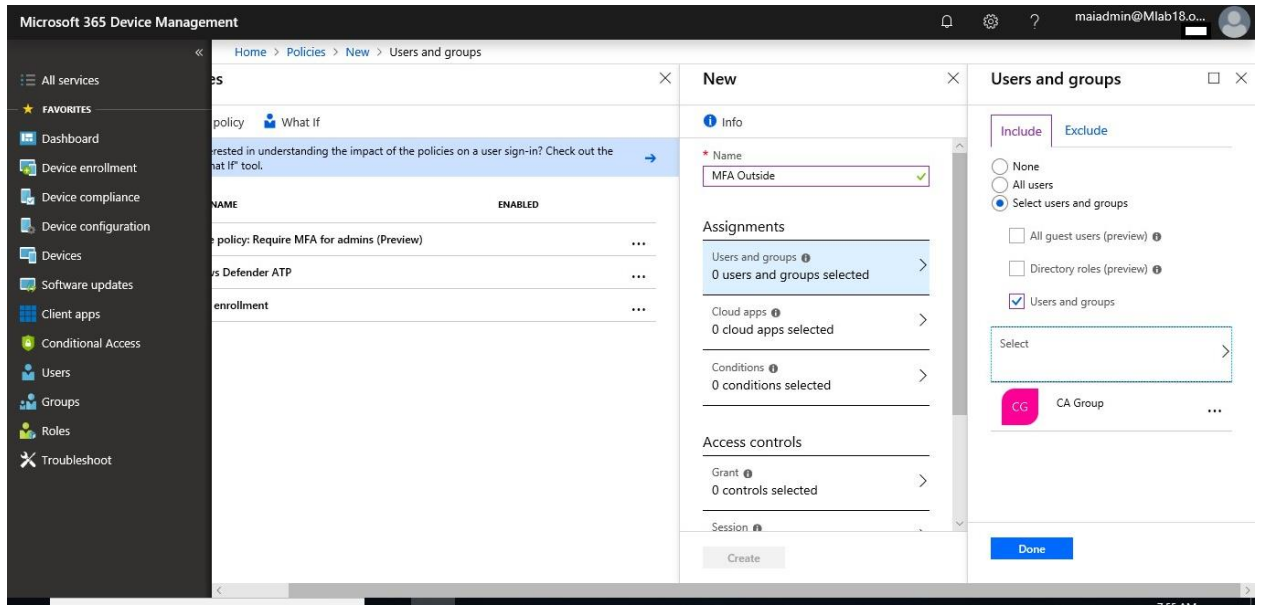
Microsoft Intune step by step on Azure portal



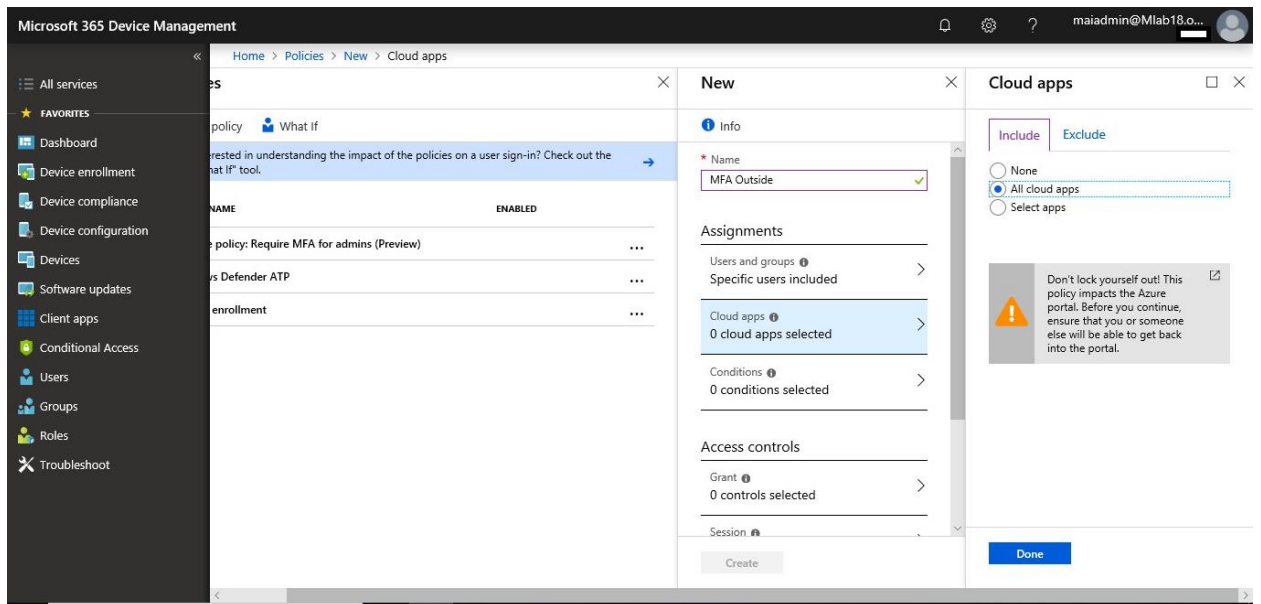
4. In the [Azure portal](#), open **Microsoft Intune > Conditional access > New policy**.



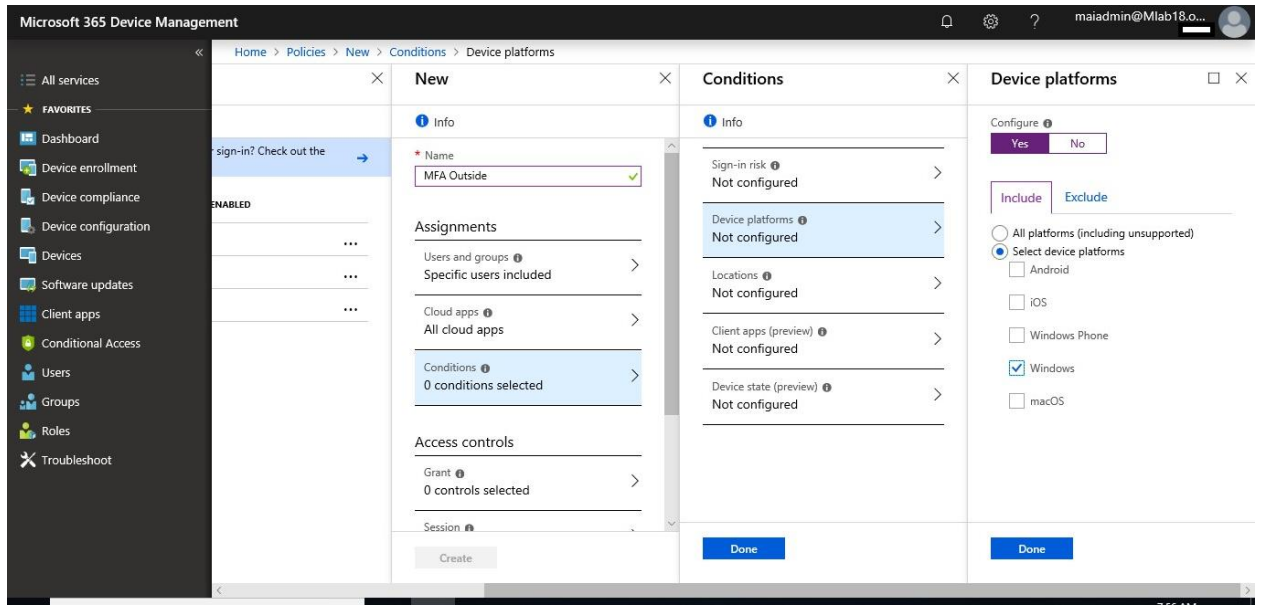
5. Enter a policy **Name** and select **Users and groups**. Use the Include or Exclude options to add your groups for the policy and select **Done**.



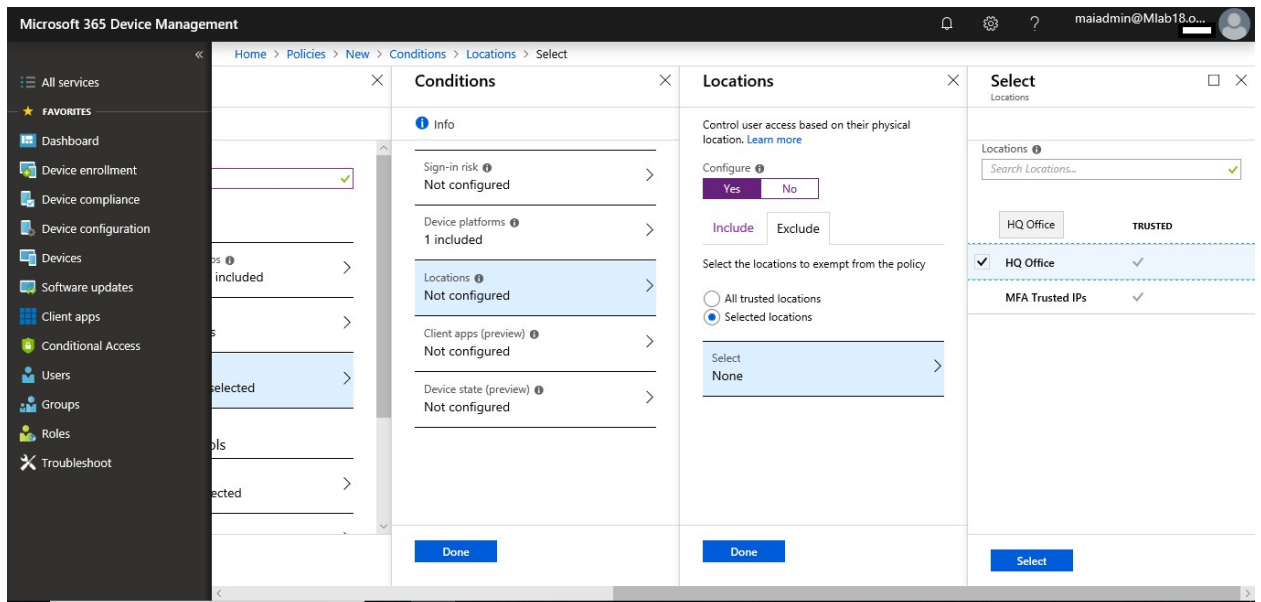
6. Select **Cloud apps** and choose which apps to protect. For example, choose **Select all cloud apps**. Select **Done** to save your changes.



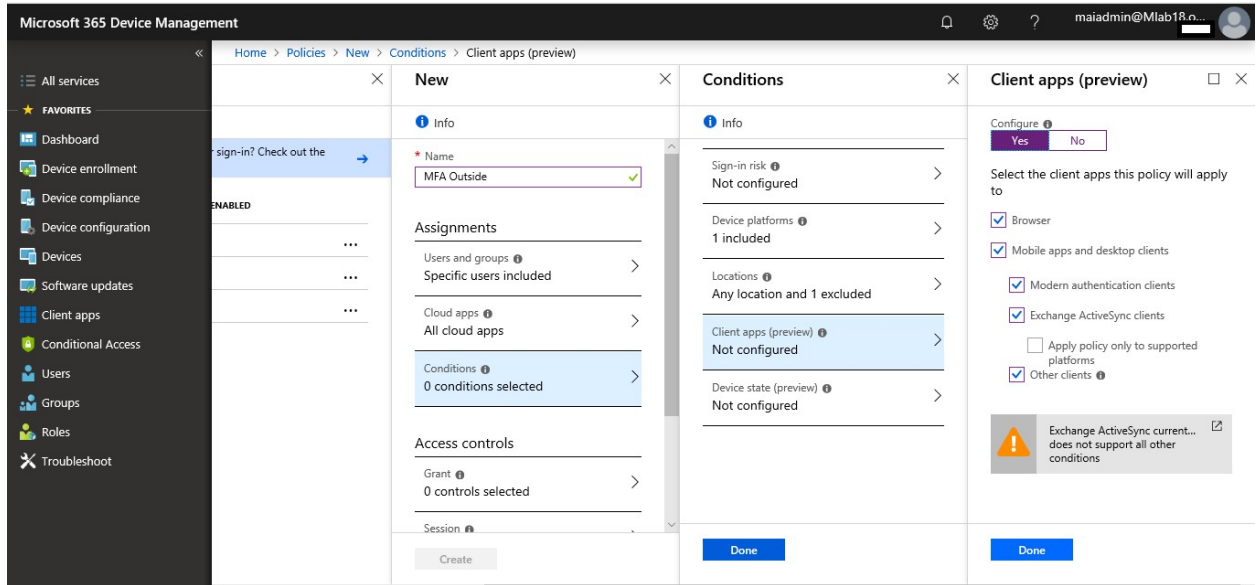
7. Select **Conditions** > **Device platforms** to apply the policy to windows PCs, Select **Done**.



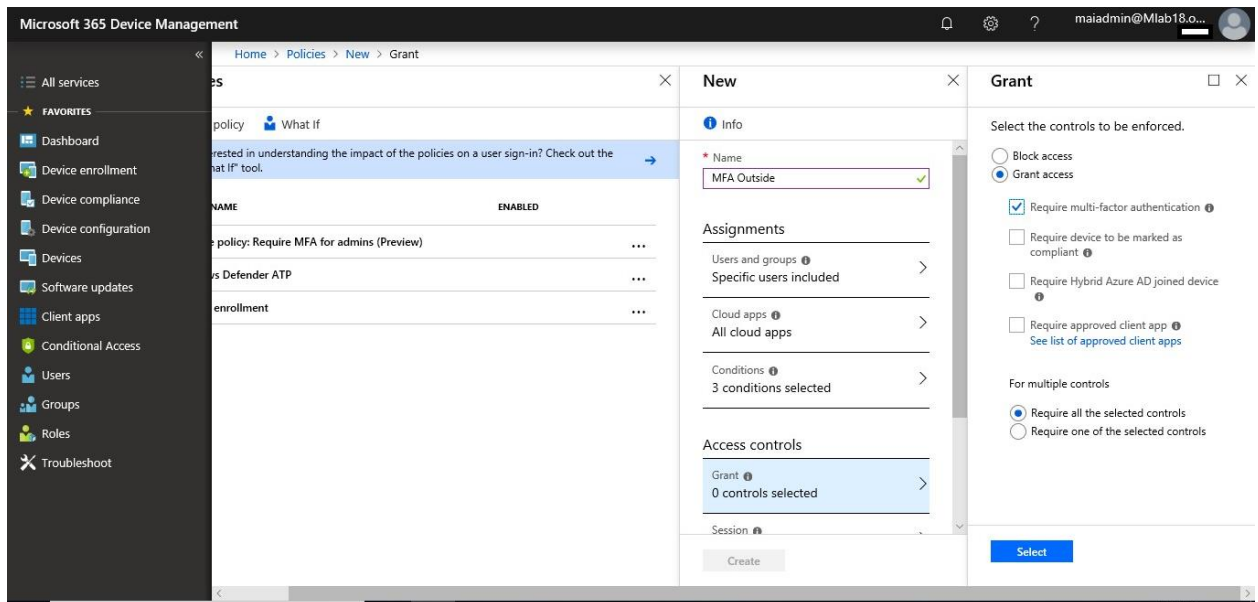
8. Select **Conditions** > **locations** to apply the policy to any location & exclude HQ office, Select **Done**.



9. Select **Conditions** > **Client apps** to apply the policy to apps and browsers. For example, select **Yes**, and then enable **Browser** and **Mobile apps and desktop clients**. Select **Done** to save your changes.



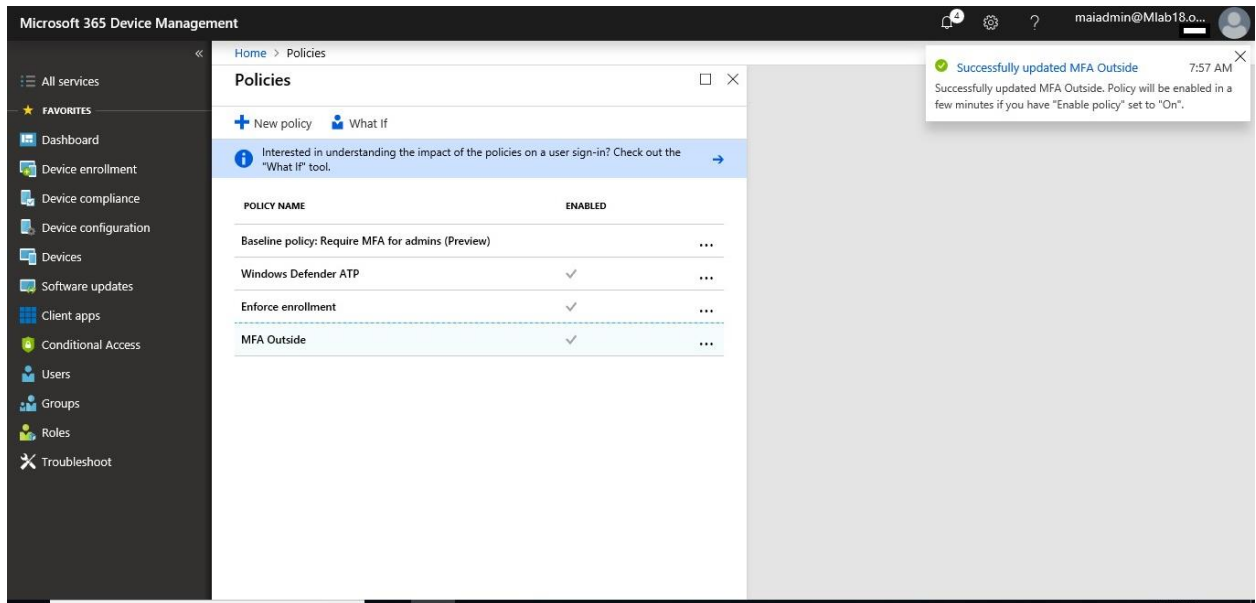
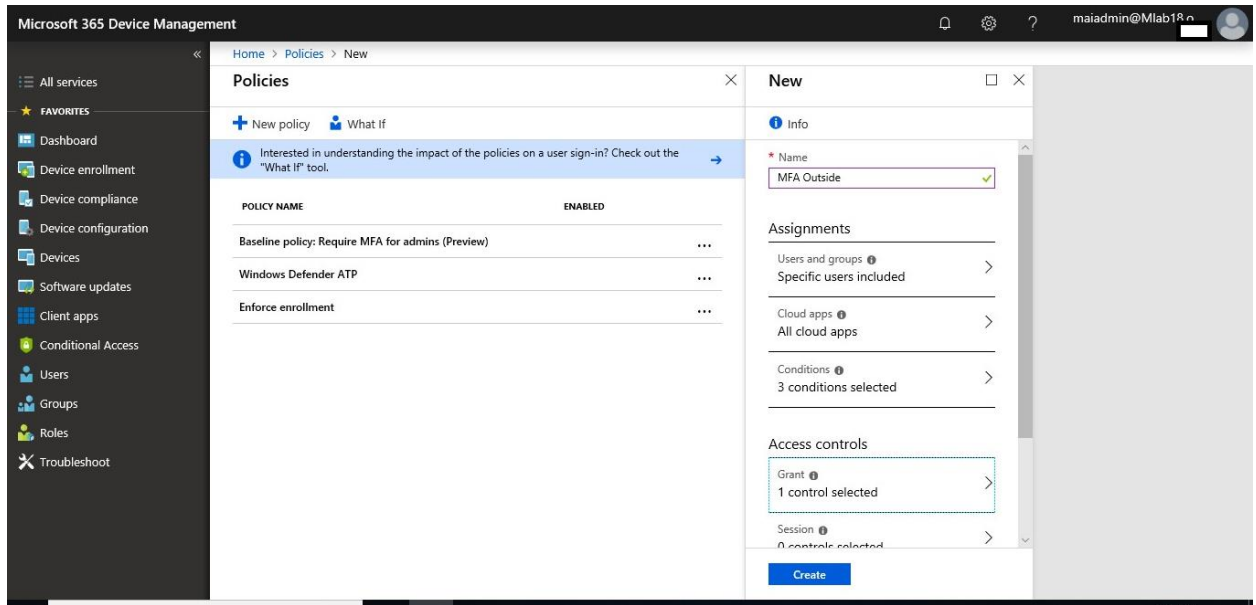
10. Select **Grant** to apply conditional access based on device compliance. For example, select **Grant access > Require multi factor authentication**. Choose **Select** to save your changes.



Note: If you choose **require device to be marked as compliant** which you choose the device **windows**, at this moment, end user won't be able to access resources outside organization unless he enroll his Window PC as MDM. Windows 7 can't enroll by Intune MDM.

11. Select **Enable policy**, and then **Create** to save your changes.

Microsoft Intune step by step on Azure portal



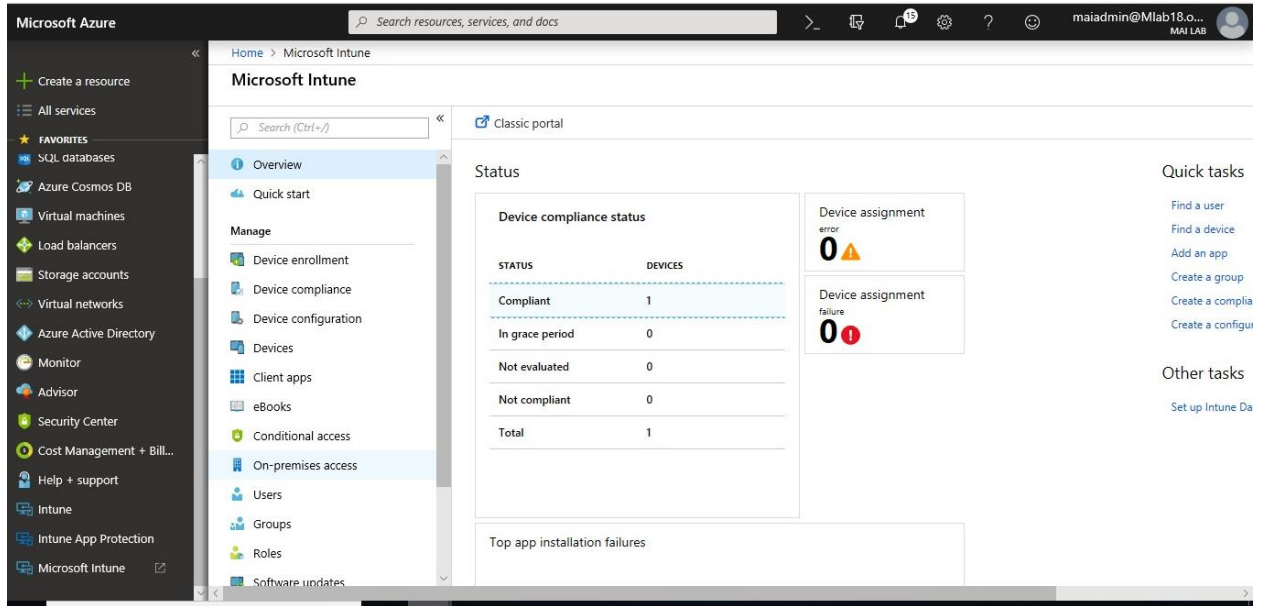
Note: To apply Conditional Access policy, you need to have Azure AD premium license.

Conditional Access Policy on Exchange On-premise

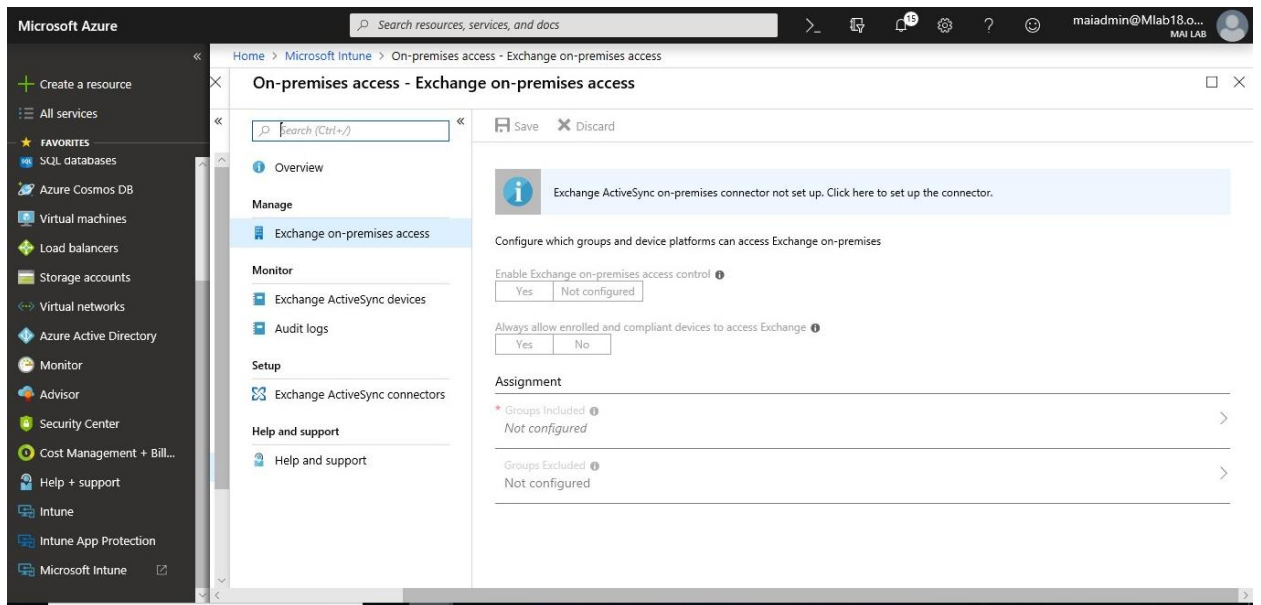
To set up a connection that enables Microsoft Intune to communicate with the on-premises Exchange Server, here are the general steps:

1. In the [Azure portal](#), select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **On-Premise Access**.

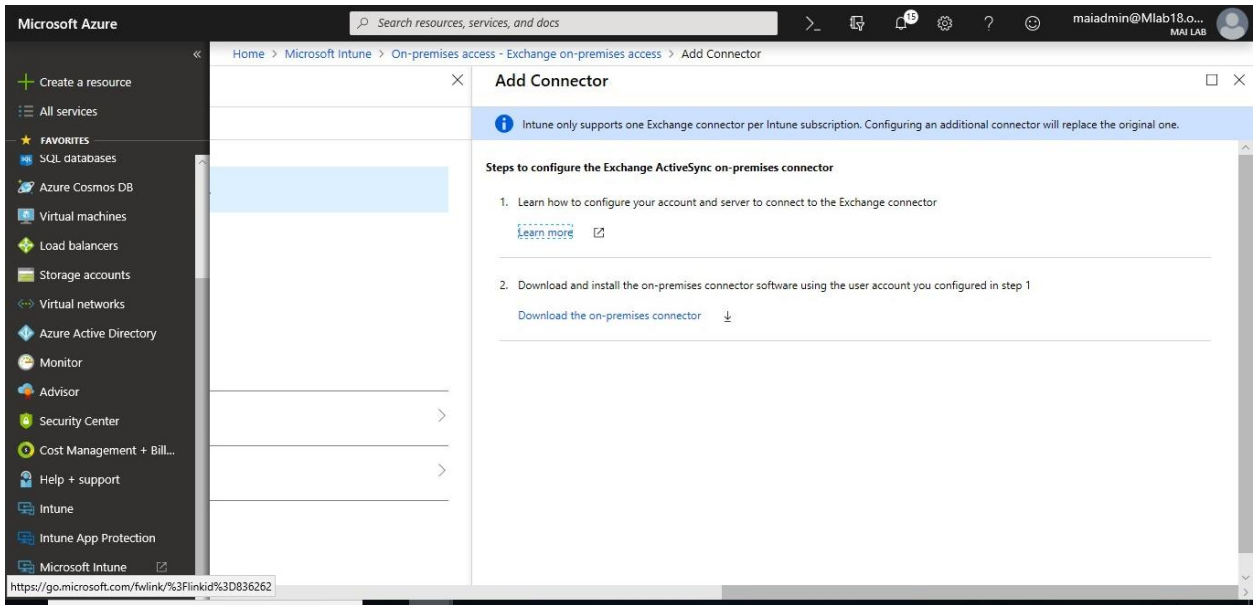
Microsoft Intune step by step on Azure portal



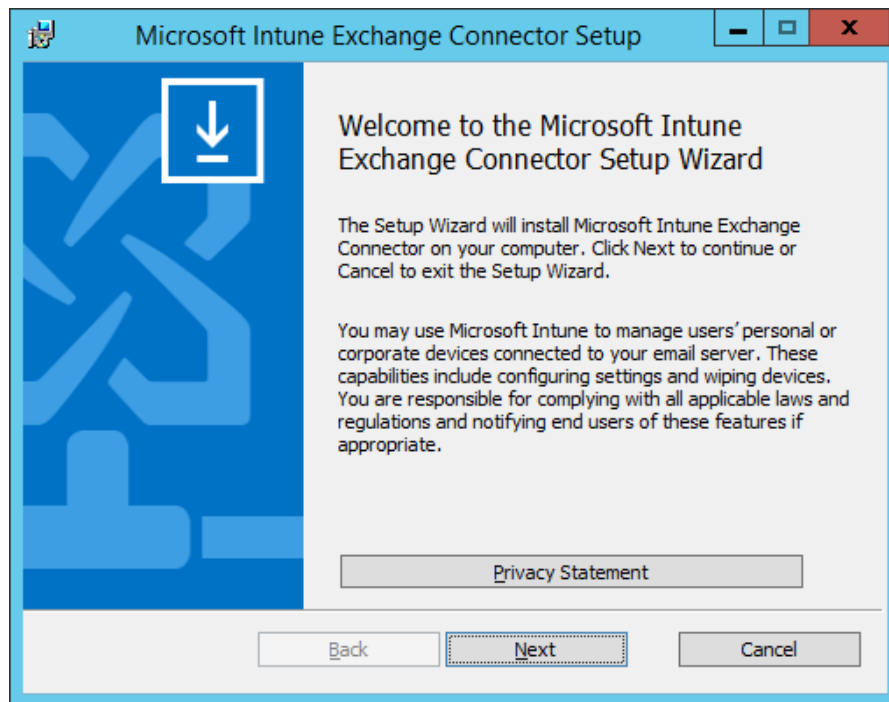
3. Select **Exchange On-Premise Access**, select on blue bar click here to set up the connector.



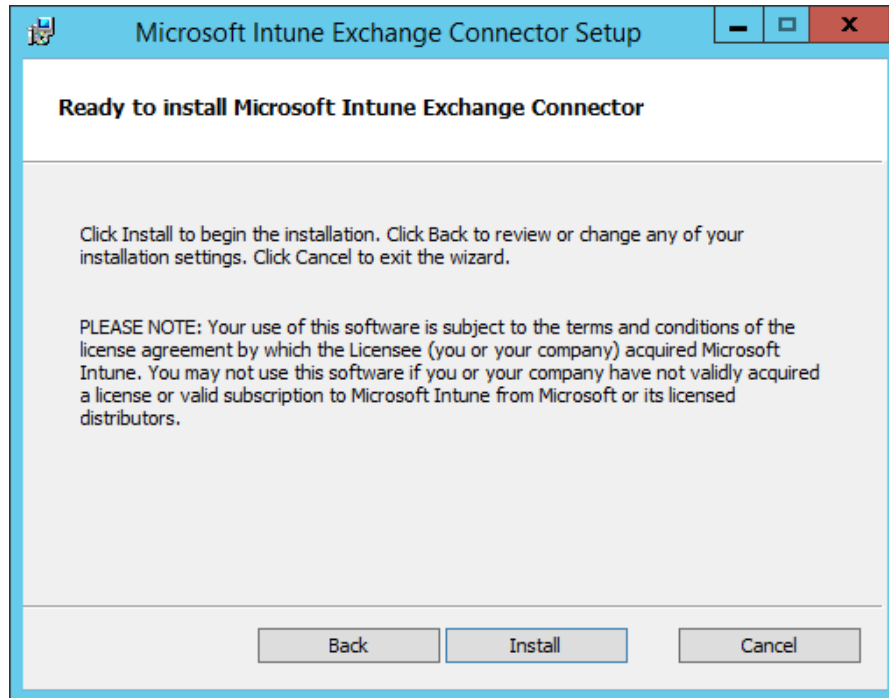
4. Select Download the on-premises connector from the Azure portal.



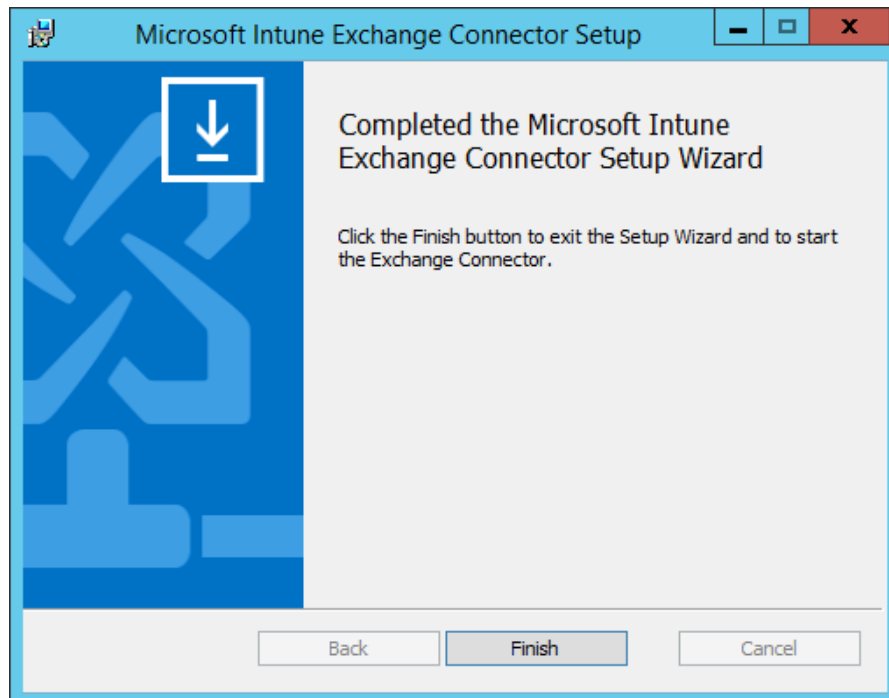
5. Install and configure the Exchange connector on a computer in the on-premises Exchange organization.
6. On a supported operating system for the on-premises Exchange connector, extract the files in **Exchange_Connector_Setup.zip** to a secure location.
7. After the files are extracted, open the extracted folder and double-click **Exchange_Connector_Setup.exe** to install the on-premises Exchange connector.



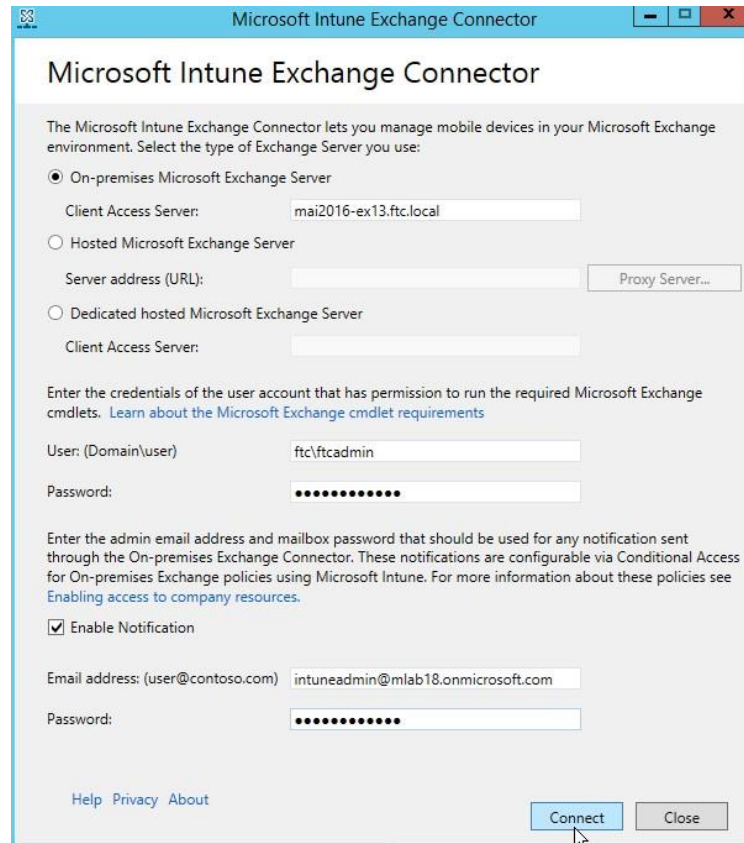
8. On Ready page, **Click Install.**



9. On Completed Microsoft Intune Connector, click **finish**.



10. On-premises Microsoft Exchange server, Write **FQDN of CAS server** and Enter **Credential of Exchange Administrator On-premises** Then click **connect**.



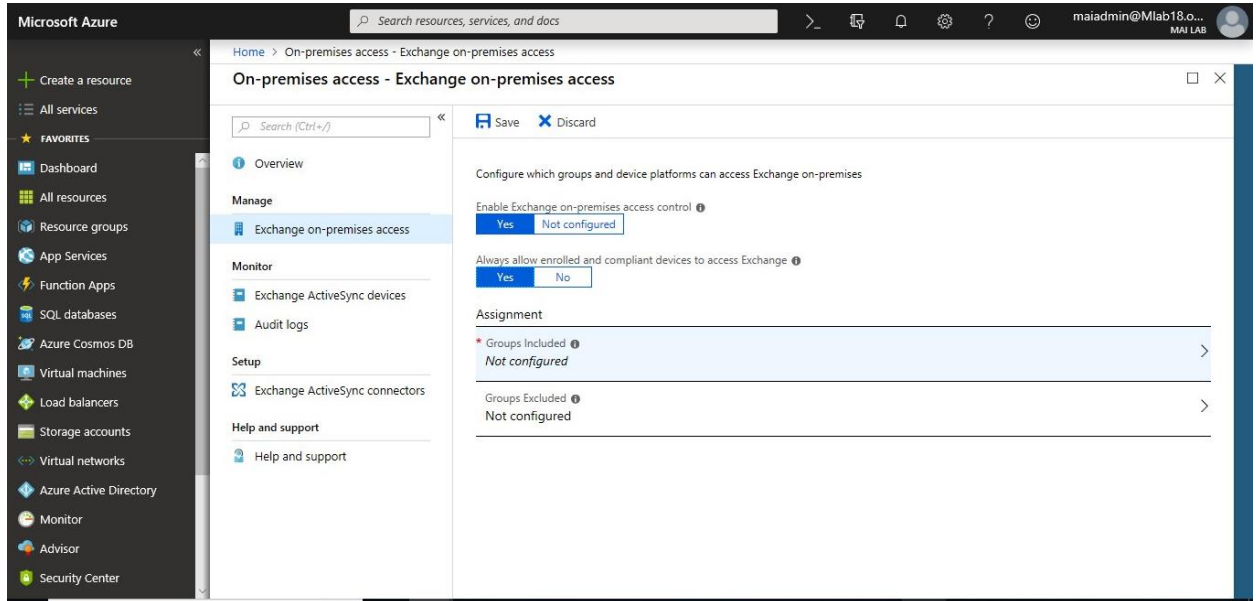
11. Connector is now installed successfully.



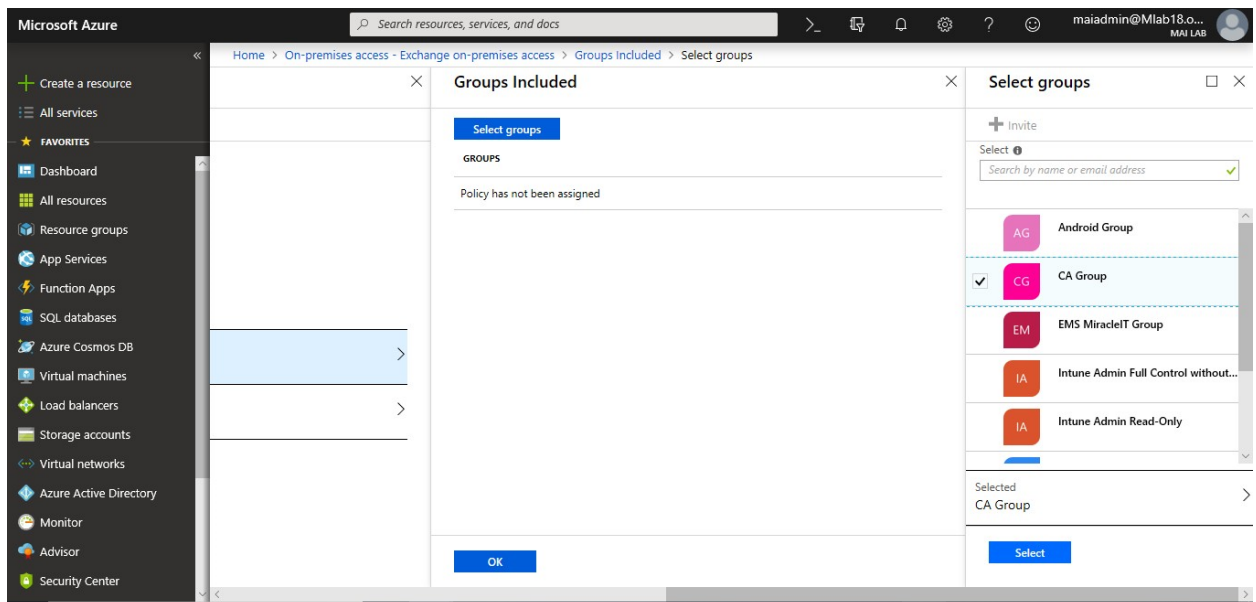
To Configure Conditional Access Policy on Exchange On-Premise, you need to follow below steps

Microsoft Intune step by step on Azure portal

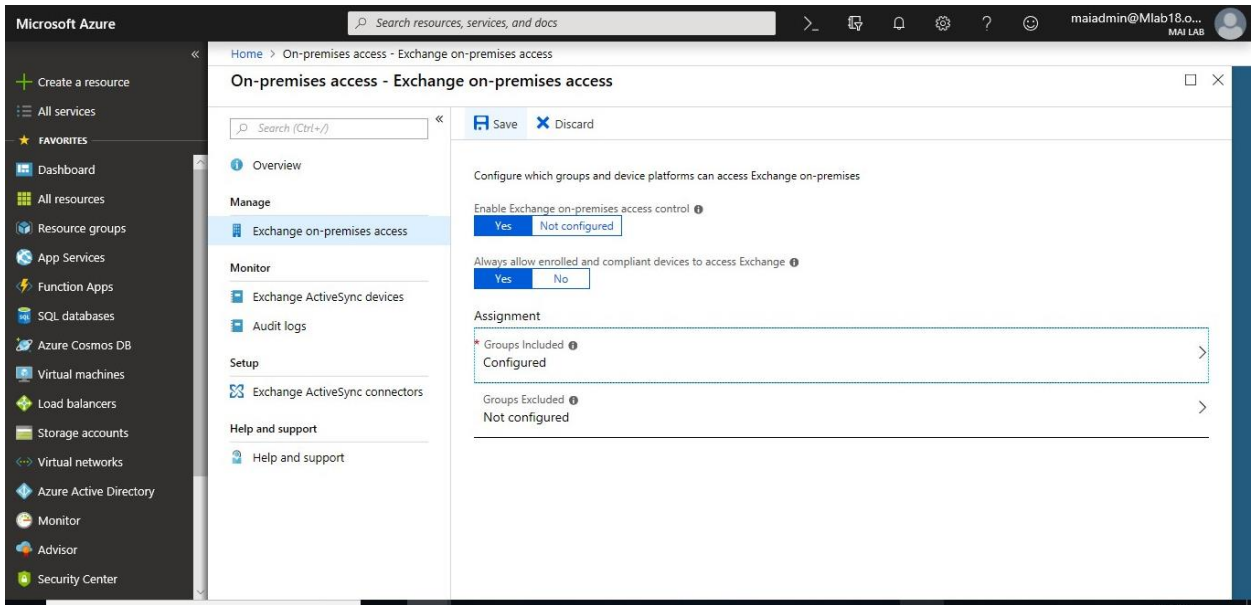
1. In the [Azure portal](#), select **All services**, filter on **Intune**, and select **Microsoft Intune** > **Select On-Premise Access**.
2. Select **Yes** to **Enable Exchange on-premise access control** & **Always allow enrolled and compliant devices**.



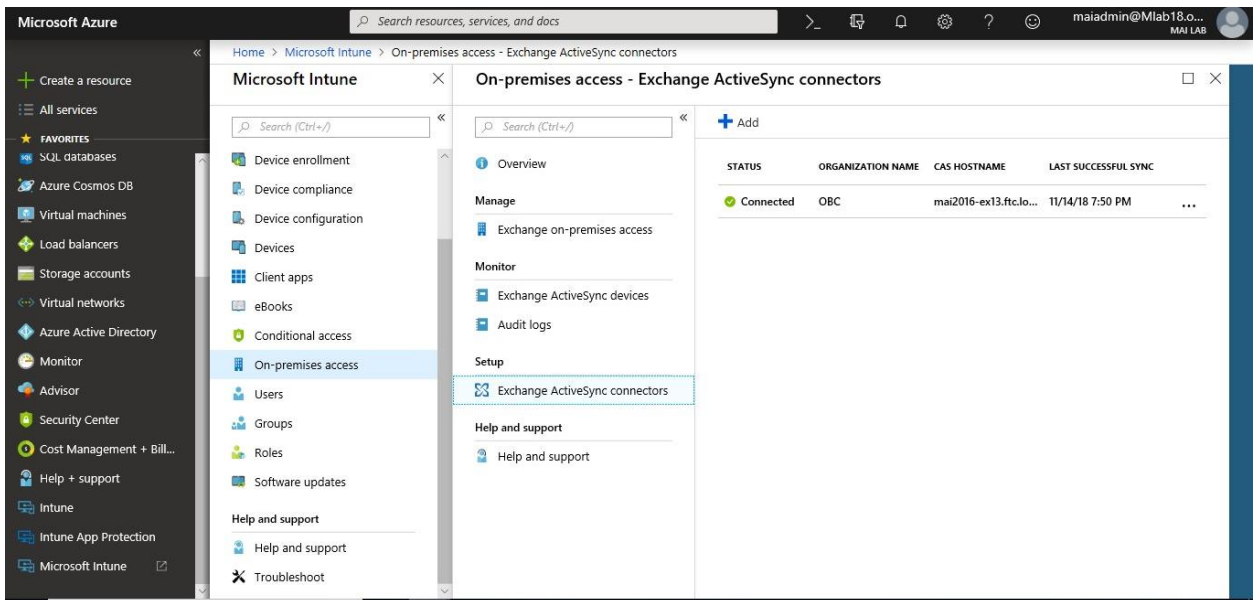
3. Select Target Group that you want to apply policy on it.



4. Click **Save**.



5. You can check health state for Exchange ActiveSync connectors and see last successful sync status.



Reset passcodes when users are locked out of their devices

Since the first step in protecting company data on mobile devices is to require a passcode to use the device, sometimes you must **reset a passcode** or help an employee do so, either by removing the passcode or setting a temporary passcode remotely. You can also **lock a device remotely** if it's lost or stolen.

Reset Device Passcode Using Intune

Reset passcode is done on device level passcode reset as well as work profile passcode reset on Android enterprise (formerly called Android for Work, or AfW) devices. It is important to note this distinction as requirements for each can vary. A device level passcode reset resets the passcode for the entire device. A work profile passcode reset resets the passcode only for the user's work profile on Android enterprise devices.

Supported platforms for device level passcode reset

Platform	Supported?
Android devices on version 6.x or earlier	Yes
Android enterprise devices in kiosk mode	Yes
iOS devices	Yes
Android devices enrolled with a work profile, version 7.0 and earlier	No
Android devices on version 7.0 or later	No
macOS	No
Windows	No

For Android devices, this effectively means that device level passcode reset is only supported on devices running 6.x or earlier, or on Android enterprise devices running in Kiosk mode. This is because Google removed support for resetting an Android 7 device's passcode/password from within a Device Administrator granted app and applies to all MDM vendors.

Supported platforms for Android enterprise work profile passcode reset

Platform	Supported?
Android enterprise devices enrolled with a work profile and running version 8.0 and later	Yes
Android enterprise devices enrolled with a work profile and running version 7.x and earlier	No
Android devices running version 7.x and earlier	No
iOS	No
macOS	No

To create a new work profile passcode, use the Reset Passcode action. This action prompts a passcode reset and creates a new, temporary passcode for the work profile only.

Reset Android work profile passcodes

Supported Android Enterprise devices enrolled with a work profile receive a new managed profile unlock password or a managed profile challenge for the end user.

Microsoft Intune step by step on Azure portal

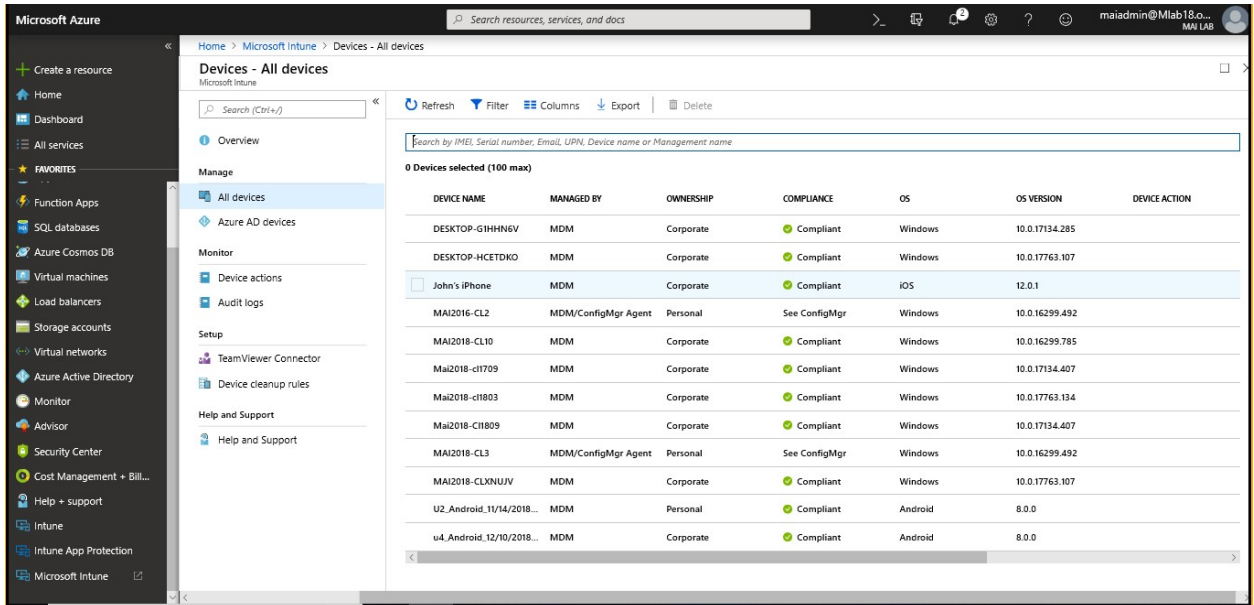
For Android Enterprise devices running version 8.x or later and enrolled with a work profile, end users get notified to activate their reset passcode right after enrollment is completed. The notification is displayed if a work profile password is required and set. Once their passcode is entered, the notification is dismissed.

Remove iOS passcodes

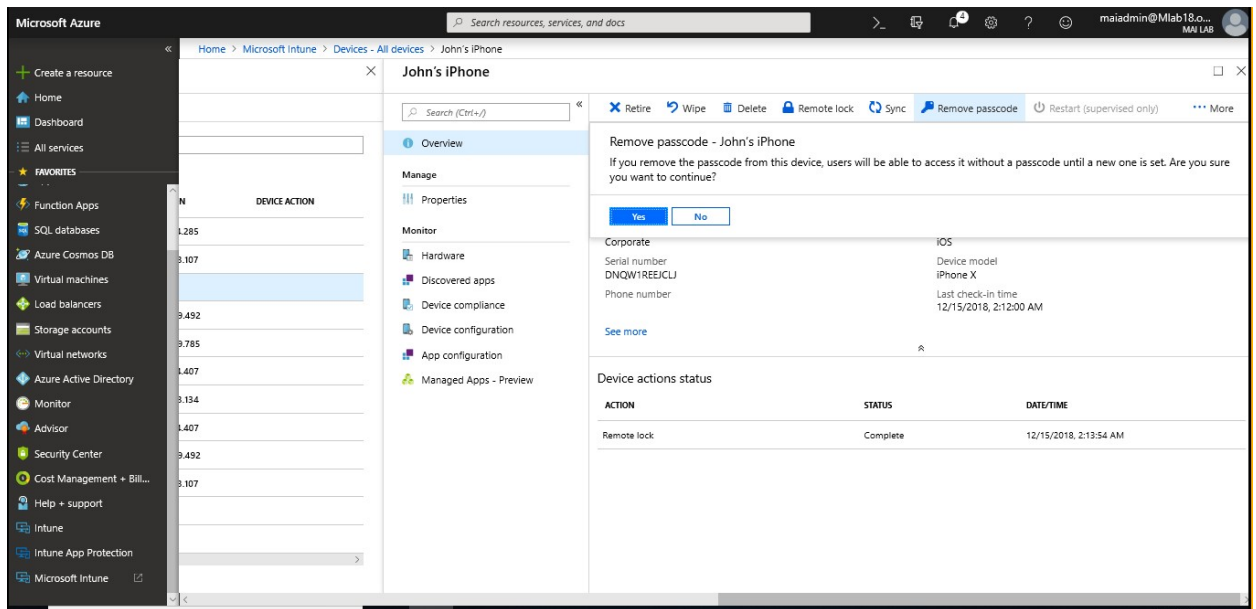
Instead of being reset, **passcodes are removed from iOS devices**. If there's a passcode compliance policy set, the device will **prompt the user to set a new passcode** in Settings.

To reset a passcode, you need to follow below steps:

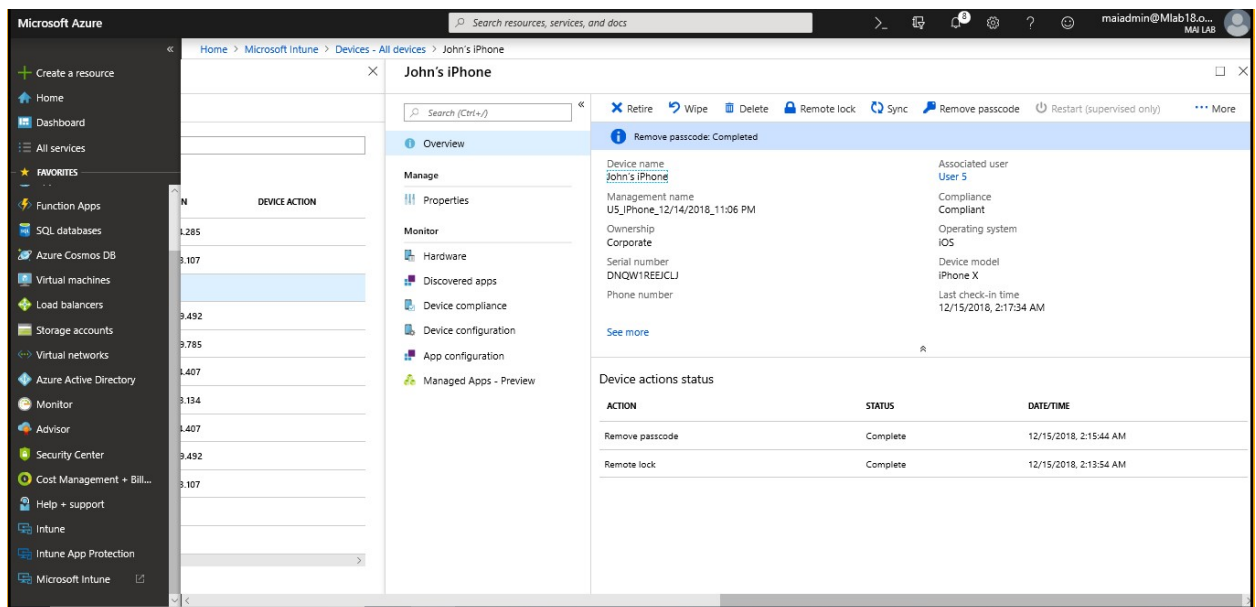
1. Sign in to the [Azure portal](#). Select **All services**, filter on **Intune**, and then select **Microsoft Intune**.
2. Select **Devices**, and then select **All devices**.



3. From the list of devices, you manage, select a device, and choose the **Remove passcode** device remote action then click **Yes**.



4. After Remove Passcode is completed, you will find that you can open iPhone without need any passcode for access.



Remotely Lock Devices Using Intune

The **Remote lock** device action locks the device. To unlock the device, the device owner enters their passcode. You can remotely lock devices that have a PIN or password set. **Devices that don't have a PIN or password can't be remotely locked.**

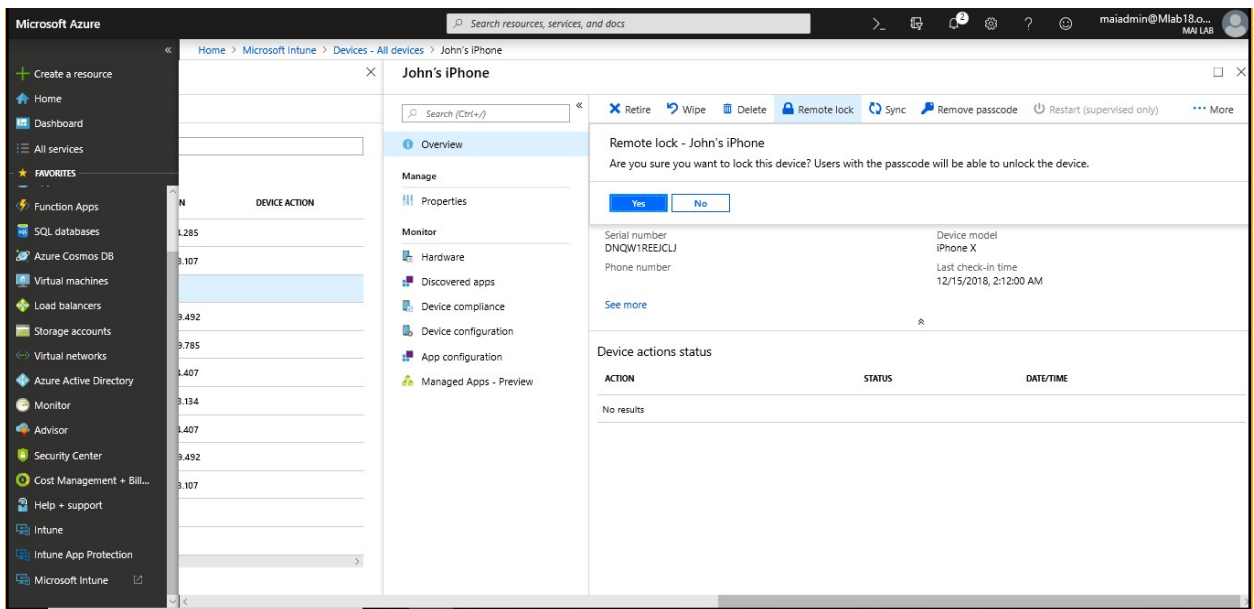
Supported platforms for remote lock

Platform	Supported?
Android	Yes
Android enterprise kiosk devices	Yes
Android enterprise work profile devices	Yes
iOS devices	Yes
macOS	Yes
Windows 10 Mobile	Yes
Windows Phone 8.1 and later	Yes
Windows 10 desktop	No

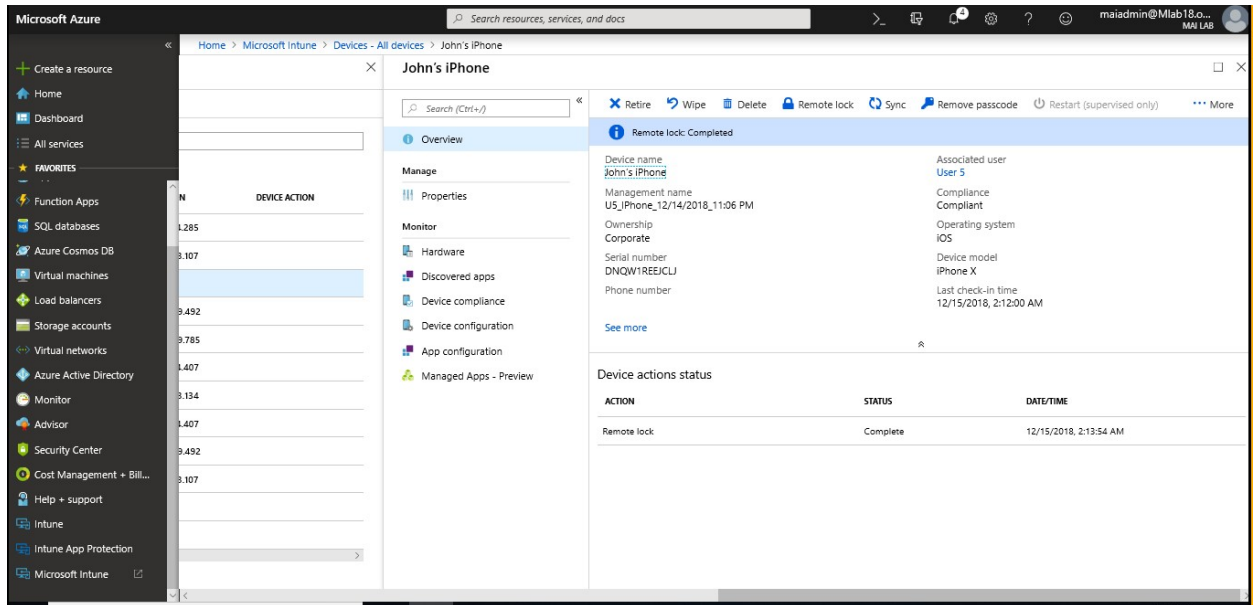
Note: For macOS devices, you set a 6-digit recovery PIN. When the device is locked, the **Device overview** displays the PIN until another device action is sent.

To remote lock a device, you need to follow below steps:

1. Sign in to the [Azure portal](#). Select **All services**, filter on **Intune**, and then select **Microsoft Intune**.
2. Select **Devices > All devices**.
3. In the list of devices, select a device, and then select the **Remote lock** action. Then click **Yes** to confirm remote lock device.



4. After Remote Lock is completed, you will find device lock.



Enable Supervised mode for iOS Devices

Apple iOS supervised mode gives administrators more options when managing Apple devices, making it useful for corporate-owned devices deployed at scale.

Note: Supervised mode for iOS devices lets you use Apple Configurator to lock down a device and limit functionality to specific business purposes. **Supervised mode is used only for corporate-owned devices.**

Turn on supervised mode using Device Enrollment Program

In Intune, you can turn on supervised mode for devices when you create an **Apple enrollment profile in DEP**. Under **Device Management Settings**, check the **Supervised** box.

Turn on supervised mode using Apple Configurator

After enrollment, the only way to turn on supervised mode is to connect an iOS device to a Mac and use the **Apple Configurator** (which will reset the device). **You can't configure a device for Supervised mode in Intune after enrollment.**

Note: To enable supervisor mode through Apple configurator, you need to prepare device and check on supervisor mode on step 5 of [enroll device with Setup Assistant](#). Then you can enroll it manual or using Apple Configurator.

Locate lost or stolen iOS devices with Intune

The **Lost mode** device action helps you enable lost mode on lost or stolen iOS devices. This mode lets you enter a message and a phone number that appears on the lock screen of the device.

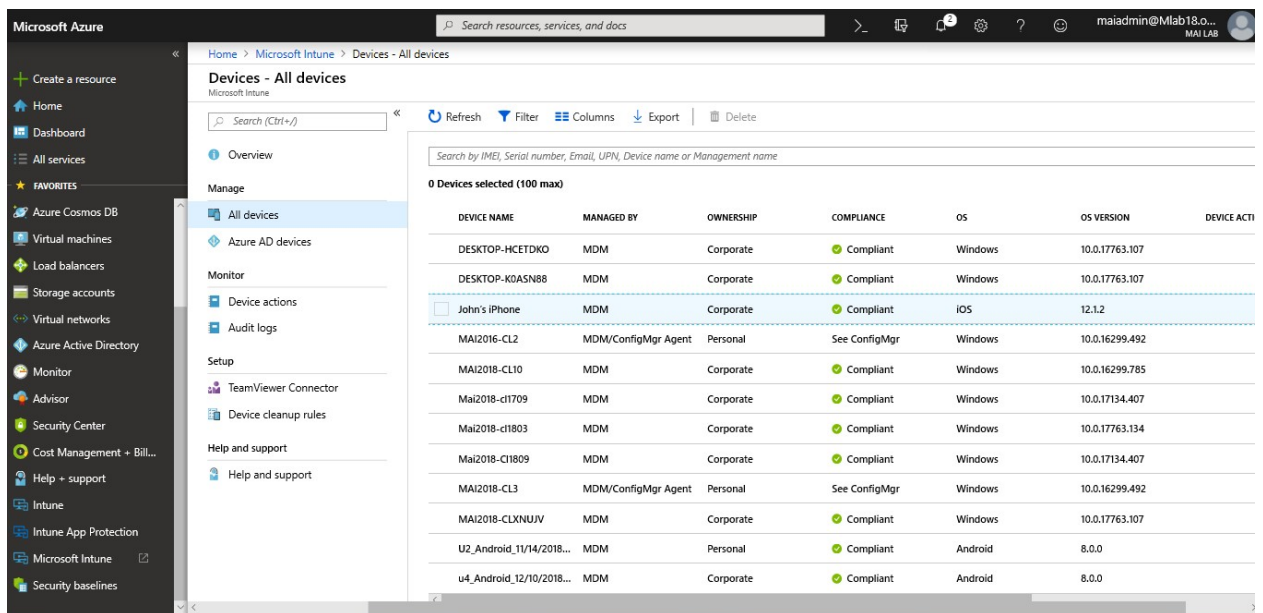
To get the location of a lost or stolen iOS device on a map, use the **Locate device** action. **The device must be in supervised mode.**

Supported platforms for locate lost

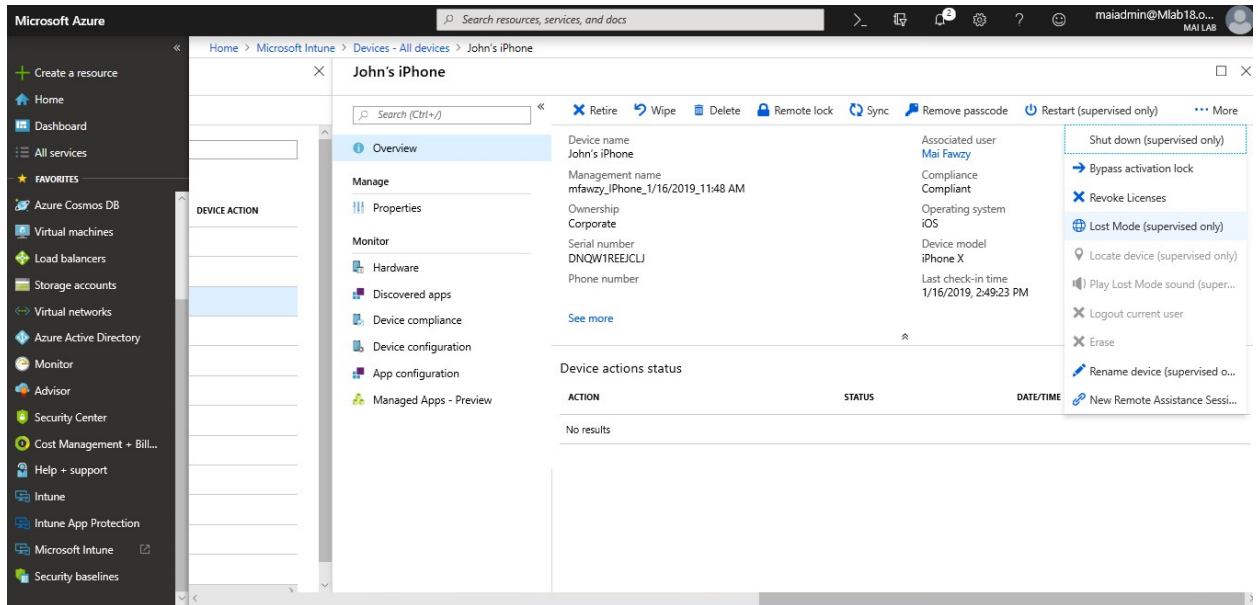
Platform	Supported?
iOS devices 9.3 or later	Yes
Android	No
macOS	No
Windows	No
Windows Phone	No

To Enable lost mode, you need to follow below steps:

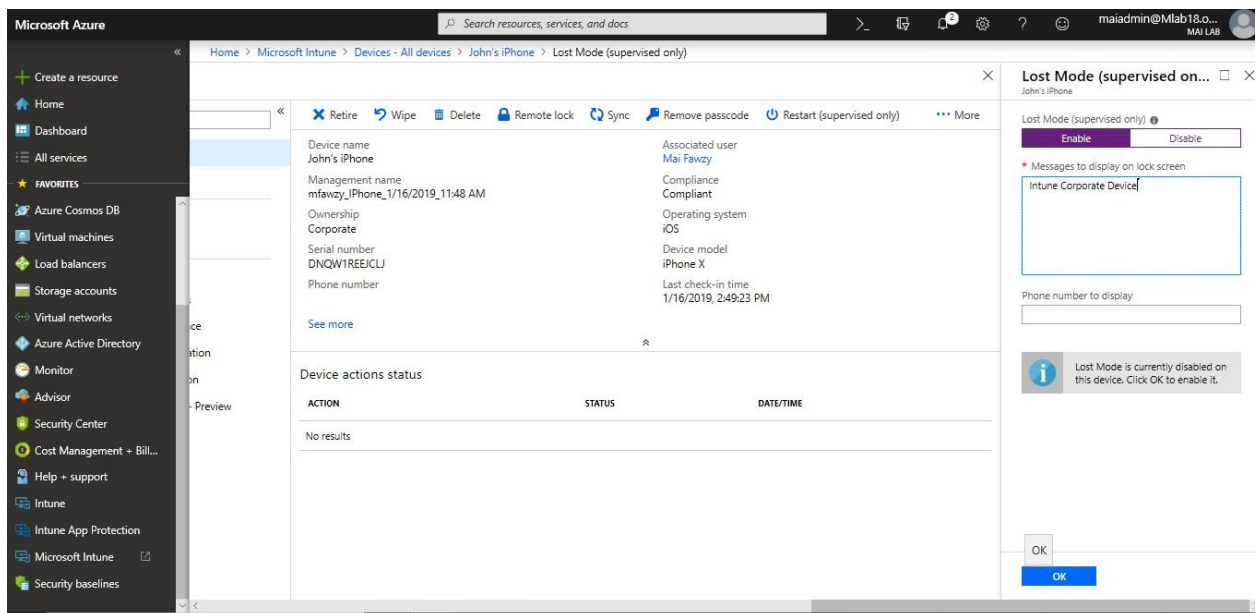
1. Sign in to the [Azure portal](#). Select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Devices**, and then select **All devices**.



3. From the list of devices, you manage, choose an iOS device, and choose **...More**. Then choose the **Lost mode (supervise only)** remote action.



4. In **Lost mode**, enable this feature. Then, enter the message to show, and a contact phone number.



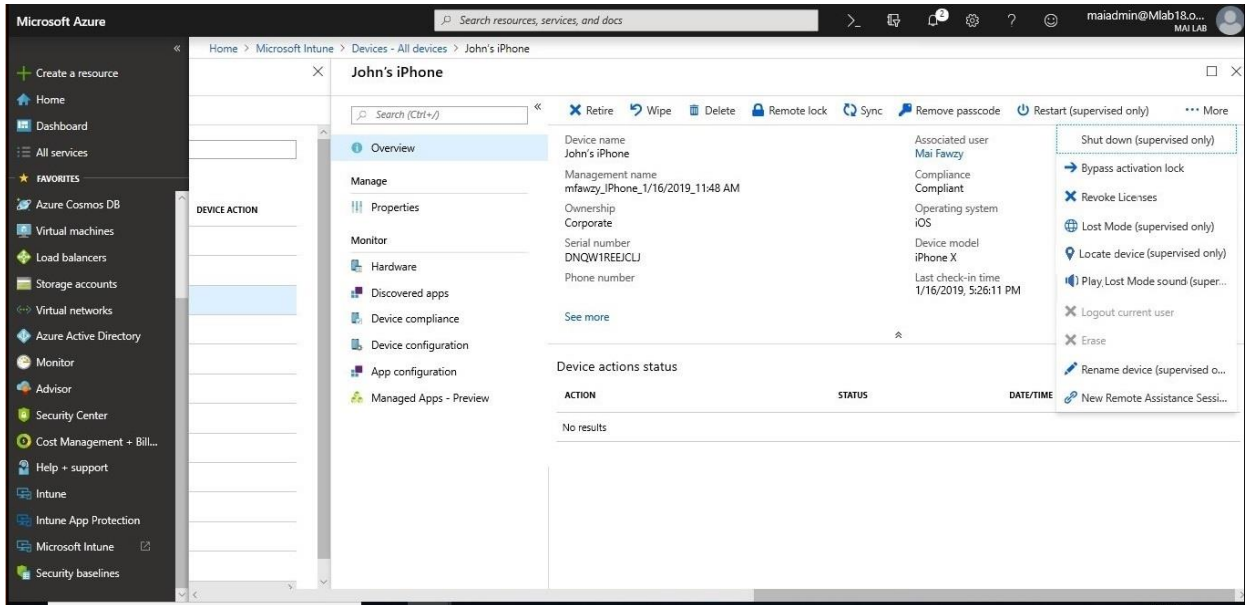
5. Select **OK** to save your changes.

When you enable lost mode, all use of the device is blocked. The end user cannot access the device until you disable lost mode. While lost mode is enabled, use the Locate device action to find the device.

To configure locate a lost or stolen device, you need to follow below steps:

Microsoft Intune step by step on Azure portal

1. Sign in to the [Azure portal](#). Select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Devices**, and then select **All devices**.
3. From the list of devices, you manage, choose an iOS device, and choose **...More**. Then choose the **Locate device** remote action.

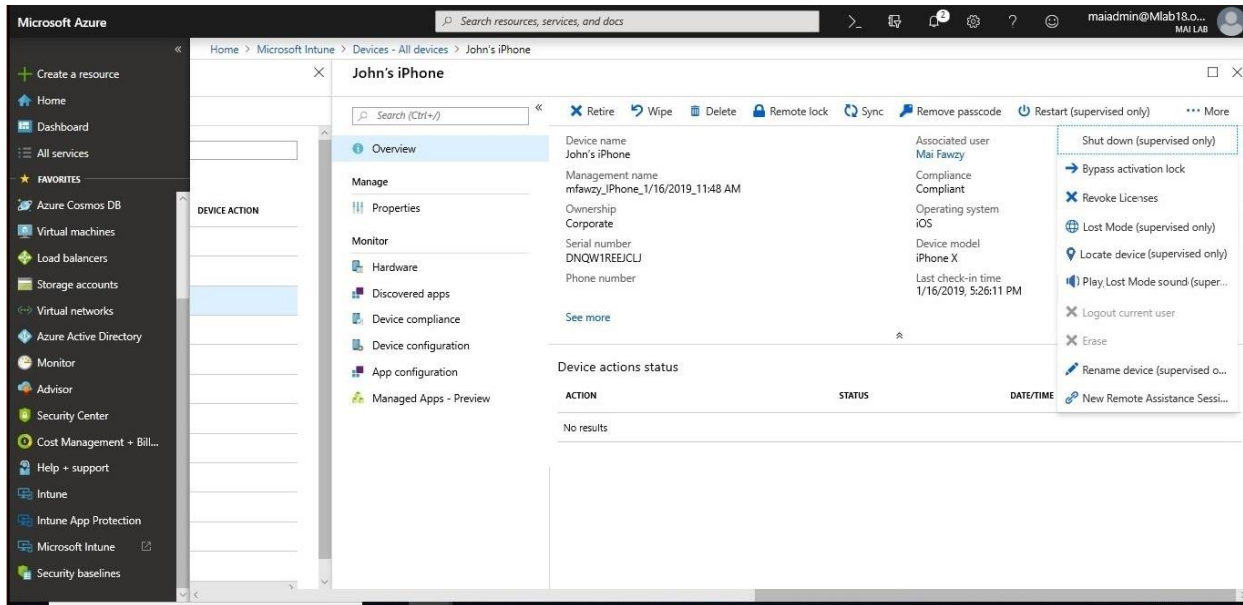


4. After the device is located, its location is shown in **Locate device (supervise only)**.

Activate lost mode sound alert on an iOS device

If someone has lost their iOS 9.3 or later device, you can remotely trigger the device to play an alert sound, so the user can find it. The device must be in lost mode.

In the [Intune in the Azure portal](#), choose **Devices > All devices >** select an iOS device **> Overview > More > Play Lost mode sound (supervise only)**.



The sound will continue to play until the user disables the sound on the device or the device is removed from lost mode.

Security and privacy information for lost mode and locate device actions

- No device location information is sent to Intune until you turn on this action.
- When you use the locate device action, the latitude and longitude coordinates of the device can be retrieved by using the Graph API.
- The data is stored for 24 hours, then removed. You cannot manually remove the location data.
- Location data is encrypted, both while stored and while being transmitted.
- When you configure lost mode, you can customize a message that appears on the lock screen. In this message, to help the person that finds the device, be sure to include specific details to return the lost device.

Bypass Activation Lock on Supervised iOS devices with Intune

Microsoft Intune can help you manage iOS Activation Lock, a feature of the Find My iPhone app for iOS 8.0 and later devices. Activation Lock is enabled automatically when a user opens the Find My iPhone app on a device. After it is enabled, the user's Apple ID and password must be entered before anyone can:

- Turn off Find My iPhone
- Erase the device
- Reactivate the device

Purpose of using Activation Lock

While Activation Lock helps secure iOS devices and improves the chances of recovering a lost or stolen device, this capability can present you, as an IT admin, with a number of challenges. For example:

- A user sets up Activation Lock on a device. The user then leaves the company and returns the device. Without the user's Apple ID and password, there is no way to reactivate the device.
- You need a report of all devices that have Activation Lock enabled.
- You want to reassign some devices to a different department during a device refresh in your organization. You can only reassign devices that do not have Activation Lock enabled.

To help solve these problems, Apple introduced Activation Lock bypass in iOS 7.1. Activation Lock bypass lets you remove the Activation Lock from supervised devices without the user's Apple ID and password. Supervised devices can generate a device-specific Activation Lock bypass code, which is stored on Apple's activation server.

Manage Activation Lock using Microsoft Intune

Intune can request the Activation Lock status of supervised devices that run iOS 8.0 and later. For supervised devices only, Intune can retrieve the Activation Lock bypass code and directly issue it to the device. If the device has been wiped, you can directly access the device by using a blank user name and the code as the password.

The business benefits of using Intune to manage Activation Lock are:

- The user gets the security benefits of the Find My iPhone app.
- You can enable users to do their work and know that when a device needs to be repurposed, you can retire or unlock it.

Configure Activation Lock bypass

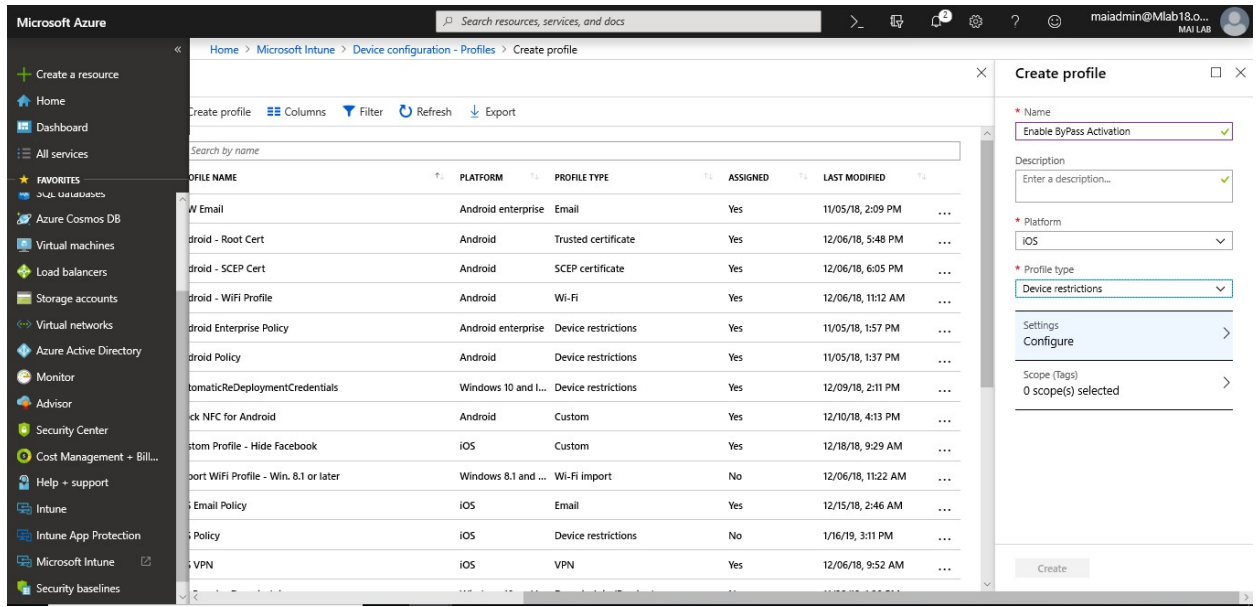
The Intune **Bypass Activation Lock** remote device action removes the Activation Lock from an iOS device without requiring the user's Apple ID and password. After you bypass the Activation Lock, the device turns on Activation Lock again when the Find My iPhone app starts. Bypass the Activation Lock only if you have physical access to the device.

Note: After you bypass the Activation Lock on a device, if the Find My iPhone app is started, a new Activation Lock is automatically applied. Because of this, **you should be in physical possession of the device before you follow this procedure.**

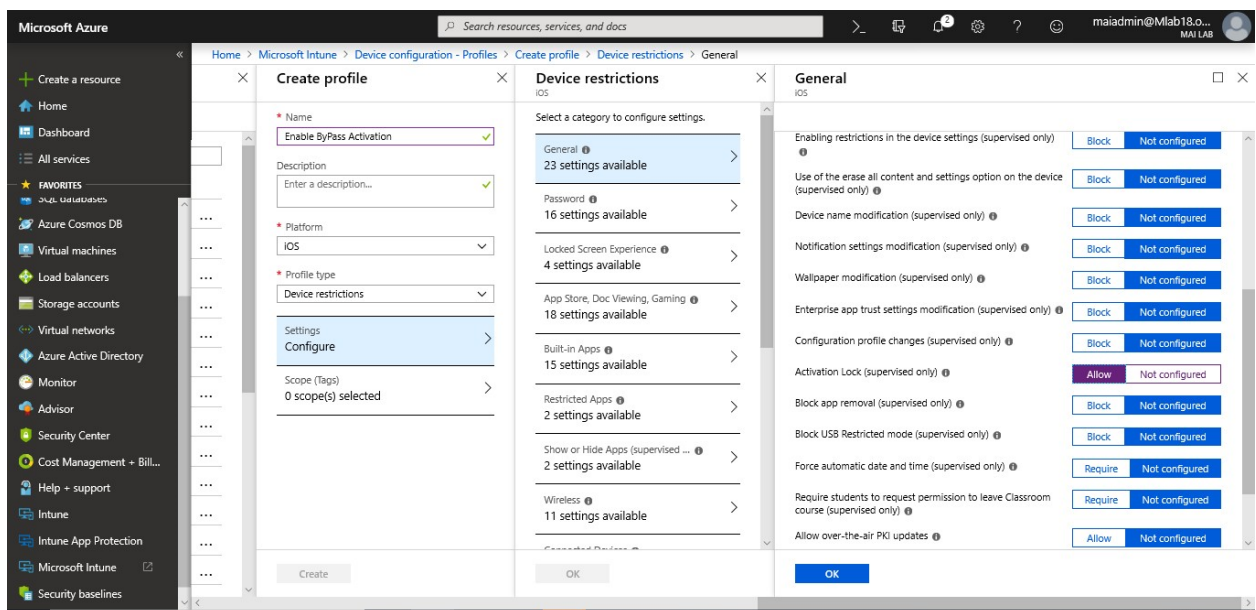
Prerequisites for Activation Lock

Before you can bypass Activation Lock on devices, you must enable it by following these instructions:

1. Configure an Intune device restriction profile for iOS.

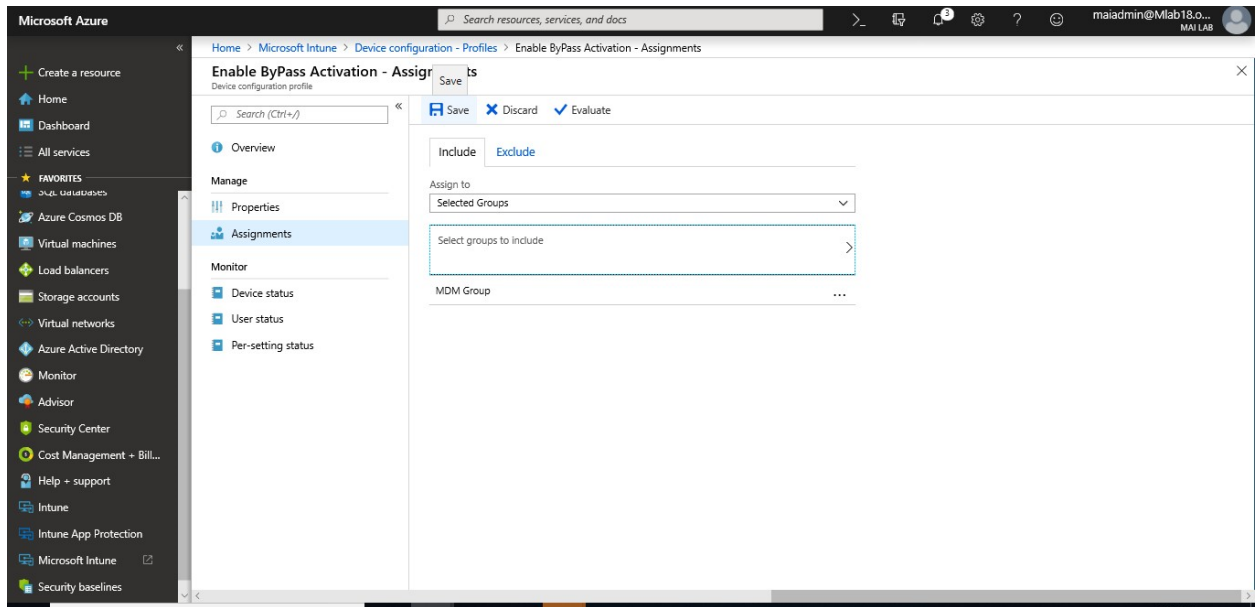


2. In the device restriction settings for iOS, under the **General** settings, enable the option **Activation Lock**.



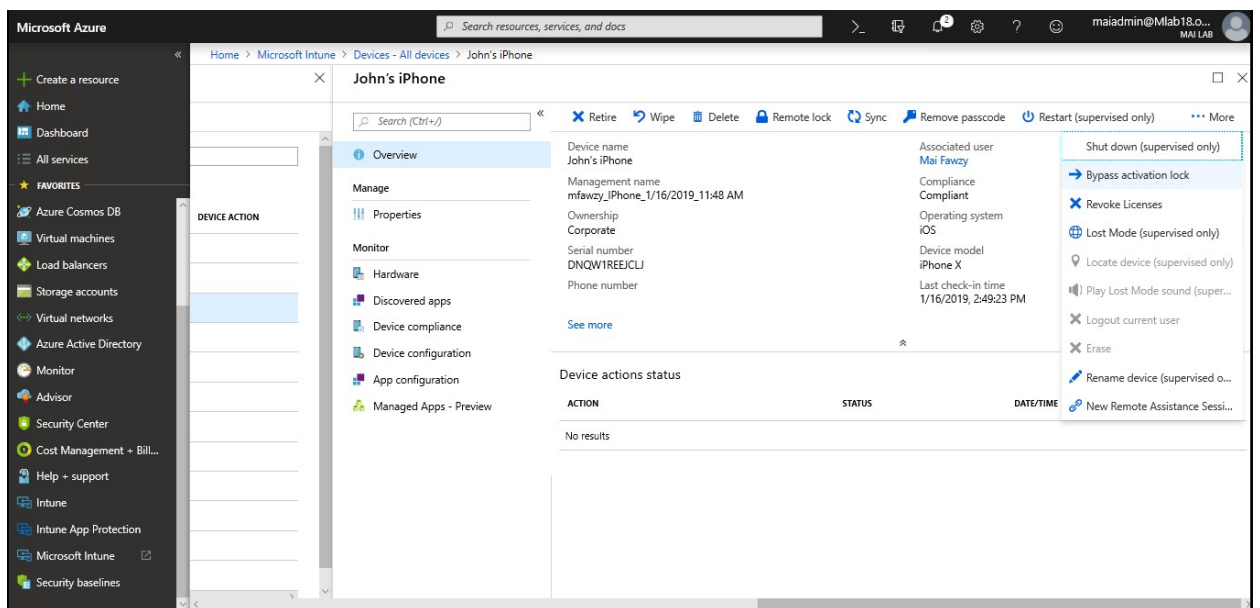
Microsoft Intune step by step on Azure portal

3. Save the profile, and then assign it to the devices on which you want to manage Activation Lock bypass.

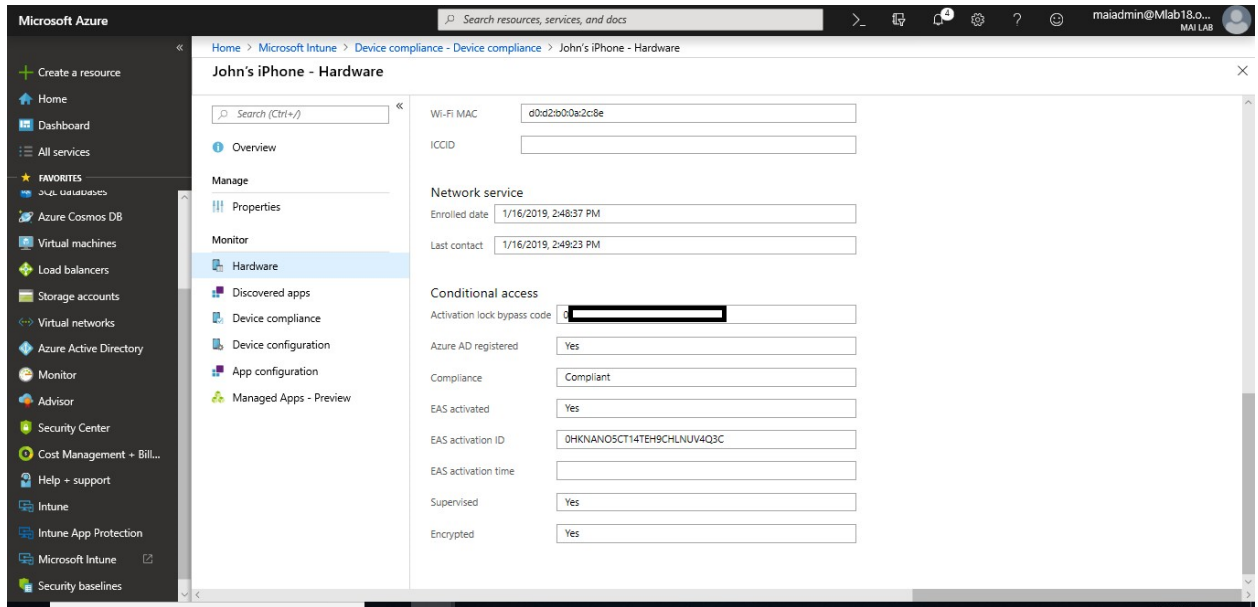


To **Bypass Activation Lock** on iOS device, you need to follow below steps:

1. Sign in to the [Azure portal](#). Select **All services** > **Intune**.
2. On the **Intune** blade, select **Devices** > **All devices**.
3. On the list of devices that you manage, select the **Bypass Activation Lock** device remote action.



4. Go to the device's "Hardware" section, and then copy the **Activation Lock bypass code** value under **Conditional Access**.



Note: Copy the bypass code before you wipe the device. If you reset the device settings before you copy the code, the code is removed from Azure.

5. Go to the **Overview** blade for the device, and then select **Wipe**.
6. After the device is reset, you are prompted for the *Apple ID* and *password*. Leave the *ID* field blank, and then enter the **bypass code** for the *password*. This removes the account from the device.

Retire Devices and Remove Data

When a device needs to be removed from Intune management (for example, a user leaves, or the device is lost or stolen), it's likely that you'll want to remove data from that device. Intune provides a range of methods to make sure your company data stays secure.

Note: In case end user remove company portal from his mobile phone, all corporate Apps will be wiped.

Wipe

The **Wipe** action restores a device to its factory default settings. The user data is kept if you choose the **Retain enrollment state and user account** checkbox. Otherwise, the drive is securely erased.

Wipe action	Retain enrollment state and user account	Removed from Intune management	Description
Wipe	Not checked	Yes	Wipes all user accounts, data, MDM policies, and settings. Resets the operating system to its default state and settings.

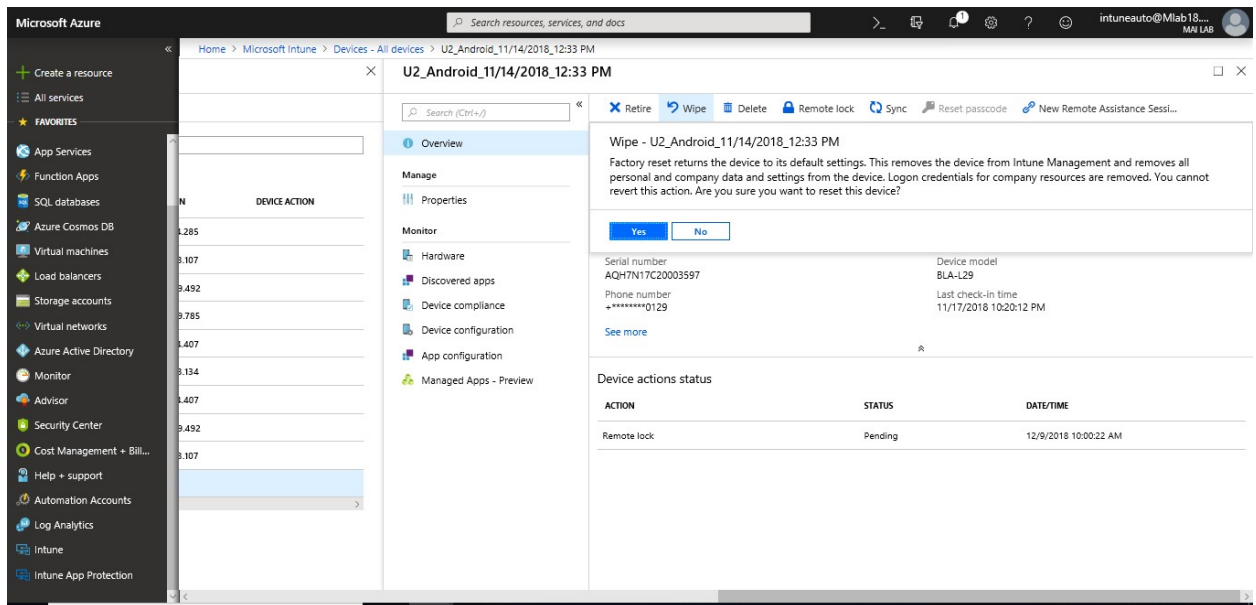
Wipe action	Retain enrollment state and user account	Removed from Intune management	Description
Wipe	Checked	No	Wipes all MDM Policies. Keeps user accounts and data. Resets user settings back to default. Resets the operating system to its default state and settings.

The **Retain enrollment state and user account** option is only available for Windows 10 version 1709 or later. MDM policies will be reapplied the next time the device connects to Intune.

A wipe is useful for resetting a device before you give the device to a new user, or when the device has been lost or stolen. Be careful about selecting **Wipe**. Data on the device cannot be recovered.

To Wipe a device, you need to follow below steps:

1. Sign in to the [Azure portal](#). Select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Devices** > **All devices**.
3. Select the name of the device that you want to wipe.
4. In the pane that shows the device name, select **Wipe**.
5. To confirm the wipe, select **Yes**.



If the device is on and connected, the **Wipe** action propagates across all device types in less than 15 minutes.

Retire

The **Retire** action removes managed app data (where applicable), settings, and email profiles that were assigned by using Intune. The device is removed from Intune management. This happens the next time the device checks in and receives the remote **Retire** action.

Retire leaves the user's personal data on the device.

The following tables describe what data is removed, and the effect of the **Retire** action on data that remains on the device after company data is removed.

iOS

Data type	iOS
Company apps and associated data installed by Intune	Apps are uninstalled. Company app data is removed. App data from Microsoft apps that use mobile app management is removed. The app is not removed.
Settings	Configurations that were set by Intune policy are no longer enforced. Users can change the settings.
Wi-Fi and VPN profile settings	Removed.
Certificate profile settings	Certificates are removed and revoked.
Management agent	The management profile is removed.
Email	Email profiles that are provisioned through Intune are removed. Cached email on the device is deleted.
Outlook	Email that's received by the Microsoft Outlook app for iOS is removed. This requires that the Outlook mobile app be deployed as a Required app to iOS users first.
Azure AD unjoin	The Azure AD record is removed.
Contacts	Contacts that are synced directly from the app to the native address book are removed. Any contacts that are synced from the native address book to another external source can't be removed. Currently, only the Outlook app is supported.

Android

Data type	Android	Android Samsung Knox Standard
Web links	Removed.	Removed.
Unmanaged Google Play apps	Apps and data remain installed.	Apps and data remain installed.

Data type	Android	Android Samsung Knox Standard
Unmanaged line-of-business apps	Apps and data remain installed.	Apps are uninstalled and data that's local to the app is removed. No data that's outside the app (for example, on an SD card) is removed.
Managed Google Play apps	App data is removed. The app isn't removed. Data that's protected by Mobile Application Management (MAM) encryption outside the app (for example, an SD card) remains encrypted and unusable, but isn't removed.	App data is removed. The app isn't removed. Data that's protected by MAM encryption outside the app (for example, an SD card) remains encrypted, but isn't removed.
Managed line-of-business apps	App data is removed. The app isn't removed. Data that's protected by MAM encryption outside the app (for example, an SD card) remains encrypted and unusable, but isn't removed.	App data is removed. The app isn't removed. Data that's protected by MAM encryption outside the app (for example, an SD card) remains encrypted and unusable, but isn't removed.
Settings	Configurations that were set by Intune policy are no longer enforced. Users can change the settings.	Configurations that were set by Intune policy are no longer enforced. Users can change the settings.
Wi-Fi and VPN profile settings	Removed.	Removed.
Certificate profile settings	Certificates are revoked but not removed.	Certificates are removed and revoked.
Management agent	Device Administrator privilege is revoked.	Device Administrator privilege is revoked.
Email	N/A (Email profiles aren't supported by Android devices)	Email profiles that are provisioned through Intune are removed. Cached email on the device is deleted.
Outlook	Email that's received by the Outlook app for Android is removed, but only if Outlook is protected by MAM policies. Otherwise, Outlook isn't wiped when the device is unenrolled.	Email that's received by the Outlook app for Android is removed, but only if Outlook is protected by MAM policies. Otherwise, Outlook isn't wiped when the device is unenrolled.
Azure AD unjoin	The Azure AD record is removed.	The Azure AD record is removed.
Contacts	<p>Contacts that are synced directly from the app to the native address book are removed. Any contacts that are synced from the native address book to another external source can't be removed.</p> <p>Currently, only the Outlook app is supported.</p>	<p>Contacts that are synced directly from the app to the native address book are removed. Any contacts that are synced from the native address book to another external source can't be removed.</p> <p>Currently, only the Outlook app is supported.</p>

Android Work Profile

Removing company data from an Android work profile device removes all data, apps, and settings in the work profile on that device. The device is retired from management with Intune. Wipe is not supported for Android work profiles.

Android Enterprise Kiosk Devices

You can only wipe kiosk devices. You can't retire Android kiosk devices.

MacOS

Data type	macOS
Settings	Configurations that were set by Intune policy are no longer enforced. Users can change the settings.
Wi-Fi and VPN profile settings	Removed.
Certificate profile settings	Certificates that were deployed through MDM are removed and revoked.
Management agent	The management profile is removed.
Outlook	If conditional access is enabled, the device doesn't receive new mail.
Azure AD unjoin	The Azure AD record is removed.

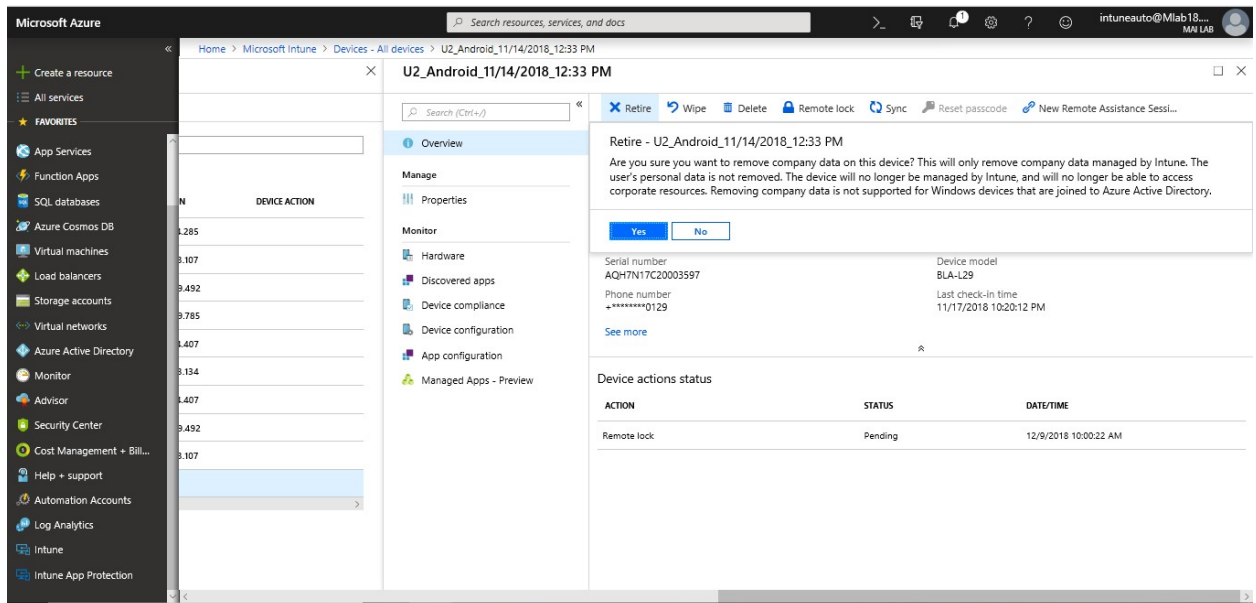
Windows

Data type	Windows 8.1 (MDM) and Windows RT 8.1	Windows RT	Windows Phone 8.1 and Windows Phone 8	Windows 10
Company apps and associated data installed by Intune	Keys are revoked for files that are protected by EFS. The user can't open the files.	Company apps aren't removed.	Apps originally installed through the Company Portal are uninstalled. Company app data is removed.	Apps are uninstalled. Sideloading keys are removed. For Windows 10 version 1703 (Creators Update) and later, Office 365 ProPlus apps aren't removed.
Settings	Configurations that were set by Intune policy are no longer enforced. Users can change the settings.	Configurations that were set by Intune policy are no longer enforced. Users can change the settings.	Configurations that were set by Intune policy are no longer enforced. Users can change the settings.	Configurations that were set by Intune policy are no longer enforced. Users can change the settings.
Wi-Fi and VPN profile settings	Removed.	Removed.	Not supported.	Removed.

Data type	Windows 8.1 (MDM) and Windows RT 8.1	Windows RT	Windows Phone 8.1 and Windows Phone 8	Windows 10
Certificate profile settings	Certificates are removed and revoked.	Certificates are removed and revoked.	Not supported.	Certificates are removed and revoked.
Email	Removes email that's EFS-enabled. This includes emails and attachments in the Mail app for Windows.	Not supported.	Email profiles that are provisioned through Intune are removed. Cached email on the device is deleted.	Removes email that's EFS-enabled. This includes emails and attachments in the Mail app for Windows. Removes mail accounts that were provisioned by Intune.
Azure AD unjoin	No.	No.	The Azure AD record is removed.	Not applicable. On Windows 10, you can't retire Azure AD-joined devices.

To retire Mobile device, you can follow below steps:

1. Sign in to the [Intune in the Azure portal](#). In the **Devices** pane, select **All devices**.
2. Select the name of the device that you want to retire.
3. In the pane that shows the device name, select **Retire**. To confirm, select **Yes**.

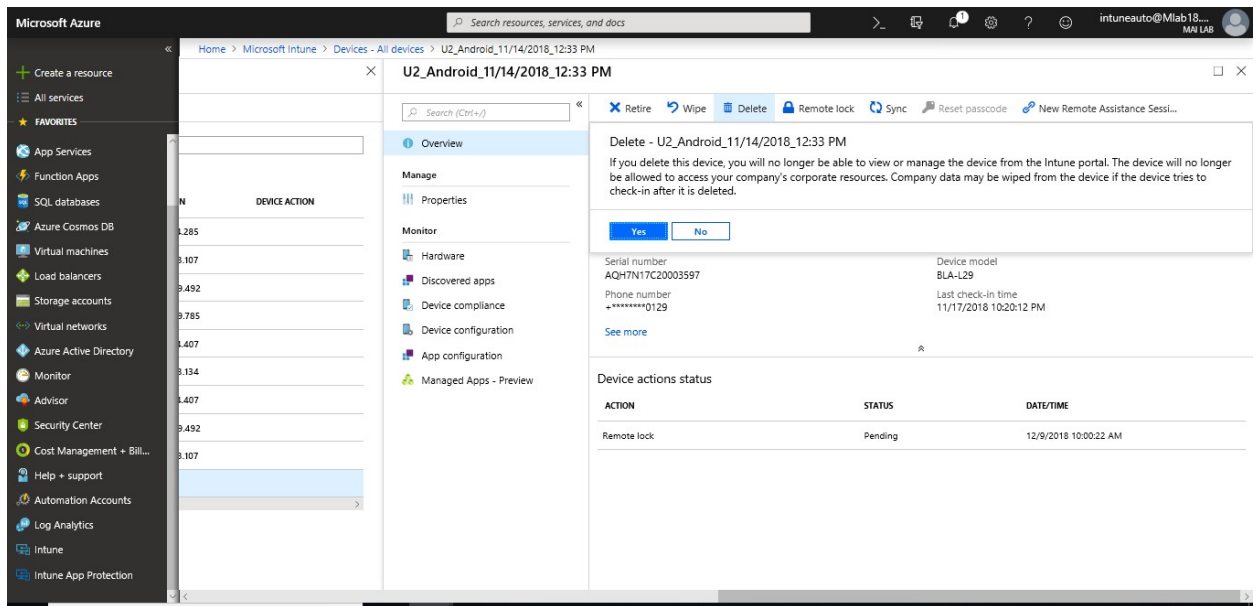


If the device is on and connected, the **Retire** action propagates across all device types in less than 15 minutes.

Delete Devices from the Intune portal

If you want to remove devices from the Intune portal, you can delete them from the specific device pane. The next time the device checks in, any company data on it will be removed.

1. Sign in to [Intune in the Azure portal](#).
2. Choose **Devices** > **All devices** > choose the devices you want to delete > **Delete**.
3. Click **Yes** to confirm.

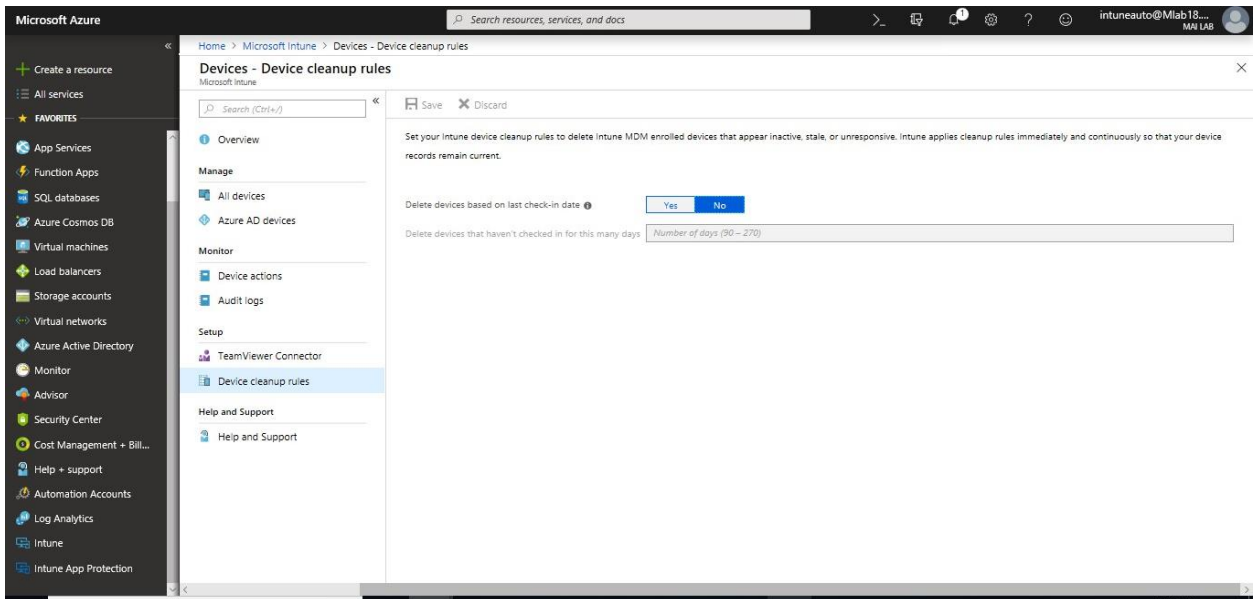


Automatically delete devices with cleanup rules

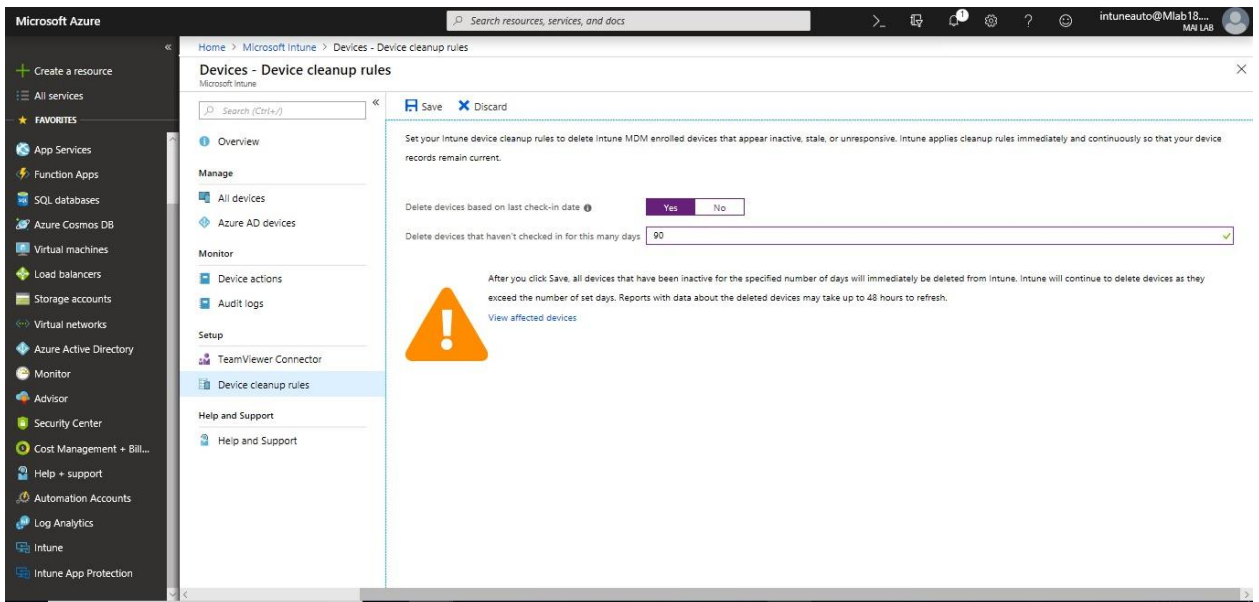
You can configure Intune to automatically delete devices that appear to be inactive, stale, or unresponsive. These cleanup rules continuously monitor your device inventory so that your device records stay current. Devices deleted in this way are removed from Intune management.

1. Sign in to the [Intune in the Azure portal](#). Choose **Devices** > **Device cleanup rules** > **Yes**.

Microsoft Intune step by step on Azure portal



2. In the **Delete devices that haven't checked in for this many day's** box, enter a number between 90 and 270.



3. Choose **Save**.

Chapter 6

Deploy Applications Using Microsoft Intune

Intune offers a range of capabilities to help you get the apps you need on the devices you want to run them on. After you've added an app to Microsoft Intune, you can assign the app to users and devices. It is important to note that you can assign an app to a device whether or not the device is managed by Intune.

Note: The Available deployment intent is not supported for device groups, **only user groups are supported.**

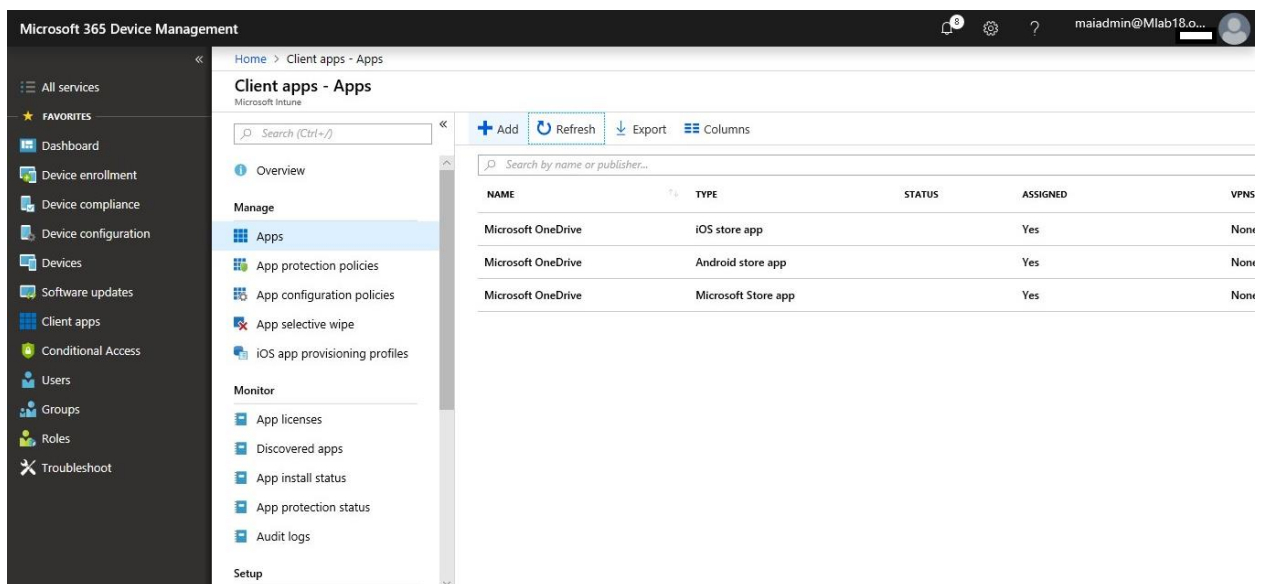
Deploy Apps “Office ProPlus” to Windows 10 MDM using Intune

Configure Office ProPlus App

In this procedure, you'll deploy Office ProPlus on windows 10 which is managed by Intune.

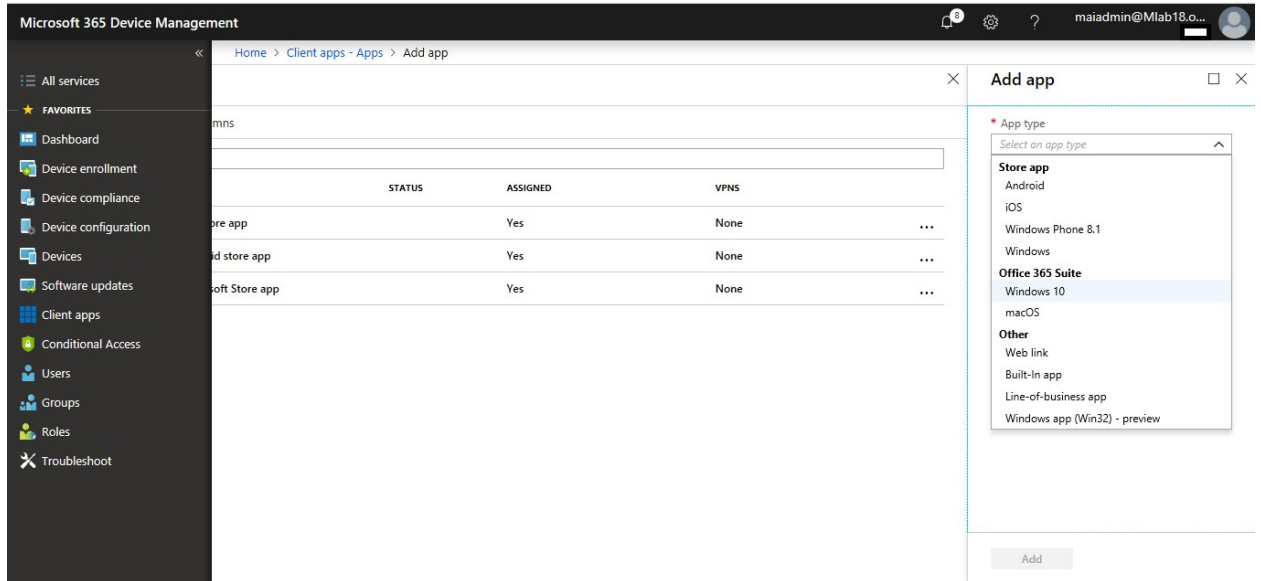
To configure Office ProPlus App

1. Sign into the [Azure portal](#) and navigate to >Intune> **Client apps** >**Apps**, Click **Add**.

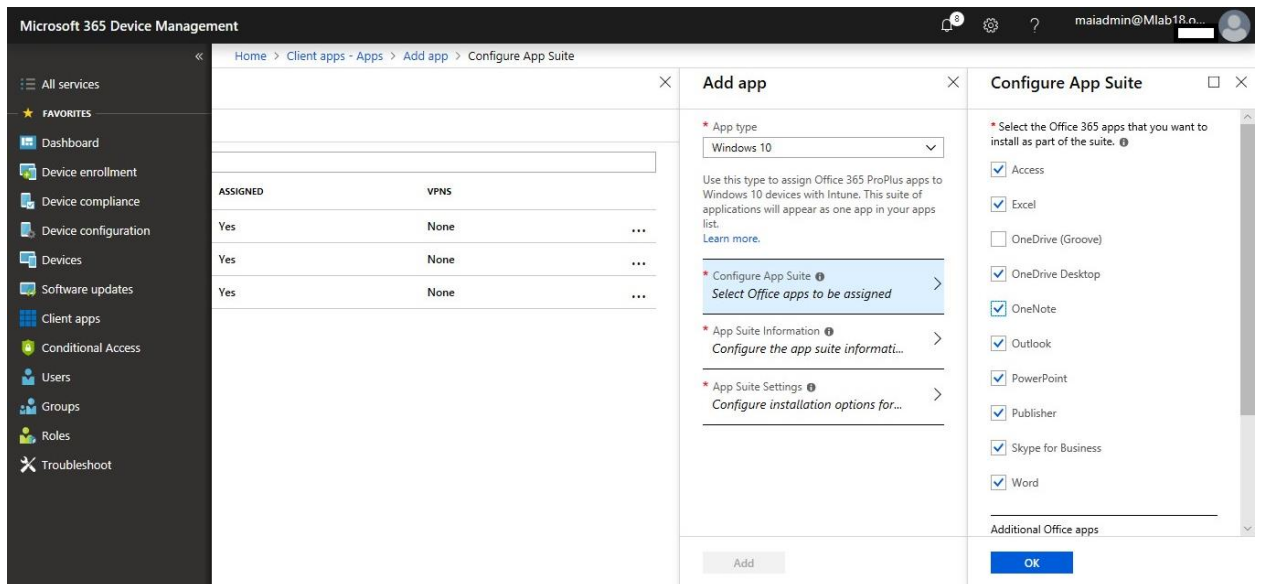


2. On the **Add App** blade, choose Office 365 Suite (Windows 10)

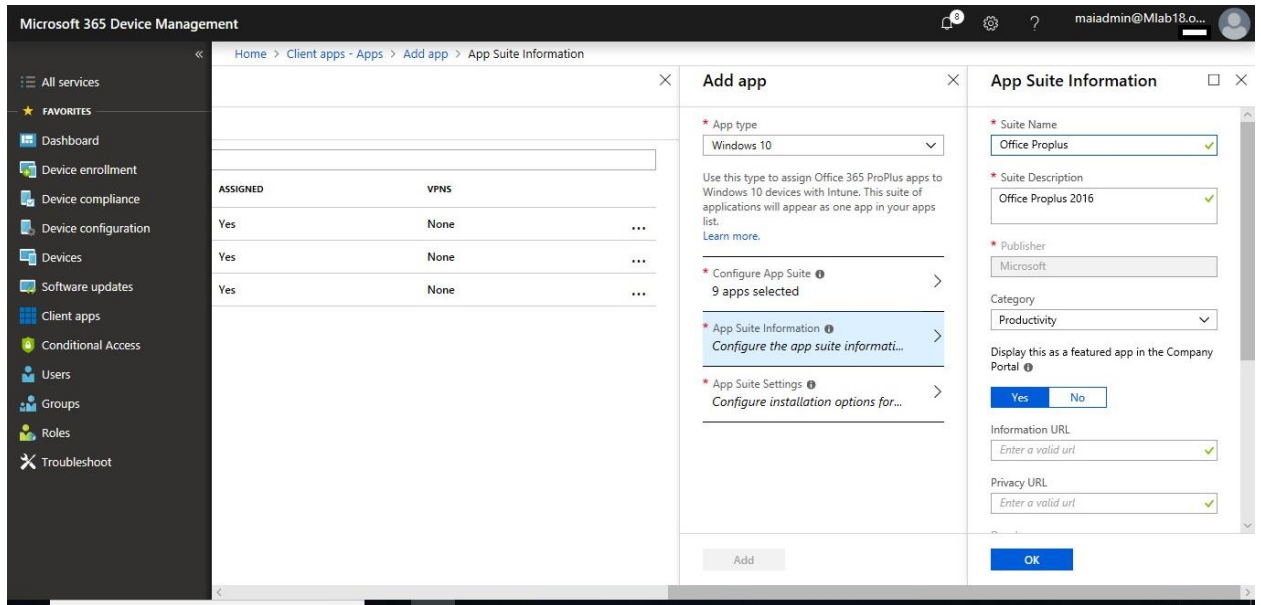
Microsoft Intune step by step on Azure portal



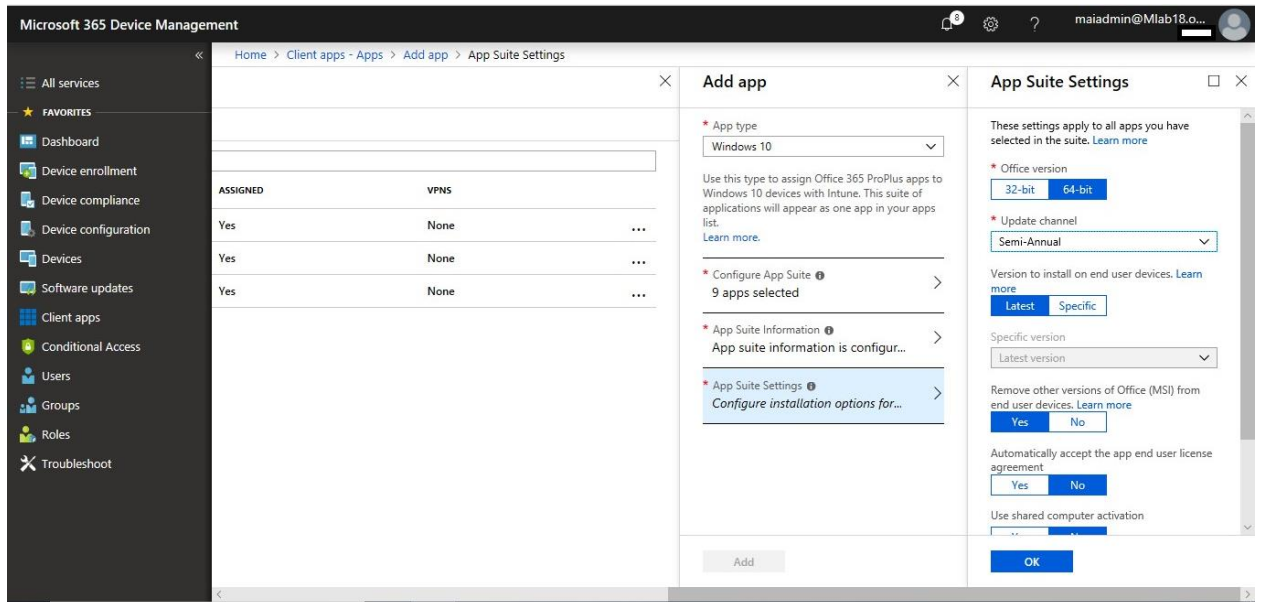
3. On the **Configure App Suite**, select all office apps that you want.



4. On the **App Suite Information**, Type **Suite Name**, **Description** & select yes to show in featured app on company portal, then click **Ok**.



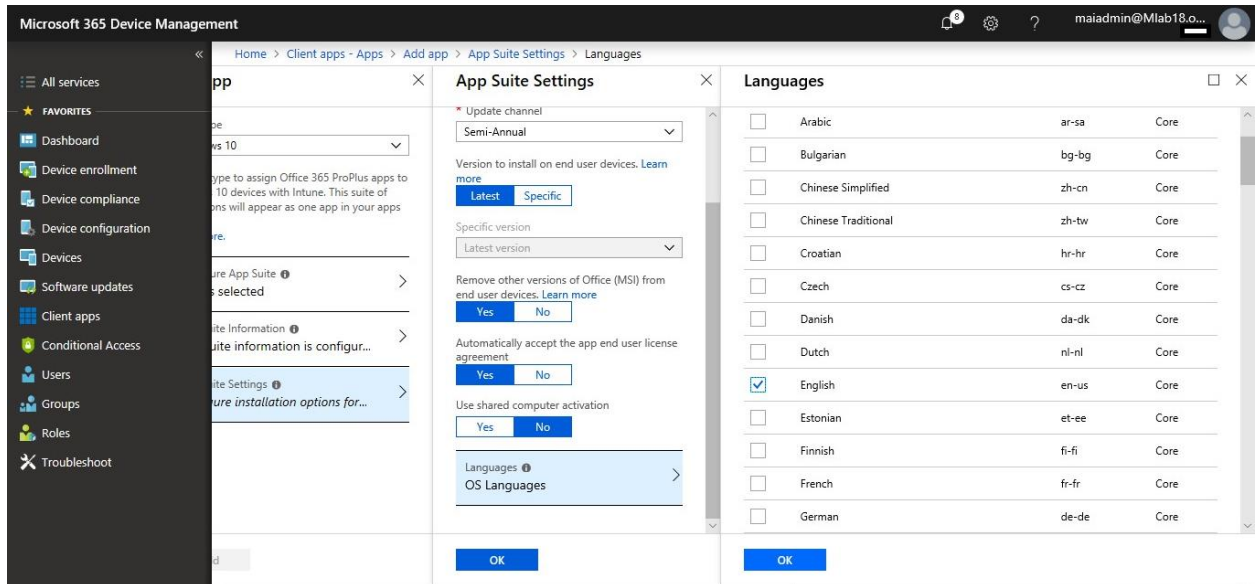
5. On the **App Suite Settings**, Select **Office Version** “64bit”, **Update Channel** “Semi-Annual”, Select **Remove other Office msi** “Yes”, Select **Automatically accept the app** “Yes”



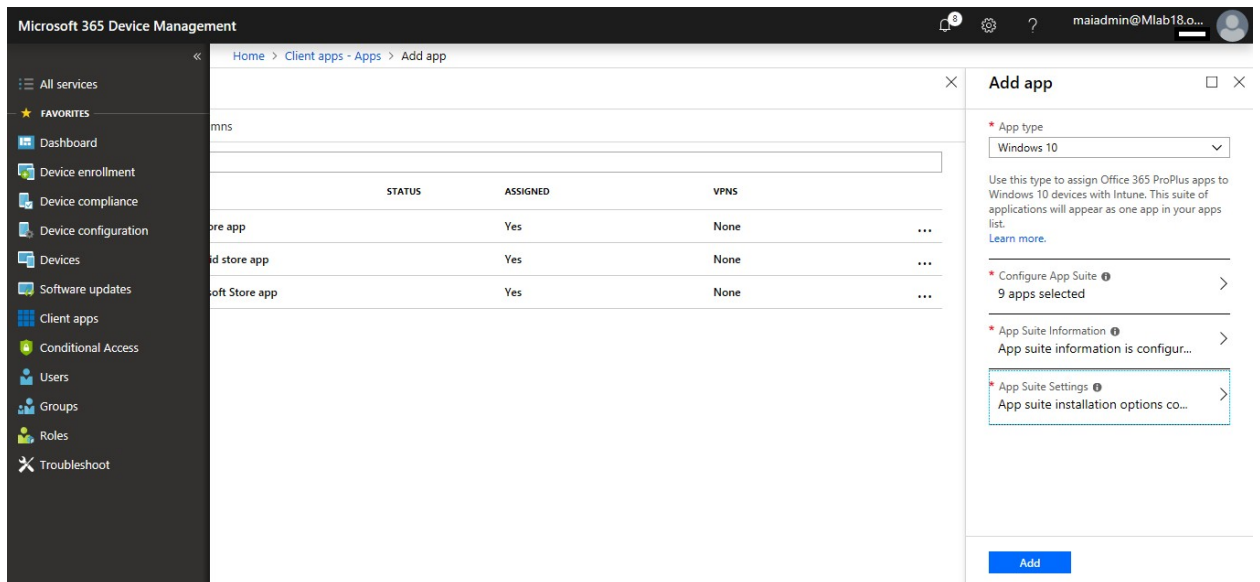
Note: If there are .msi Office apps on the end-user device, you must use the **Remove MSI** feature to safely uninstall these apps. Otherwise, the Intune delivered Office 365 apps will fail to install. You must use Office 365 ProPlus licenses to activate Office 365 ProPlus apps deployed through Microsoft Intune. Currently, **Office 365 Business edition is not supported by Intune.**

6. **Language** Select “English” then click **Ok**

Microsoft Intune step by step on Azure portal



7. Click Add.



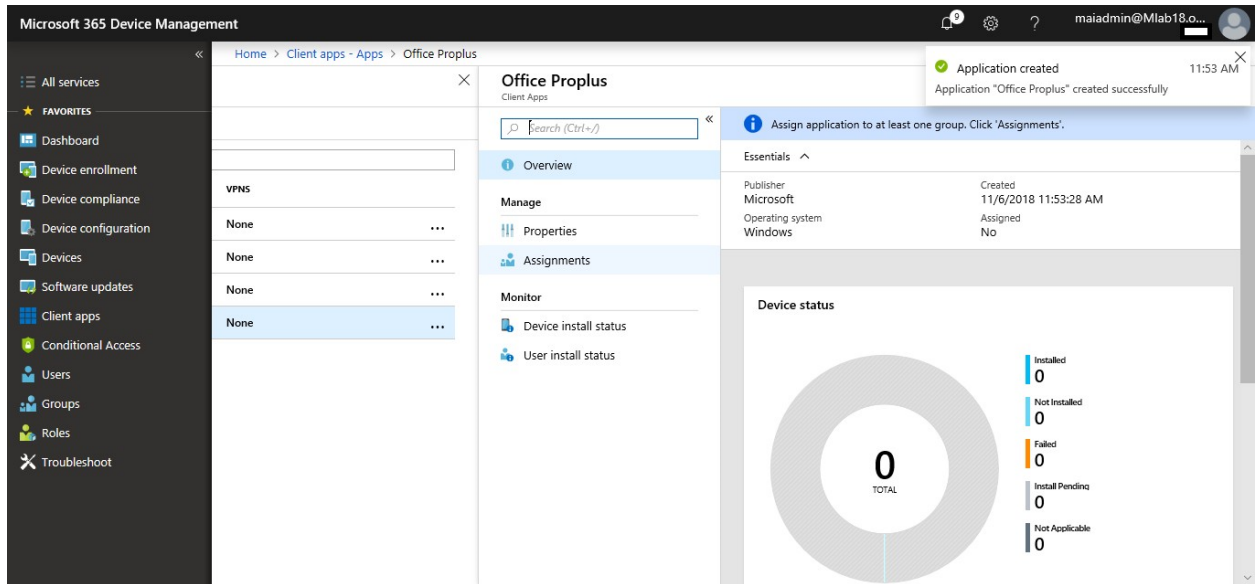
Assign the App

In this procedure, you'll deploy the app to specific group.

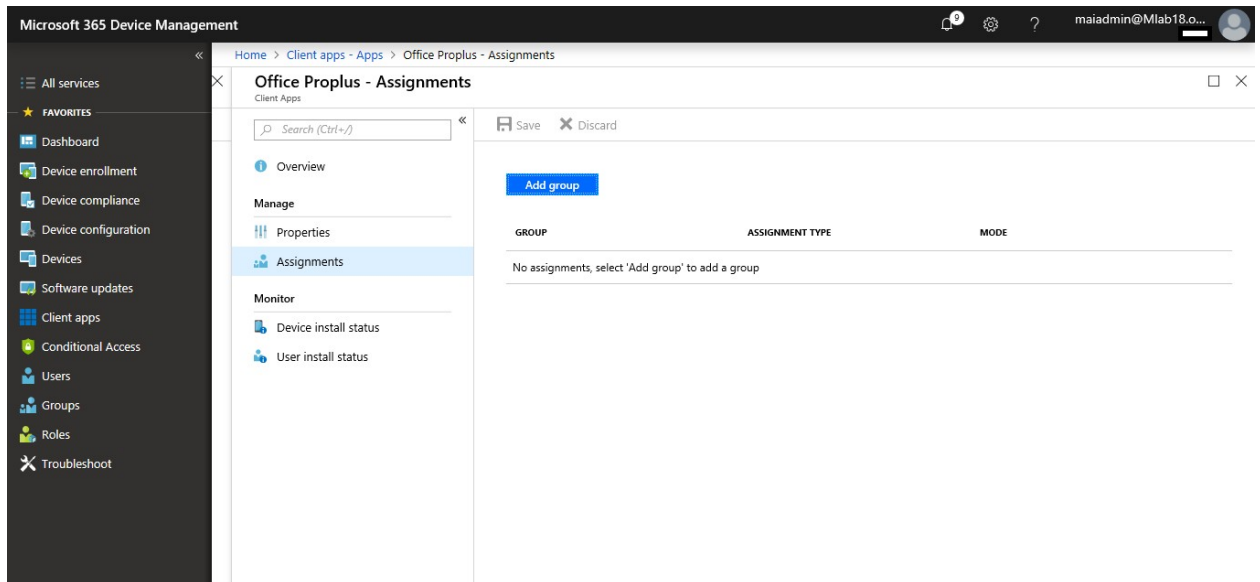
To Assign the App, you can follow below steps:

1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** menu, select **Client apps**. In the **Manage** section of the menu, select **Apps**.
3. In the **Apps** pane, select the app you want to assign.

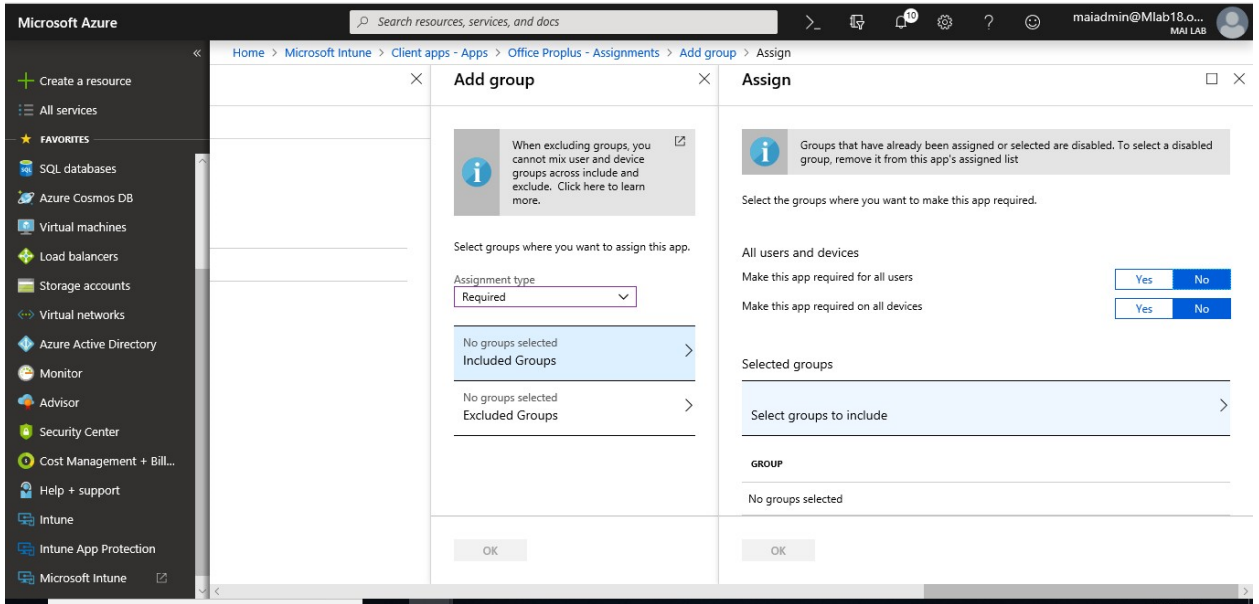
Microsoft Intune step by step on Azure portal



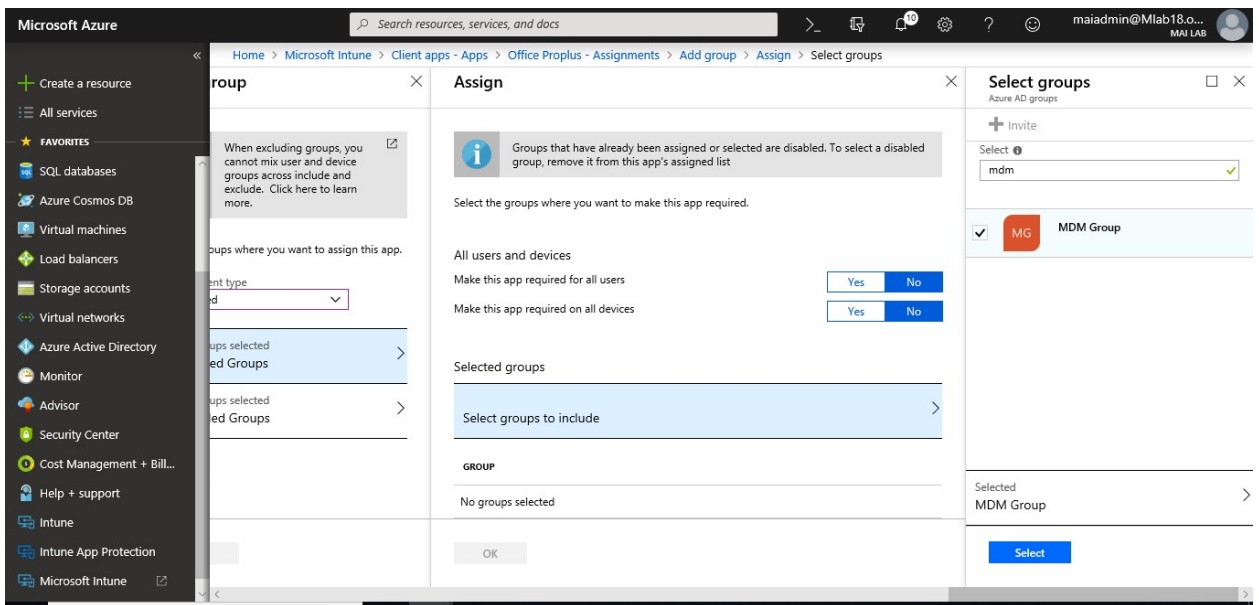
4. In the **Manage** section of the menu, select **Assignments**.
5. Select **Add Group** to open the **Add group** pane that is related to the app.



6. For the specific app, select an **assignment type**: Required if you want it as silent deployment. Or available for enrolled device to be available it on company portal & end user can install it if he wants.
7. To select the groups of users that are affected by this app assignment, select **Included Groups**.

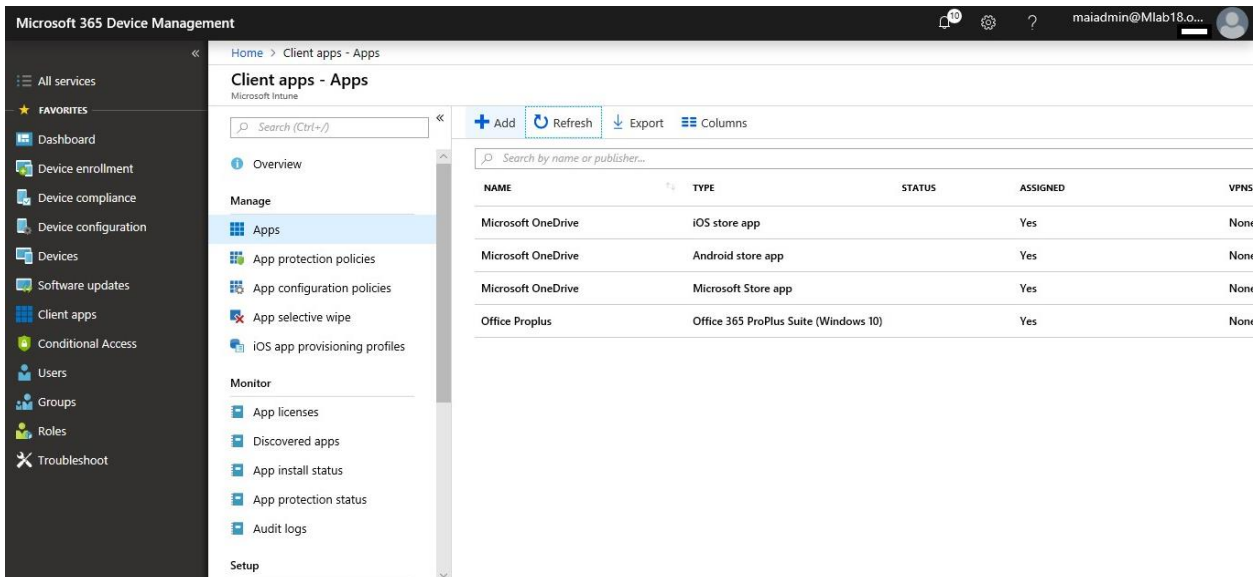
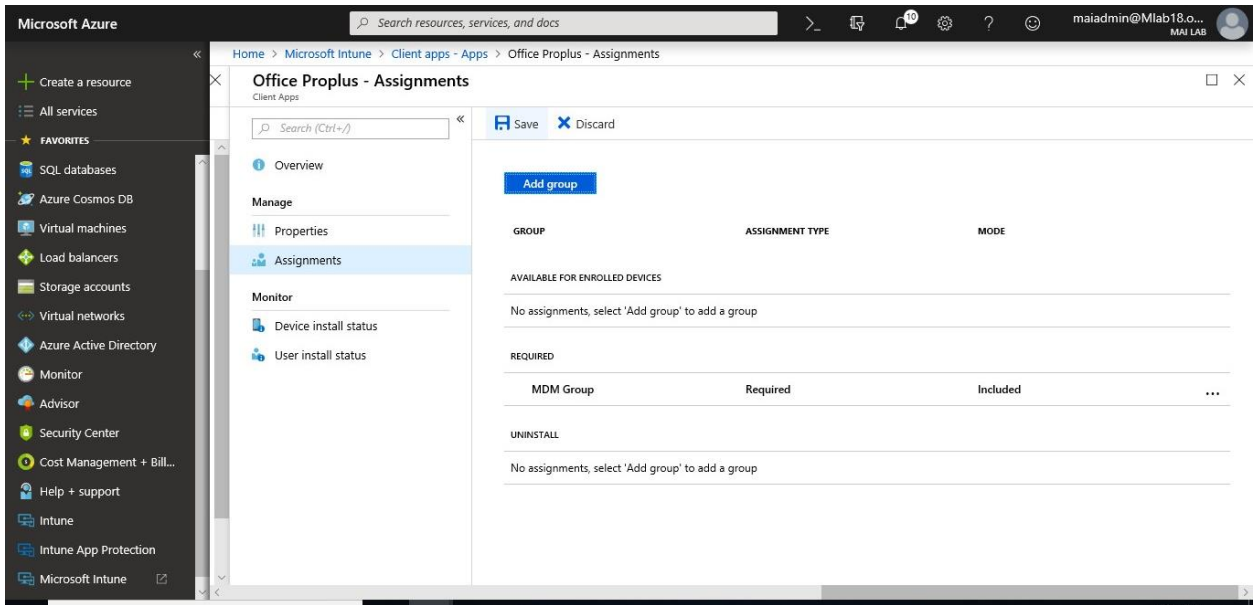


8. In the **Assign** pane, select **OK** to complete the included groups selection.



9. If you want to exclude any groups of users from being affected by this app assignment, select **Exclude Groups**. If you have chosen to exclude any groups, in **Select groups**, select group that you want to exclude it. In the **Add group** pane, select **OK**.
10. In the app **Assignments** pane, select **Save**.

Microsoft Intune step by step on Azure portal



Monitor the App

You can see the apps you manage, and their deployment status in the Intune console.

To view the Apps, you manage and their status

1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** menu, select **Client apps**.
3. In the **Manage** section of the menu, select **Apps**.
4. In the list of apps, select an app to monitor. You'll then see the app pane, which includes an overview of the device status and the user status.

Microsoft Intune step by step on Azure portal

Microsoft Azure portal showing the configuration page for Office ProPlus. The page displays a donut chart for device status:

Category	Count
Installed	2
Not Installed	0
Failed	1
Install Pending	0
Not Applicable	1
TOTAL	4

Microsoft Azure portal showing the Managed Apps - Preview page for Mai2018-CI1809. The page displays a table of installed applications:

APPLICATION	RESOLVED INTENT	INSTALLATION STATUS
Microsoft Teams Desktop	Available	Available for install
Adobe Reader 11.0	Available	Available for install
Skype for Business	Available	Available for install
7Zip (x64)	Available	Available for install
Microsoft Excel	Available	Available for install
Intune Company Portal	Available	Available for install
Microsoft OneDrive	Available	Available for install
Office ProPlus	Required install	Installed

5. On Client machine, you should find Office ProPlus installed.

Windows search interface showing the results for the search term 'word'. The results include:

- Best match: Word (Desktop app)
- Apps: WordPad
- Settings: Highlight misspelled words, Choose if Narrator reads typed words, Autocorrect misspelled words
- Search suggestions: word - See web results

Deploy Apps to Mobile Devices Using Microsoft Intune

Intune supports a wide range of app types. The available options differ for each app type. Intune lets you add and assign the following app types:

App types	Installation	Updates
Apps from the store (store apps)	Intune installs the app on the device.	App updates are automatic.
Apps on the web (web link)	Intune creates a shortcut to the web app on the device home screen.	App updates are automatic.
Apps that are built-in (built-in apps)	Intune installs the app on the device.	App updates are automatic.
Apps written in-house (line-of-business)	Intune installs the app on the device (you supply the installation file).	You must update the app.

You can deploy app on Mobile devices using 4 deployment types:

- [Deploy Store Apps.](#)
- [Deploy Web App.](#)
- [Deploy Built-in App.](#)
- [Deploy Line of Business App.](#)

After you've added an app to Microsoft Intune, you can assign the app to users and devices. The following table lists the various options for assigning apps to users and devices:

Features	Devices enrolled with Intune	Devices not enrolled with Intune
Assign to users	Yes	Yes
Assign to devices	Yes	No
Assign wrapped apps or apps that incorporate the Intune SDK (for app protection policies)	Yes	Yes
Assign apps as Available	Yes	Yes
Assign apps as Required	Yes	No
Uninstall apps	Yes	No
Receive app updates from Intune	Yes	No
End users install available apps from the Company Portal app	Yes	No
End users install available apps from the web-based Company Portal	Yes	Yes

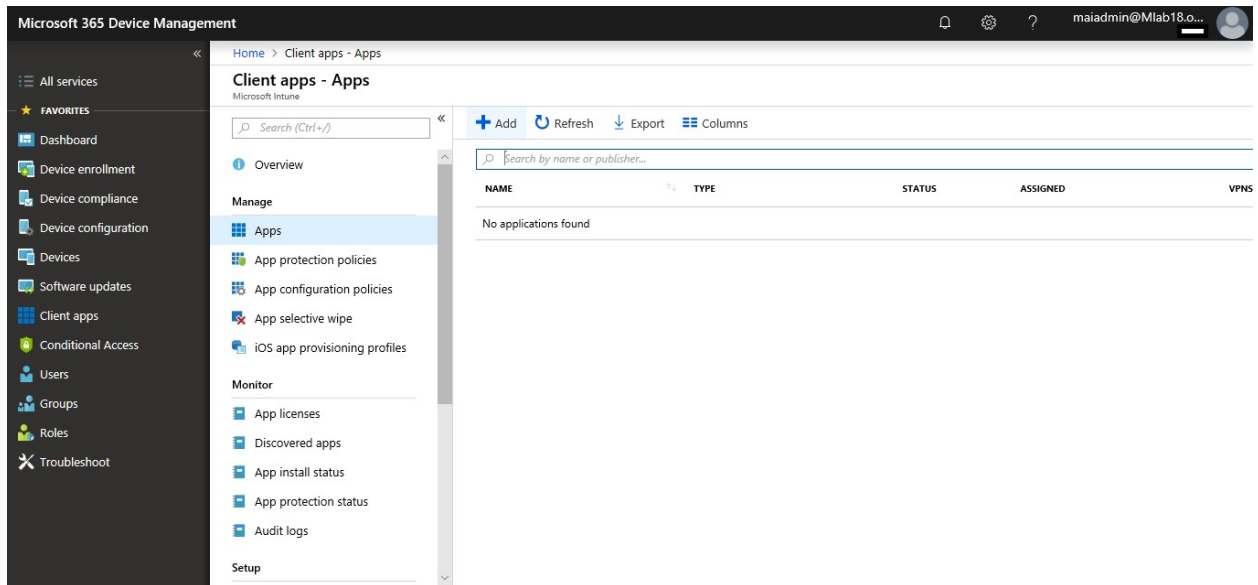
Note: Currently, you can assign iOS and Android apps (line-of-business and store-purchased apps) to devices that aren't enrolled with Intune.

To receive app updates on devices that aren't enrolled with Intune, device users must go to their organization's Company Portal and manually install app updates.

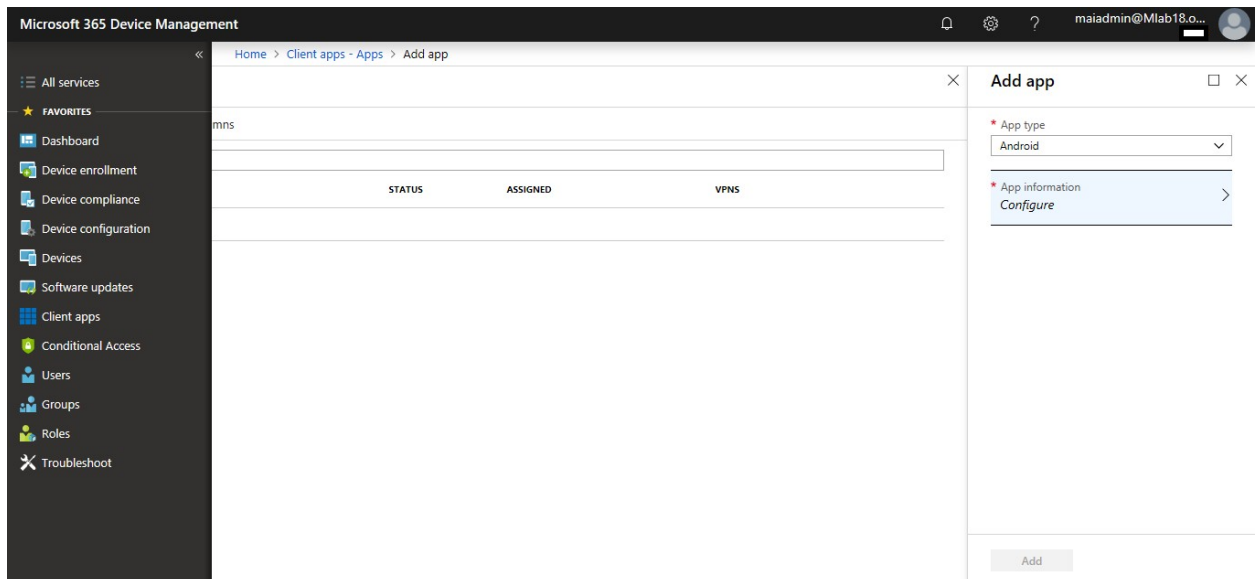
Configure Store App

To configure Android Store App

1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** pane, select **Client apps**.
3. In the **Client apps** workload pane, under **Manage**, select **Apps**. Select **Add**.

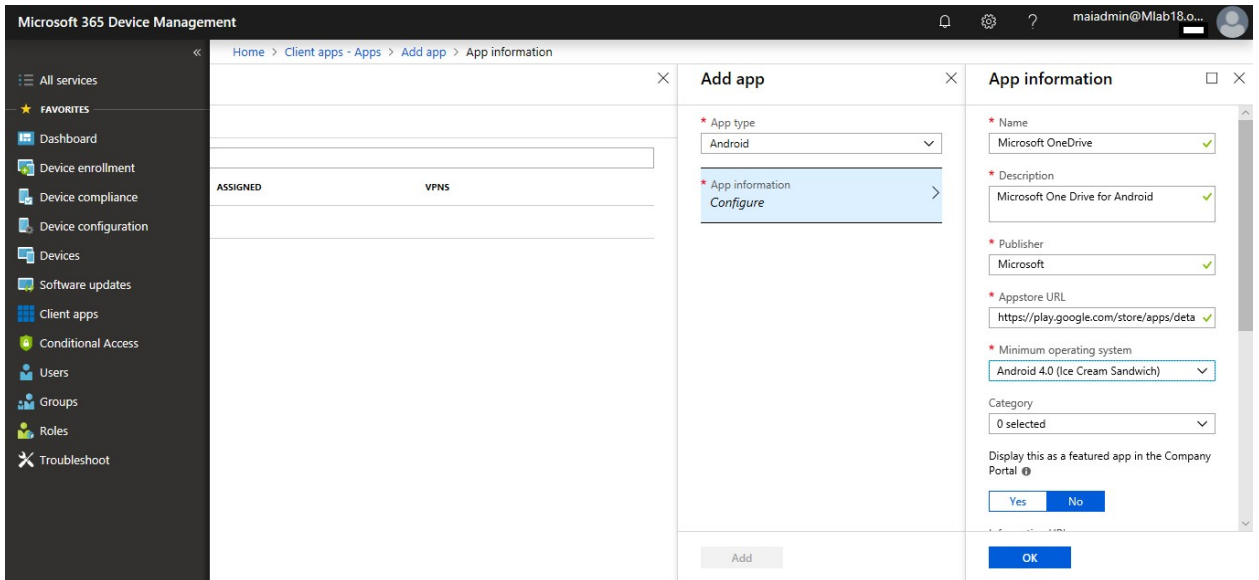


4. In the **Add App** pane, under the available **Store apps** types, select **Android**.

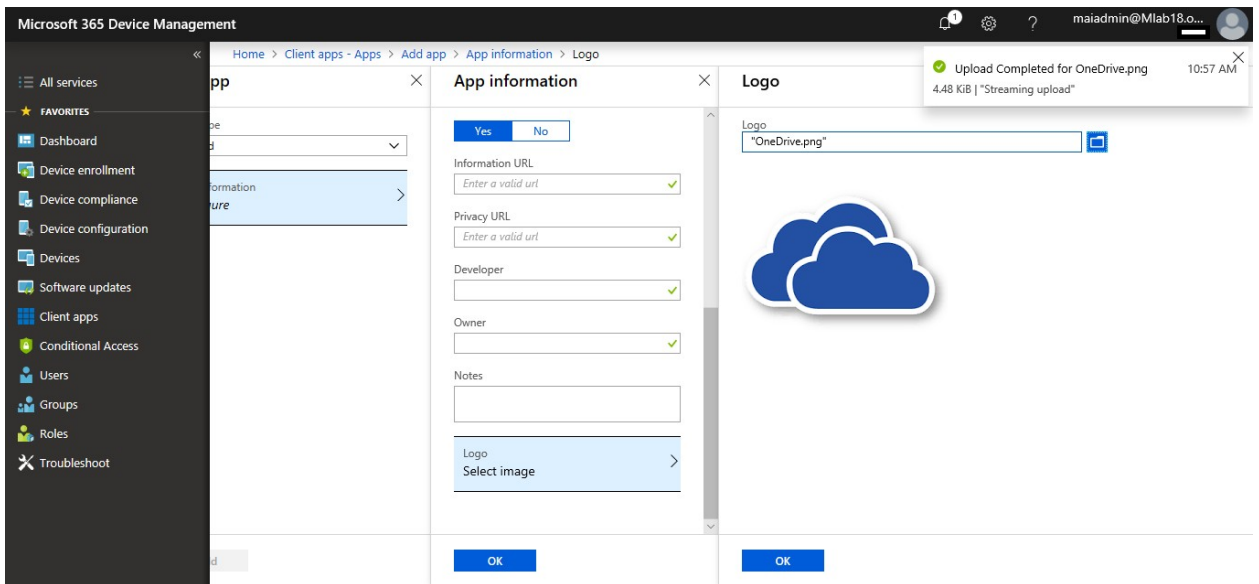


5. To configure the app information, select **Configure**, and then provide the following information. For Android apps, navigate to the [Google Play store](#) and search for the app you want to deploy.

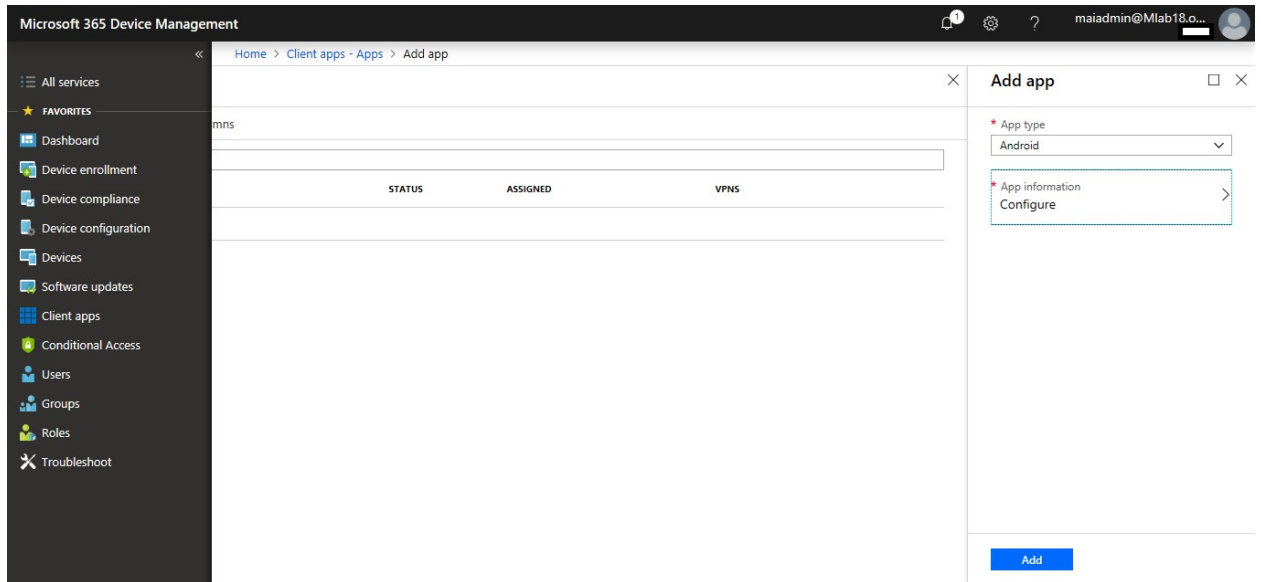
Microsoft Intune step by step on Azure portal



6. Select **OK**.

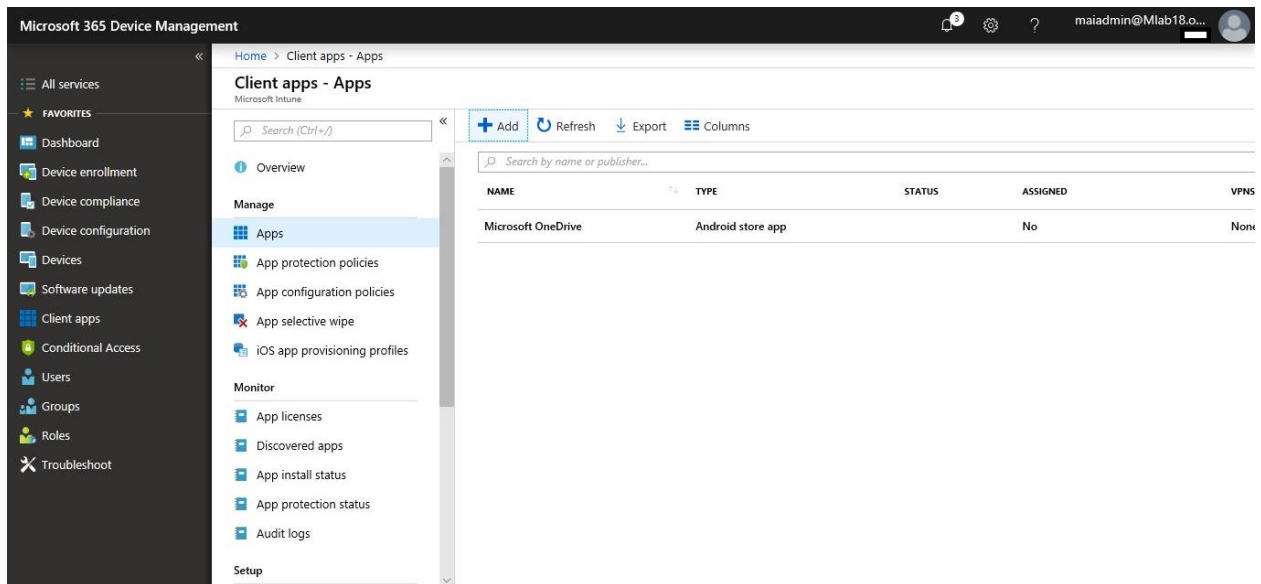


7. Select **Add**.

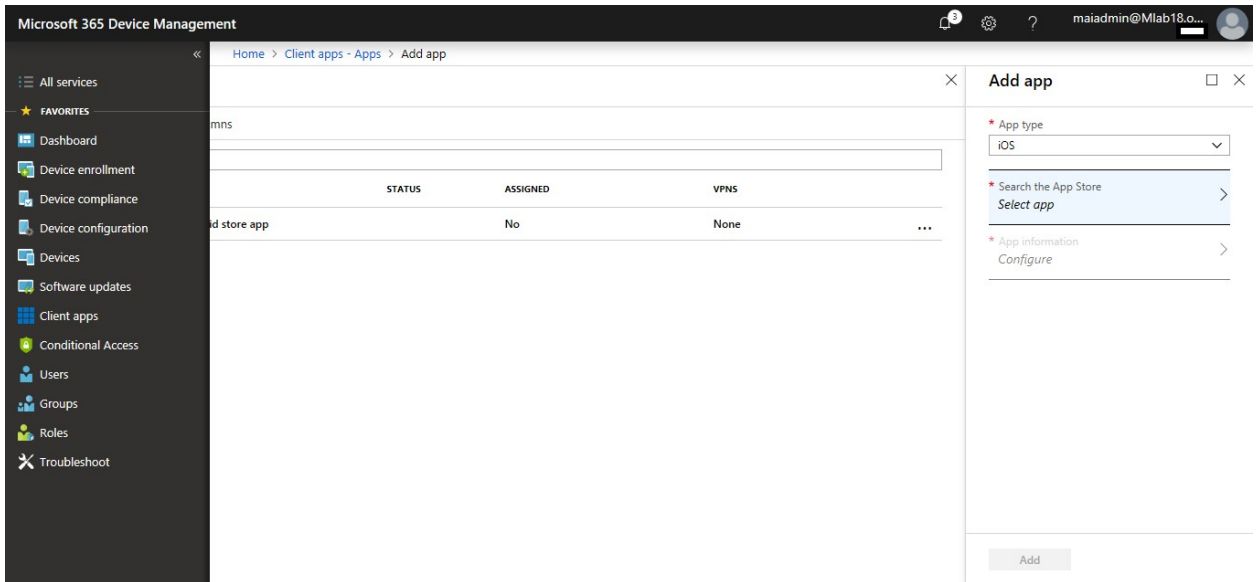


To configure iOS Store App

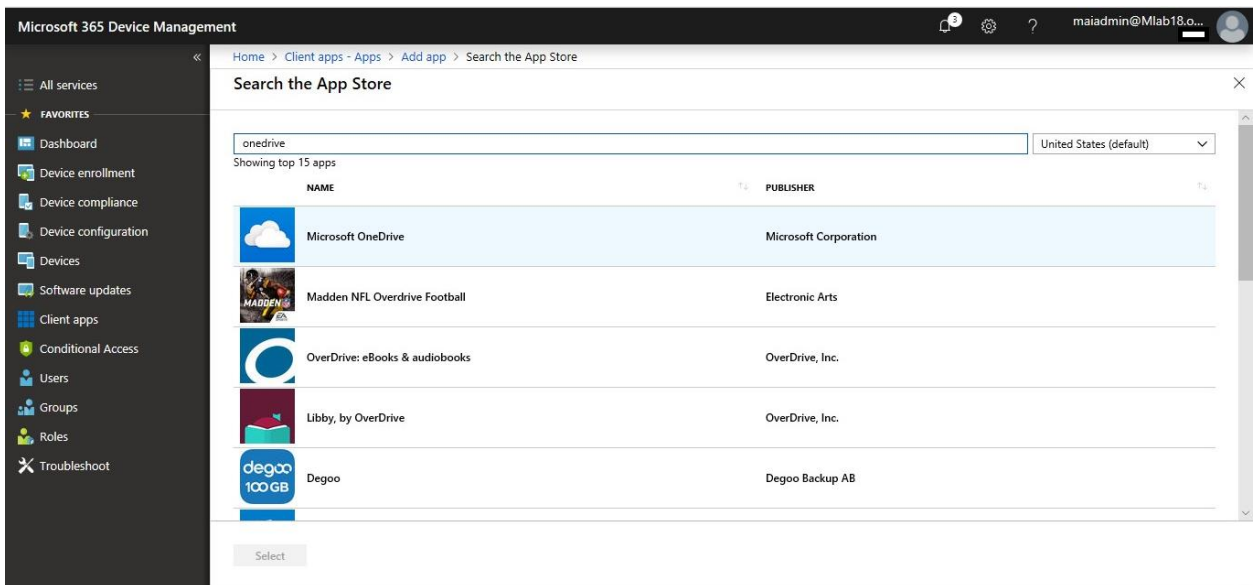
1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** pane, select **Client apps**.
3. In the **Client apps** workload pane, under **Manage**, select **Apps**.
4. In the **Apps** pane, select **Add**.



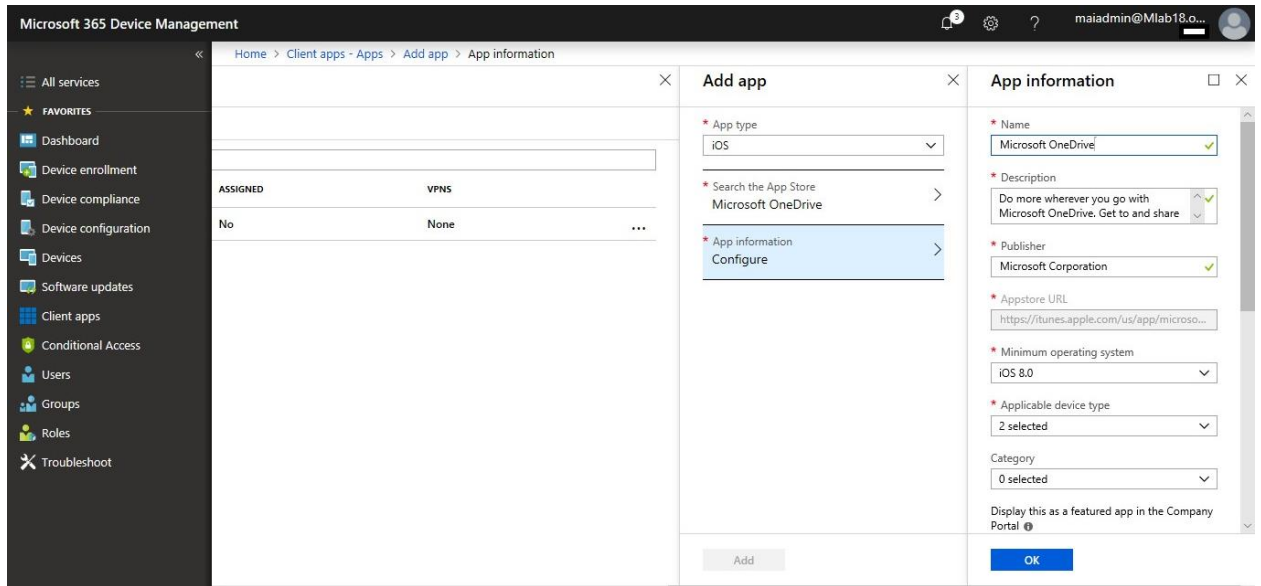
5. In the **App type** list, under the **Store app** types, select **iOS**.



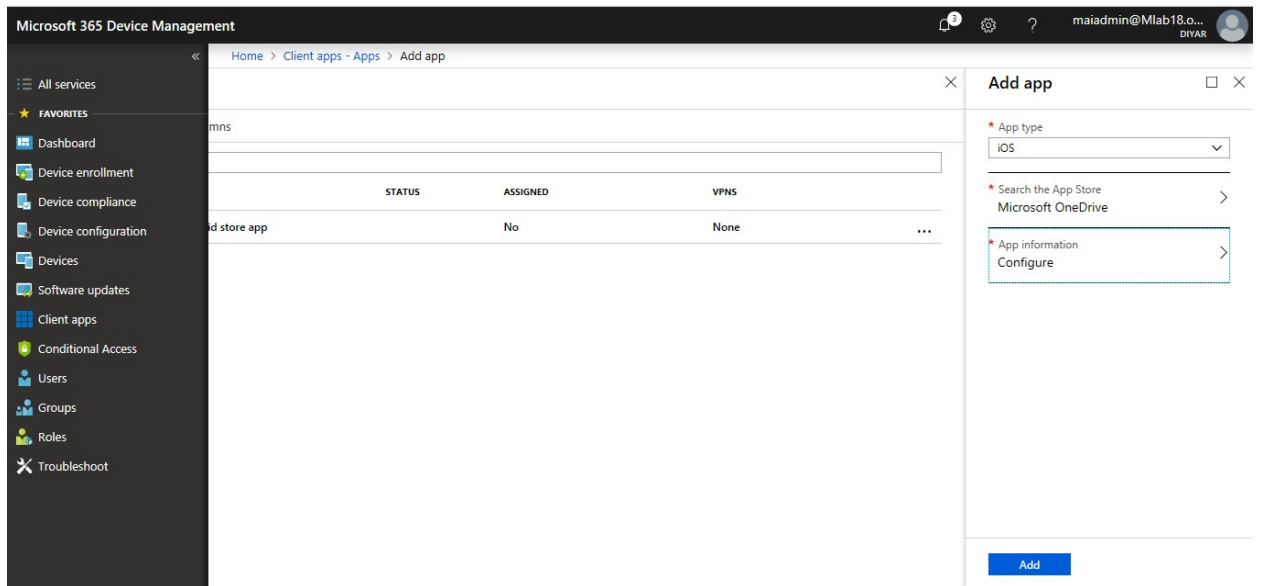
6. Select **Search the App Store**. In the **Search the App Store** pane, select the App Store country locale.
7. In the **Search** box, type the name (or part of the name) of the app. Intune searches the store and returns a list of relevant results. In the results list, select the app you want, and then click **Select**.



8. In the **Add app** pane, select **App information** to configure the app.

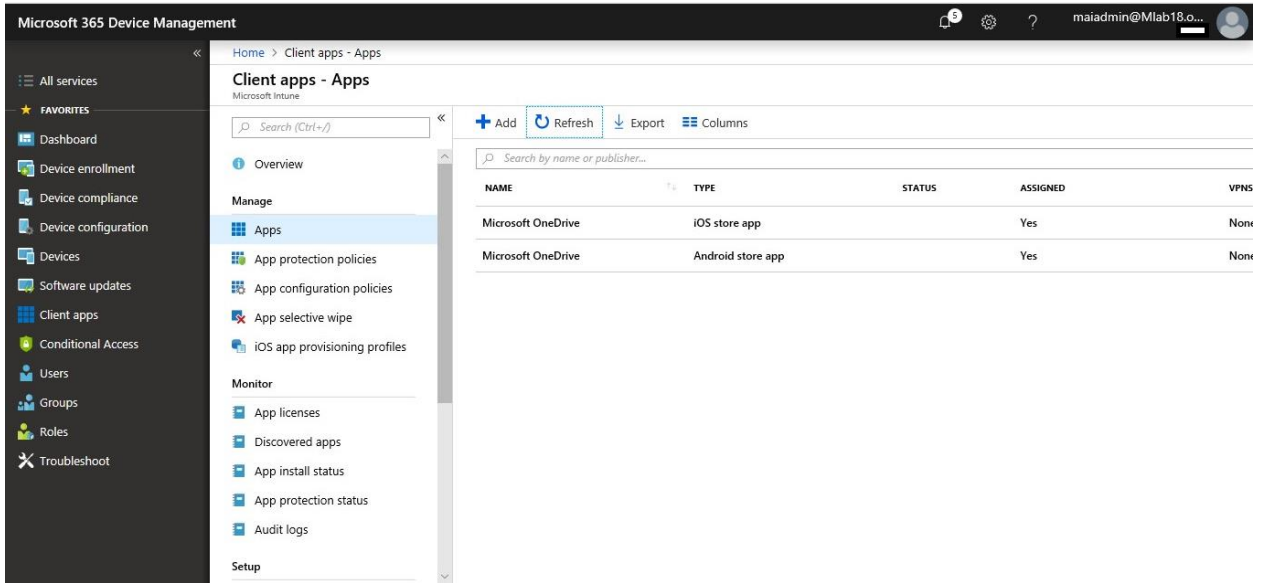


9. In the **App information** pane, add the app information. Select **OK**.
10. Select **Add**.

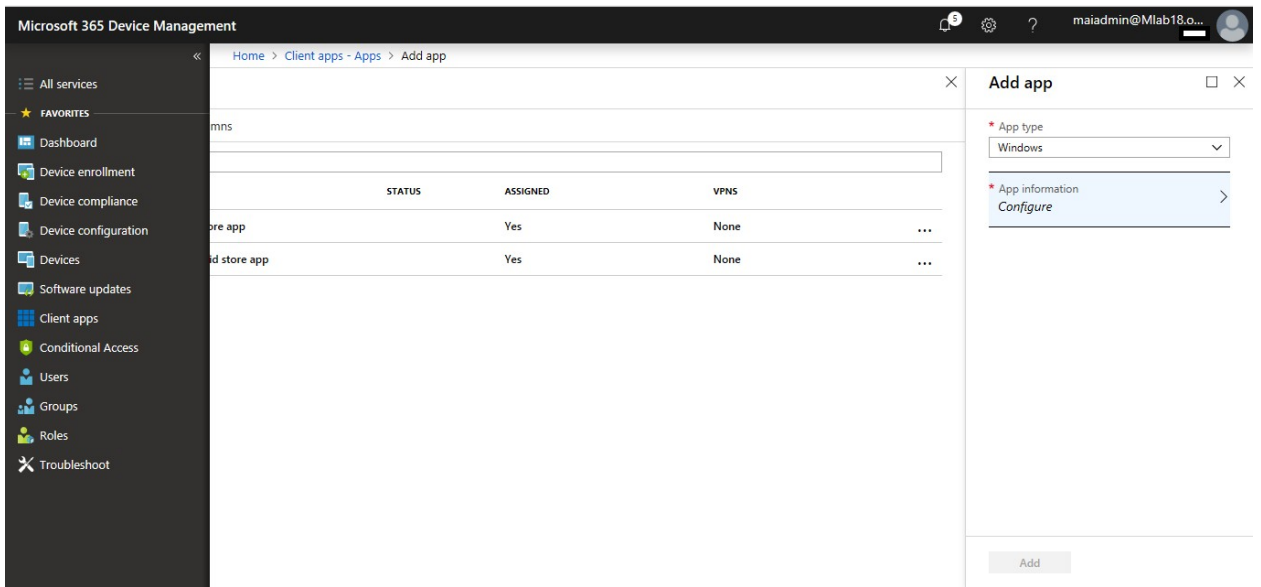


To Configure Windows Store App

1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** pane, select **Client apps**.
3. In the **Client apps** workload pane, under **Manage**, select **Apps**.
4. In the **Apps** pane, select **Add**.

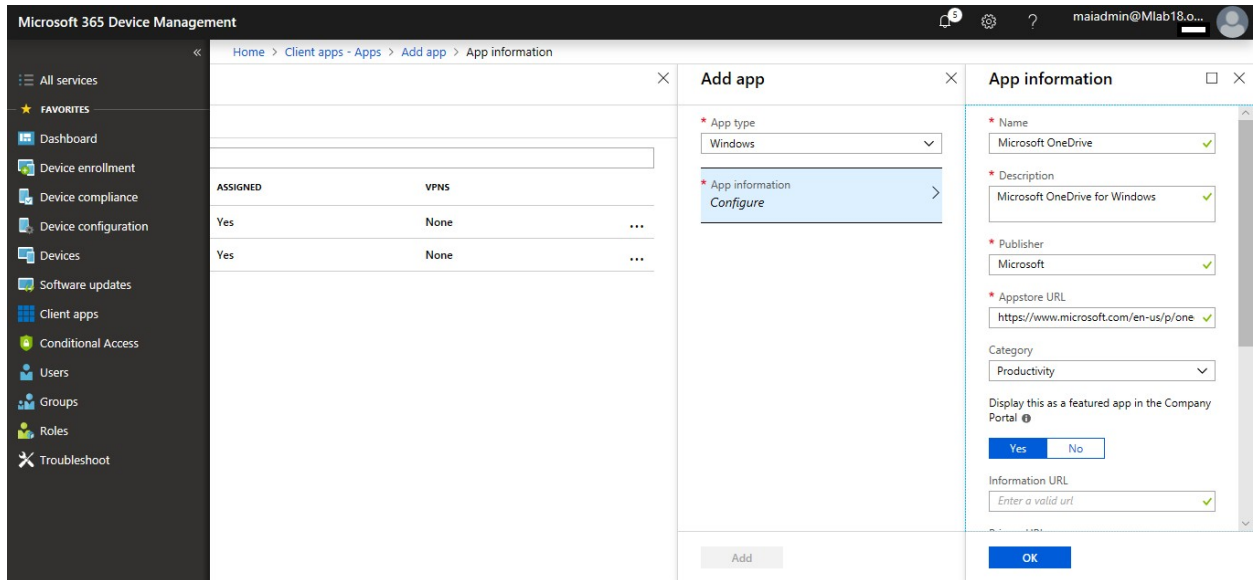


5. In the **Add app** pane, select an **App type** of **Windows**, and then select **App information**.

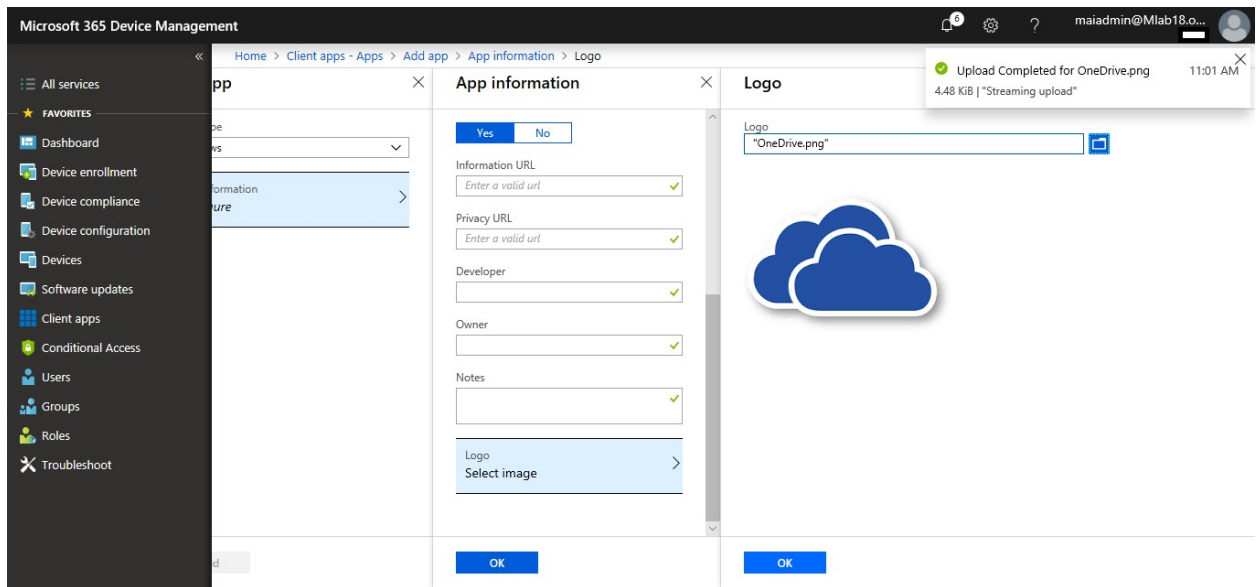


6. In the **App information** pane, add the app information.

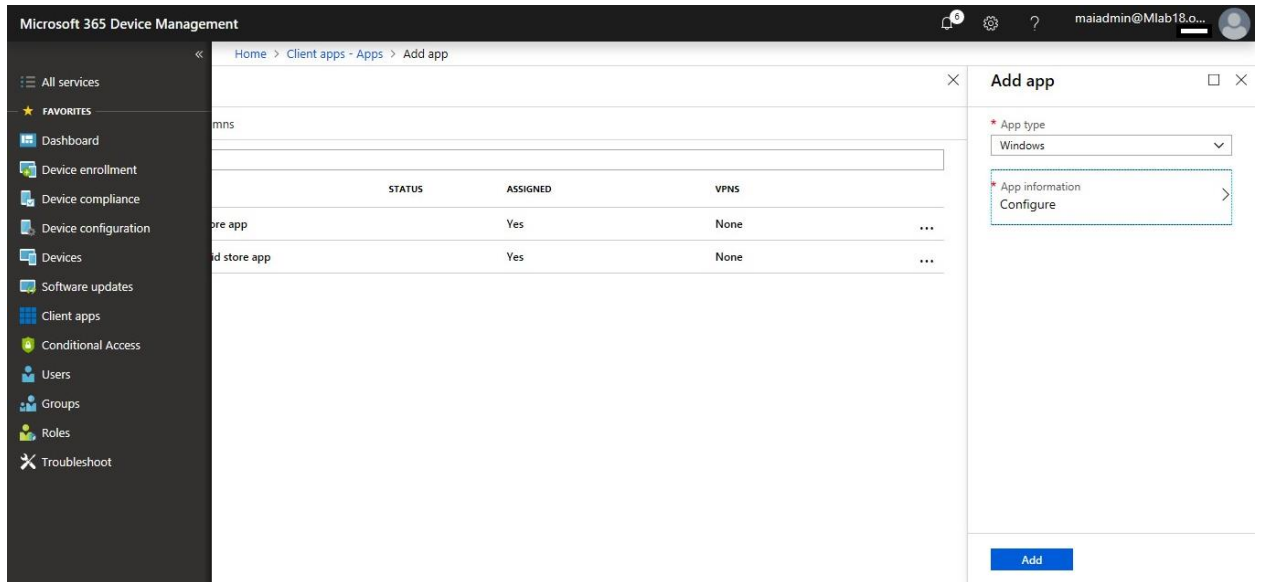
Microsoft Intune step by step on Azure portal



7. In the **App information** pane, add the app information. Select **OK**.

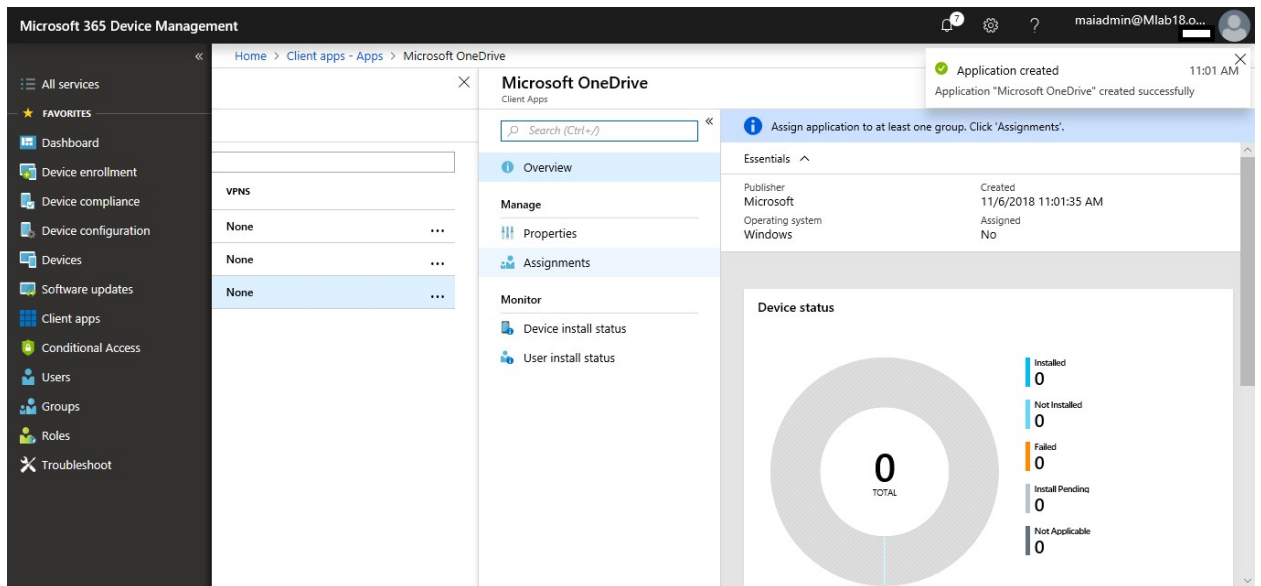


8. Select **Add**.



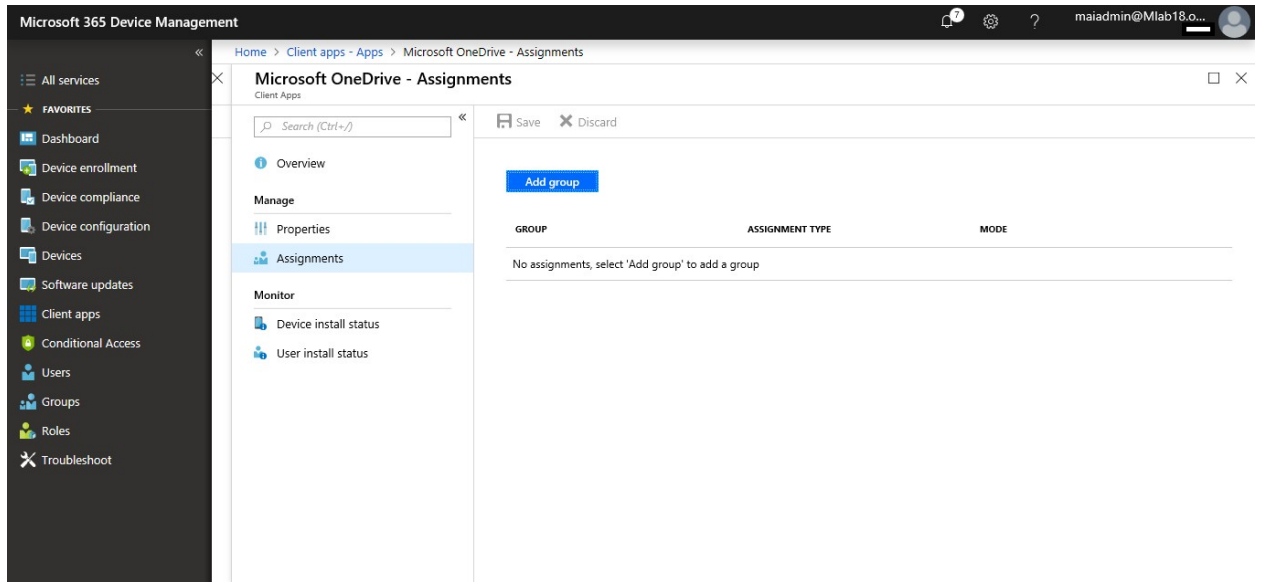
To assign specific group on Store App

1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** menu, select **Client apps**.
3. In the **Manage** section of the menu, select **Apps**.
4. In the **Apps** pane, select the app you want to assign.

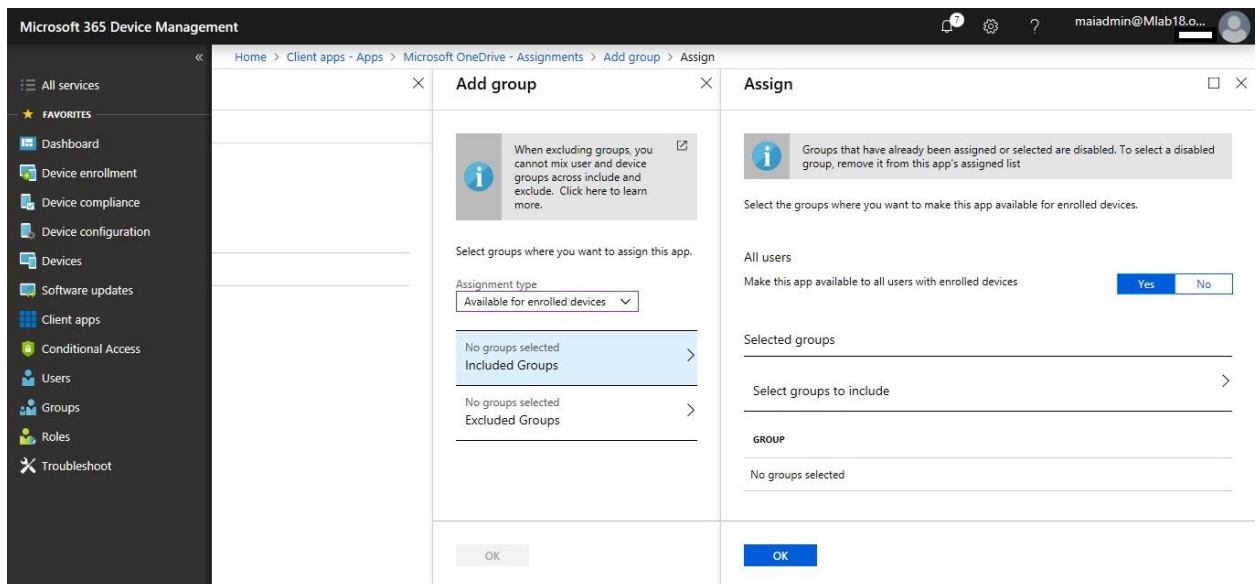


5. In the **Manage** section of the menu, select **Assignments**.
6. Select **Add Group** to open the **Add group** pane that is related to the app.

Microsoft Intune step by step on Azure portal

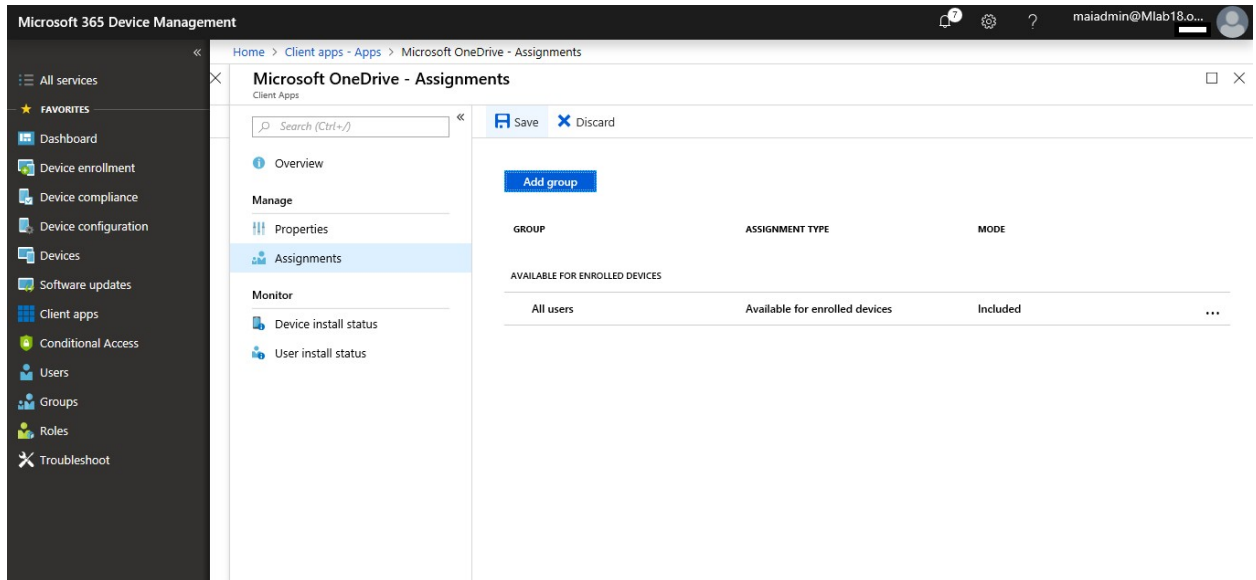


7. For the specific app, select an **assignment type**: Available for enrolled devices
8. To select the groups of users that are affected by this app assignment, select **Included Groups**. click “All Users”
9. In the **Assign** pane, select **OK** to complete the included groups selection.



10. In the app **Assignments** pane, select **Save**.

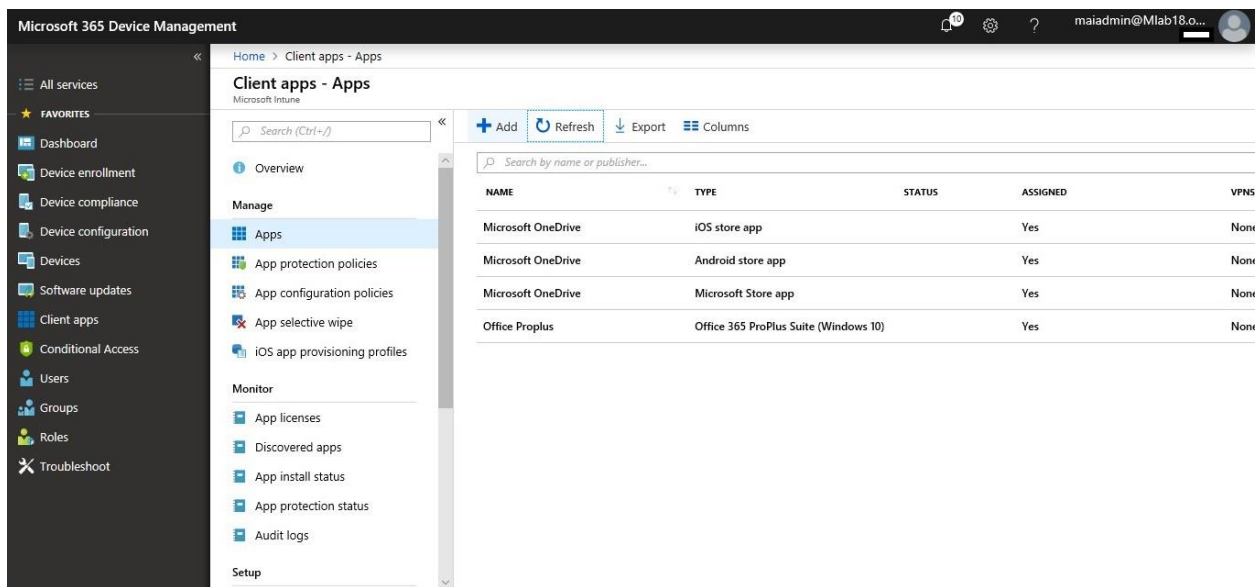
Microsoft Intune step by step on Azure portal



Configure Web App

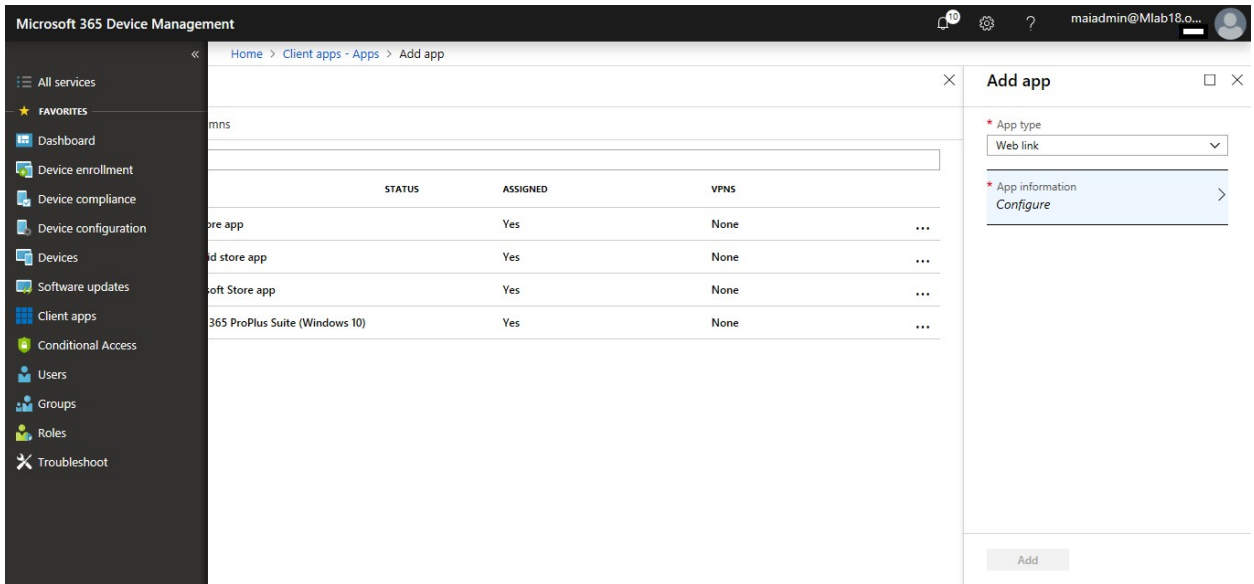
To add an app to Intune as a shortcut to an app on the web, do the following:

1. Sign in to the [Azure portal](#).
2. Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
3. In the **Intune** pane, select **Client apps**.
4. In the **Client apps** workload pane, under **Manage**, select **Apps**.
5. In the **Apps** pane, select **Add**.

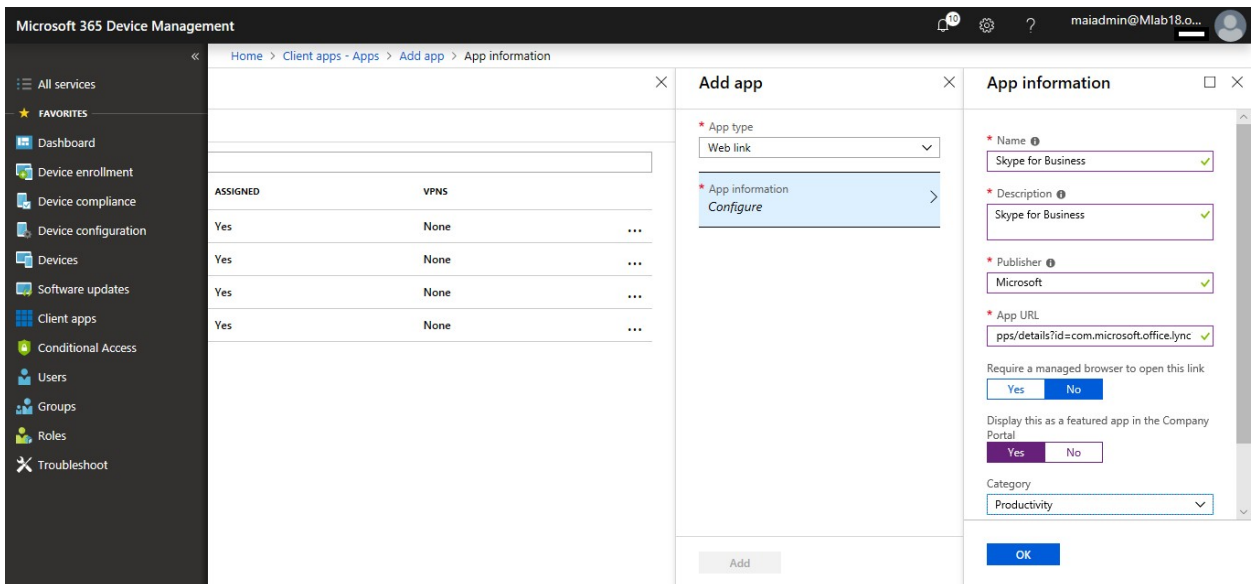


6. In the **Add app** pane, in the **App type** drop-down list, select the **Web link** type. Select **Configure**.

Microsoft Intune step by step on Azure portal

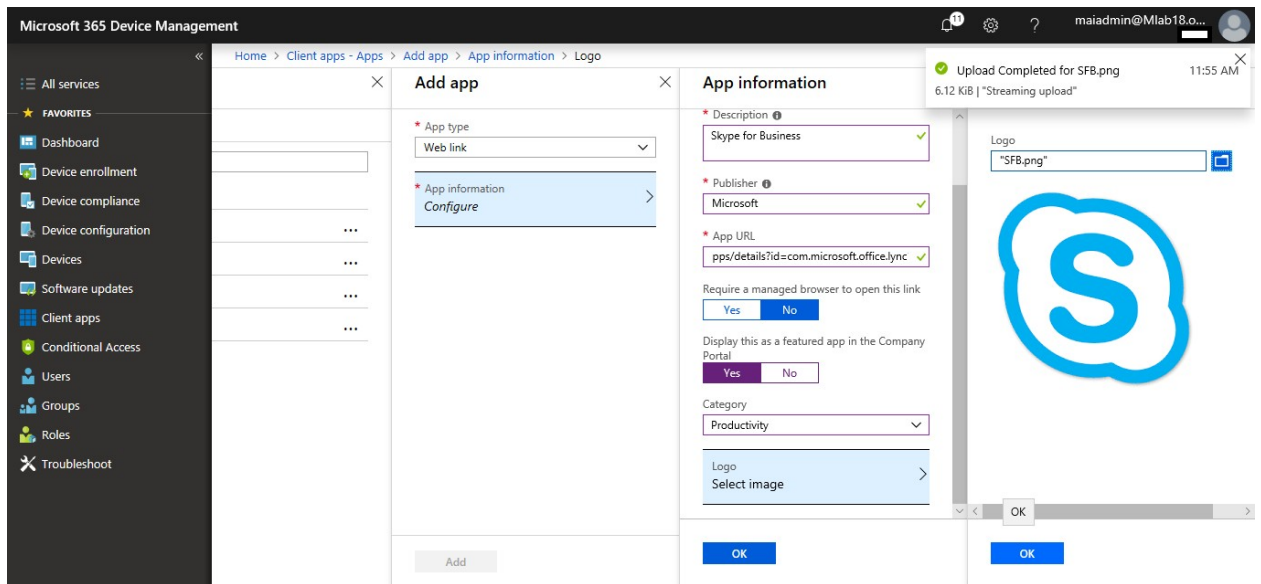


7. In the **App information** pane, add the following information

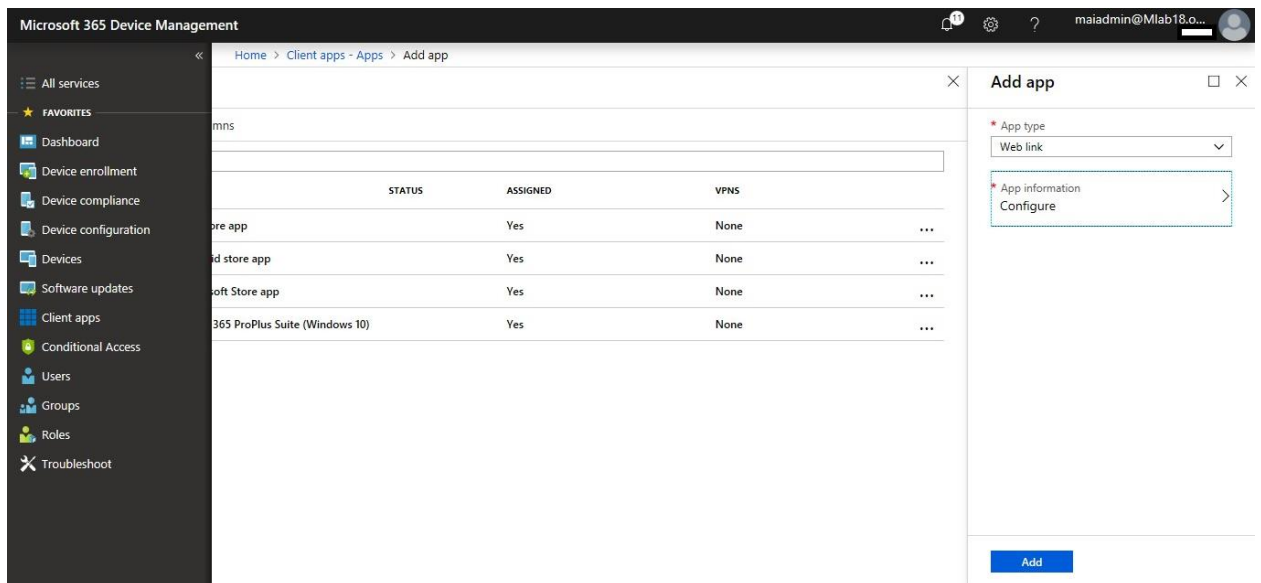


8. Select **OK**.

Microsoft Intune step by step on Azure portal

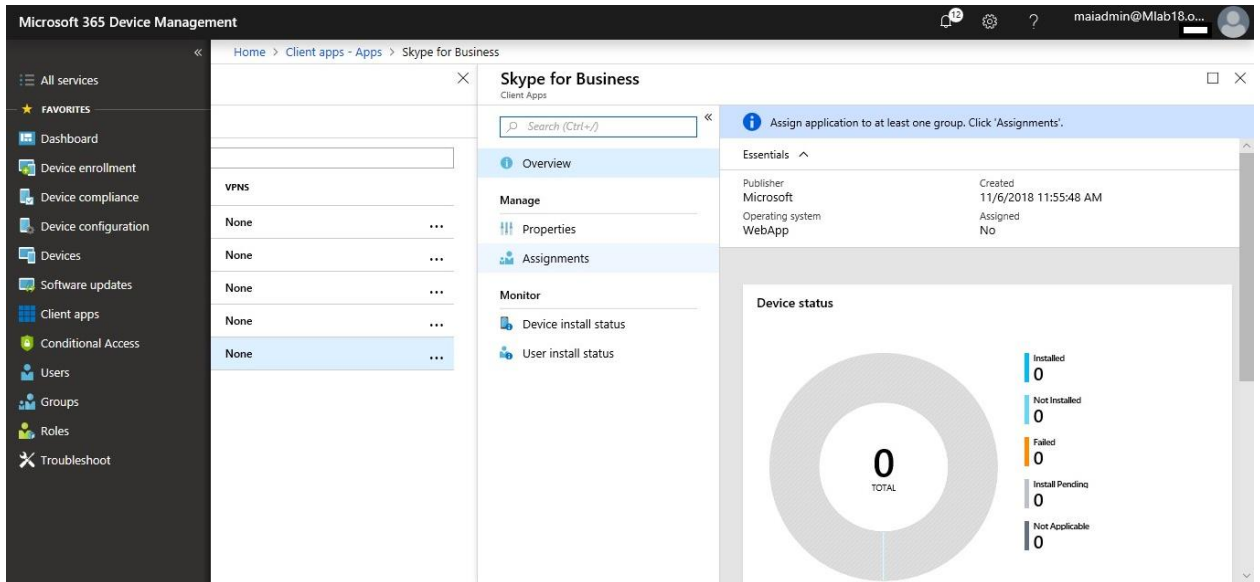


9. In the **Add app** pane, select **Add**.

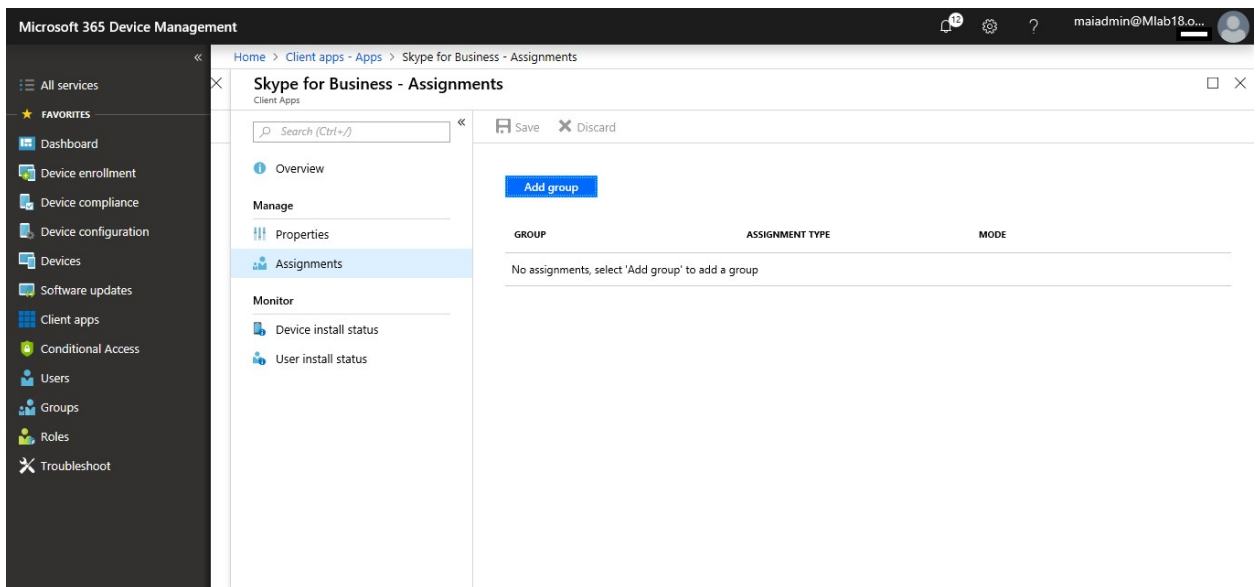


To assign specific group on Web App

1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** menu, select **Client apps**.
3. In the **Manage** section of the menu, select **Apps**.
4. In the **Apps** pane, select the app you want to assign.
5. In the **Manage** section of the menu, select **Assignments**.

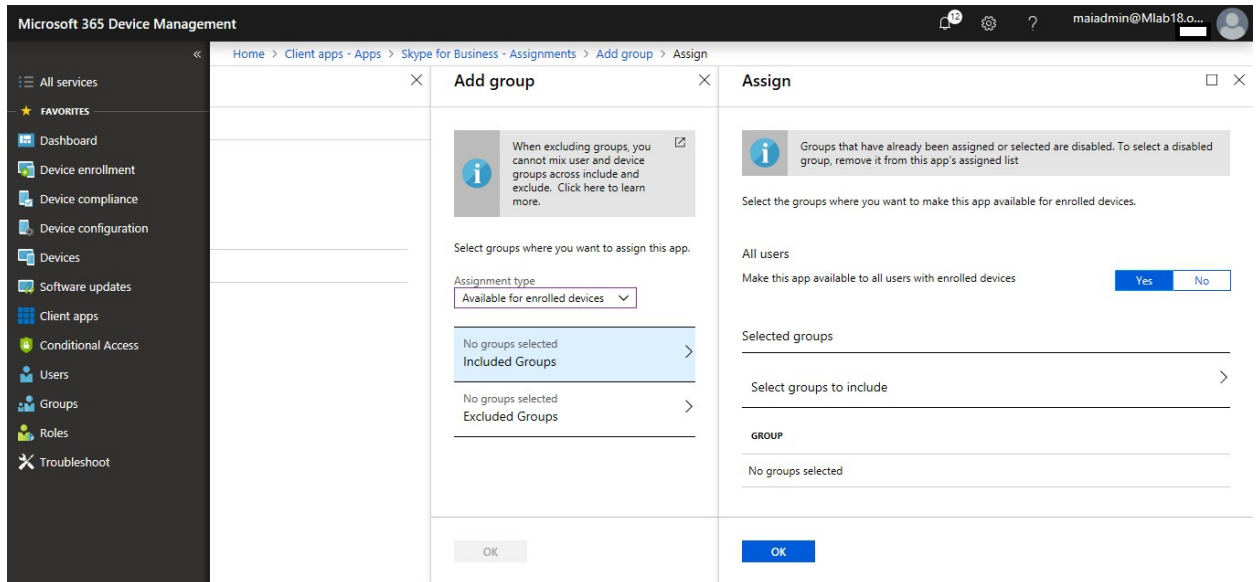


6. Select **Add Group** to open the **Add group** pane that is related to the app.

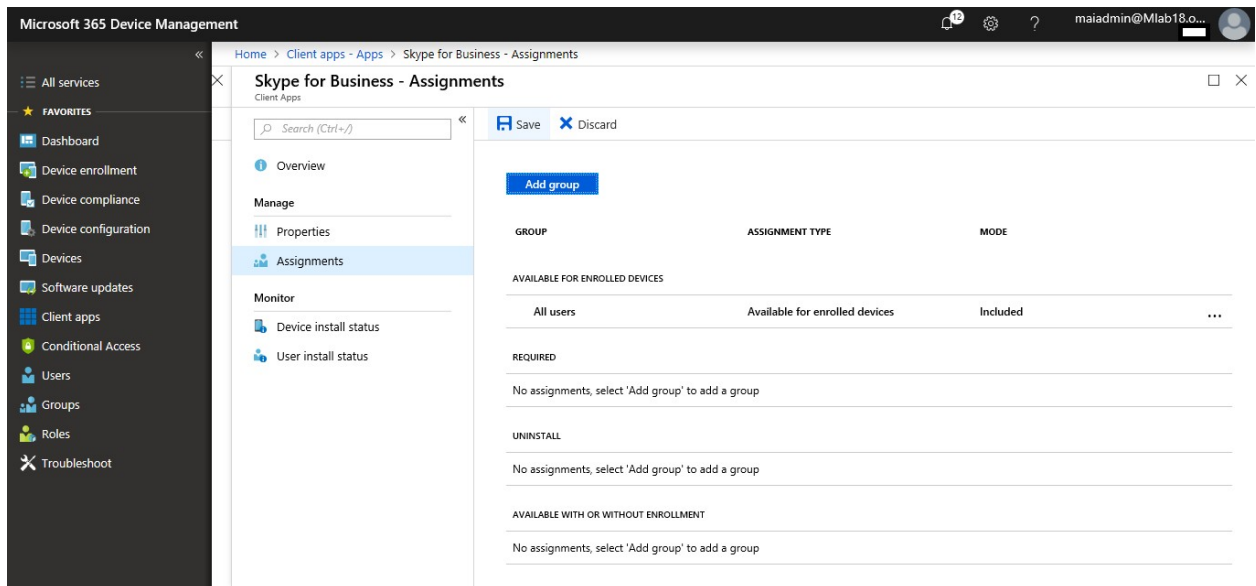


7. For the specific app, select an **assignment type**:
8. To select the groups of users that are affected by this app assignment, select **Included Groups**. After you have selected one or more groups to include, Click **Select**.
9. In the **Assign** pane, select **OK** to complete the included groups selection.

Microsoft Intune step by step on Azure portal



10. In the app **Assignments** pane, select **Save**.



Configure Built-in App

To add a built-in app to your available apps in Microsoft Intune, do the following:

1. Sign in to the [Azure portal](#). To display the Microsoft Intune pane, select **More Services > Monitoring + Management > Intune**.
2. In the **Intune** pane, select **Client apps**.
3. In the **Client apps** pane, under **Manage**, select **Apps**.
4. Select **Add**.

Microsoft Intune step by step on Azure portal

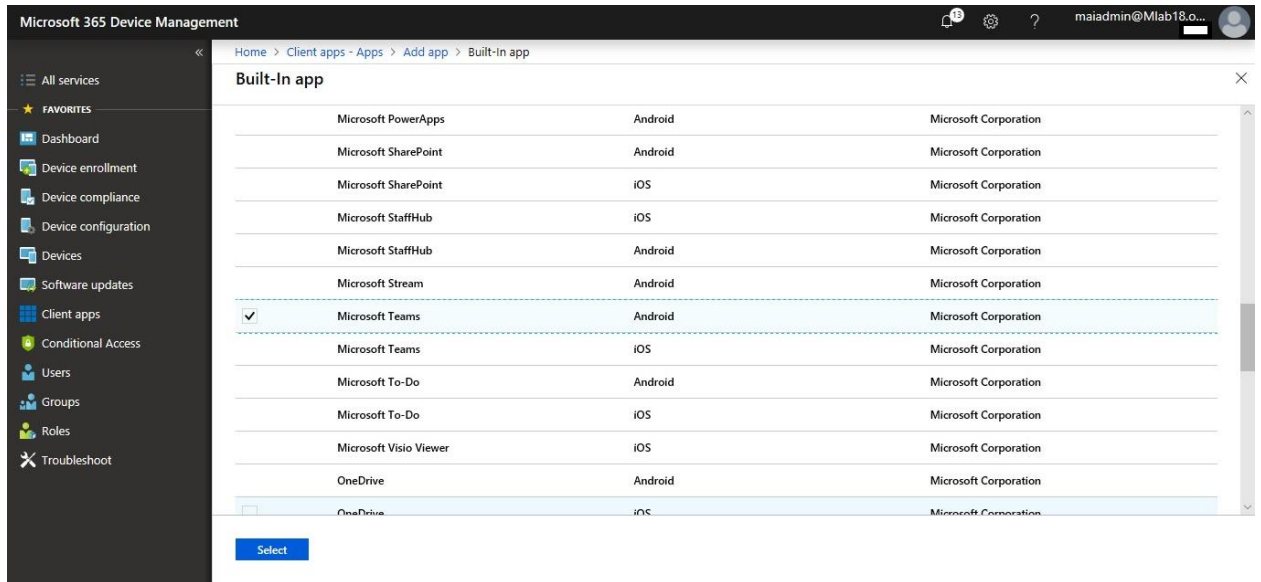
The screenshot shows the Microsoft 365 Device Management console. The left sidebar contains navigation options like Dashboard, Device enrollment, and Client apps. The main area is titled 'Client apps - Apps' and features a search bar, '+ Add' button, and a table of installed apps. The table has columns for NAME, TYPE, STATUS, ASSIGNED, and VPNS.

NAME	TYPE	STATUS	ASSIGNED	VPNS
Microsoft OneDrive	iOS store app		Yes	None
Microsoft OneDrive	Android store app		Yes	None
Microsoft OneDrive	Microsoft Store app		Yes	None
Office ProPlus	Office 365 ProPlus Suite (Windows 10)		Yes	None
Skype for Business	Web link		No	None

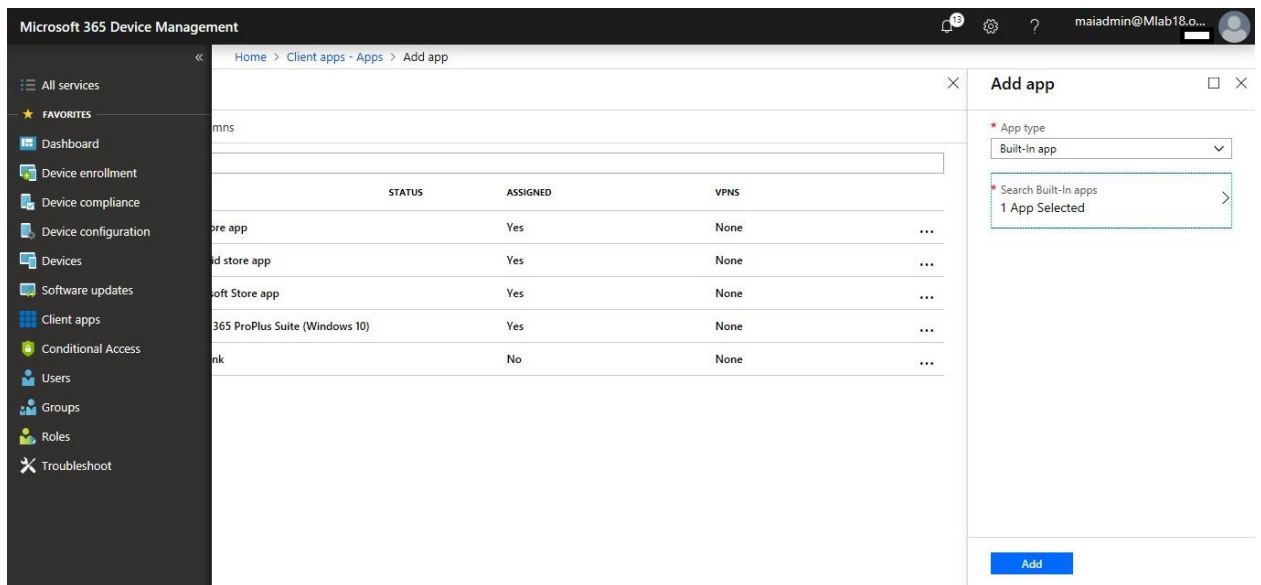
5. In the **Add** app pane, in the **App type** list, select **Built-In app**. Click **Select app**.

The screenshot shows the 'Add app' pane in the Microsoft 365 Device Management console. The pane is open over the 'Client apps - Apps' page. It features a dropdown menu for 'App type' with 'Built-In app' selected. Below the dropdown is a search bar for 'Search Built-In apps' with a 'Select app' button. An 'Add' button is visible at the bottom of the pane.

6. In the **Built-In app** pane, select the apps that you want to include.

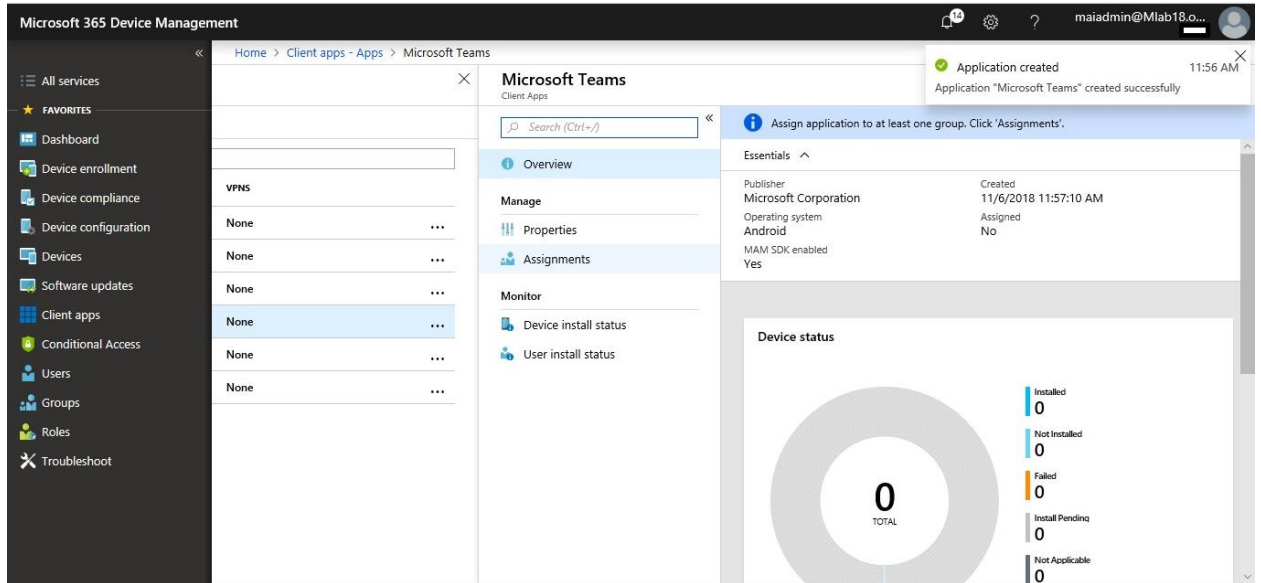


7. In the **Add app** pane, select **Add**.

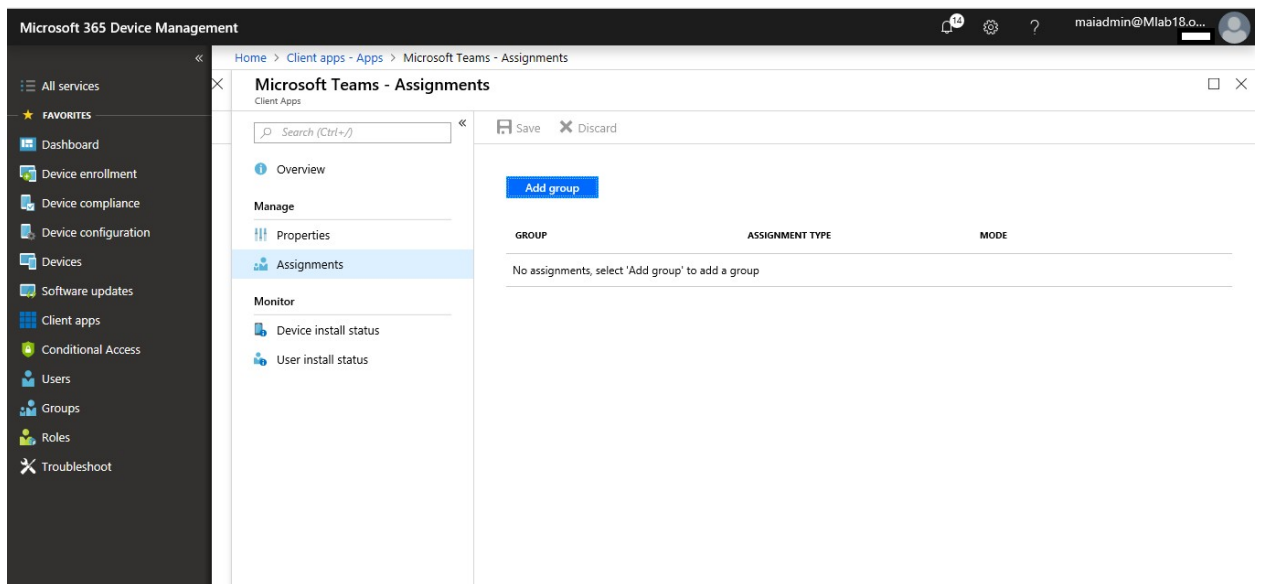


To assign specific group on built-in App

1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** menu, select **Client apps**.
3. In the **Manage** section of the menu, select **Apps**.
4. In the **Apps** pane, select the app you want to assign.
5. In the **Manage** section of the menu, select **Assignments**.

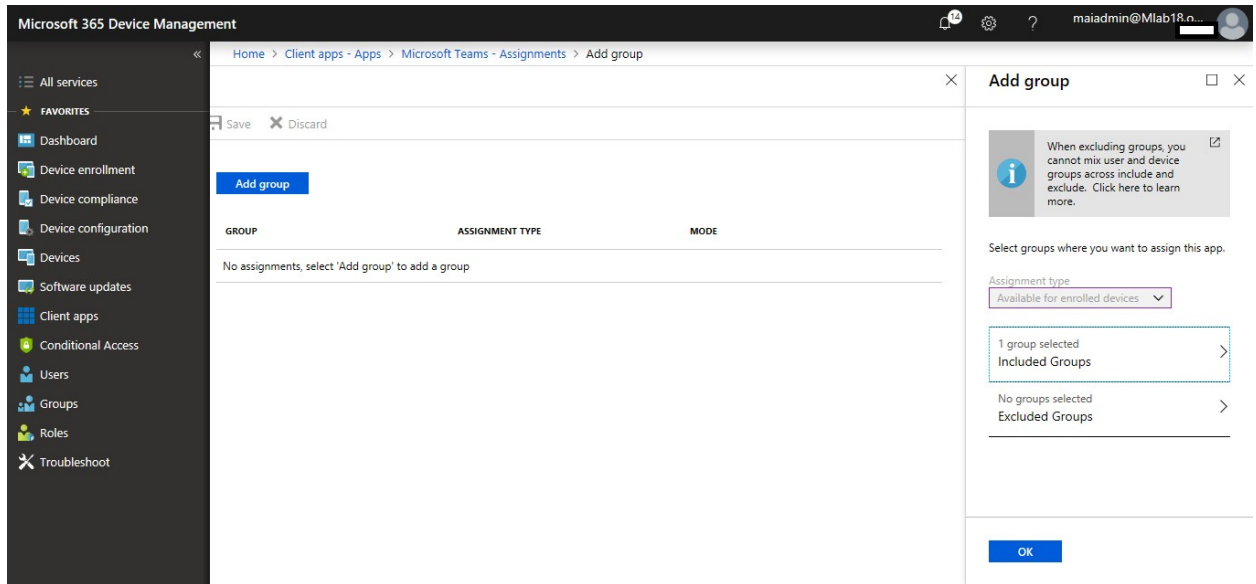


6. Select **Add Group** to open the **Add group** pane that is related to the app.

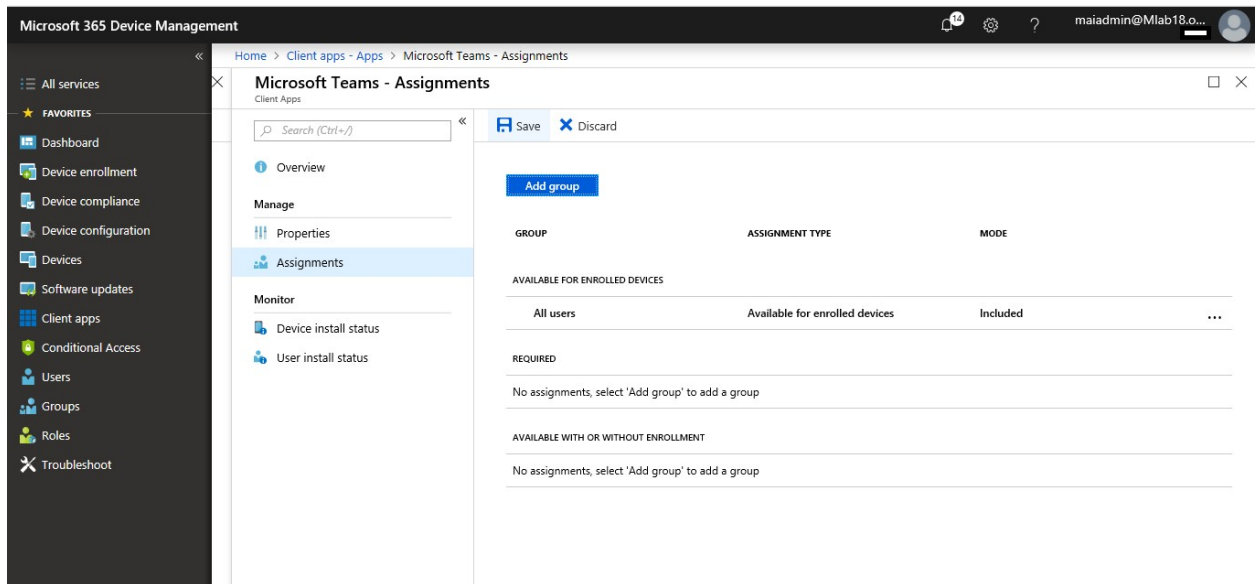


7. For the specific app, select an **assignment type**:
8. To select the groups of users that are affected by this app assignment, select **Included Groups**. After you have selected one or more groups to include, Click **Select**.
9. In the **Assign** pane, select **OK** to complete the included groups selection.

Microsoft Intune step by step on Azure portal



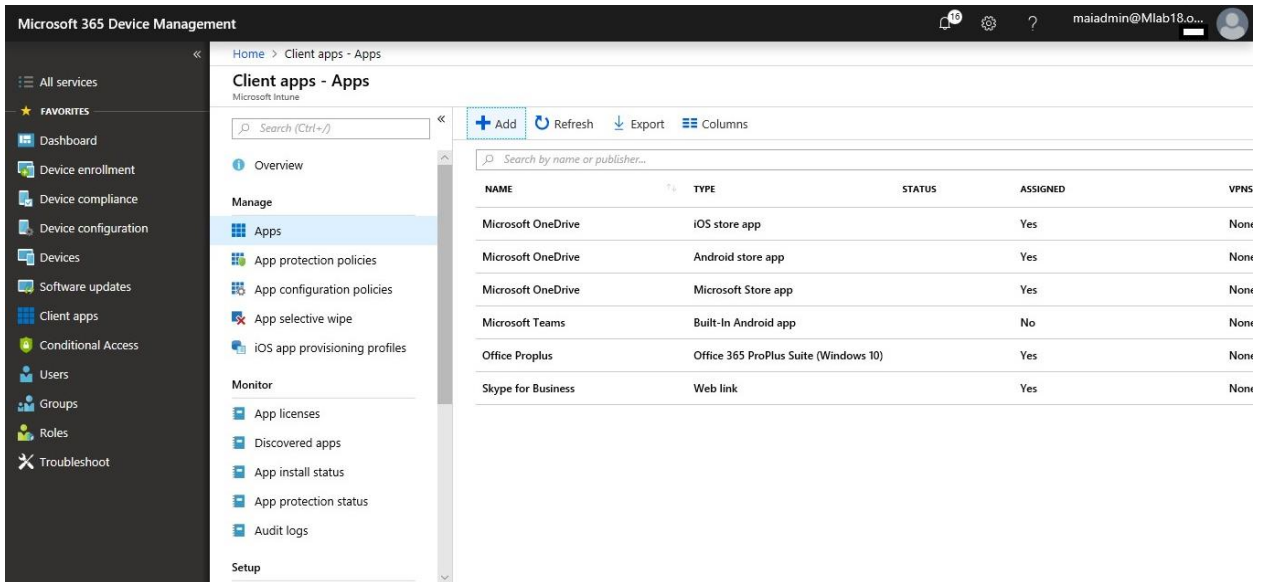
10. In the app **Assignments** pane, select **Save**.



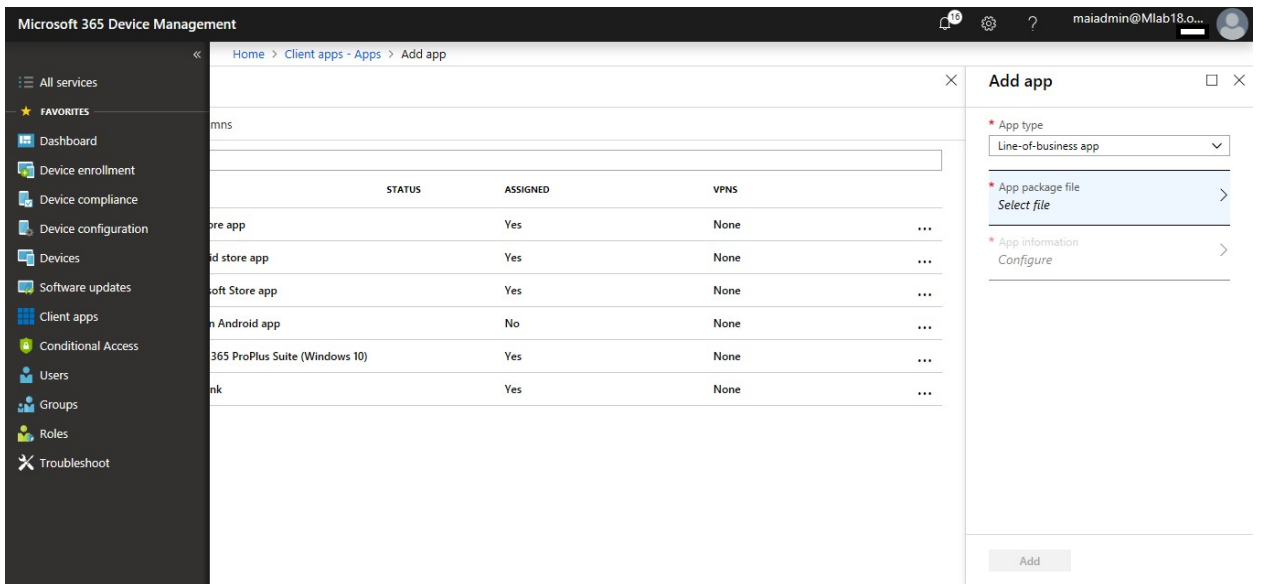
Configure Line of Business App

To add a line of business app to your available apps in Microsoft Intune, do the following:

1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is in the **Monitoring + Management** section.
2. In the **Intune** pane, select **Client apps**.
3. In the **Client apps** workload, select **Manage** > **Apps**.
4. Above the list of apps, select **Add**.

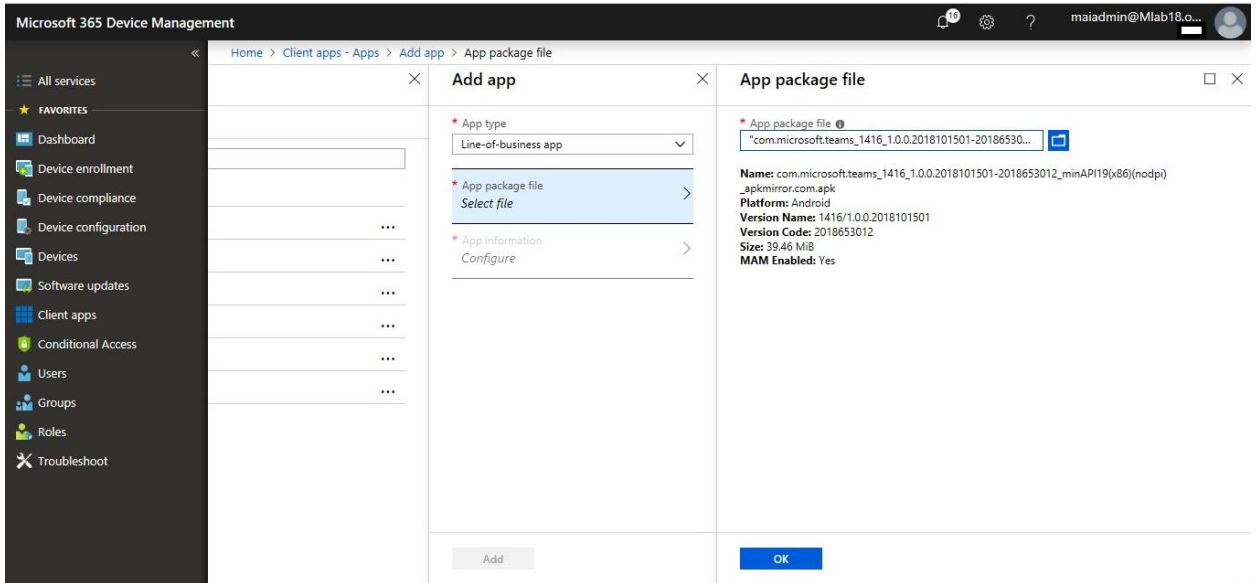


5. In the **Add app** pane, select **Line-of-business app**.

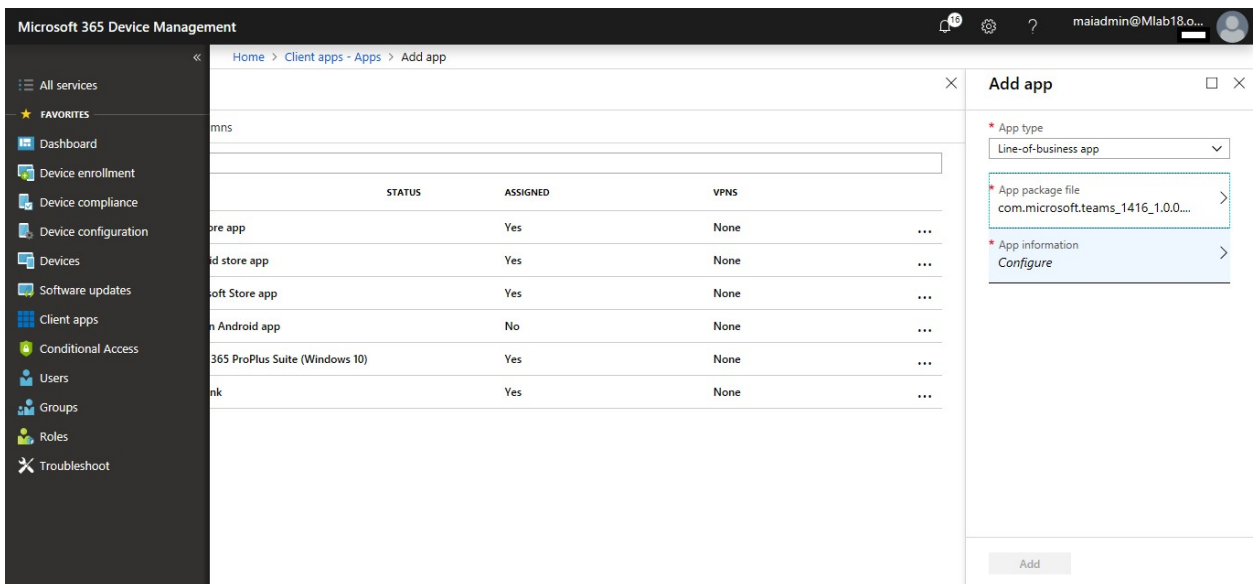


6. In the **Add app** pane, select **App package file**.

7. In the **App package file** pane, select the browse button. Then select an Android installation file with the extension **.apk**. When you're finished, select **OK**.

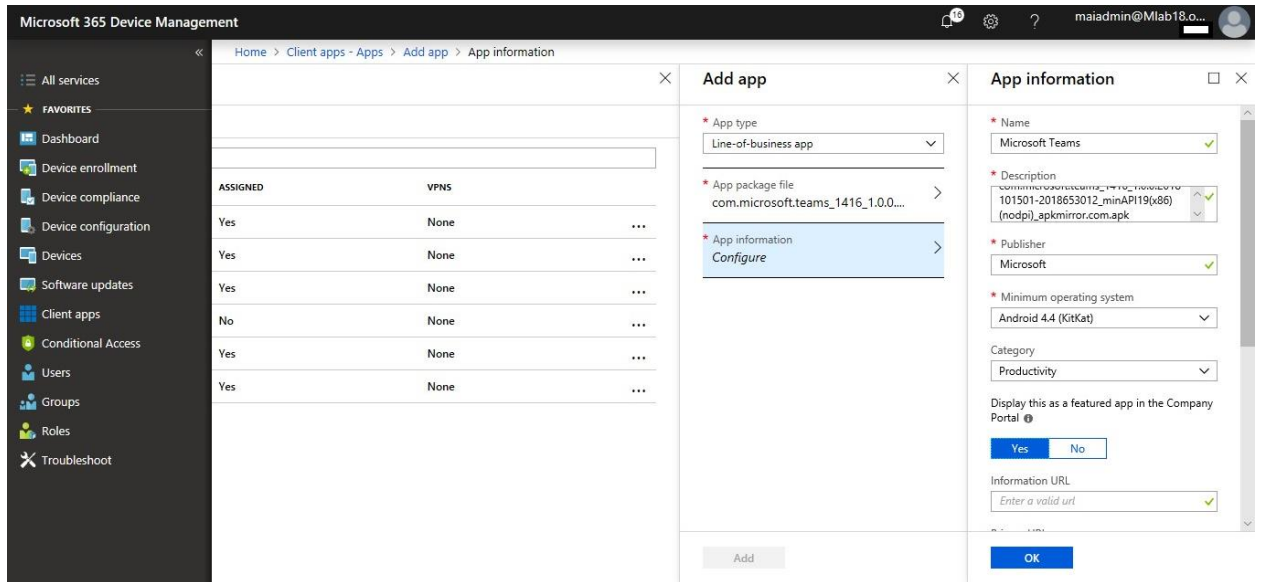


8. In the **Add app** pane, select **App information**.

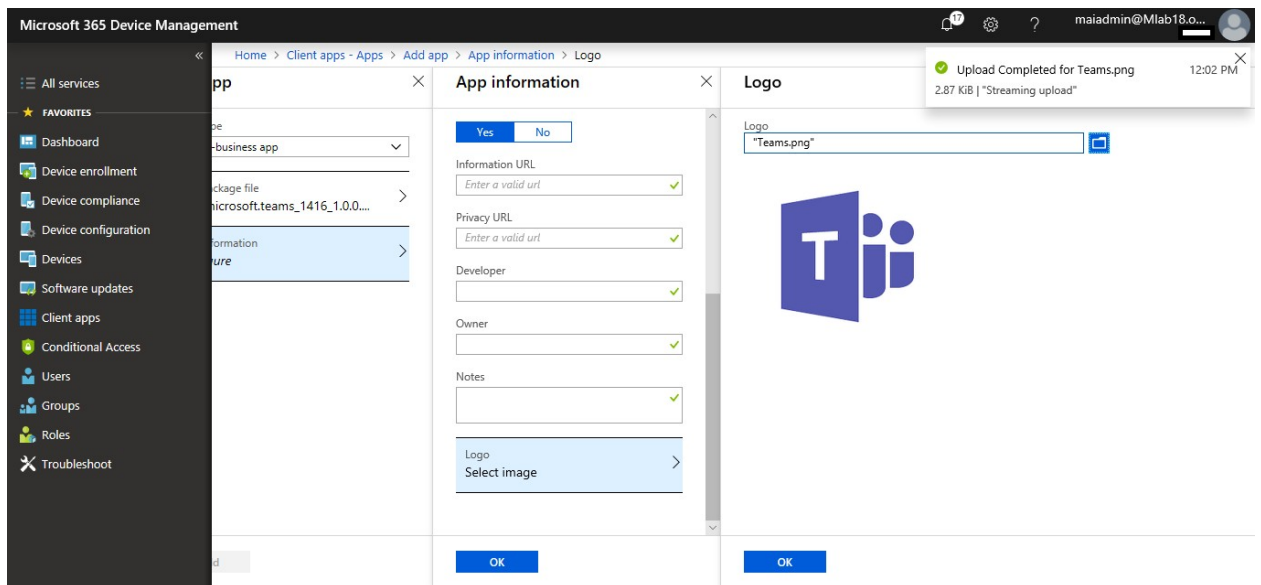


9. In the **App information** pane, add the details for your app.

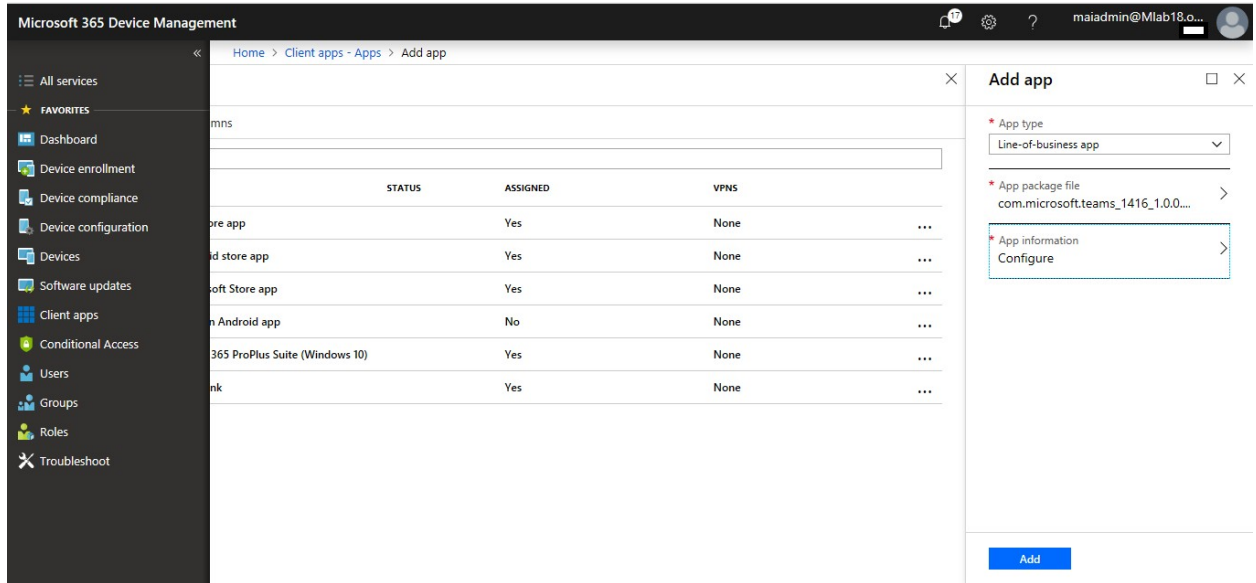
Microsoft Intune step by step on Azure portal



10. When you're finished, select **OK**.

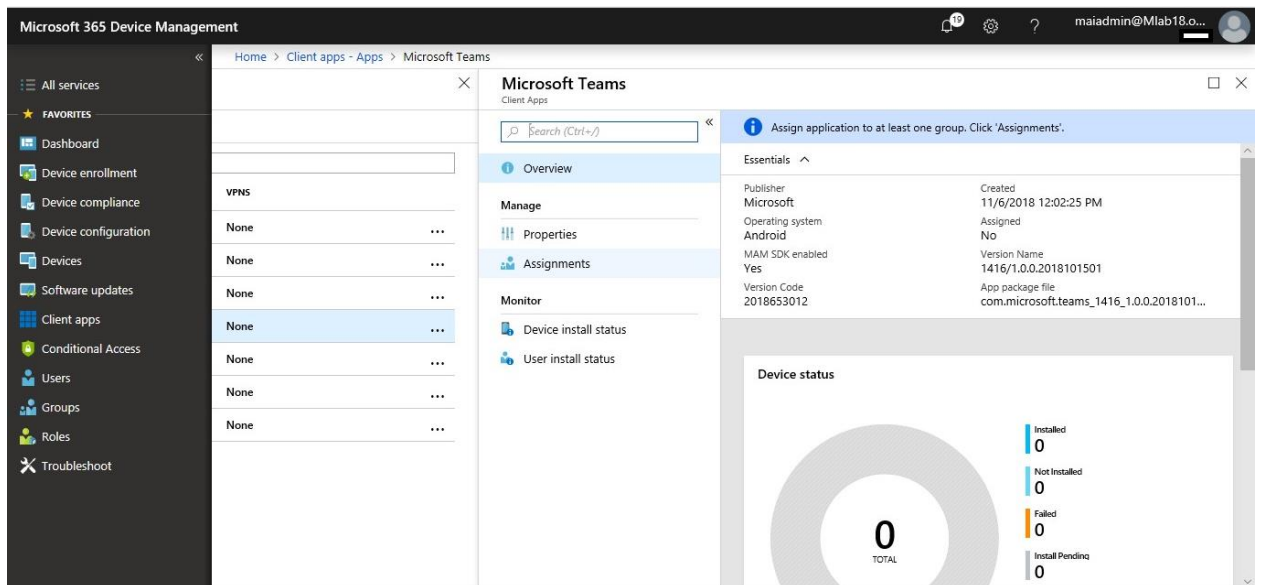


11. In the **Add app** pane, verify that the details of your app are correct. Select **Add** to upload the app to Intune.



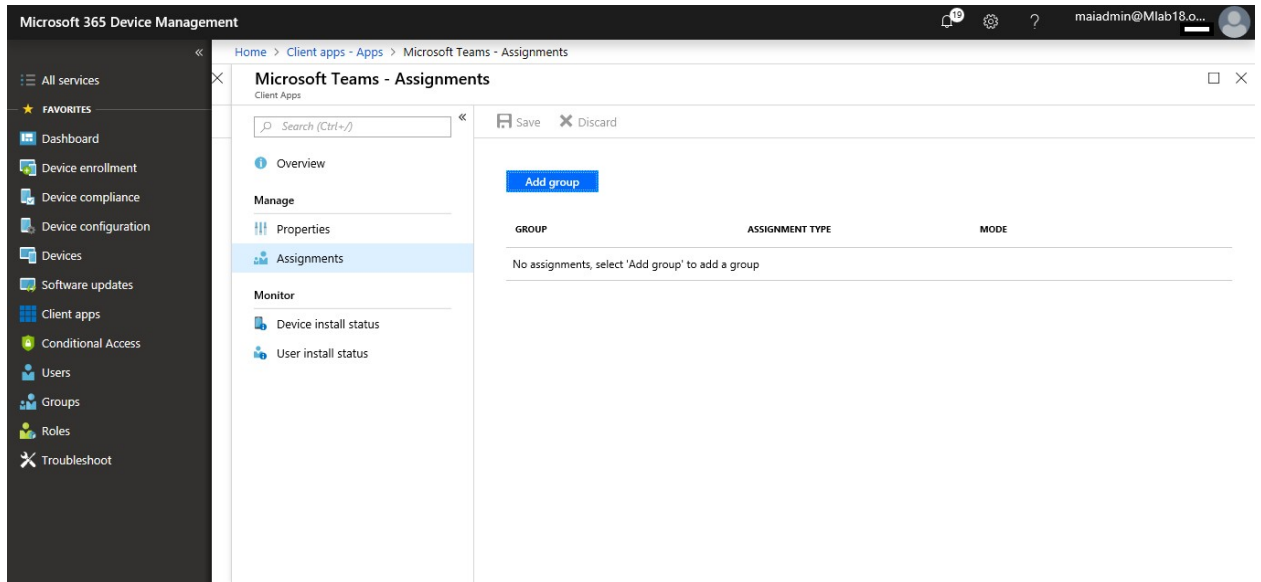
To assign specific group on Line of Business App

1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** menu, select **Client apps**.
3. In the **Manage** section of the menu, select **Apps**.
4. In the **Apps** pane, select the app you want to assign.
5. In the **Manage** section of the menu, select **Assignments**.

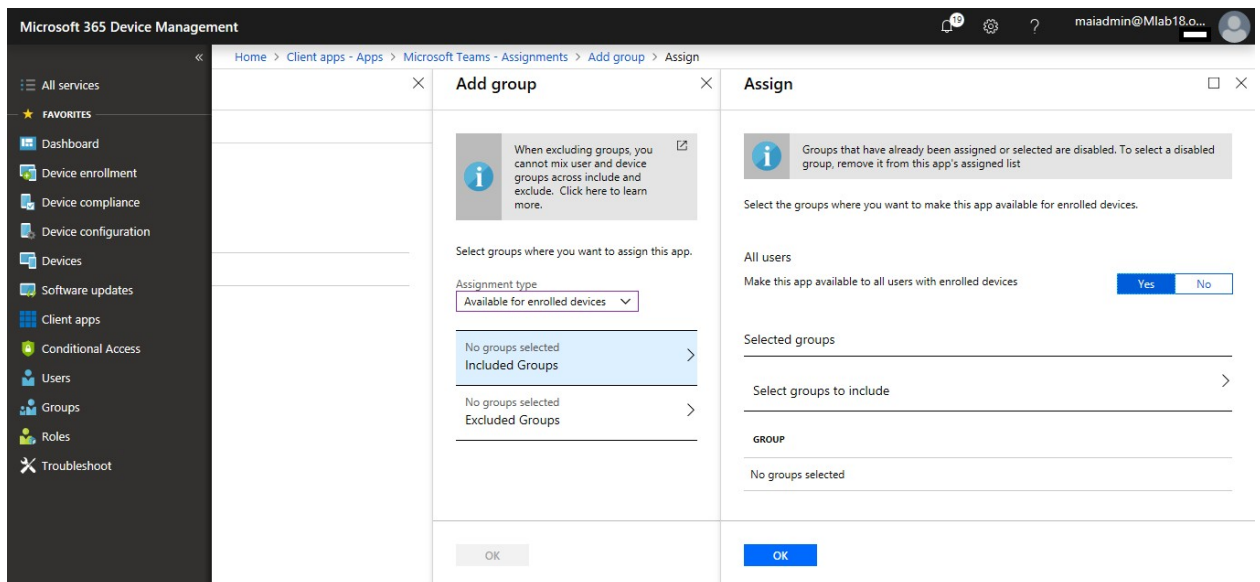


6. Select **Add Group** to open the **Add group** pane that is related to the app.

Microsoft Intune step by step on Azure portal

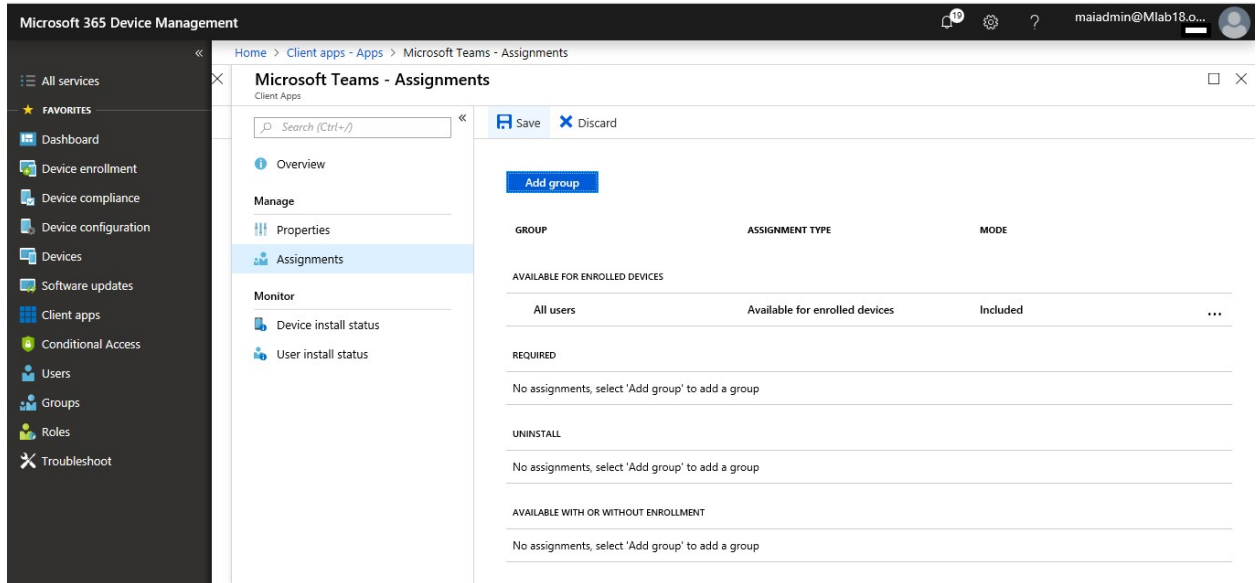


7. For the specific app, select an **assignment type**: Available for enrolled devices
8. To select the groups of users that are affected by this app assignment, select **Included Groups**. After you have selected one or more groups to include, Click **Select**.
9. In the **Assign** pane, select **OK** to complete the included groups selection.



10. In the app **Assignments** pane, select **Save**.

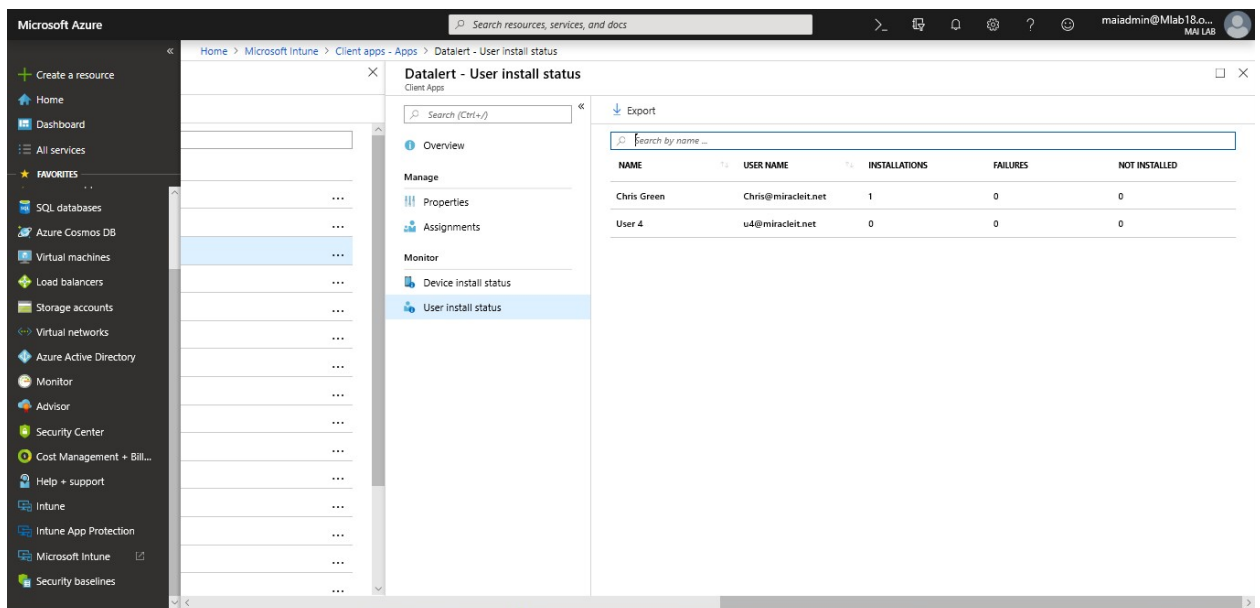
Microsoft Intune step by step on Azure portal



Monitor App

Intune provides several ways to monitor the properties of apps that you manage and to manage app assignment status.

1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** menu, select **Client apps** > **Apps**.
3. In the list of apps, select an app to monitor. You'll then see the app pane, which includes an overview of the device status and the user status.



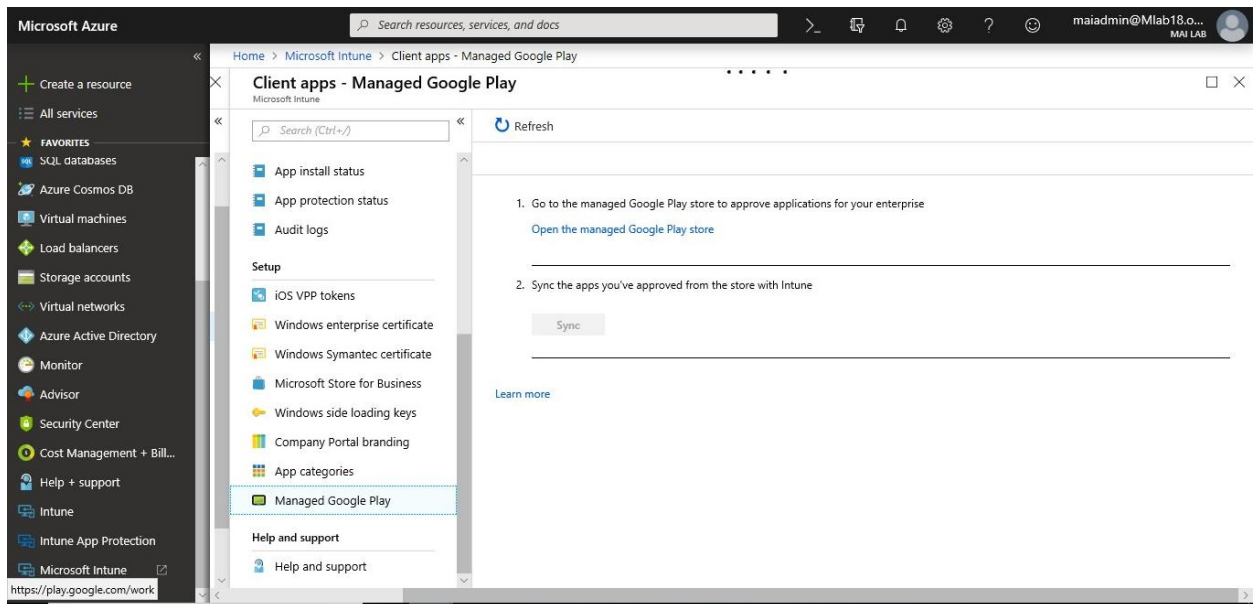
Note: Android apps deployed as **Available with or without enrollment** only report app installation status for enrolled devices. App installation status is not available for devices that are not enrolled in Intune.

Deploy App to Android Enterprise “Android for Work” Mobile Devices

Intune helps you deploy apps and settings to Android work profile devices to make sure work and personal information are separate. All apps you install on Android work profile devices come from the Managed Google Play store.

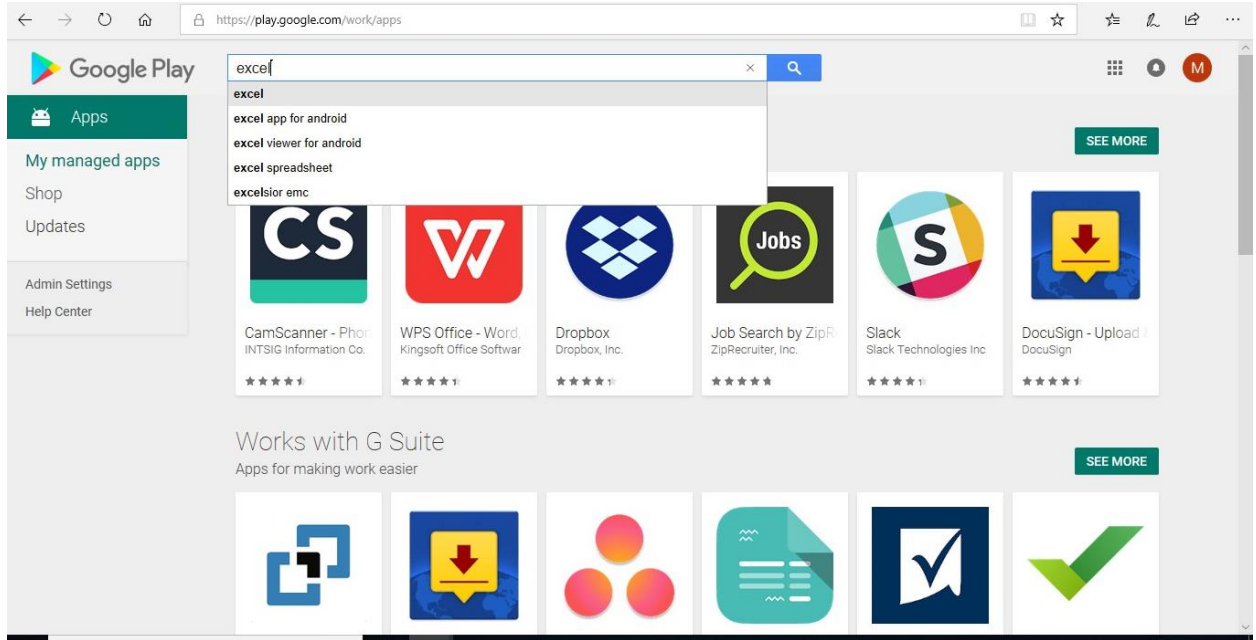
Setup Managed Google Play Store & Add App

1. Sign in to the [Intune in Azure Portal](#). Select **Client apps** workload pane, under **Setup**, select **Managed Google Play**.

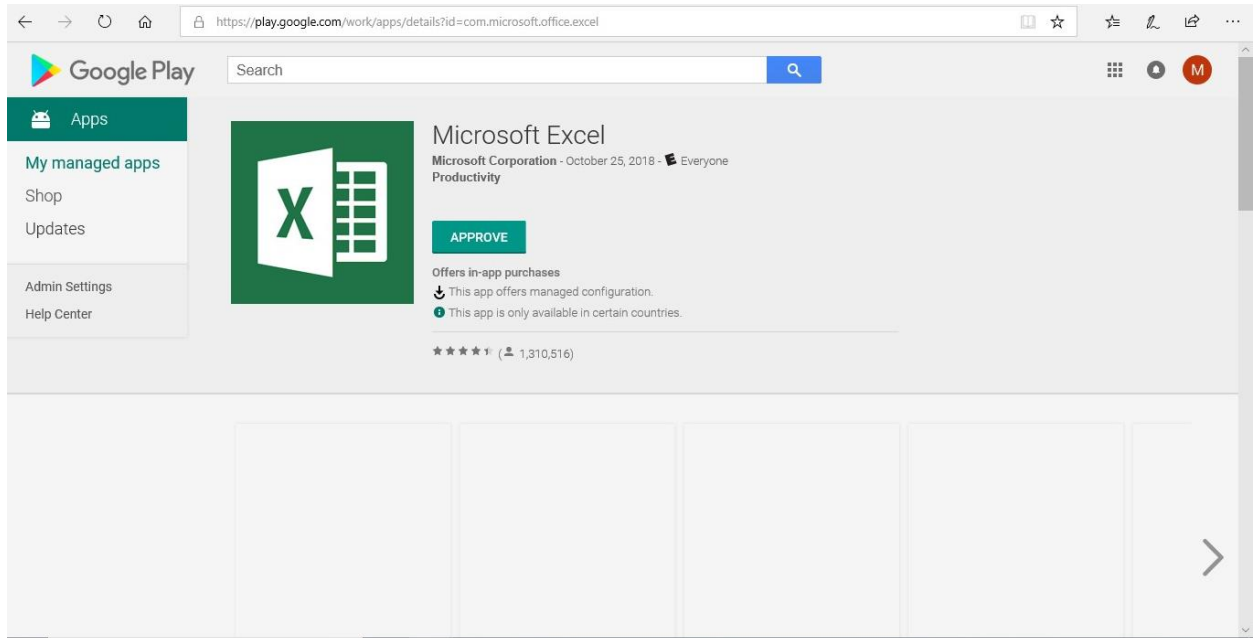


2. Go to the [Managed Google Play store](#). Sign in with the same account you used to configure the connection between Intune and Android enterprise.
3. Search the store and select the app you want to assign by using Intune.

Microsoft Intune step by step on Azure portal

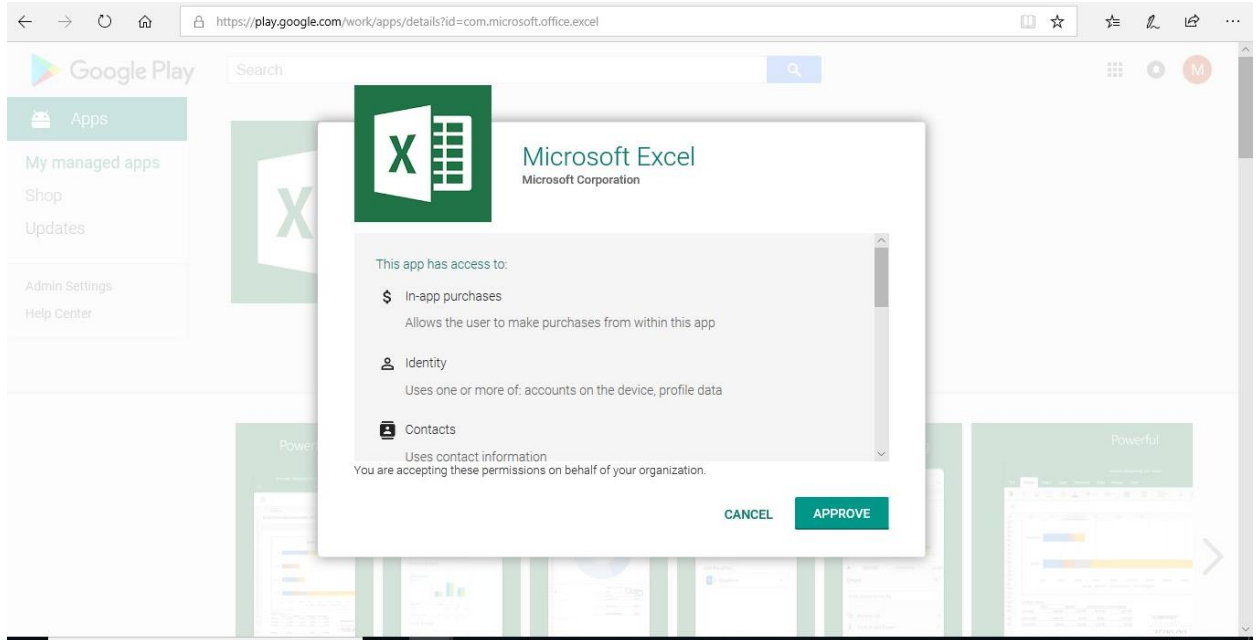


4. On the page that displays the app, select **Approve**.

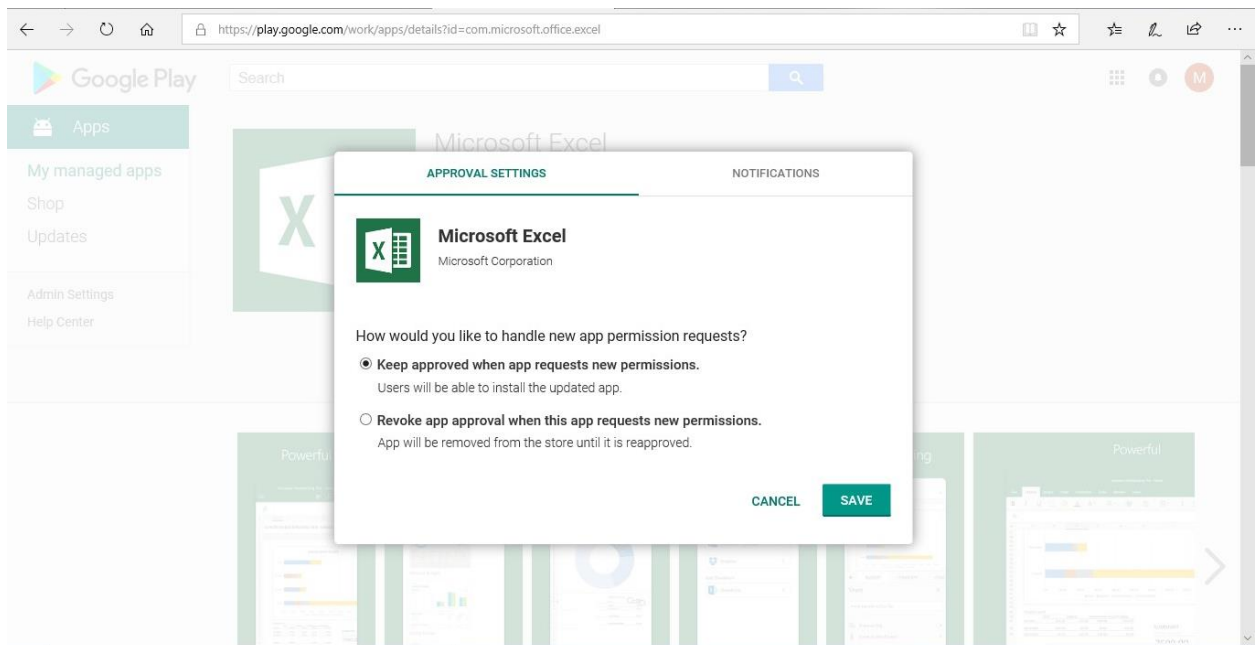


5. Select **Approve** to accept the app permissions and continue.

Microsoft Intune step by step on Azure portal



6. Select an option for handling new app permission requests, and then select **Save**.

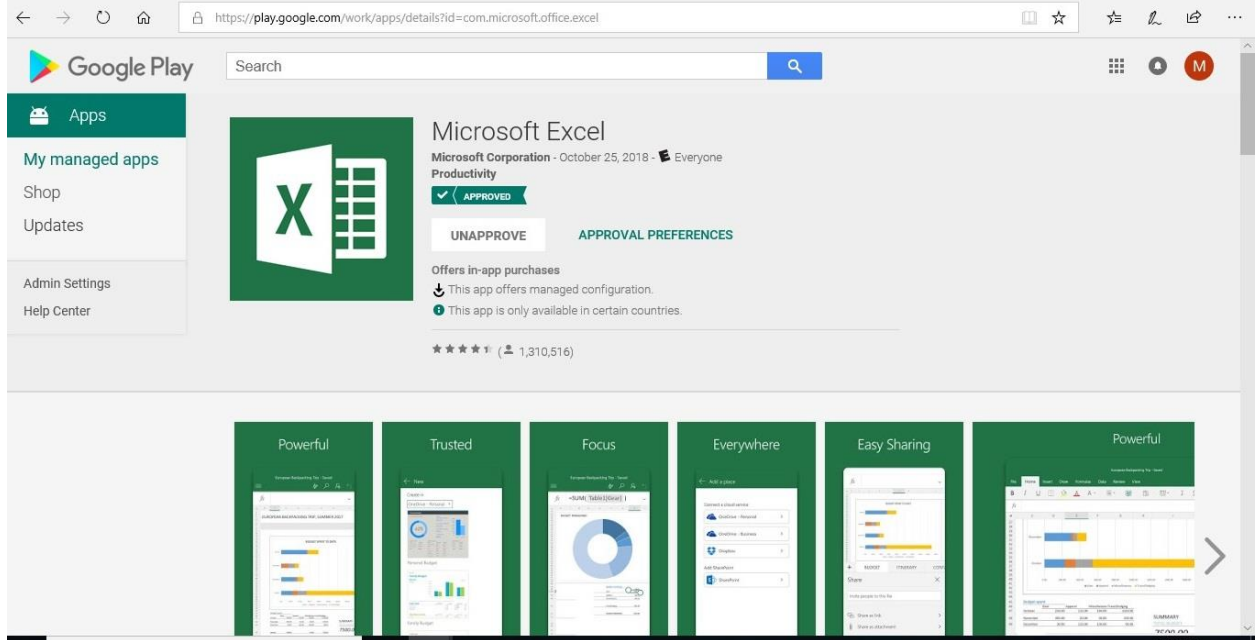


Note: If you choose option Keep approved, end user will see application on Managed play store. But if you choose option Revoke app, it will be silent deployment and app will remove from managed store. End user won't be able to get any update for this app.

7. The app is approved, and it is displayed in your IT admin console.

Note: After you approve the app, you should find all approved app on My managed apps.

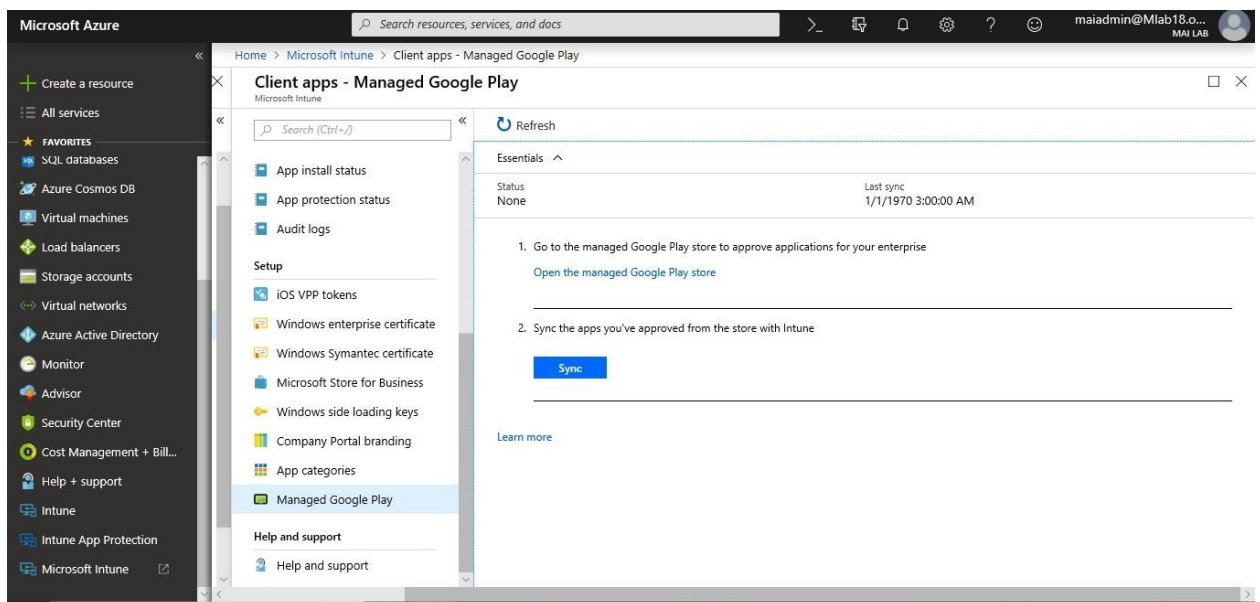
Microsoft Intune step by step on Azure portal



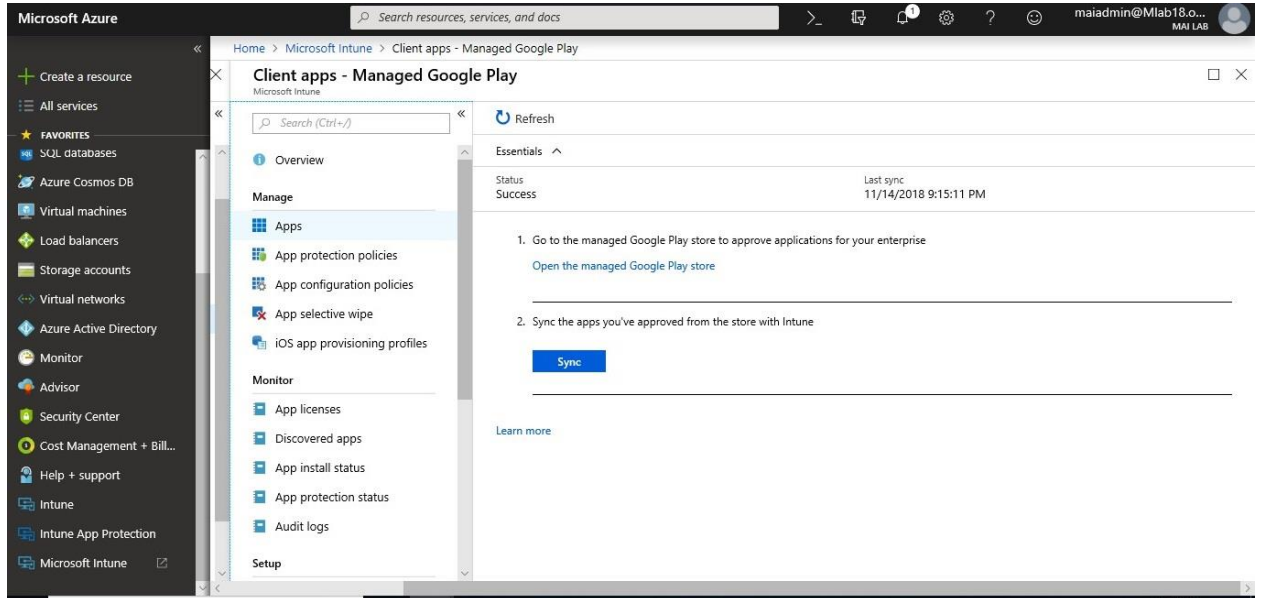
Synchronize Managed Google Play App with Intune

If you have approved an app from the store and don't see it in the **Licensed apps** node of the **Client apps** workload, force an immediate sync as follows:

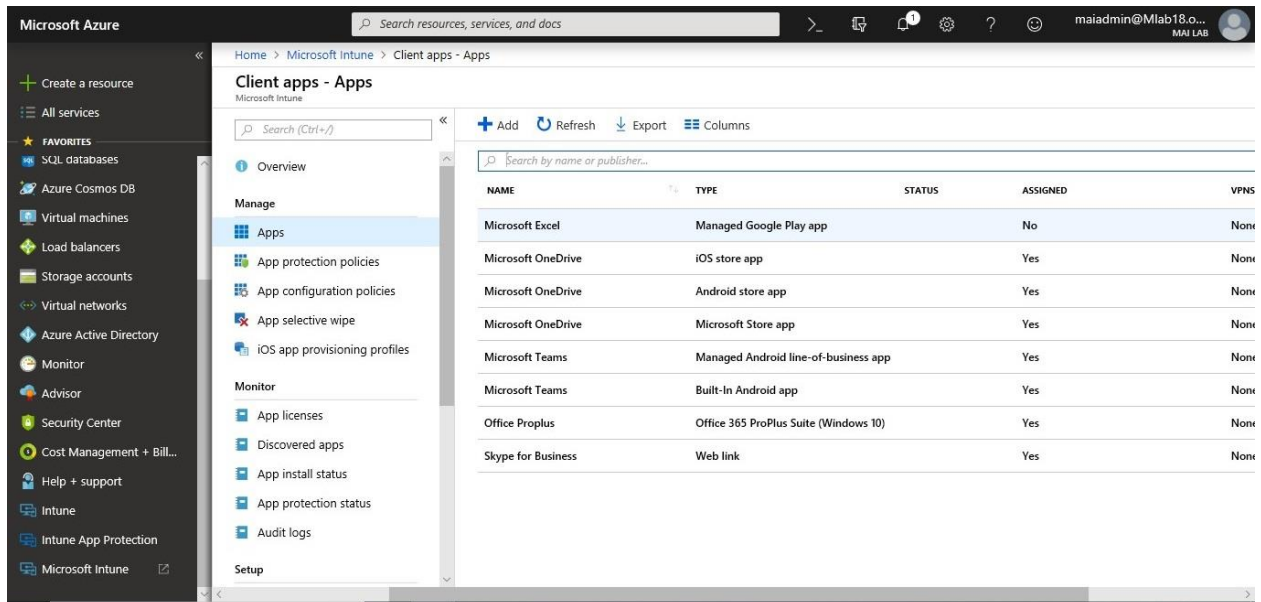
1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** pane, select **Client apps**.
3. In the **Client apps** workload pane, under **Setup**, select **Managed Google Play**.
4. In the **Managed Google Play** pane, Select **Sync**.



5. Choose **Refresh**. The page updates the time and status of the last sync.



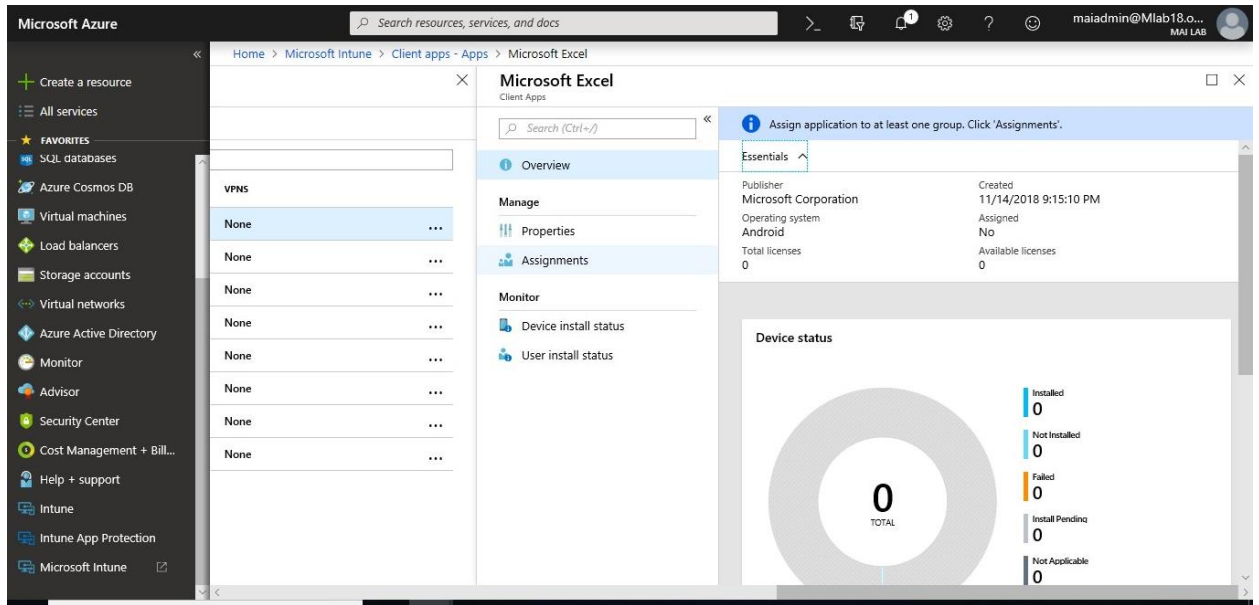
6. In the **Client apps** workload pane, select **App**.



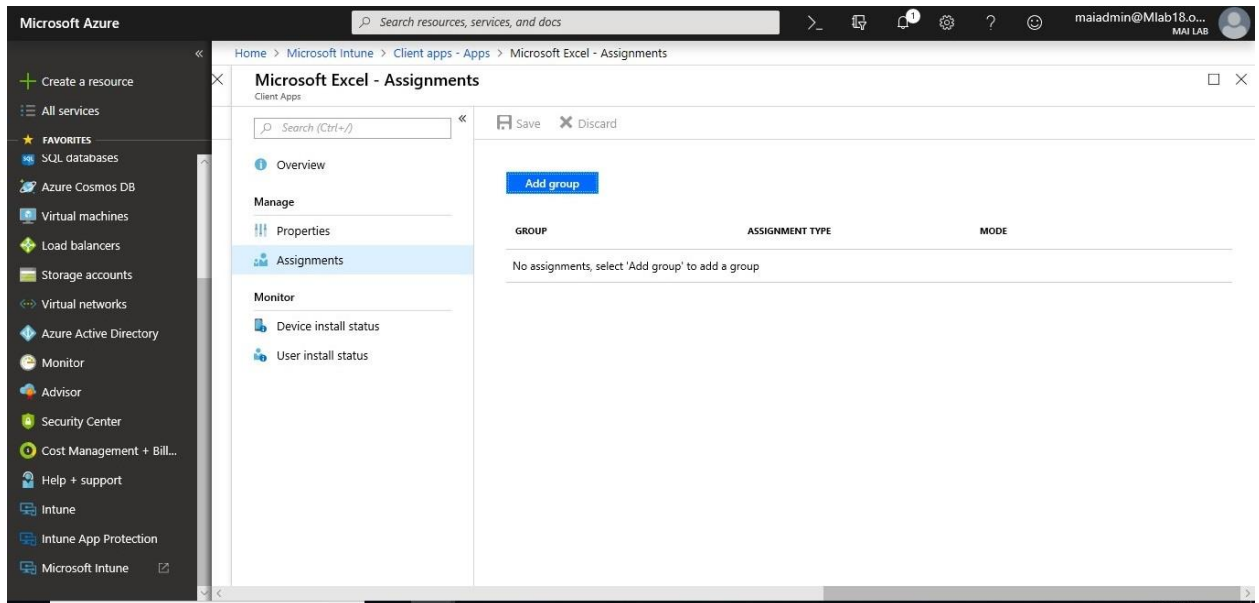
Assign Specific Group on Managed Google Play App.

1. Sign in to the [Intune in Azure portal](#). In the **Intune** menu, select **Client apps**.
2. In the **Manage** section of the menu, select **Apps**, select the app you want to assign.
3. In the **Manage** section of the menu, select **Assignments**.

Microsoft Intune step by step on Azure portal

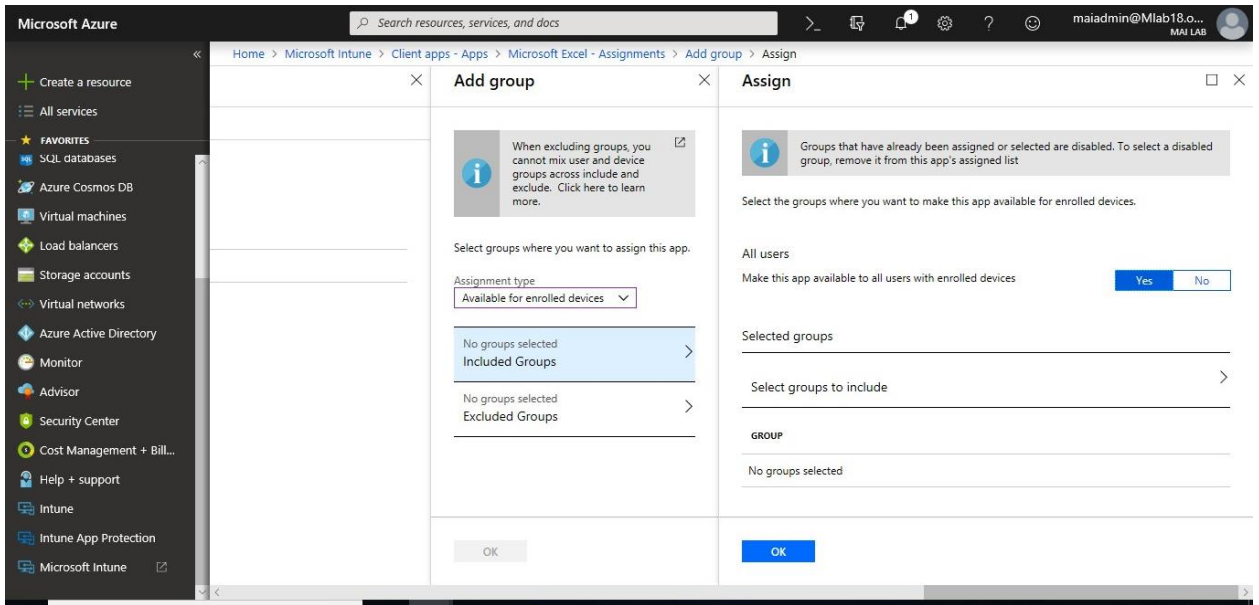


4. Select **Add Group** to open the **Add group** pane that is related to the app.

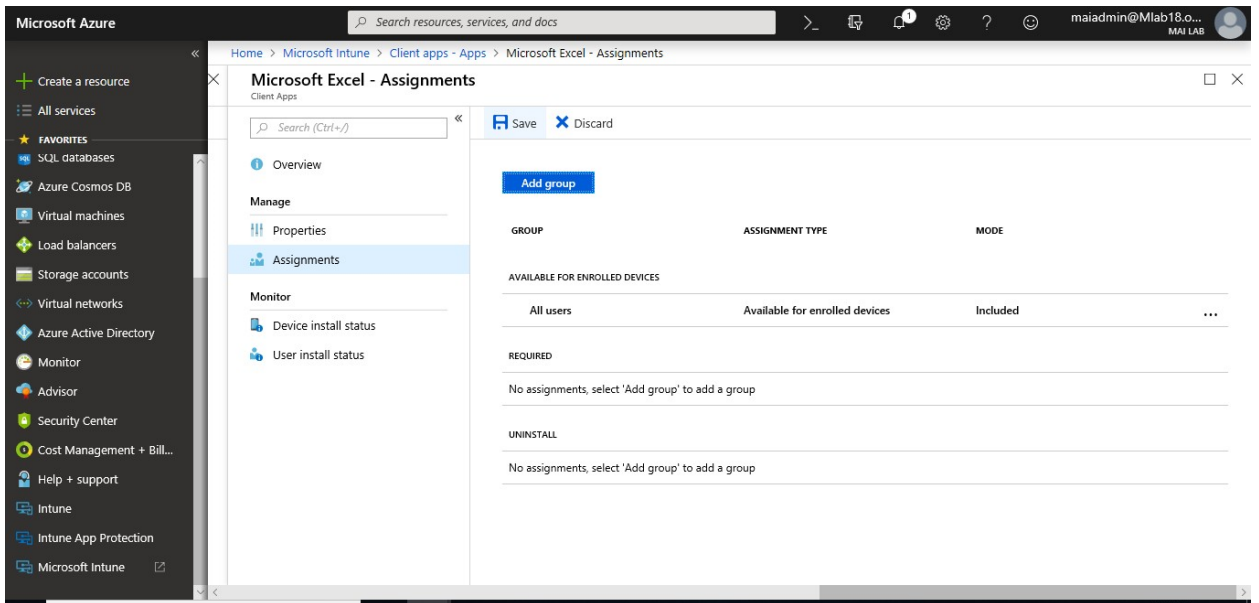


5. For the specific app, select an **assignment type**: Available for enrolled devices
6. To select the groups of users that are affected by this app assignment, select **Included Groups**. After you have selected one or more groups to include, Click **Select**.
7. In the **Assign** pane, select **OK** to complete the included groups selection.

Microsoft Intune step by step on Azure portal



8. In the app **Assignments** pane, select **Save**.



Chapter 7

Intune App Protection “Mobile Application Management”

You can use Microsoft Intune to manage the client apps that your company's workforce uses. This functionality is in addition to managing devices and protecting data. One of an admin's priorities is to ensure that end users have access to the apps they need to do their work. This goal can be a challenge because:

- There are a wide range of device platforms and app types.
- You might need to manage apps on both company devices and users' personal devices.
- You must ensure that your network and your data remain secure.

Mobile application management policies in Microsoft Intune let you modify the functionality of apps that you deploy to help bring them into line with your company compliance and security policies. For example, you can restrict cut, copy and paste operations within a managed app, or configure an app to open all web links inside a managed browser\Edge. MAM policies will only work with Managed Apps or line of Business Apps using Wrapped tool.

You can use Mobile Application Management (MAM) without enrolling a device to Intune MDM policies or even when the device is enrolled into a third-party MDM solution like Citrix or AirWatch.

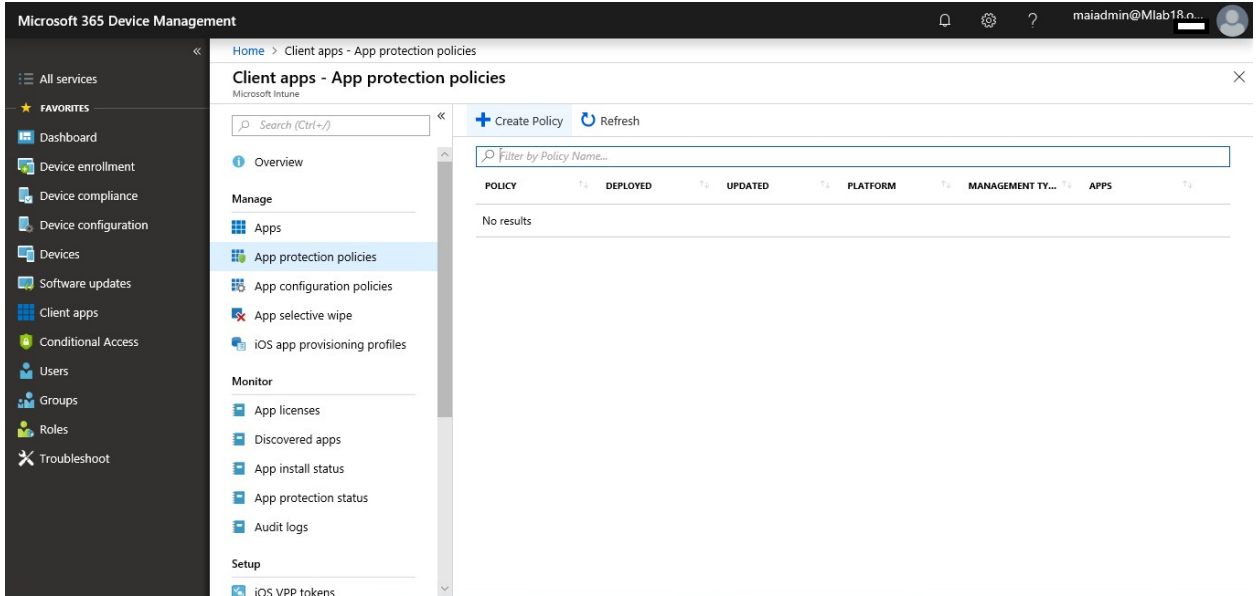
Note: Mobile application Management policy applied on Office 365 Apps like Exchange online, One Drive, SharePoint, Teams & Skype Online so that it required end user to have license for both **Office 365** and **Intune**.

iOS App Protection Policy

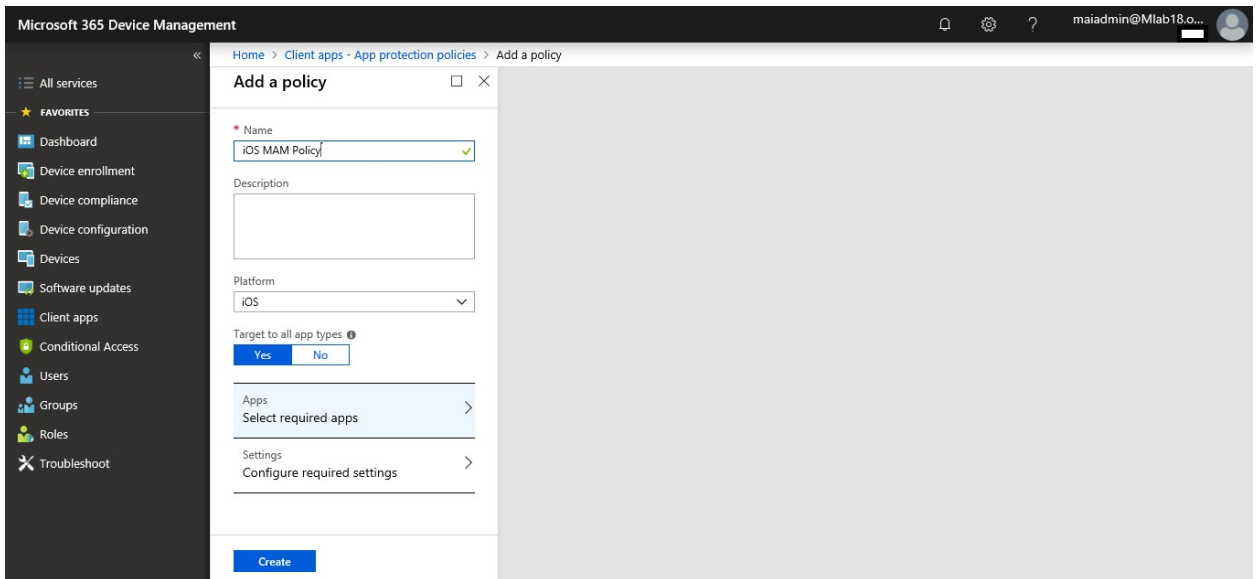
In this topic, we will configure restriction policy on Managed application to prevent end user from copy or cut from managed app “Outlook, Teams” to unmanaged app “Facebook, or WhatsApp”. Also restrict save as location to only save on OneDrive & SharePoint Online. Use Pin code or fingerprint to access managed app.

Create an app protection policy using access actions

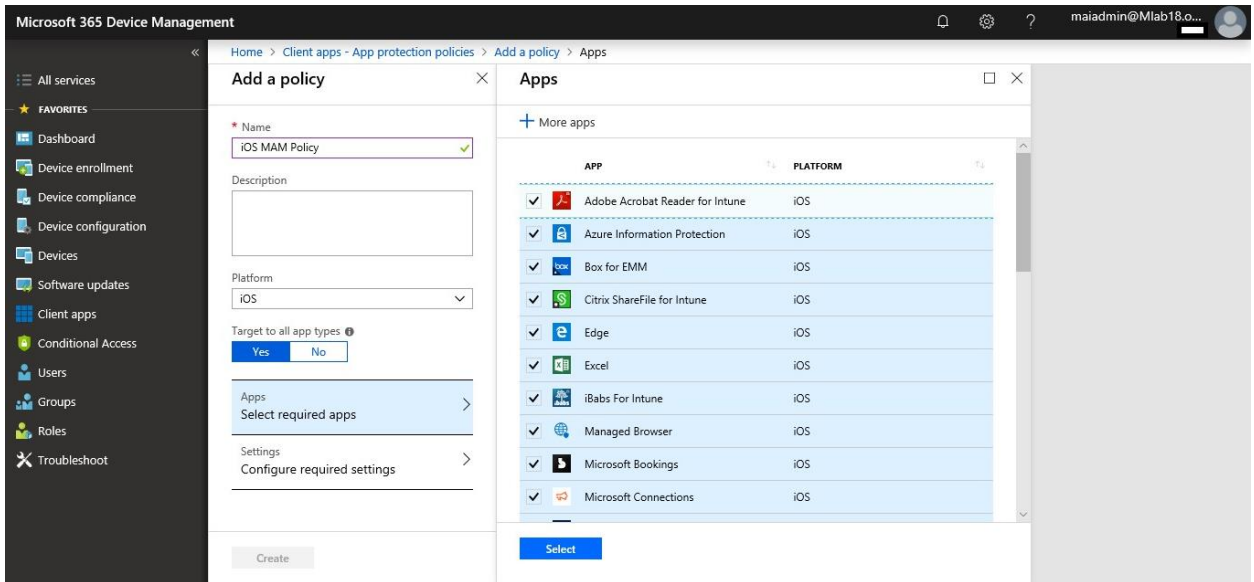
1. Sign in to the [Azure portal](#). Select **All services > Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** pane, select **Client apps > App protection Policies**.
3. Click **Create a policy** (You can also edit an existing policy).



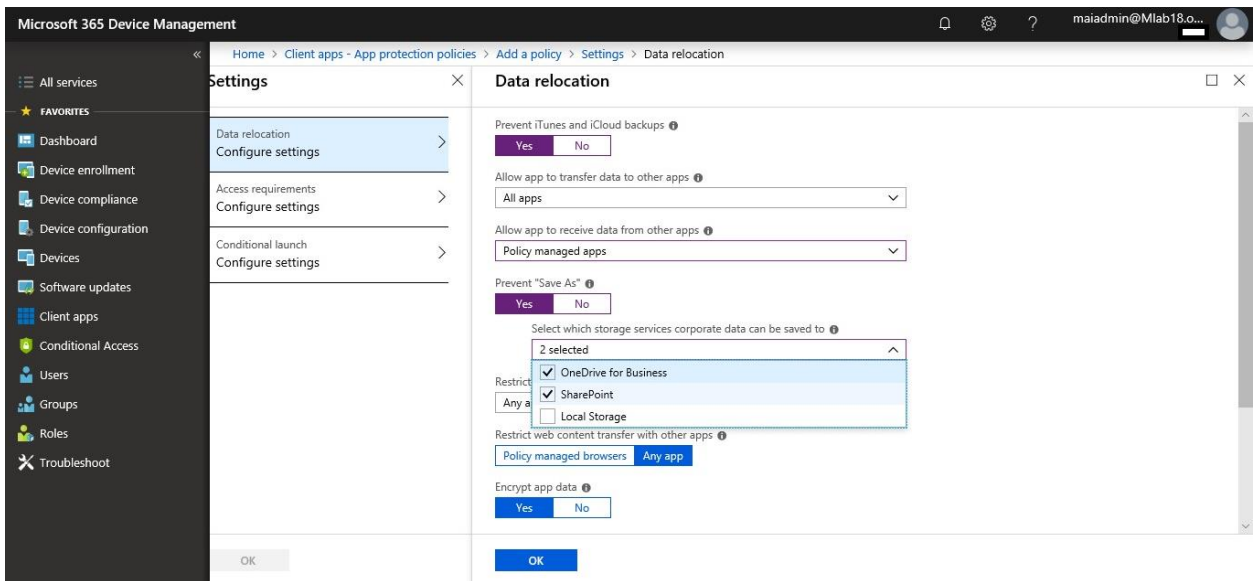
4. Type Policy Name and Select Platform.



5. Select Required App.

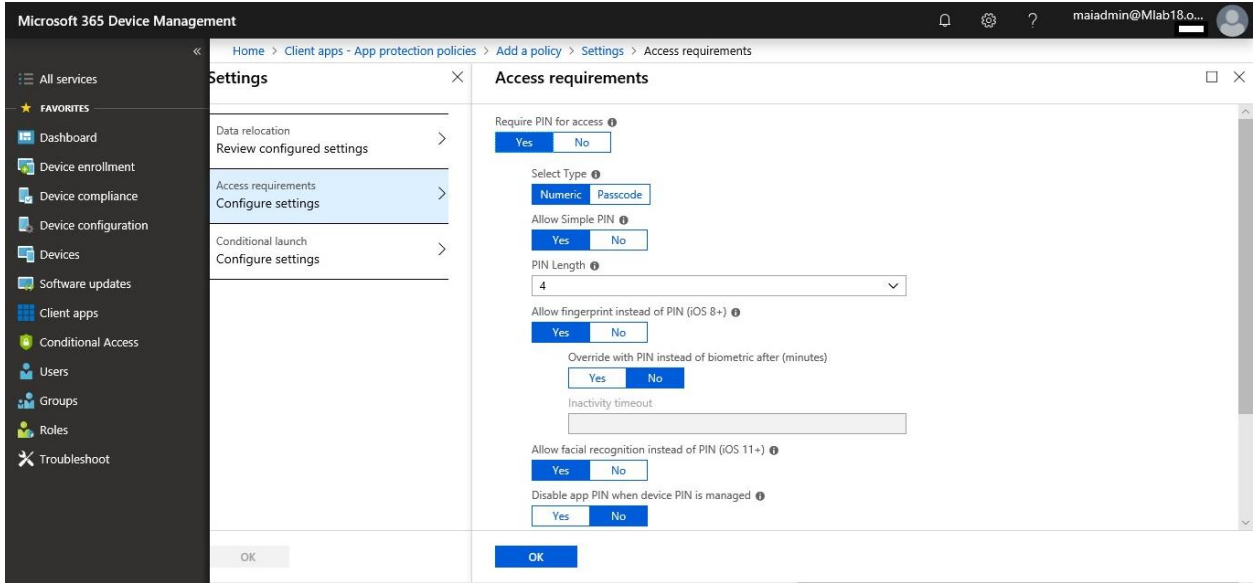


6. Click **Configure required settings** to see the list of settings available to be configured for the policy.
7. Select **Data relocation**, set policy as required on your environment.

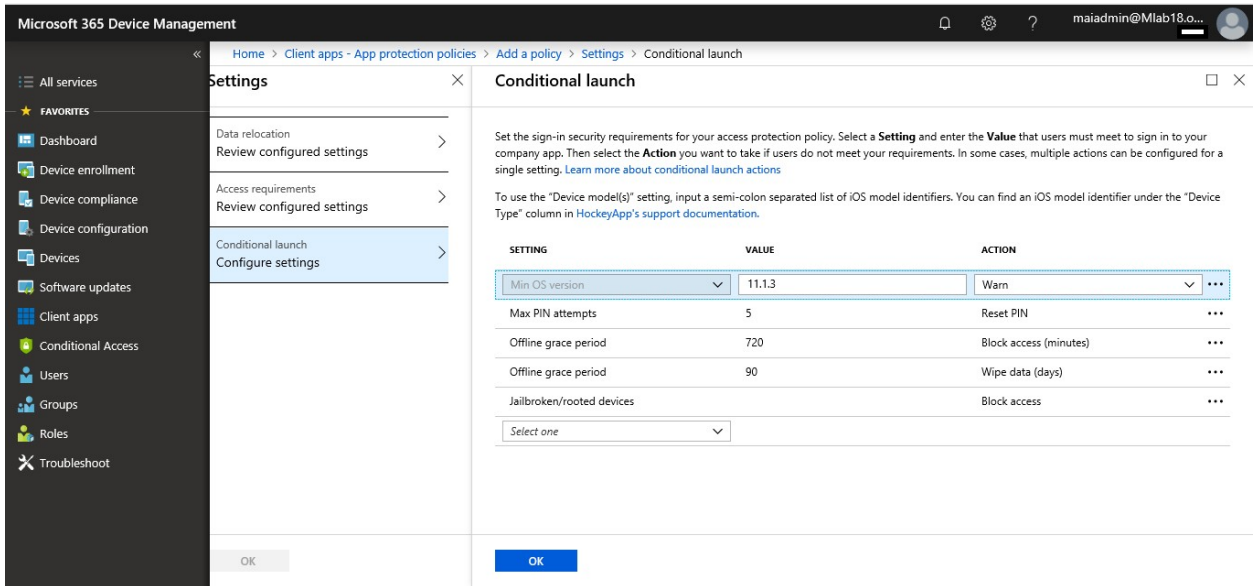


Note: If iOS phone doesn't have any password on device, when you enable encrypt app data, will force end user to configure password on device because encryption on app data happened when device lock. So, if you don't want to have password on device, disable encrypt feature.

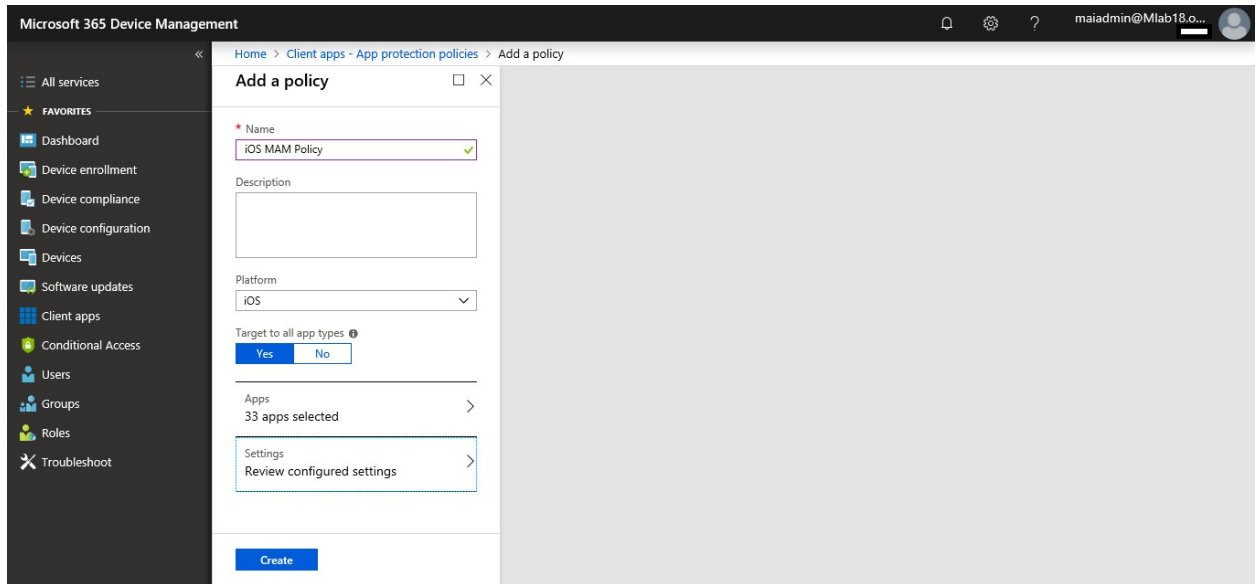
8. Select **Access requirement**, enable require PIN for access and allow fingerprint.



9. Select **Conditional Launch**.



10. Click **Create**.



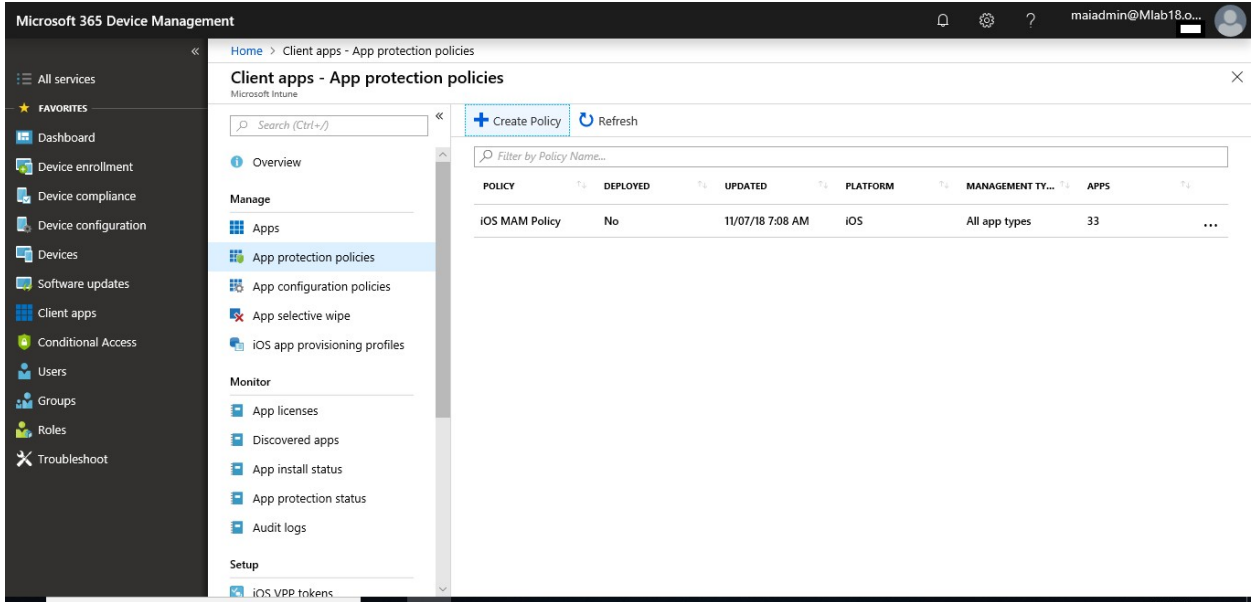
Note: MAM policy for iOS don't block screen capture on managed app as Android. Until now, this feature not exist on iOS. **MAM WE for iOS** will require end user to configure the **Microsoft Authenticator app**.

Android App Protection Policy

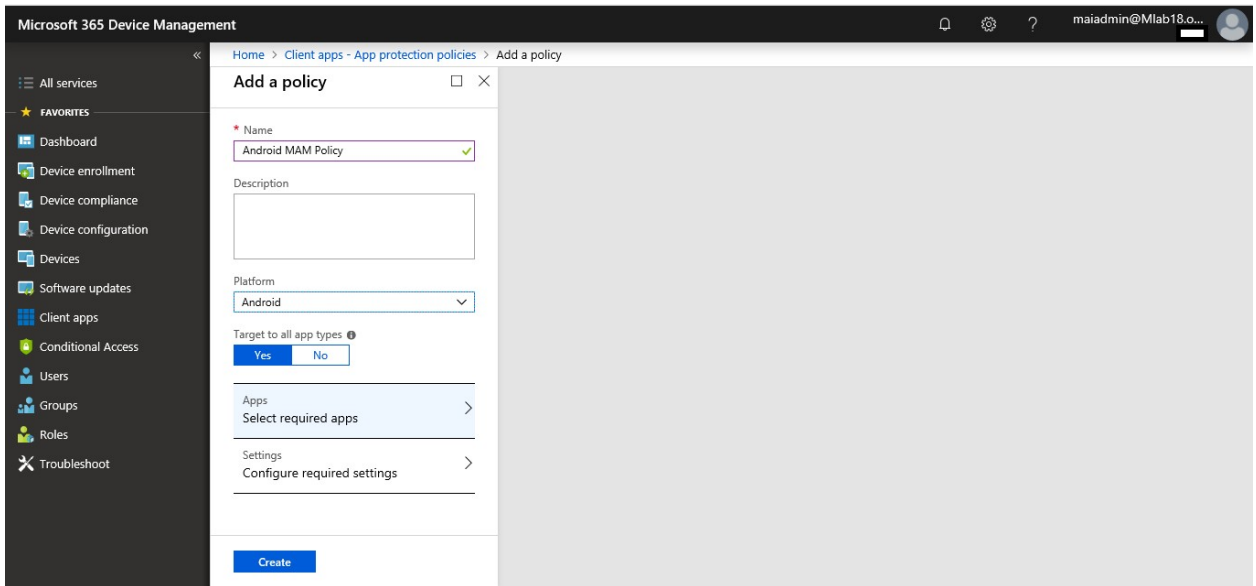
In this topic, we will configure restriction policy on Managed application to prevent end user from copy or cut from managed app "Outlook, Teams" to unmanaged app "Facebook, or WhatsApp". Also restrict save as location to only save on OneDrive & SharePoint Online and prevent screenshot on managed App. Use Pin code or fingerprint to access managed app.

Create an app protection policy using access actions

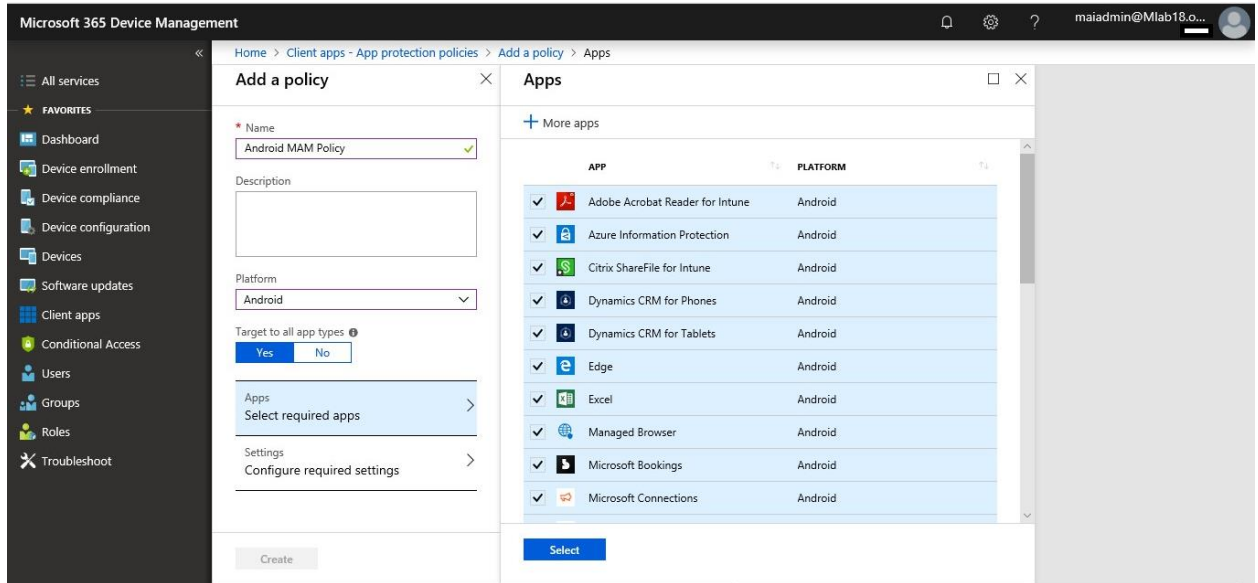
1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** pane, select **Client apps** > **App protection Policies**.
3. Click **Create a policy** (You can also edit an existing policy).



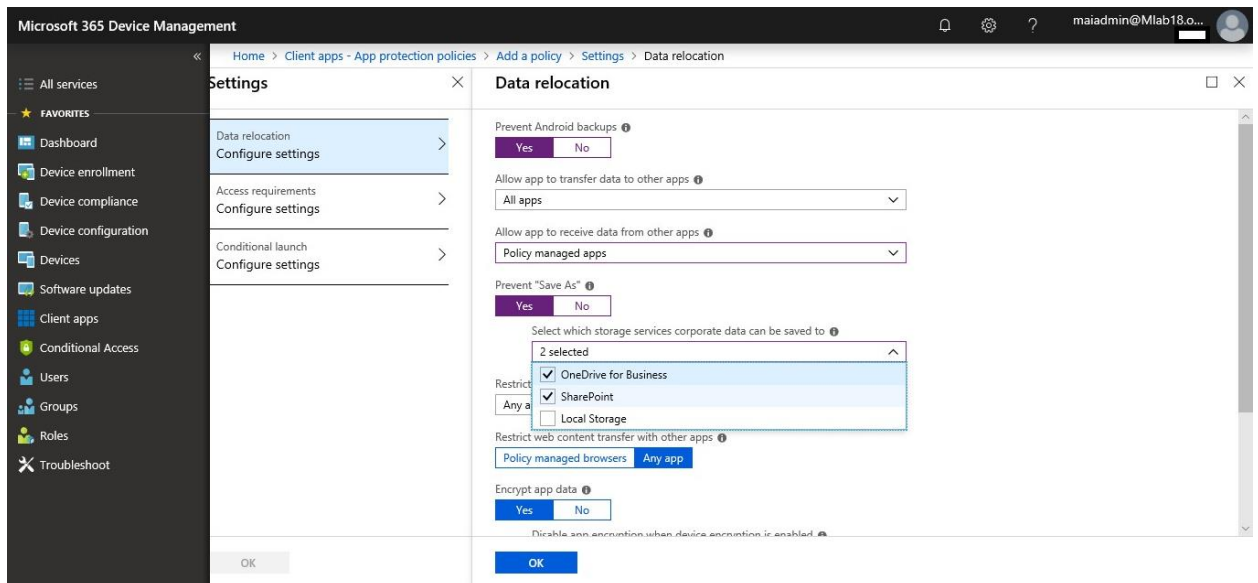
4. Type Policy Name and Select Platform.



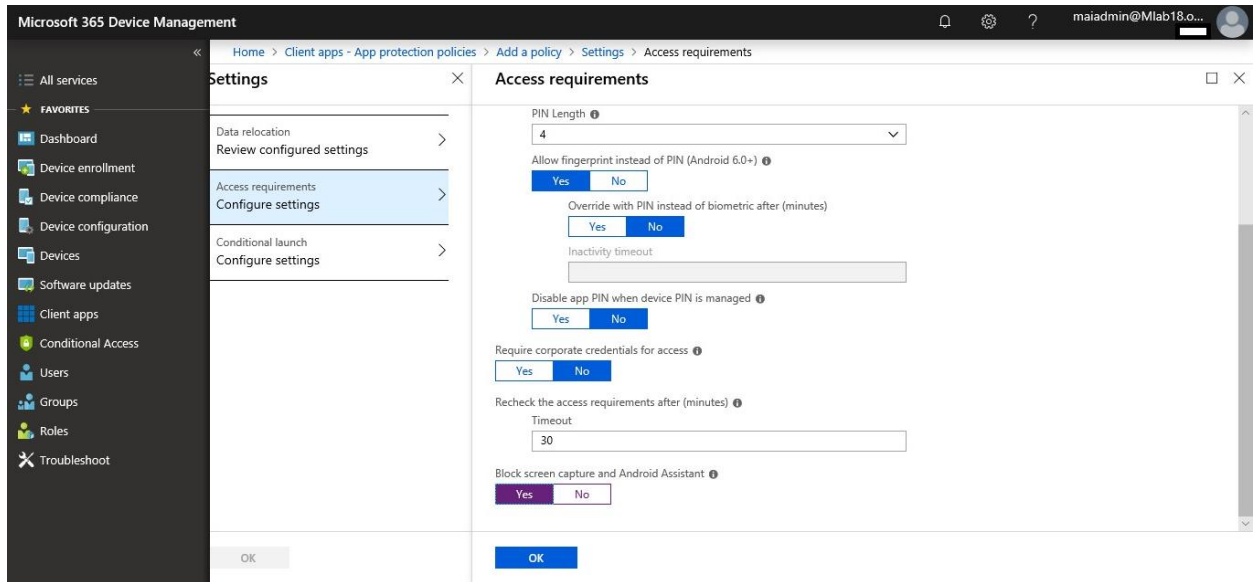
5. Select Required App.



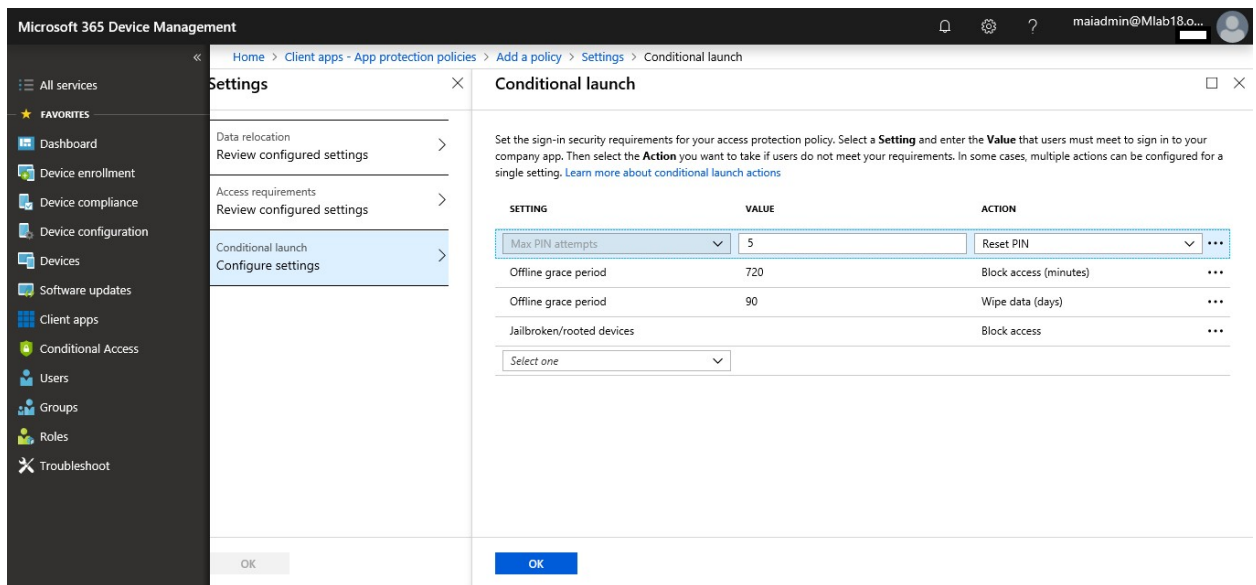
6. Click **Configure required settings** to see the list of settings available to be configured for the policy.
7. Select **Data relocation**, set policy as required on your environment.



8. Select **Access requirement**, enable require PIN for access and allow fingerprint. Select **Block Screen Capture**.



9. Select Conditional Launch.



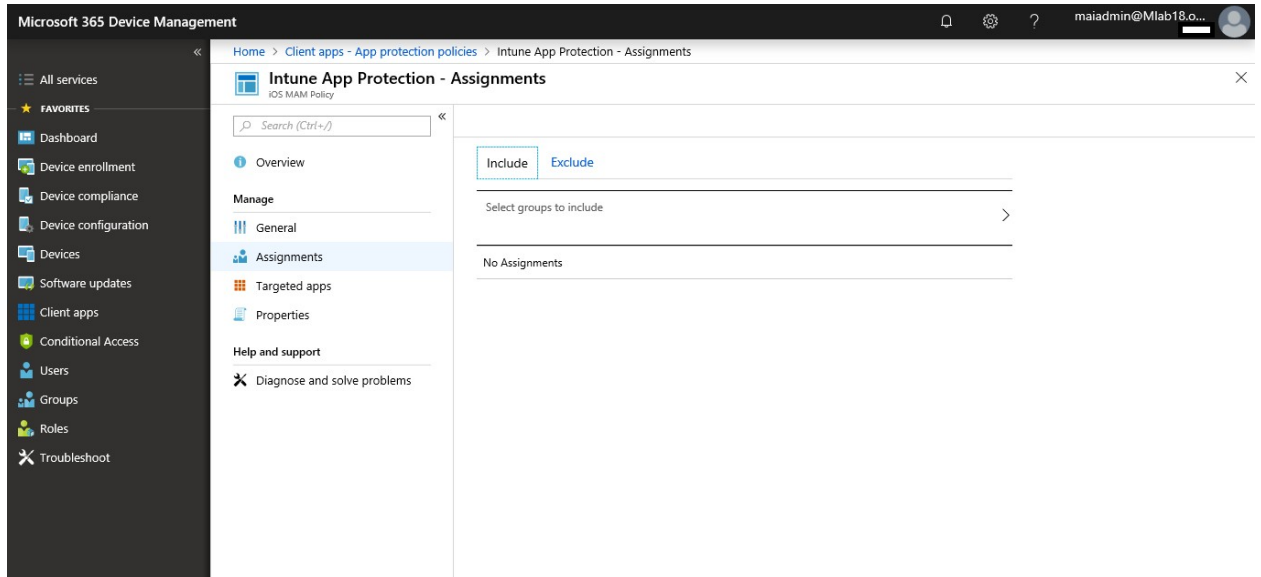
10. Click Create.

Note: MAM WE for Android will require end user to install Intune company portal without need to sign in.

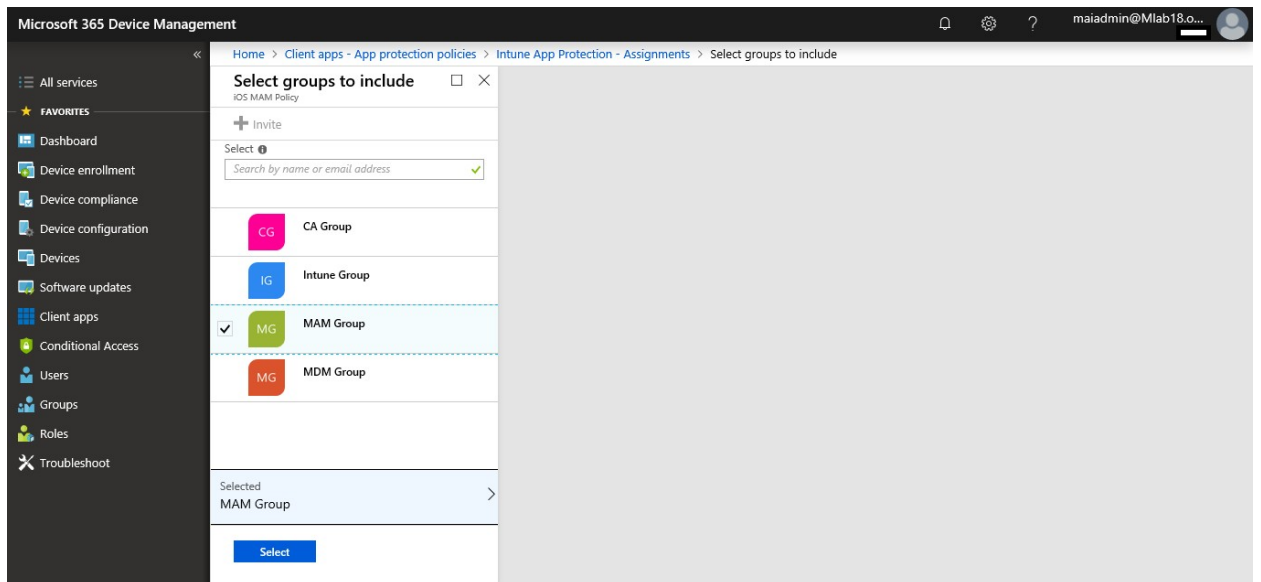
To assign specific group on App Protection policy

1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** pane, select **Client apps** > **App protection Policies**
3. In the **App protection policies** pane, select a policy.

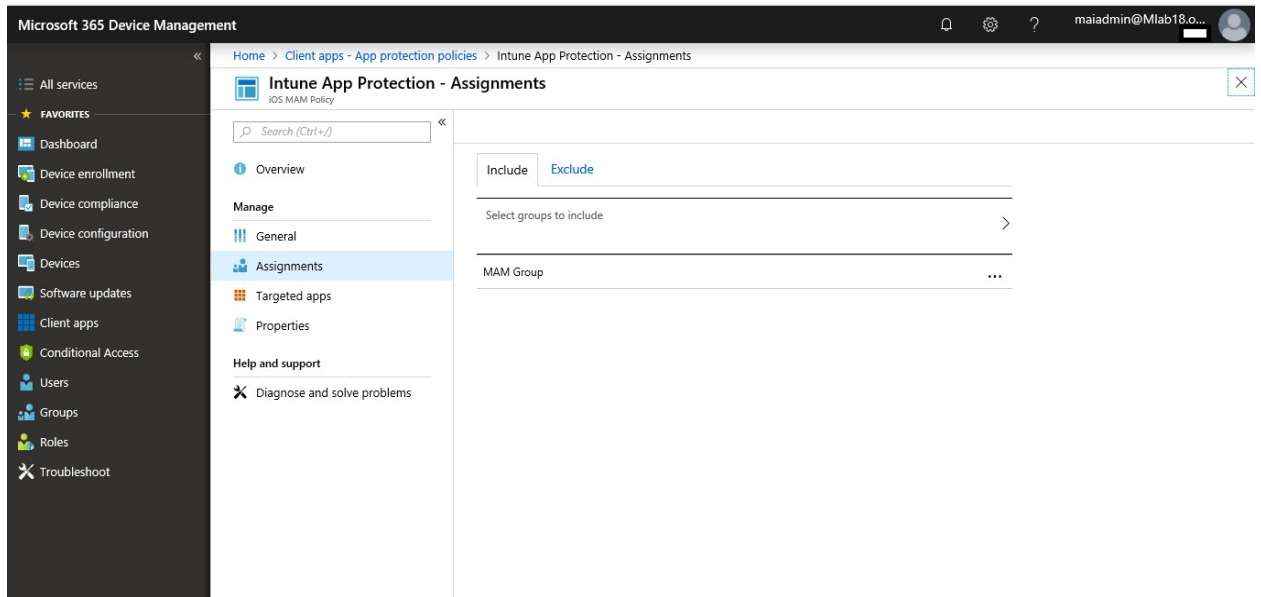
4. In the **Intune App Protection** pane, select **Assignments** to open the **Intune App Protection - Assignments** pane.



5. On the **Include** tab, select **Select groups to include**.



6. Click **X** to close this tab.

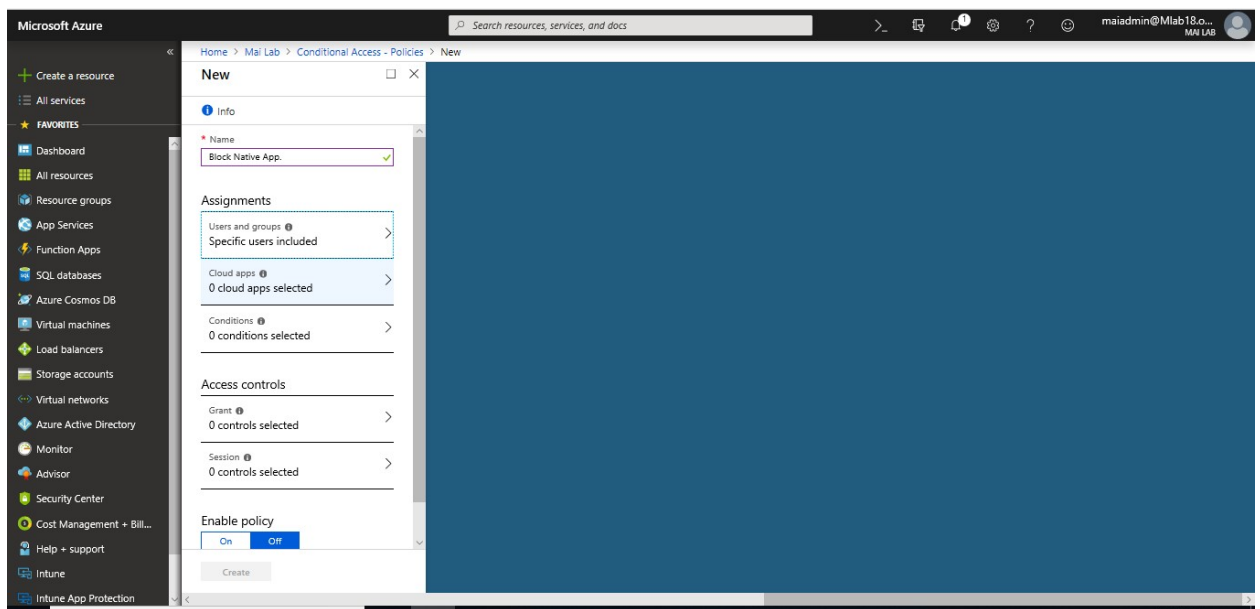


Enforce users to use Managed App. on Mobile devices

The conditional access policy blocks access to resources on Mobile devices *if* the device doesn't use Microsoft Approved App. So, if a device uses native app or third-party app, you can block access to corporate resources, such as SharePoint or Exchange Online.

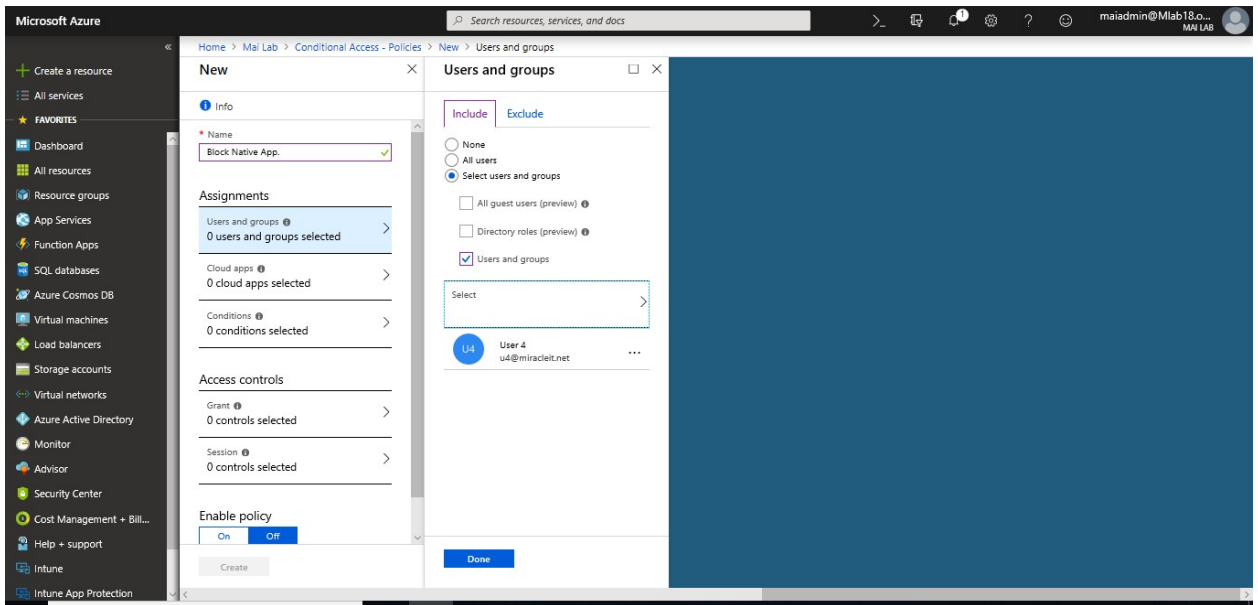
To Create Conditional Access Policy on Cloud App using managed App., you can follow below steps

1. In the [Azure portal](#), open **Azure Active Directory > Conditional access > New policy.**

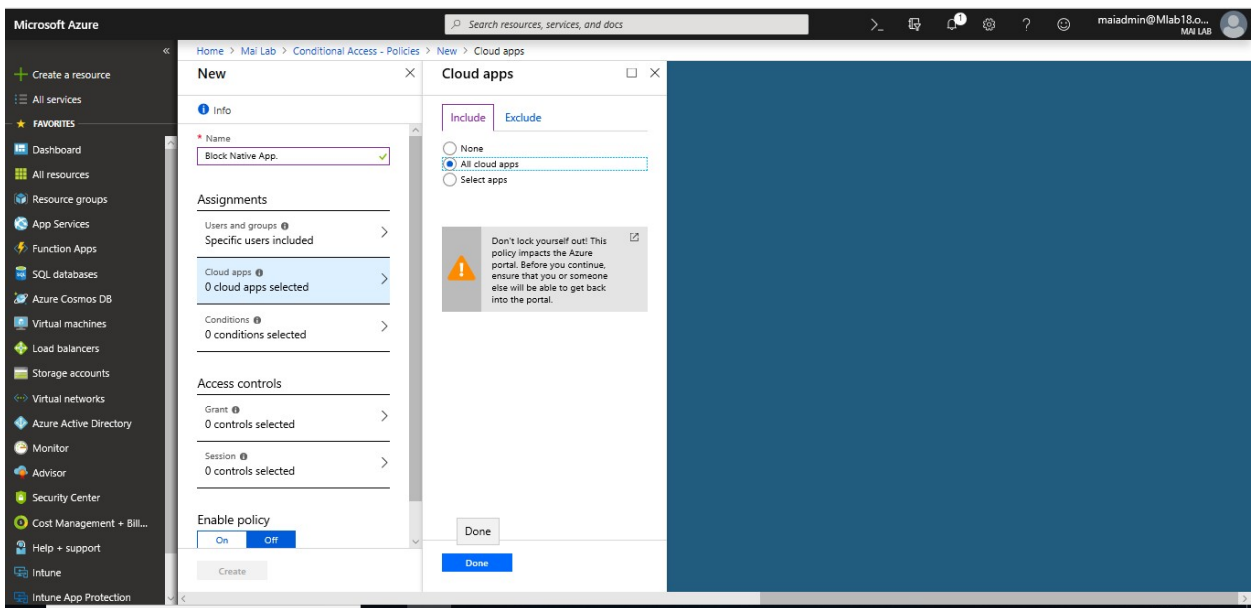


Microsoft Intune step by step on Azure portal

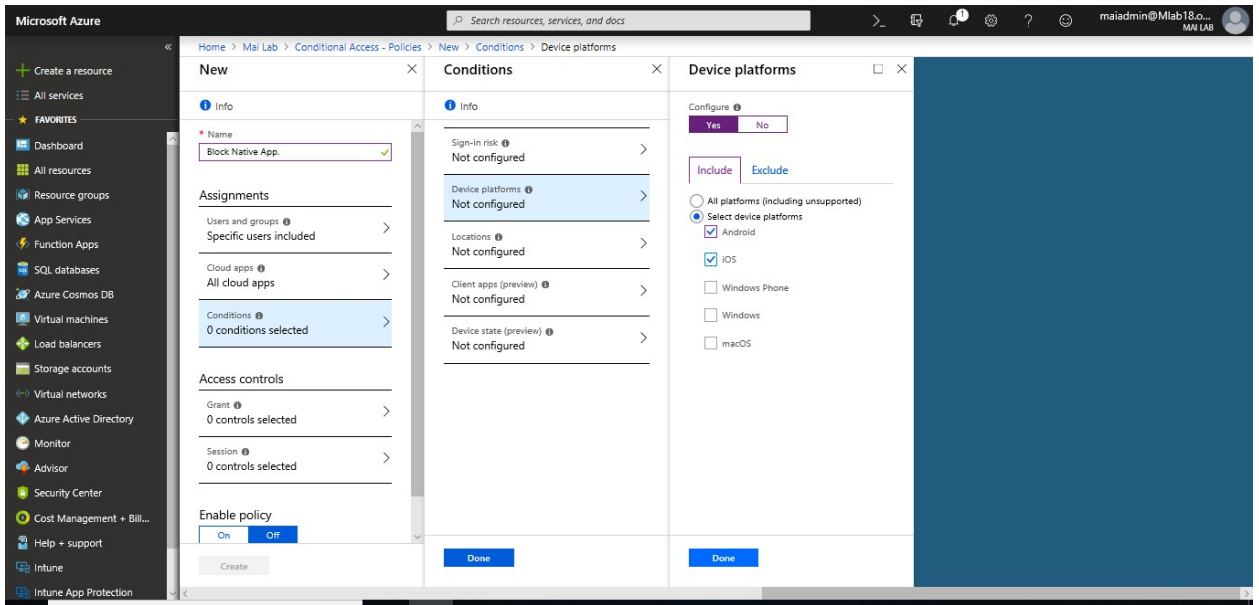
2. Enter a policy **Name** and select **Users and groups**. Use the Include or Exclude options to add your groups for the policy and select **Done**.



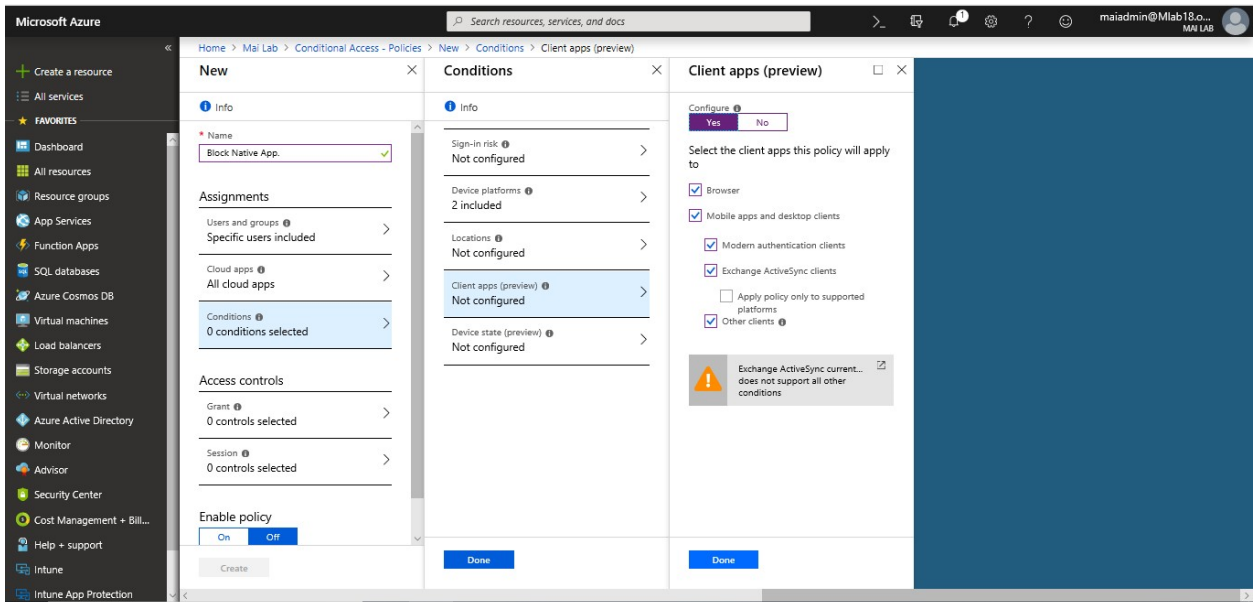
3. Select **Cloud apps** and choose which apps to protect. For example, choose **All cloud apps**. Select **Done** to save your changes.



4. Select **Conditions** > **Devices Platform** to apply policy “**Android, iOS**”

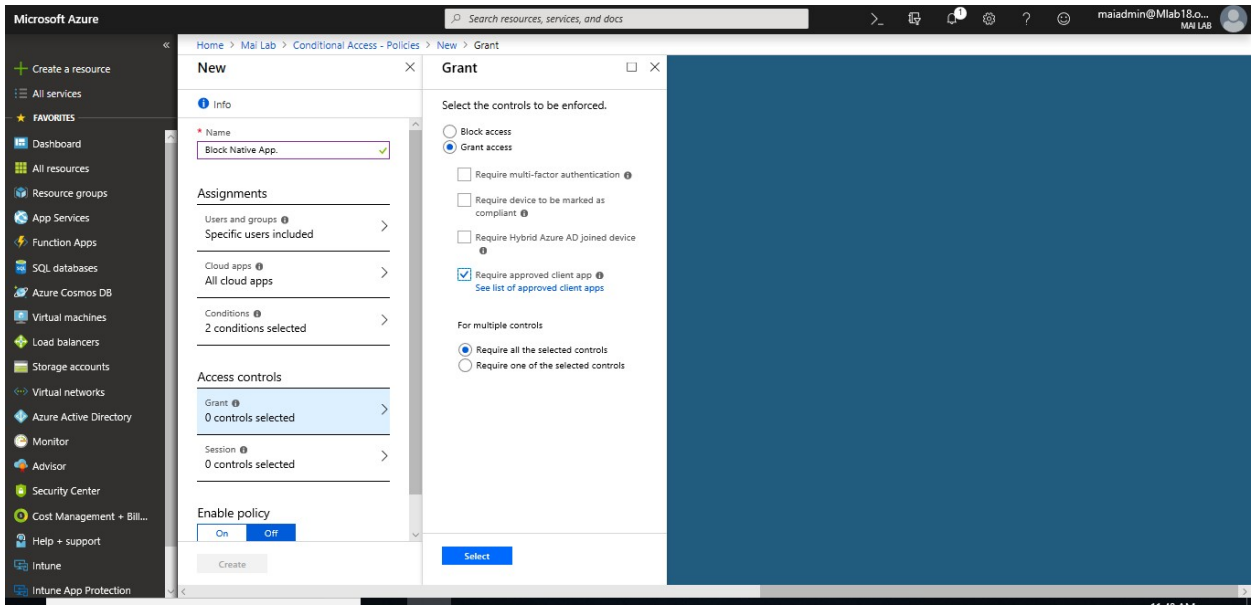


5. Select **Conditions** > **Client apps** to apply the policy to apps and browsers. For example, select **Yes**, and then enable **Browser** and **Mobile apps and desktop clients**. Select **Done** to save your changes.

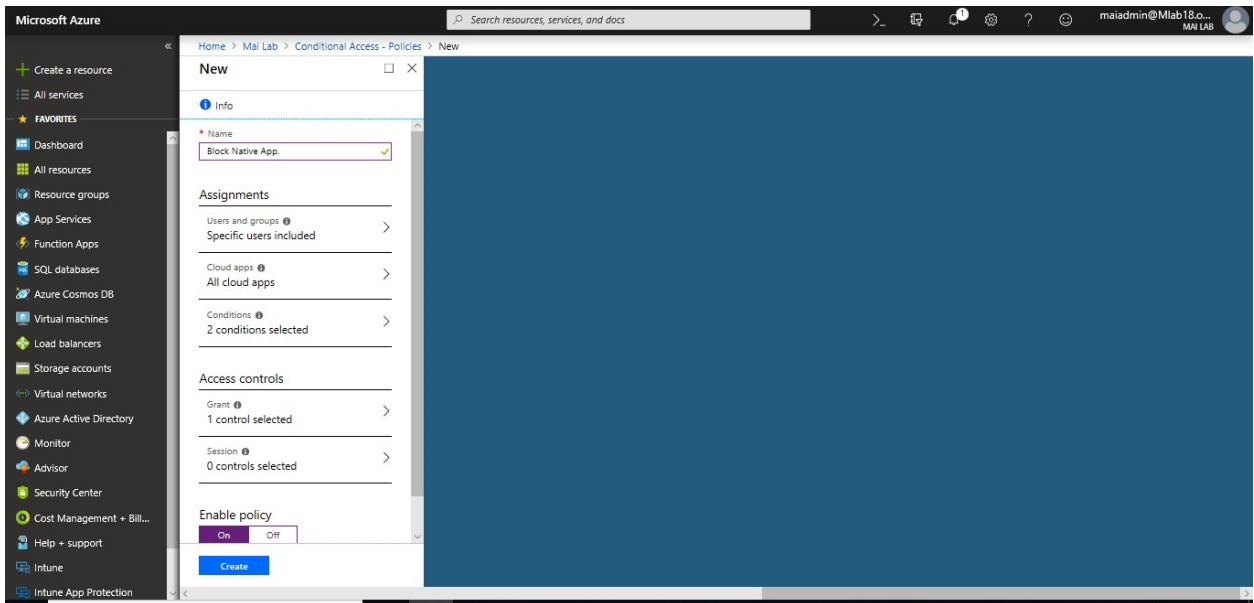


6. Select **Grant** to apply conditional access based on device compliance. For example, select **Grant access** > **Require approved client app**. Choose **Select** to save your changes.

Microsoft Intune step by step on Azure portal



7. Select **Enable policy**, and then **Create** to save your changes.



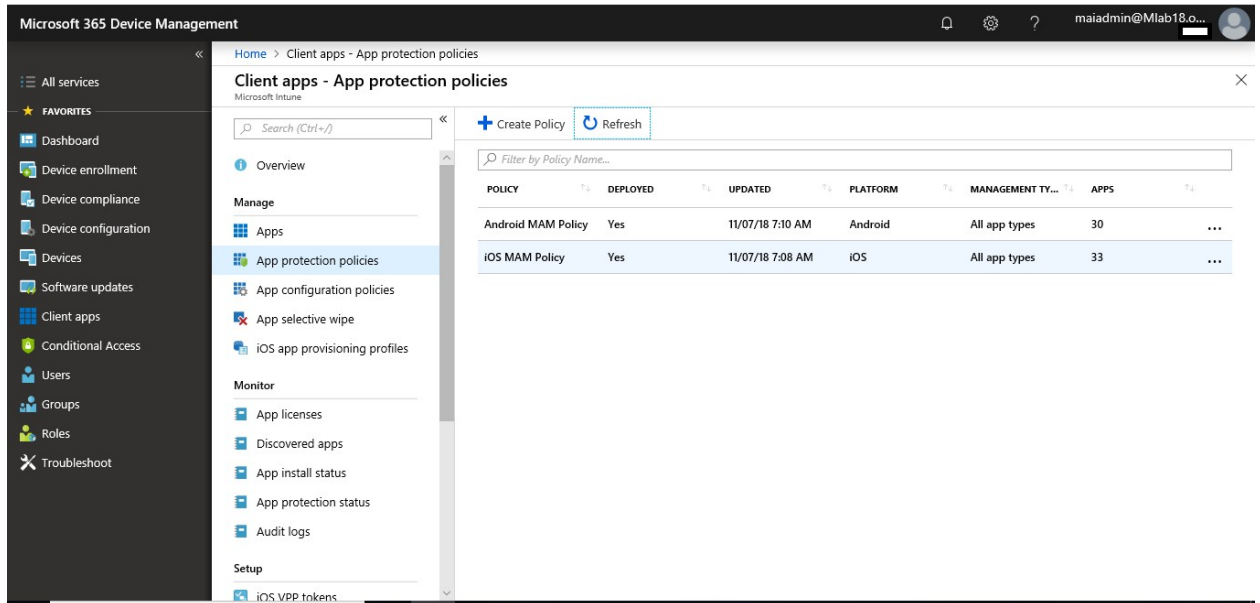
Windows Information Protection (WIP) App Protection policy

In this topic, we will configure restriction policy on Managed application to prevent end user from copy or cut from managed app “SharePoint” to unmanaged app “chrome”. Use windows hello for Business as a method for signing into Windows.

You can create a WIP-specific policy as below.

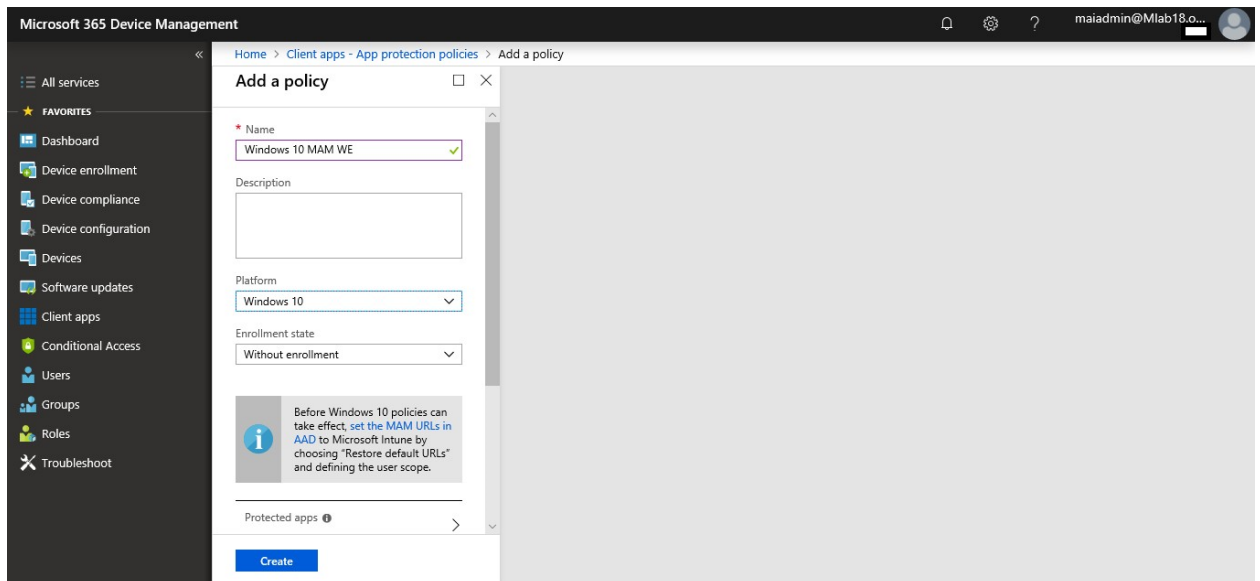
1. Sign in to the [Azure portal](#). Choose **All Services** > **Intune**.
2. Select **Client apps** on the **Microsoft Intune** blade.

3. Select **App protection policies** on the **Client apps** blade.
4. Select **Create a policy** to display the **Add a policy** blade.



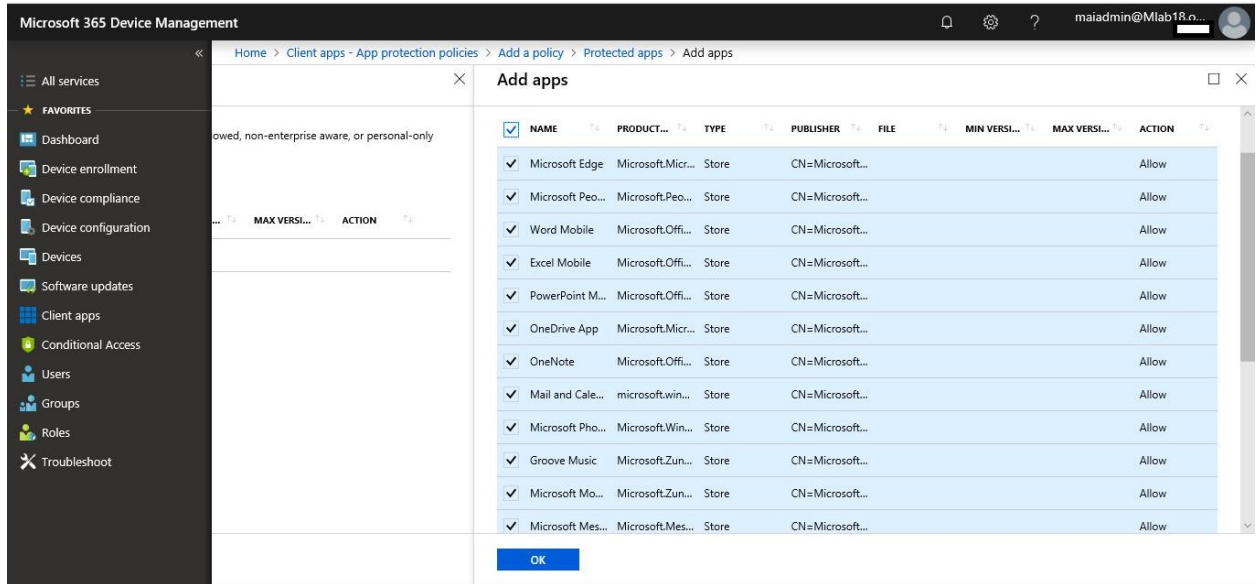
5. Add the following values:

- **Name:** Type a name (required) for your new policy.
- **Description:** (Optional) Type a description.
- **Platform:** Choose **Windows 10** as the supported platform for your app protection policy.
- **Enrollment state:** Choose **Without enrollment** as the enrollment state for your policy.

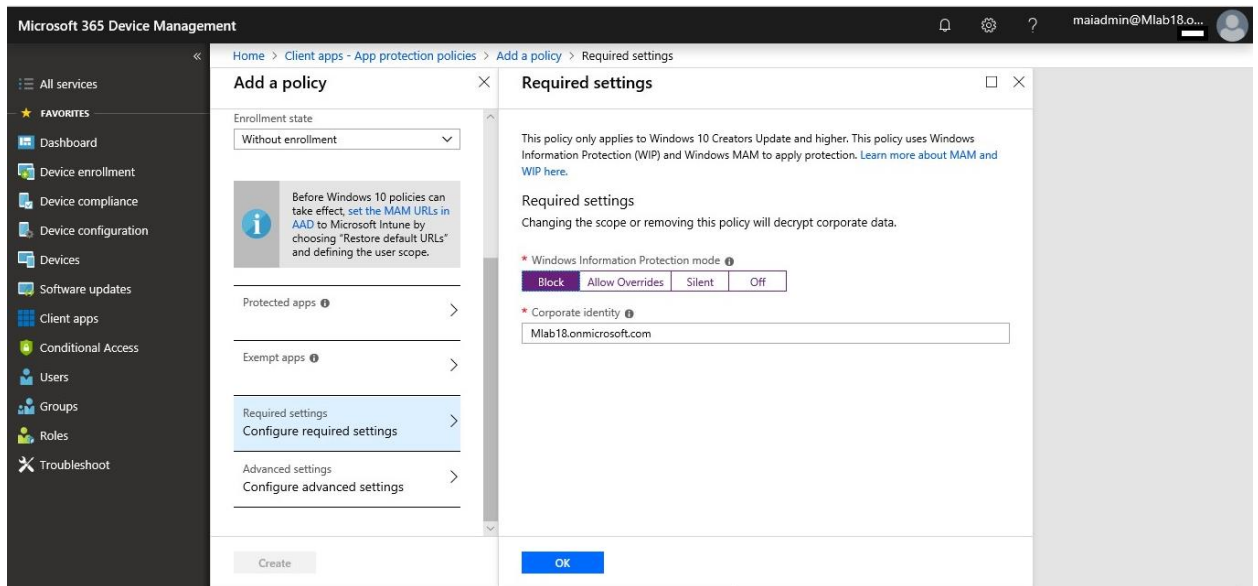


Note: When you apply policy without enrollment, the end user will need to register device on Azure AD using join workplace.

6. Select all Protected Apps.



7. Select Required Setting, select Block to prevent copy from managed app to unmanaged app.



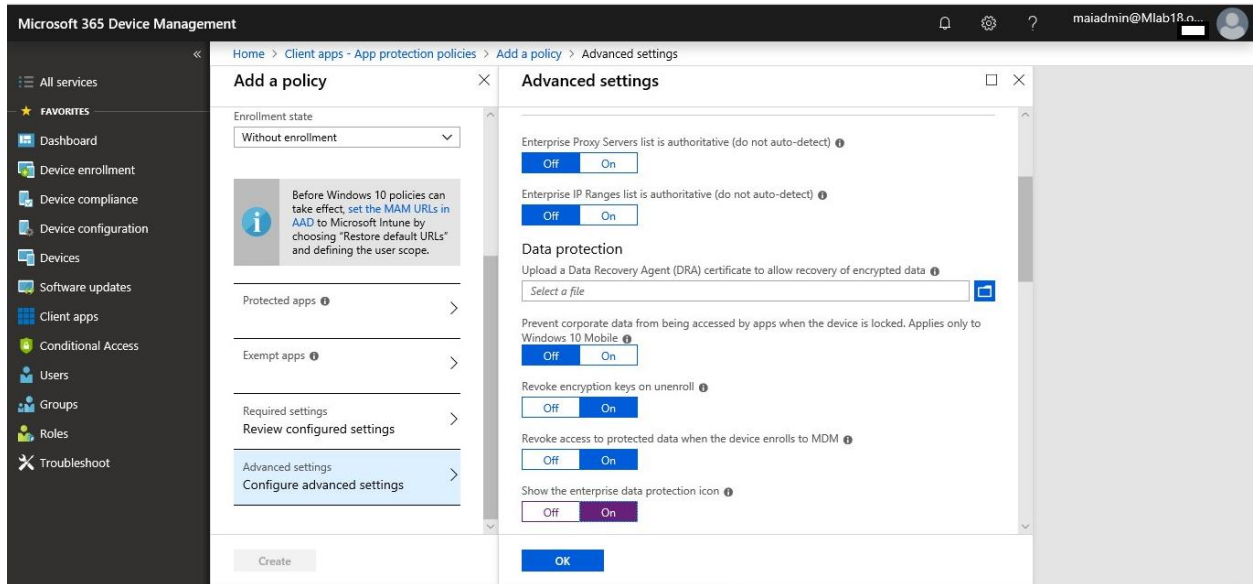
8. Select Advanced Settings, select show the enterprise data protection icon.

Note: Enterprise Proxy Servers list is authoritative (do not auto-detect). Click this box if you want Windows to treat the proxy servers you specified in the network boundary definition as the complete list of proxy servers available on your network.

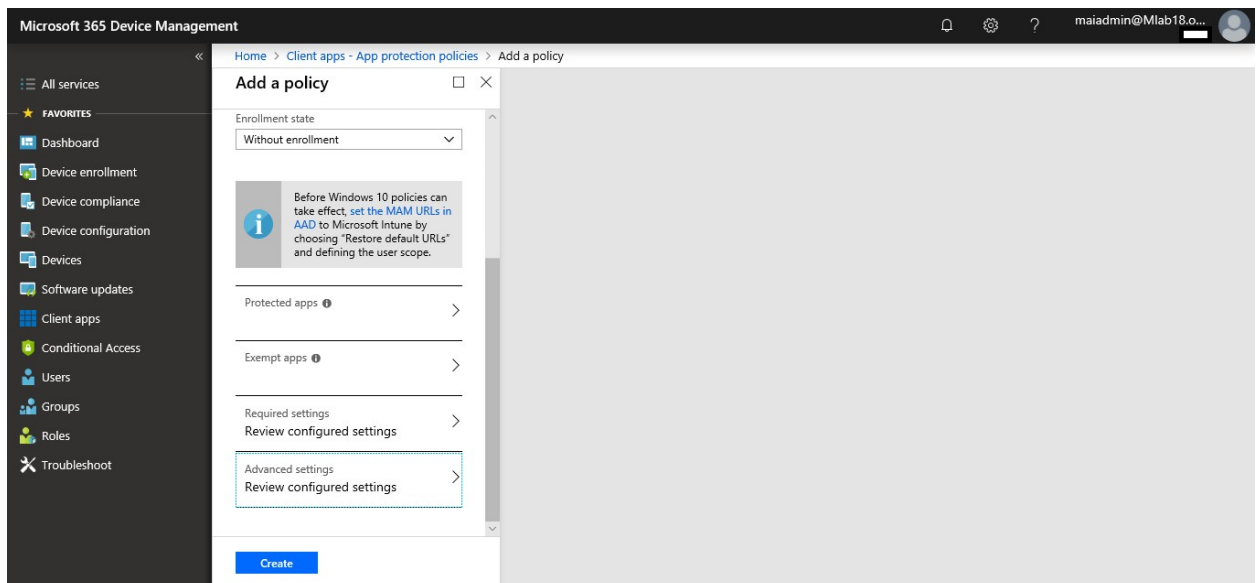
Enterprise IP Ranges list is authoritative (do not auto-detect). Click this box if you want Windows to treat the IP ranges you specified in the network boundary definition as the complete list of IP ranges available on your network.

DRA certificate isn't mandatory. Data Recovery Agent (DRA) certificate lets Windows use an included public key to encrypt the local data while you maintain the private key that can unencrypt the data. **Use Azure RMS for WIP** using Azure Rights Management encryption with WIP. By turning this option on, you can also add a TemplateID GUID to specify who can access the Azure Rights Management protected files, and for how long.

Use Windows Hello for Business as a method for signing into Windows



9. Choose **Create**. The policy is created and appears on the **App protection policies** blade.



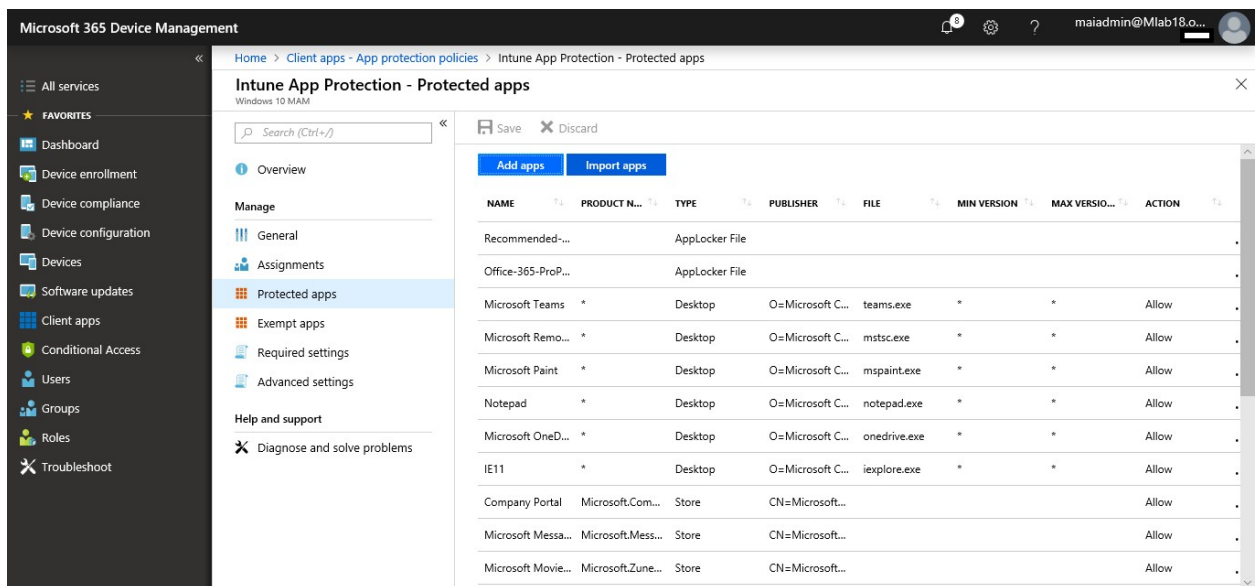
Note: MAM Policy for iOS & Android are same for enrollment or without enrollment but WIP Policy is different. You have 2 WIP policy with enrollment or without enrollment. Take care if your device already enrolls, the WIP policy without enrollment won't apply. So, make sure that you apply policy on correct target group. WIP Policy should apply on windows 10 creator "1709 or later"

Additional Configuration on WIP

In this topic, we need to apply WIP on Office Desktop App. and apply it on OWA.

To add office desktop app., you need to follow below steps:

1. On the **Microsoft Intune** blade, Select **Client apps** > Select **App protection policies**.
2. On the **App protection policies** blade, choose the policy you want to modify. The **Intune App Protection** blade is displayed.
3. Choose **Protected apps** from the **Intune App Protection** blade. The **Protected apps** blade opens showing you all apps that are already included in the list for this app protection policy.
4. Select **Add apps**. The **Add apps** information shows you a filtered list of apps.

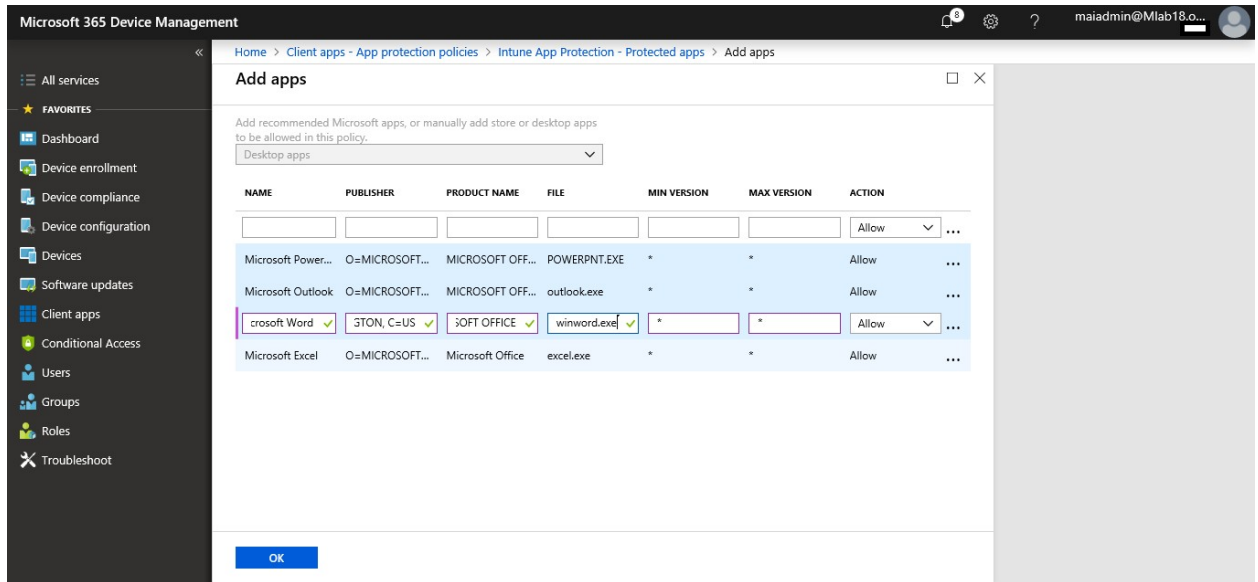


The screenshot displays the Microsoft 365 Device Management console. The left-hand navigation pane shows various service categories, with 'Client apps' selected. The main content area is titled 'Intune App Protection - Protected apps' and shows a table of protected applications. The table has columns for NAME, PRODUCT N., TYPE, PUBLISHER, FILE, MIN VERSION, MAX VERSIO..., and ACTION. The table lists several applications, including Microsoft Teams, Microsoft Remo..., Microsoft Paint, Notepad, Microsoft OneD..., IE11, Company Portal, Microsoft Messa..., and Microsoft Movie... Each application has an 'Allow' action button.

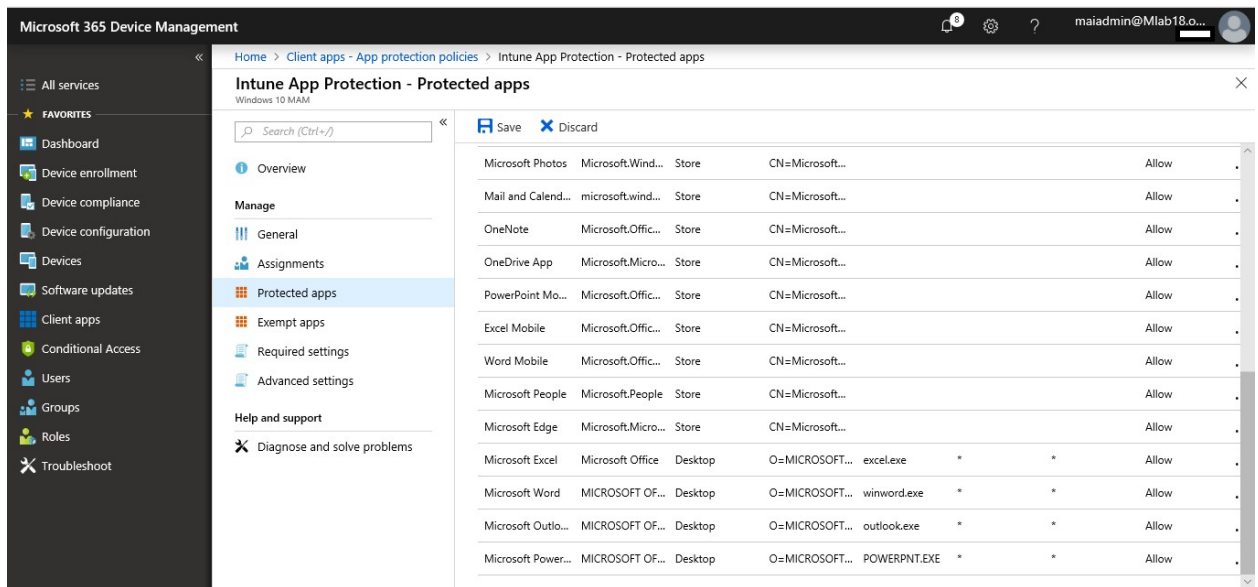
NAME	PRODUCT N.	TYPE	PUBLISHER	FILE	MIN VERSION	MAX VERSIO...	ACTION
Recommended...		AppLocker File					
Office-365-ProP...		AppLocker File					
Microsoft Teams	*	Desktop	O=Microsoft C...	teams.exe	*	*	Allow
Microsoft Remo...	*	Desktop	O=Microsoft C...	mstsc.exe	*	*	Allow
Microsoft Paint	*	Desktop	O=Microsoft C...	mspaint.exe	*	*	Allow
Notepad	*	Desktop	O=Microsoft C...	notepad.exe	*	*	Allow
Microsoft OneD...	*	Desktop	O=Microsoft C...	onedrive.exe	*	*	Allow
IE11	*	Desktop	O=Microsoft C...	ieexplore.exe	*	*	Allow
Company Portal	Microsoft.Cem...	Store	CN=Microsoft...				Allow
Microsoft Messa...	Microsoft.Mess...	Store	CN=Microsoft...				Allow
Microsoft Movie...	Microsoft.Zune...	Store	CN=Microsoft...				Allow

5. Add each app that you want to apply WIP policy on it.

Microsoft Intune step by step on Azure portal



6. Click **OK**. The **Protected apps** blade is updated showing all selected apps.



7. Click **Save**.

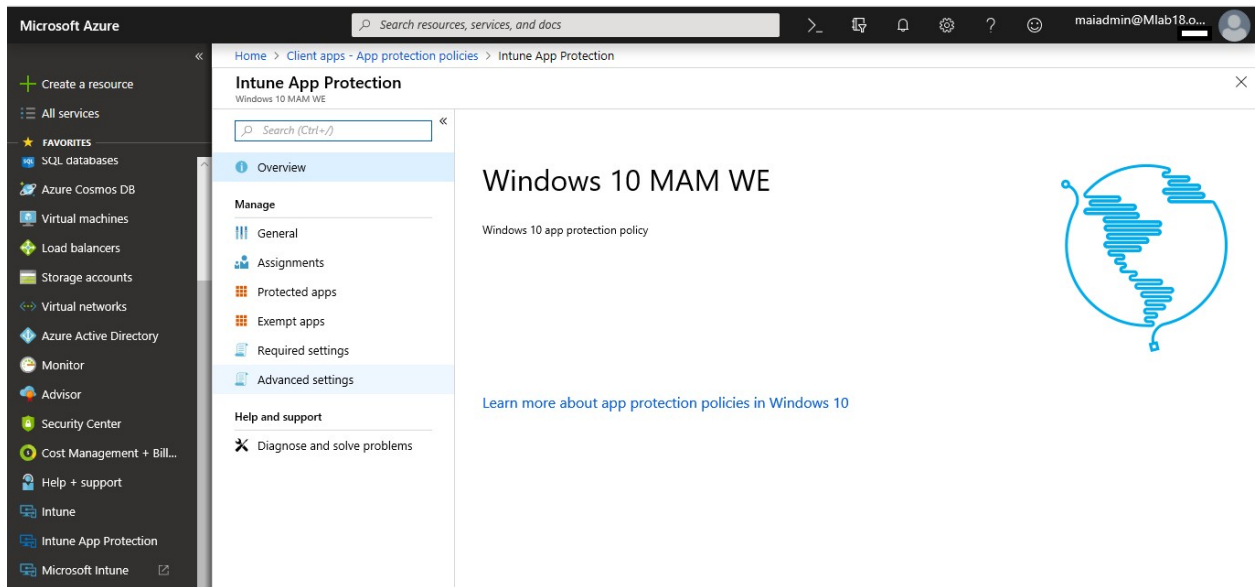
This is table of office applications

Name	Publisher	ProductName	File	Min. Version	Max. Version	Action
Microsoft PowerPoint	O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	MICROSOFT OFFICE	POWERPNT.EXE	*	*	Allow

Name	Publisher	ProductName	File	Min. Version	Max. Version	Action
Microsoft Outlook	O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	MICROSOFT OFFICE	OUTLOOK.EXE	*	*	Allow
Microsoft Word	O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	MICROSOFT OFFICE	WINWORD.EXE	*	*	Allow
Microsoft Excel	O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	MICROSOFT OFFICE	EXCEL.EXE	*	*	Allow

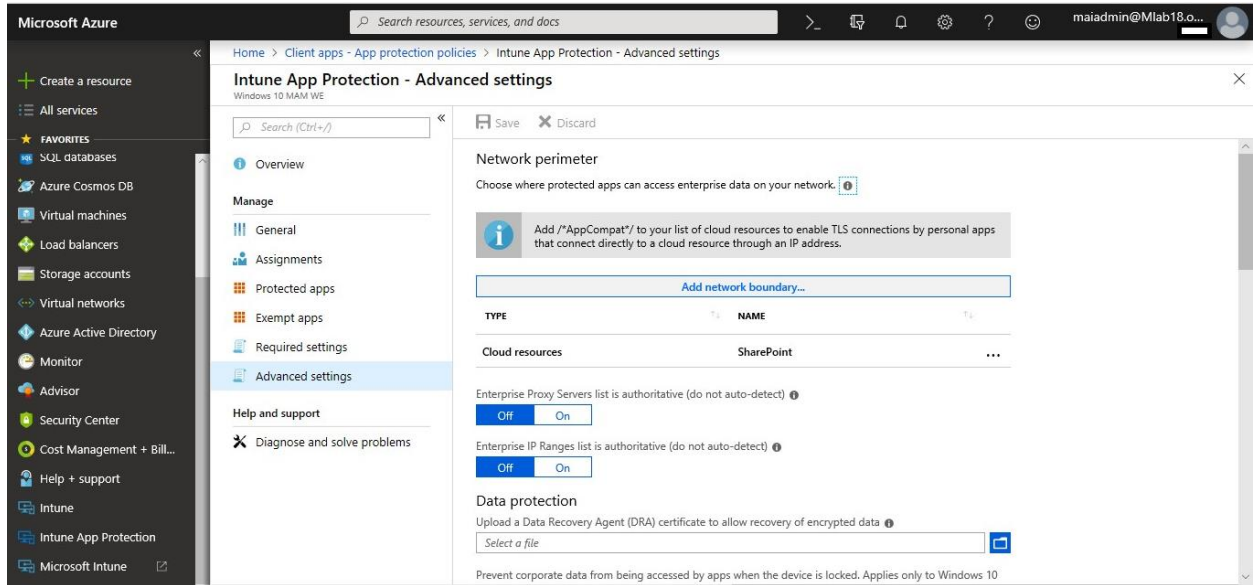
To protect OWA, you need to follow below steps:

1. Select **Client apps** on the **Microsoft Intune** blade.
2. Select **App protection policies** on the **Client apps** blade.
3. On the **App protection policies** blade, choose the policy you want to modify. The **Intune App Protection** blade is displayed.
4. Choose **Advanced settings** from the **Intune App Protection** blade.

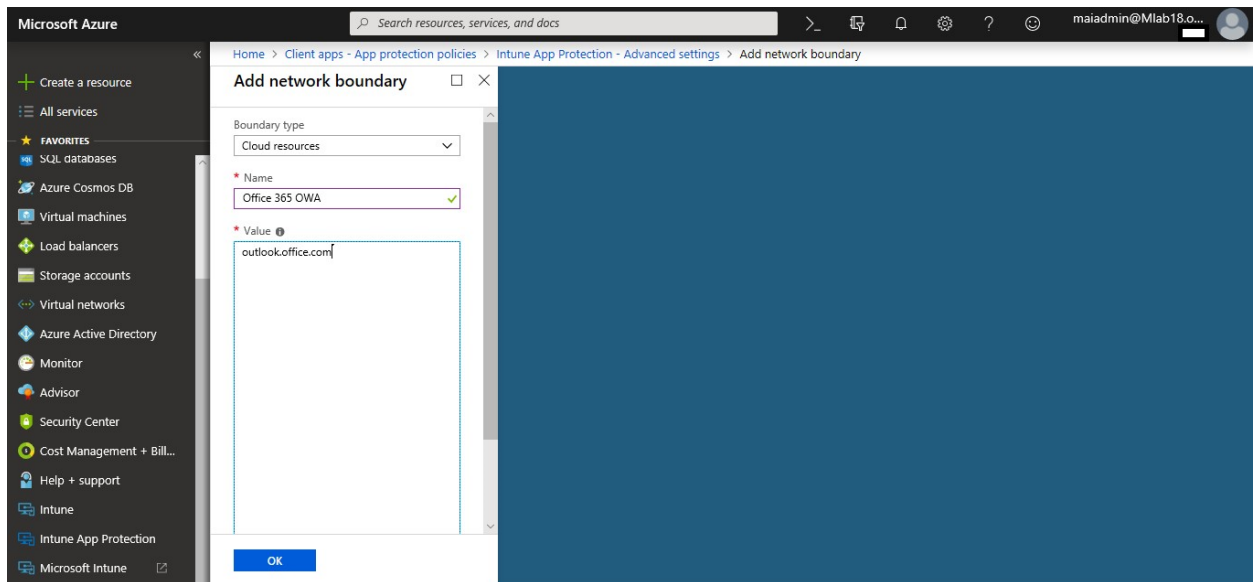


5. Click **Add network boundary**

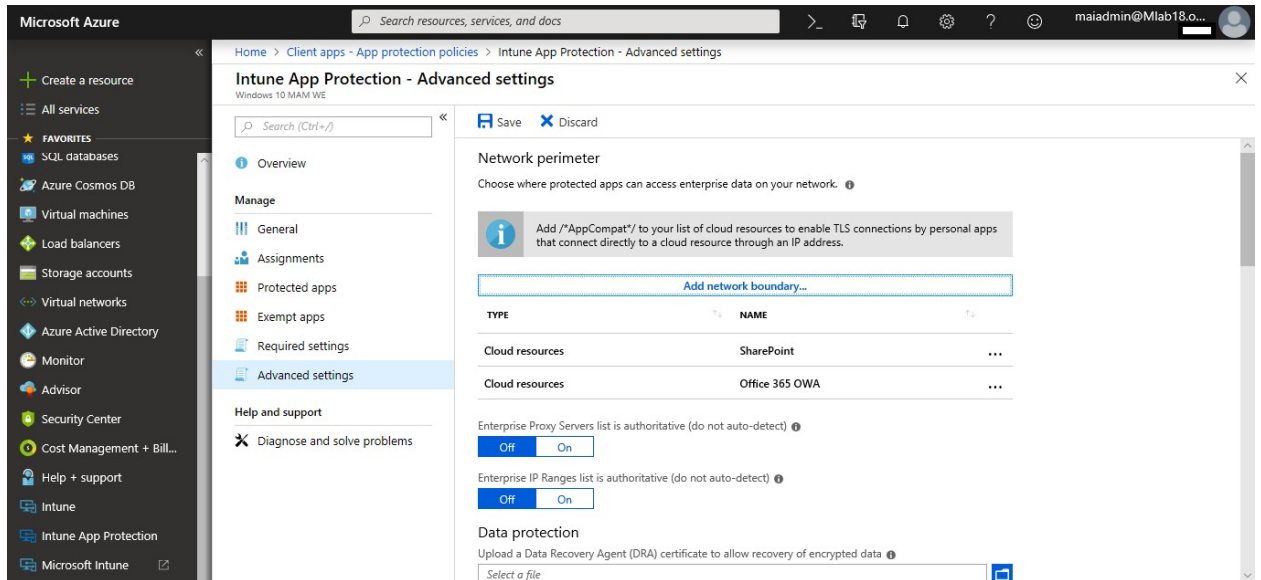
Microsoft Intune step by step on Azure portal



6. Select **Cloud resources**, type name and type value **outlook.office.com**



7. Click **Save**



Note: After you apply WIP on windows 10 PCs, it will block browsing any site on non-Microsoft web app like chrome or Firefox. To allow browsing on those browsers, you need to add on cloud resources value `/*AppCompat*/` in the value field and click ok.

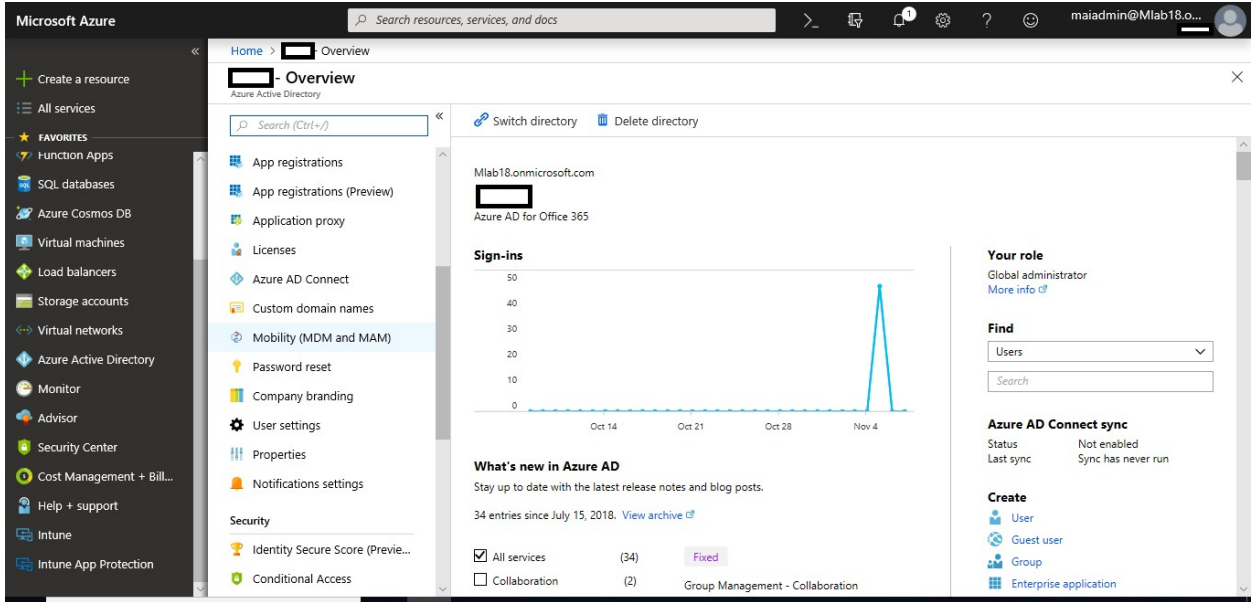
Enable MAM Provider in Azure AD

Enable mobile application management (MAM) for Windows 10 by setting the MAM provider in Azure AD. Setting a MAM provider in Azure AD allows you to define the enrollment state when creating a new Windows Information Protection (WIP) policy with Intune. The enrollment state can be either MAM or mobile device management (MDM).

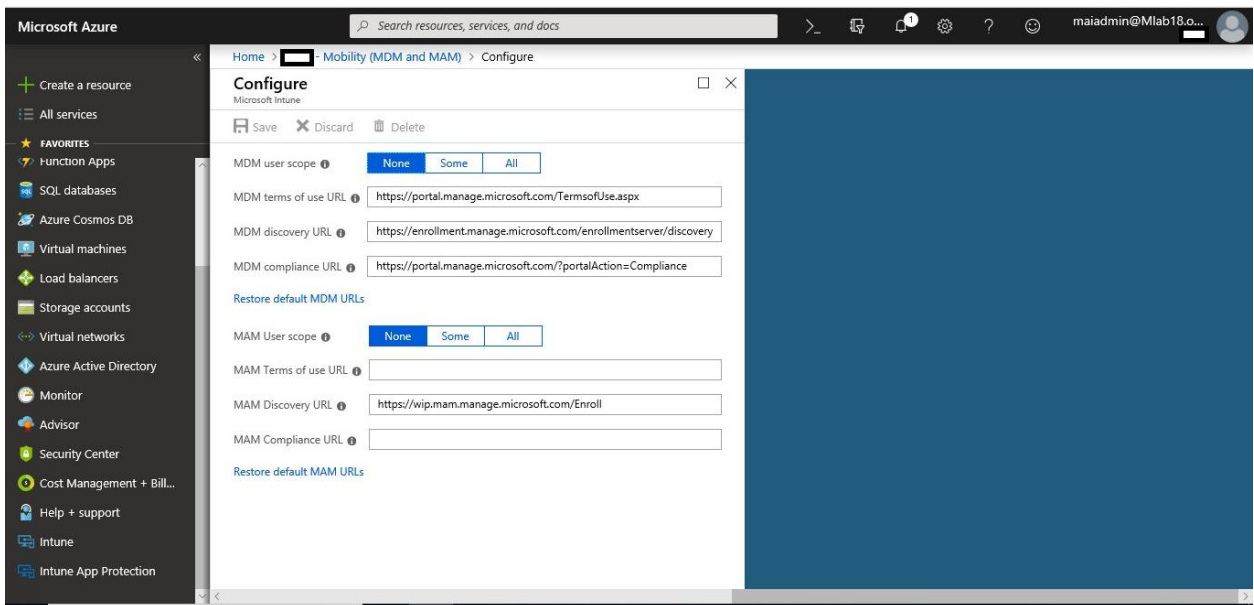
To configure the MAM provider

1. Sign in to the [Azure portal](#) and choose **Azure Active Directory**.
2. Choose **Mobility (MDM and MAM)** in the **Manage** group.

Microsoft Intune step by step on Azure portal

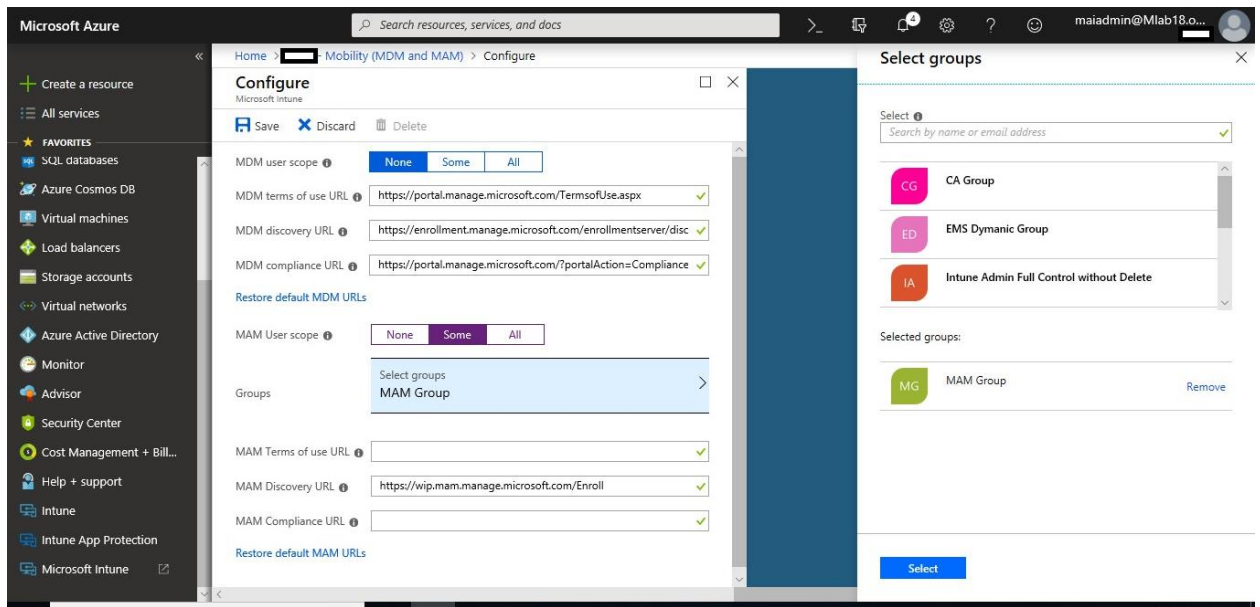


3. Click **Microsoft Intune**.

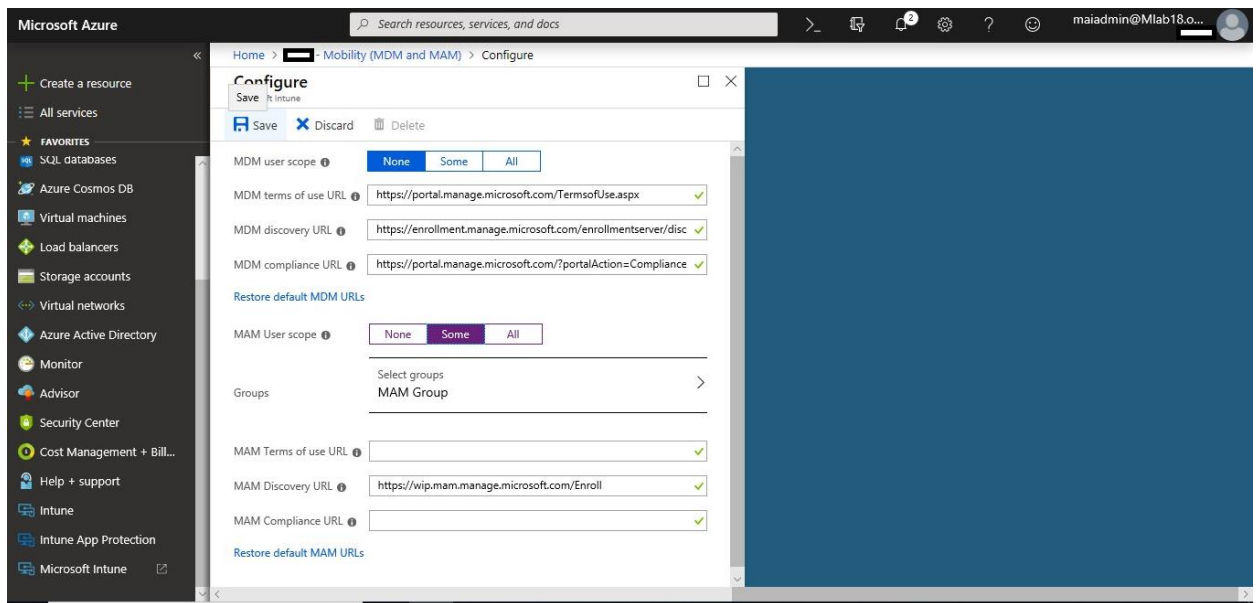


4. Configure the settings in the **Restore default MAM URLs** group on the **Configure** blade.

Microsoft Intune step by step on Azure portal



5. Click Save.



Note: When you configure automatic enrollment for Windows 10 using MDM or MAM, make sure that target group for both are different users because once device is registered with Azure AD or join Azure AD, the URLs for discovery is publishing to client which are different. MAM URL is different than MDM URL, which do conflict in this case.

App Configuration Policy

Use app configuration policies in Microsoft Intune to provide configuration settings for an iOS or Android app. These configuration settings allow an app to be customized. You do not assign

Microsoft Intune step by step on Azure portal

these configuration policies directly to users and devices. Instead, you associate a configuration policy with an app, and then assign the app. The configuration settings are used whenever the app checks for them. Typically, an app checks for configuration settings the first time the app is run by the user.

You have two options for how to use app configurations with Intune:

- **Managed devices** - The device is managed by Intune as the mobile device management (MDM) provider.
- **Managed apps** - An app is managed without device enrollment.

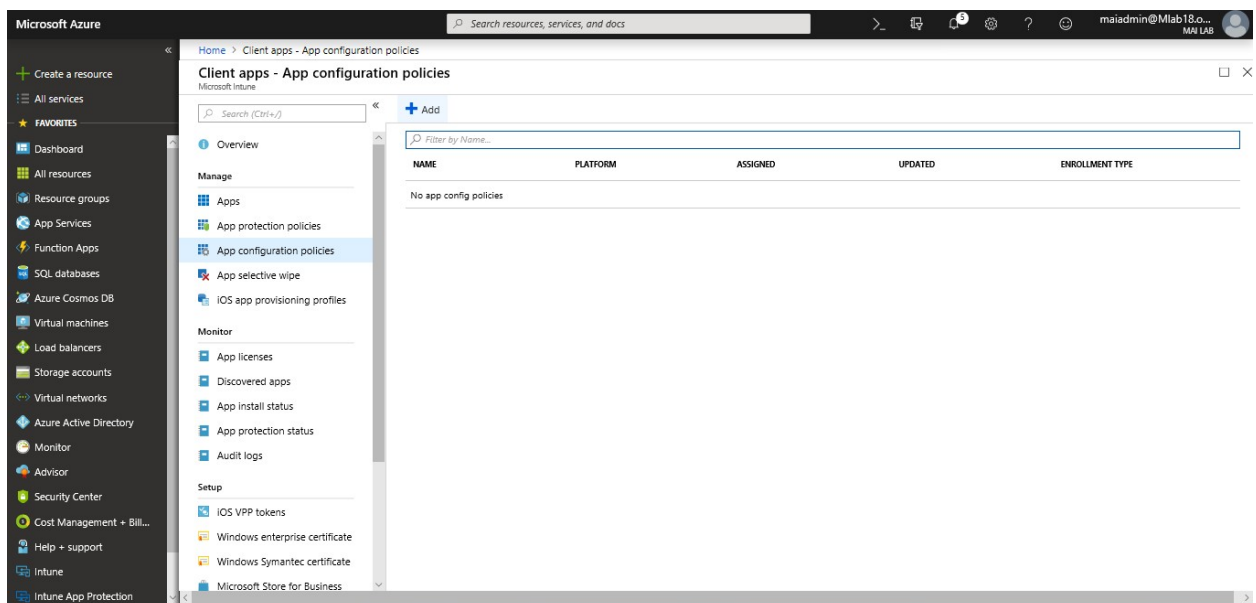
Note: As the Microsoft Intune admin, you can control which user accounts are added to Microsoft Office applications on managed devices. You can limit access to only allowed organization user accounts and block personal accounts on enrolled devices. The supporting applications process the app configuration and remove and block unapproved accounts.

App Configuration Policies for Managed Devices

Use app configuration policies in Microsoft Intune to provide custom configuration settings for an iOS or Android for work app. These configuration settings allow an app. to be customized based on the suppliers' direction.

To configure email profile for outlook on managed iOS device, you need to follow below steps:

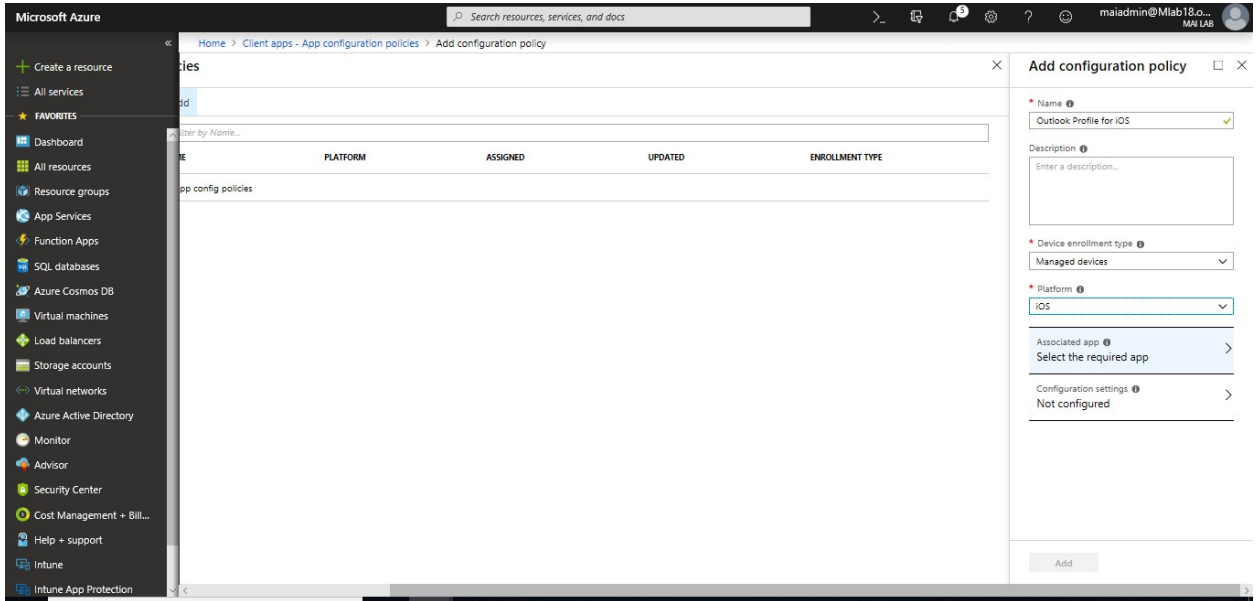
1. Sign into the [Azure portal](#). Choose **All services** > **Intune App Protection**.
2. Choose **App configuration policies** in the **Manage** group, and then choose **Add**.



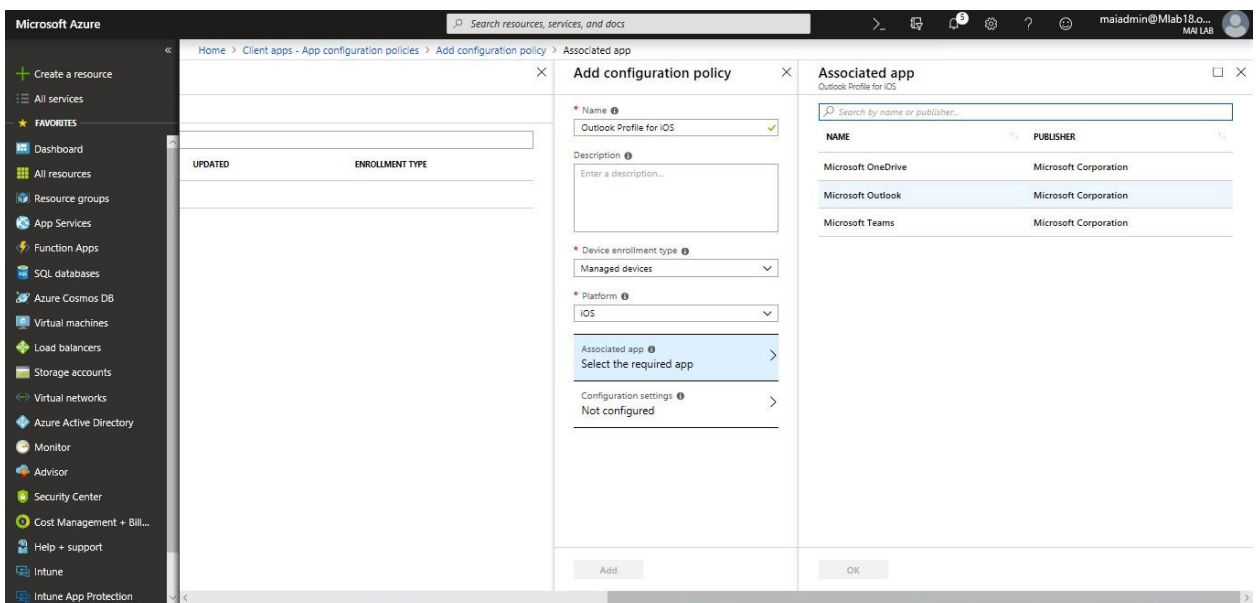
3. Set the following details:

Microsoft Intune step by step on Azure portal

- **Name** - The name of the profile that appears in the Azure portal.
 - **Description** - The description of the profile that appears in the Azure portal.
 - **Device enrollment type** - Choose **Managed devices**.
4. Select **iOS** for **Platform**.



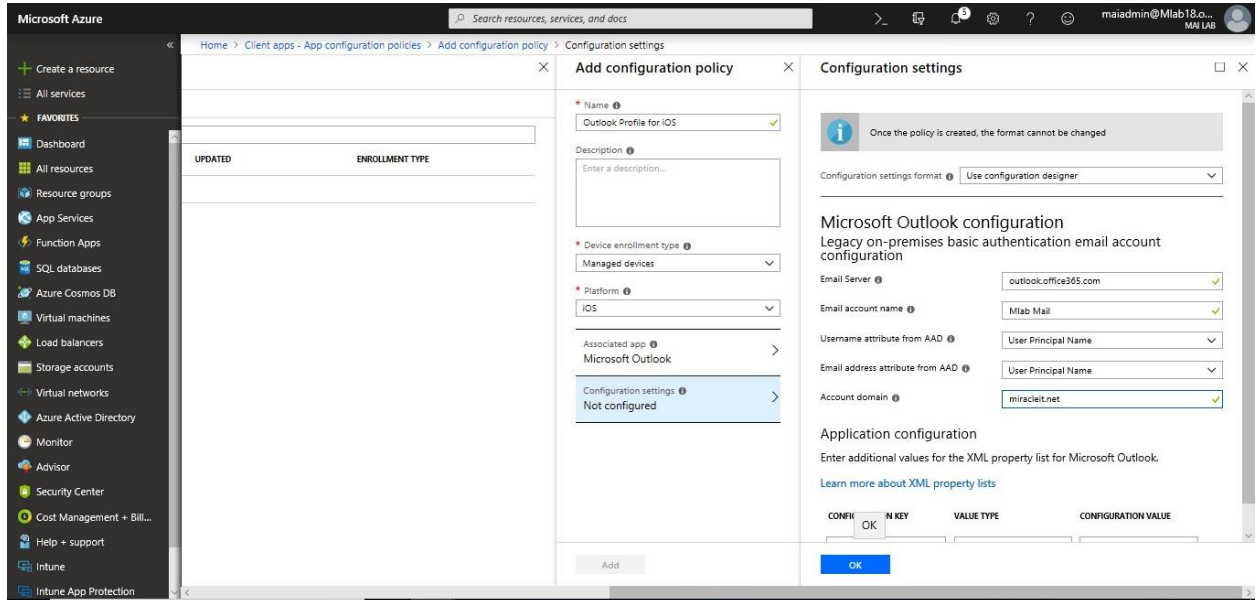
5. Choose **Associated app**. Then, on the **Associated app** pane, choose the managed app to which you want to apply the configuration and select **OK**.



Note: To select outlook on associated app, you need to **add outlook application from client app** to be able to select it.

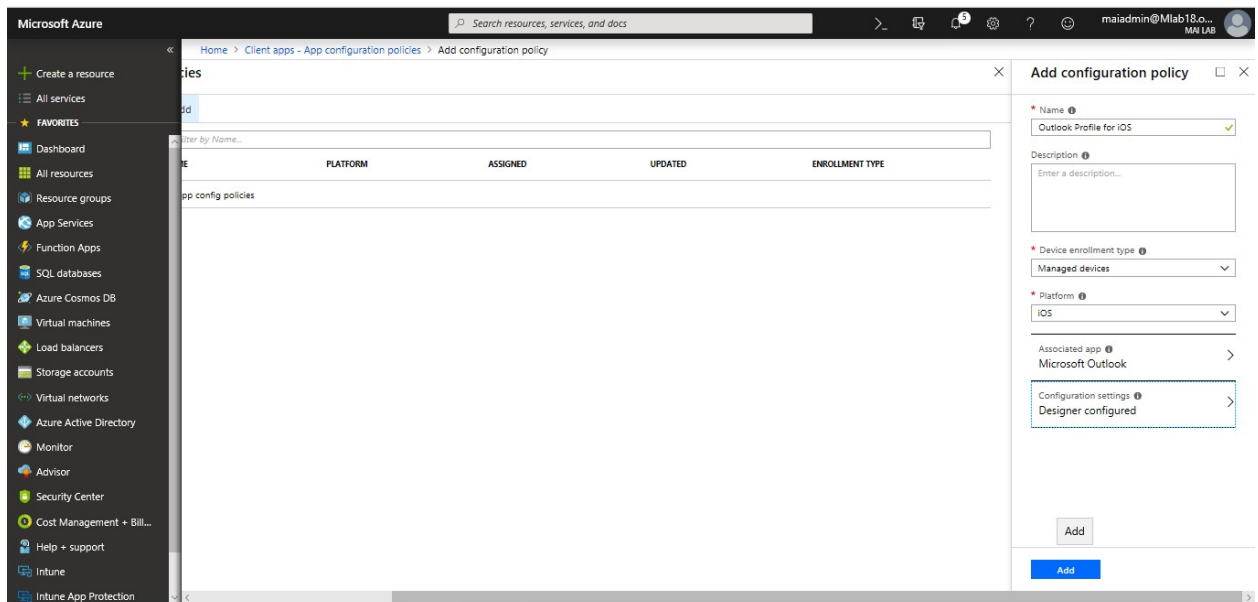
6. On the **Add configuration policy** pane, choose **Configuration settings**.

7. Select **Configuration settings** format. Select **Use configuration designer**

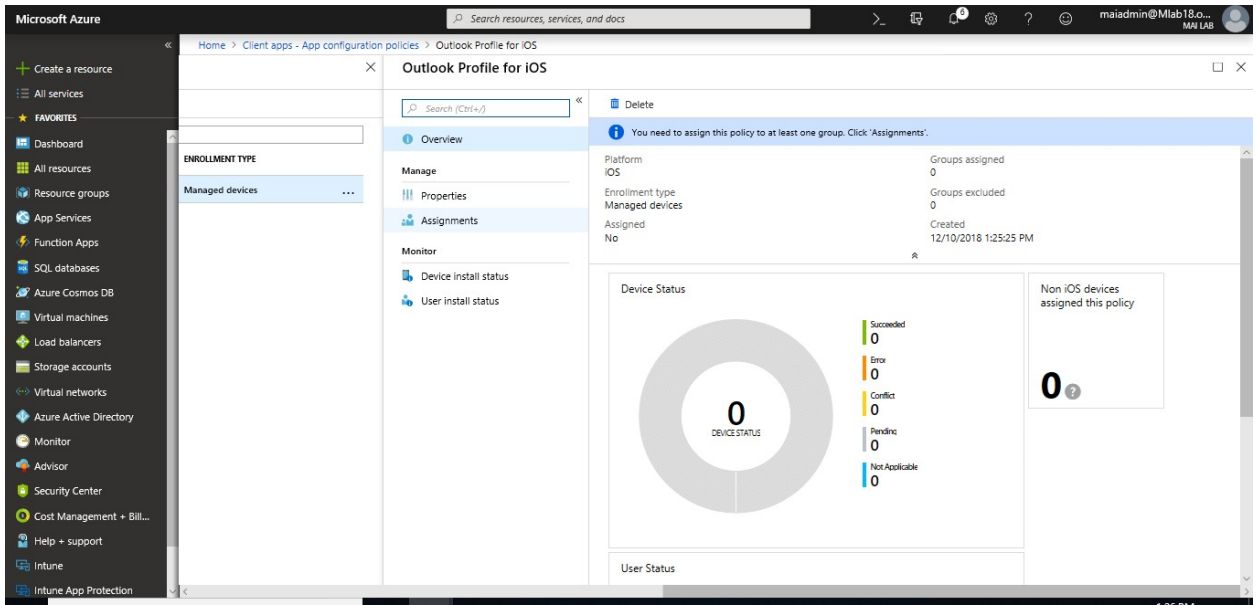


Note: If you choose Enter XML data. Once you have added your XML information, choose **OK**, and then choose **Add** to add the configuration policy. The overview pane for the configuration policy is displayed.

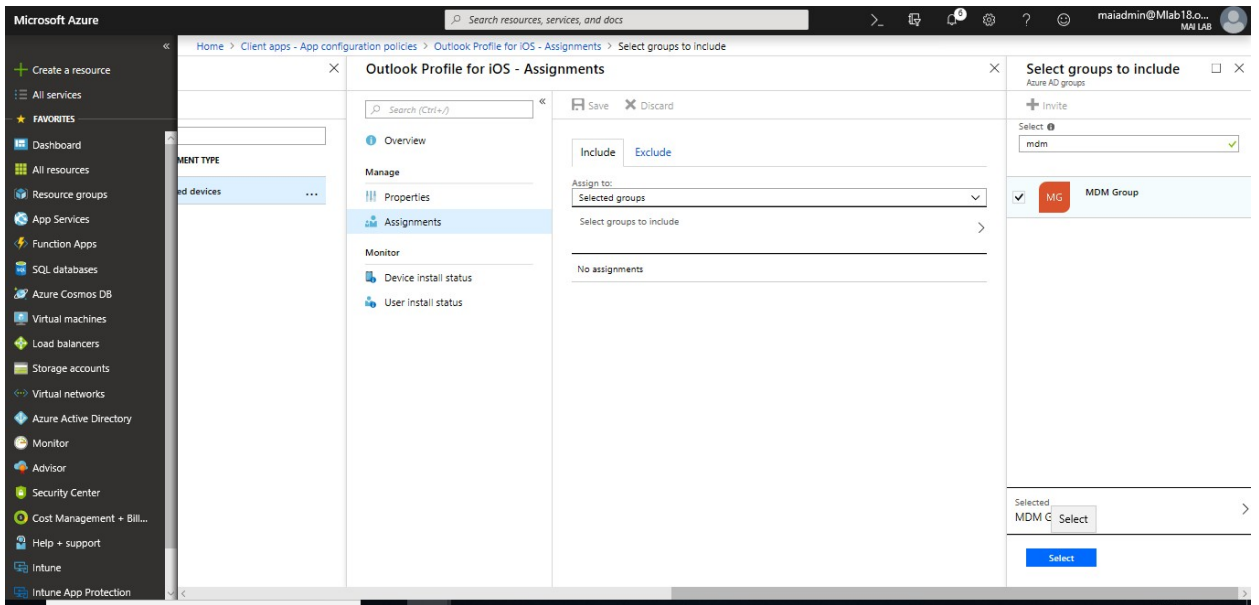
8. Click **Add** to add configuration policy.



9. Select **Assignments** to display the include and exclude options.



10. Select **group** on the **Include** tab.

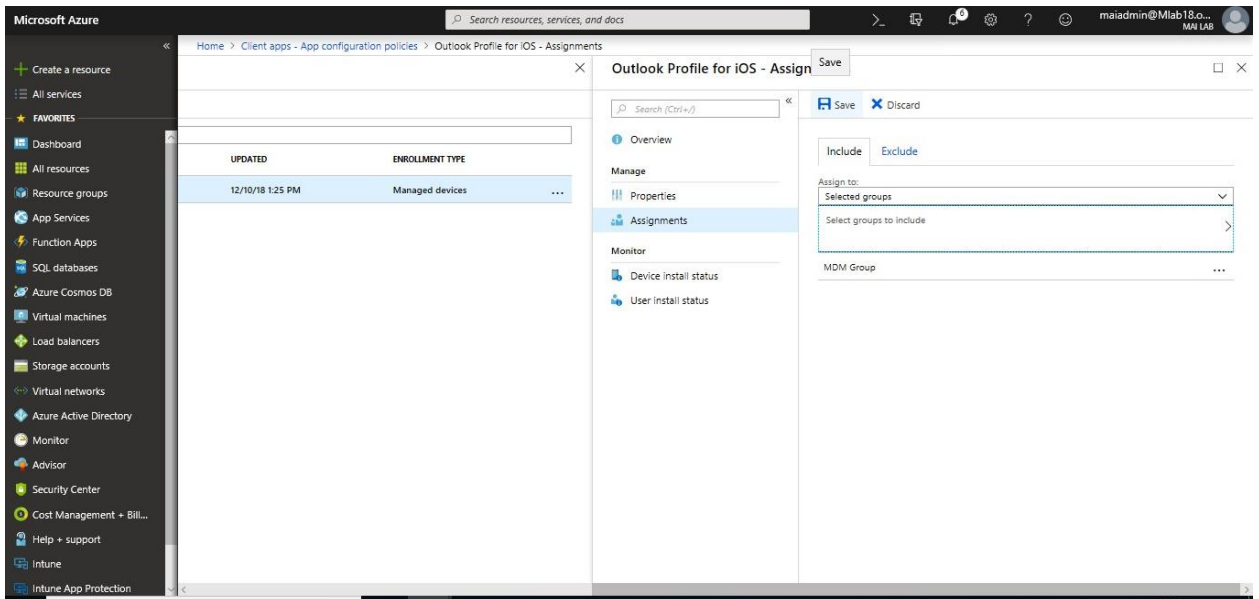


11. Select the **Exclude** Tab. Click **Select groups to exclude** to display the related pane.

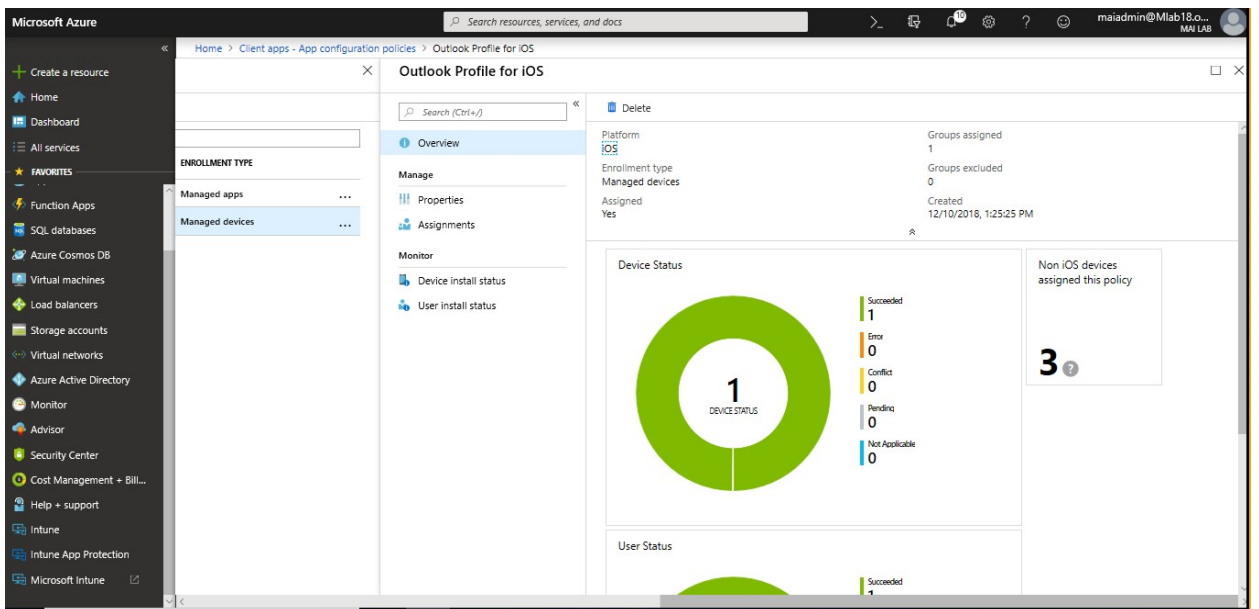
Note: Adding a group, if any other group has already been included for a given assignment type, it is pre-selected and unchangeable for other include assignment types. Therefore, that group that has been used, cannot be used as an excluded group.

12. Click **Save**.

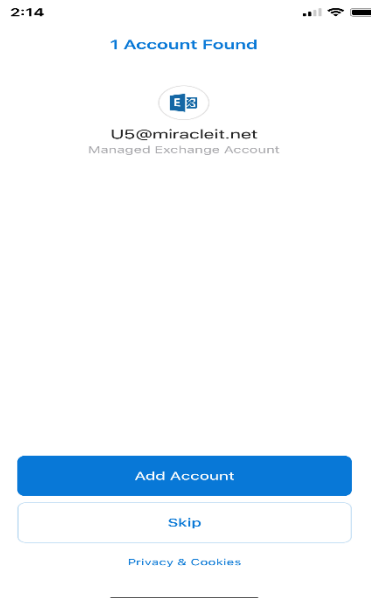
Microsoft Intune step by step on Azure portal



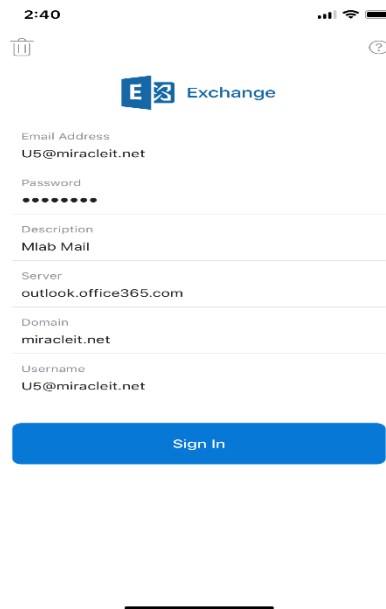
13. After outlook profile push to device, it should appear on Intune Portal.



14. From end user side, on outlook for his mobile phone, he should find profile already push as below, Click **Add**.



15. Enter **password** & click **Sign in**.



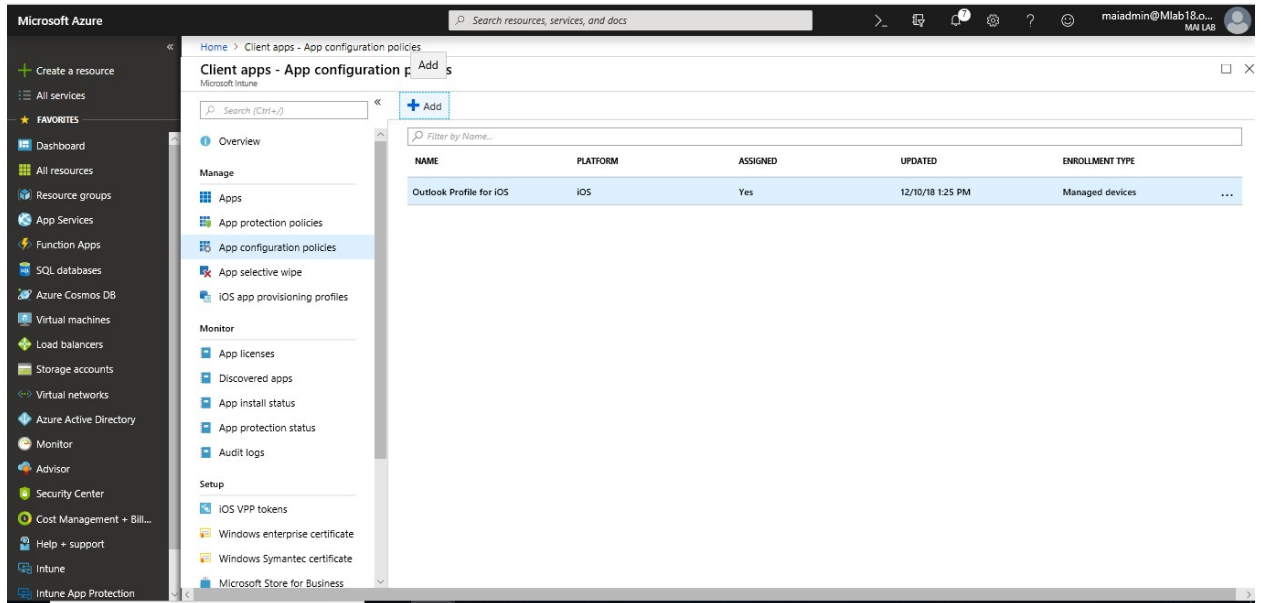
App Configuration Policies for Managed Apps

You can use app configuration policies with managed apps that support the Intune App SDK, even on devices that are not enrolled.

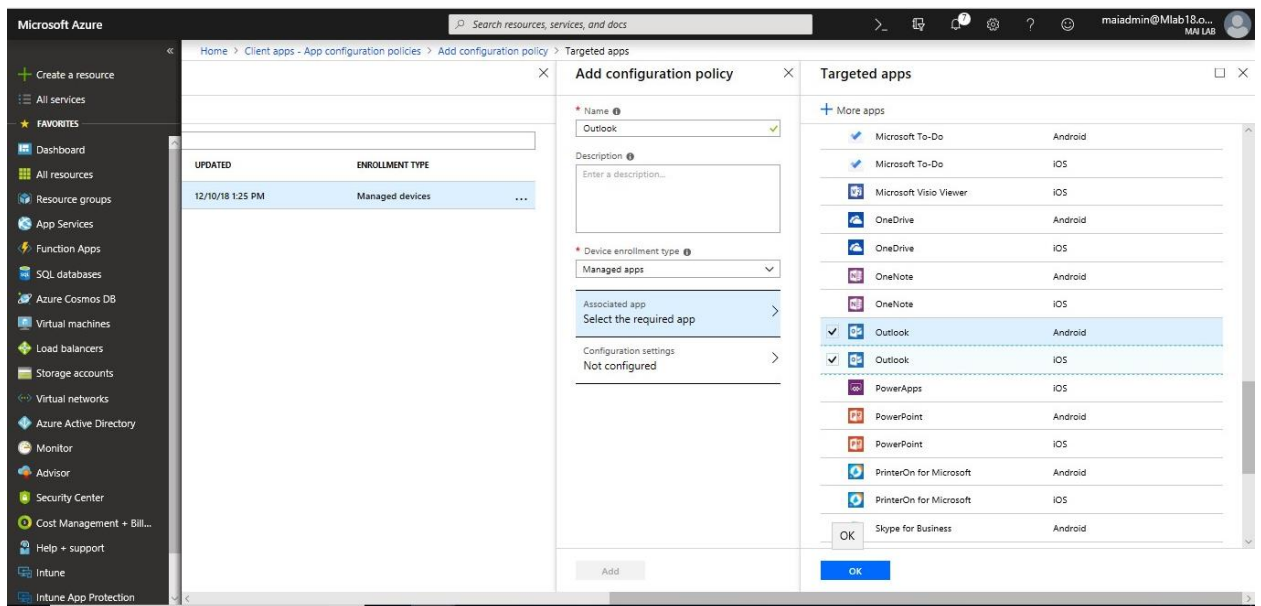
To configure email profile on outlook Managed App for iOS & Android, you need to follow below steps:

1. Sign into the [Azure portal](#). Choose **All services > Intune App Protection**.

2. Choose **App configuration policies** in the **Manage** group, and then choose **Add**.



3. Set the following details:
 - o **Name:** The name of the profile that will appear in the Azure portal.
 - o **Description:** The description of the profile that will appear in the Azure portal.
 - o **Device enrollment type:** Choose **Manage apps**.
4. Select **Associated app** to choose the app that you are going to configure. Select the app from the list of apps that you have approved and synchronized with Intune.



5. For each configuration setting that the app supports, type the **Name** and **Value**, and choose the ellipsis (...). To delete a configuration, choose the ellipsis (...) and select **Delete**.

Microsoft Intune step by step on Azure portal

Name	Value
com.microsoft.outlook.EmailProfile.EmailAddress	{{mail}}
com.microsoft.outlook.EmailProfile.EmailAccountName	{{username}}
com.microsoft.outlook.EmailProfile.EmailUPN	{{userprincipalname}}
com.microsoft.outlook.EmailProfile.ServerHostName	outlook.office365.com
com.microsoft.outlook.EmailProfile.AccountDomain	Custom domain "miracleit.net"

Microsoft Azure

Home > Client apps > App configuration policies > Add configuration policy > Configuration

Add configuration policy

Name: Outlook

Description: Enter a description...

Device enrollment type: Managed apps

Associated app: 2 Apps Selected

Configuration settings: Not configured

Configuration

Intune SDK-enabled apps support configurations in key-value pairs. Consult the documentation for each app to learn more about which key-value configurations are supported.

Intune supports string values and token replacement values. Learn more about which tokens Intune supports.

NAME	VALUE
com.microsoft.outlook.EmailProfile.AccountDomain	miracleit.net
com.microsoft.outlook.EmailProfile.ServerHostName	outlook.office365.com
com.microsoft.outlook.EmailProfile.EmailUPN	{{userprincipalname}}
com.microsoft.outlook.EmailProfile.EmailAccountName	{{username}}
com.microsoft.outlook.EmailProfile.EmailAddress	{{mail}}

OK

6. Click **Add** to add configuration policy.

Microsoft Azure

Home > Client apps > App configuration policies > Add configuration policy

Add configuration policy

Name: Outlook

Description: Enter a description...

Device enrollment type: Managed apps

Associated app: 2 Apps Selected

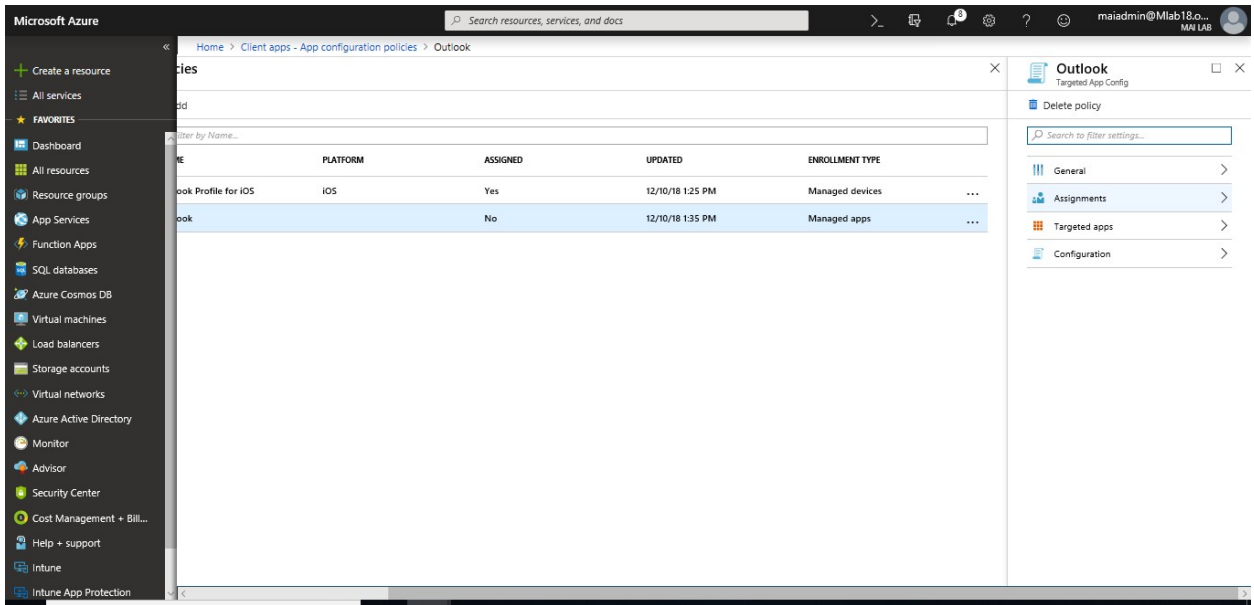
Configuration settings: Configuration settings

Add

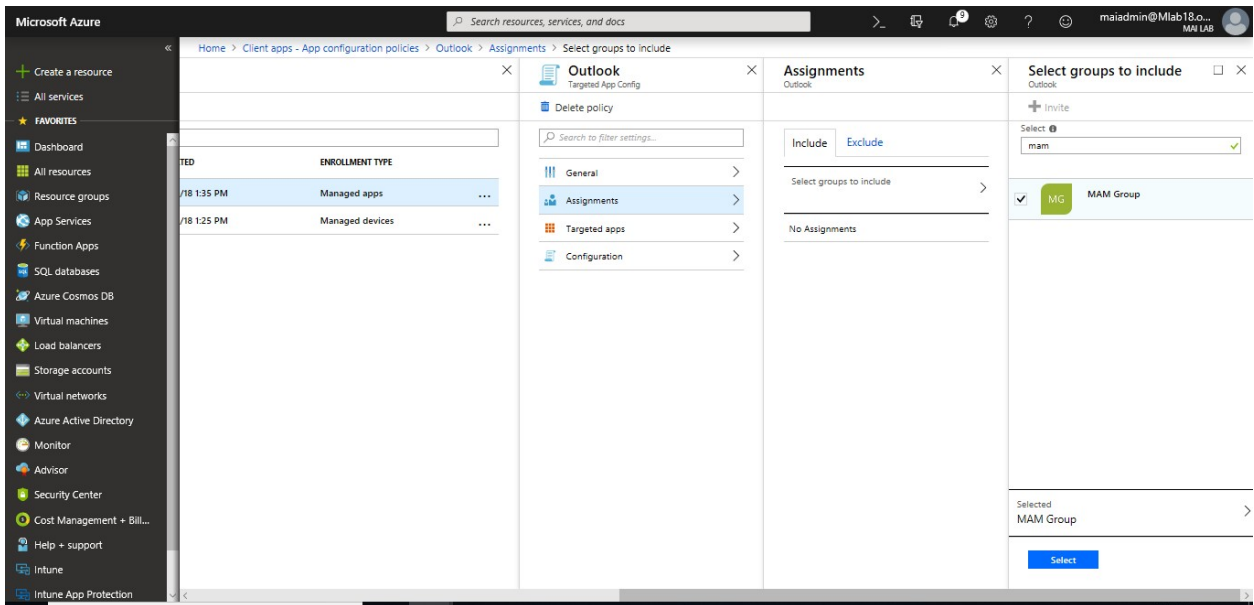
Filter by Name...

NAME	PLATFORM	ASSIGNED	UPDATED	ENROLLMENT TYPE
Outlook Profile for iOS	IOS	Yes	12/10/18 1:25 PM	Managed devices

7. Select **Assignments** to display the include and exclude options.



8. Select **group** on the **Include** tab.



9. Click **X** to close this tab.

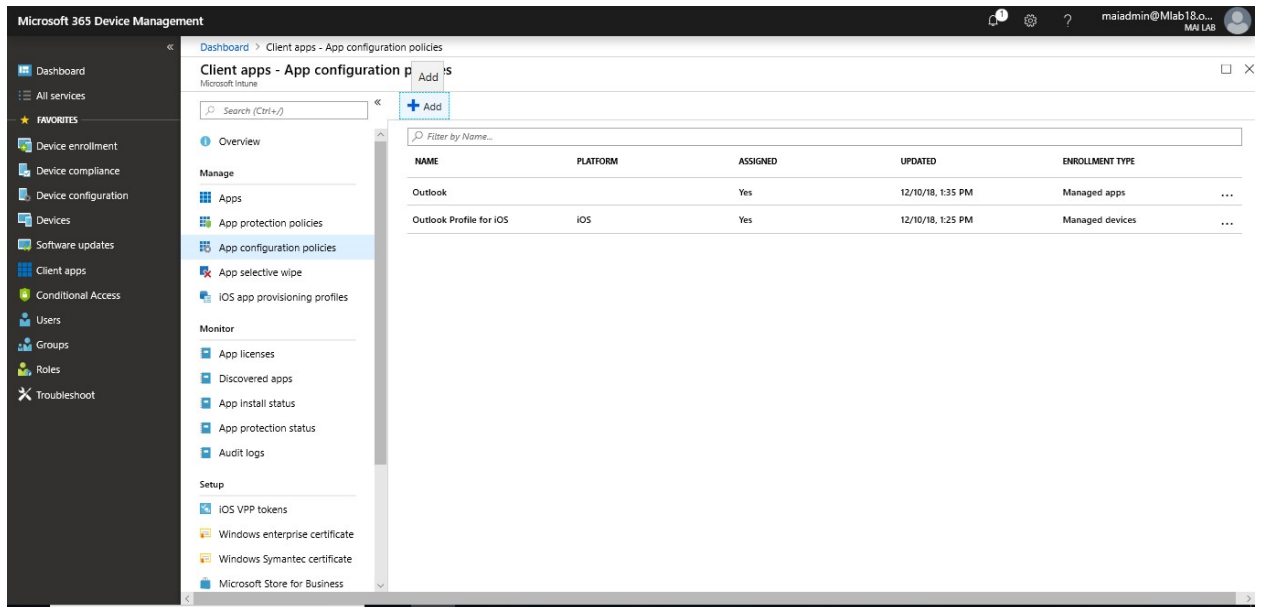
Protected Browser App on Mobile Devices

You can use app configuration policies with managed apps to block & allow some URLs, and configure bookmarks & home page.

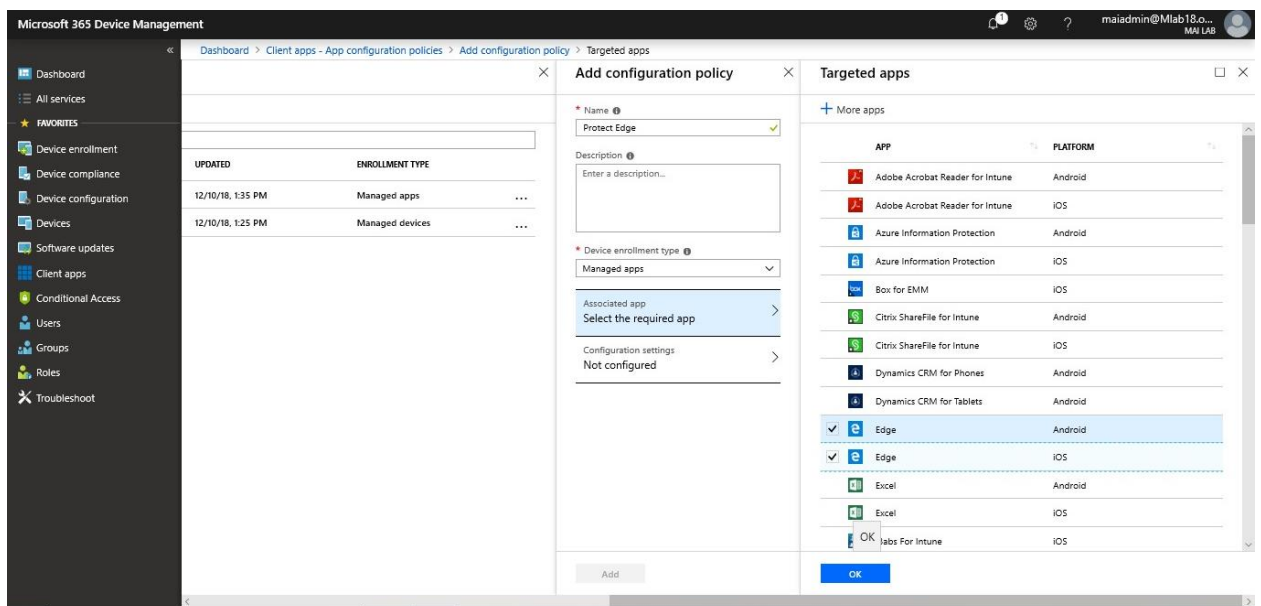
To block URLs & configure home page on Edge Managed App for iOS & Android, you need to follow below steps:

Microsoft Intune step by step on Azure portal

1. Sign into the [Azure portal](#). Choose **All services** > **Intune App Protection**.
2. Choose **App configuration policies** in the **Manage** group, and then choose **Add**.



3. Set the following details:
 - o **Name:** The name of the profile that will appear in the Azure portal.
 - o **Description:** The description of the profile that will appear in the Azure portal.
 - o **Device enrollment type:** Choose **Manage apps**.
4. Select **Associated app** to choose the app that you are going to configure. Select the app from the list of apps that you have approved and synchronized with Intune.



Microsoft Intune step by step on Azure portal

- For each configuration setting that the app supports, type the **Name** and **Value**, and choose the ellipsis (...). To delete a configuration, choose the ellipsis (...) and select **Delete**.

Name	Value
com.microsoft.intune.mam.managedbrowser.homepage	https://www.bing.com
com.microsoft.intune.mam.managedbrowser.bookmarks	Bing https://www.bing.com Microsoft https://www.microsoft.com
com.microsoft.intune.mam.managedbrowser.AllowListURLs	http://*.microsoft.com/ https://www.bing.com/ https://expertsfab.wordpress.com/
com.microsoft.intune.mam.managedbrowser.BlockListURLs	http://*.yahoo.com

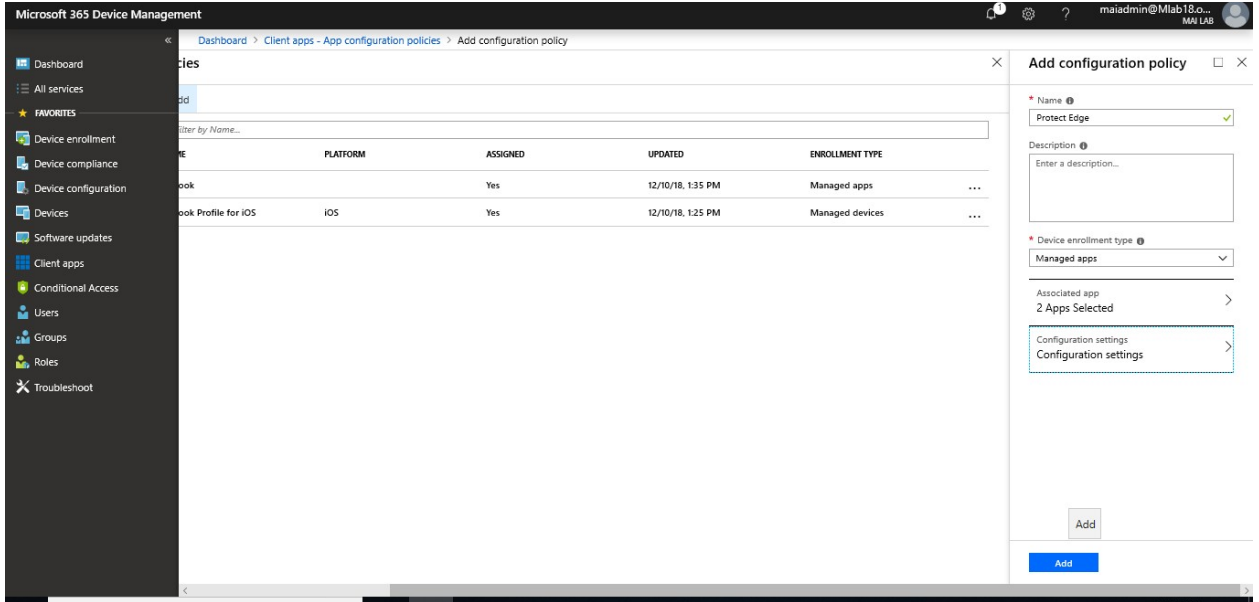
The screenshot shows the Microsoft 365 Device Management console. The 'Add configuration policy' dialog is open, showing the following fields:

- Name:** Protect Edge
- Description:** Enter a description...
- Device enrollment type:** Managed apps
- Associated app:** 2 Apps Selected
- Configuration settings:** Not configured

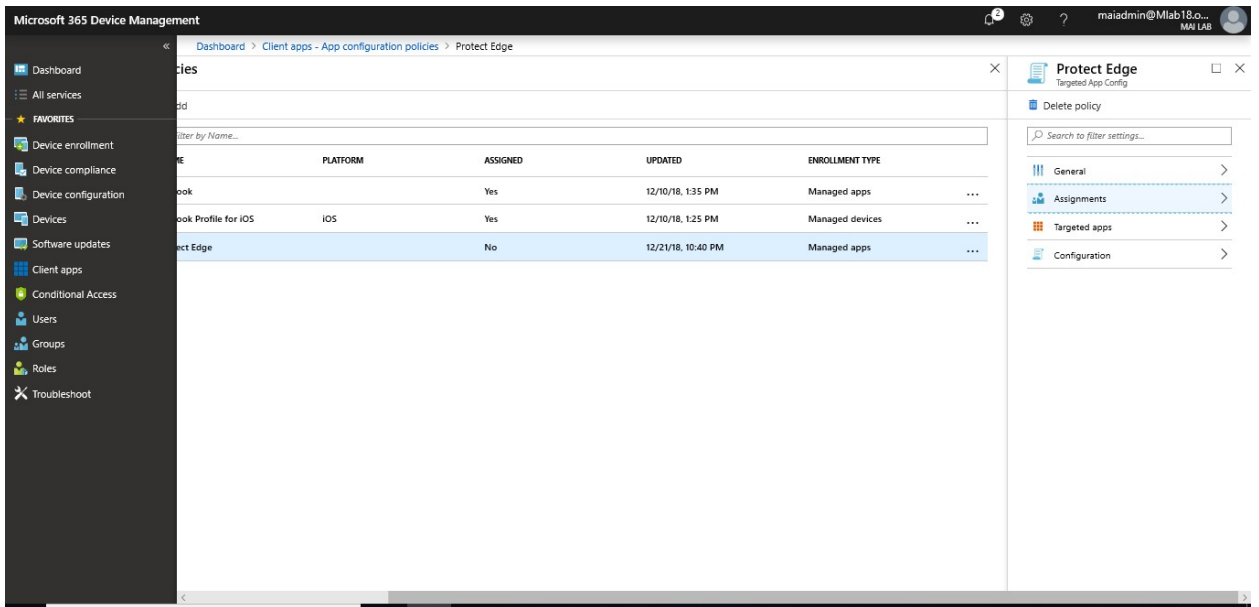
The 'Configuration' panel on the right shows a table of configurations:

NAME	VALUE
com.microsoft.intune.mam.managedbrowse...	http://*.yahoo.com
com.microsoft.intune.mam.managedbrowse...	http://*.microsoft.com/ https://www.bing.co...
com.microsoft.intune.mam.managedbrowse...	Bing https://www.bing.com Microsoft https:...
com.microsoft.intune.mam.managedbrowse...	https://www.bing.com

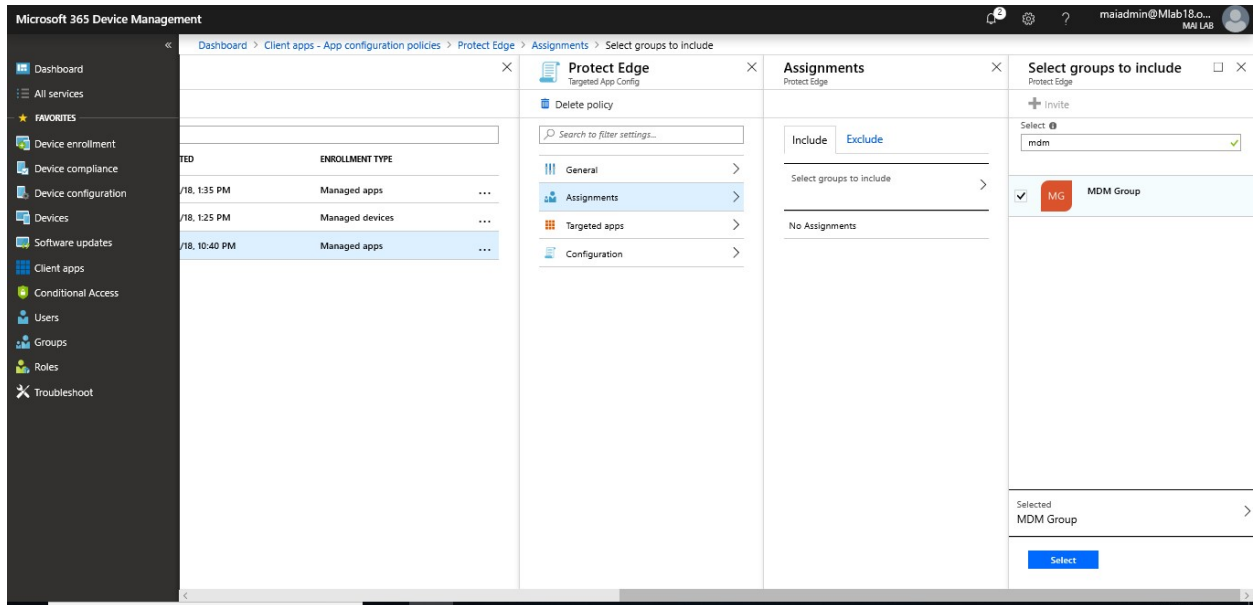
- Click **Add** to add configuration policy.



7. Select **Assignments** to display the include and exclude options.



8. Select **group** on the **Include** tab.



9. Click **X** to close this tab.

Monitor App Protection

Monitor the compliance status of the mobile app management (MAM) policies that you've applied to users at the Intune app protection

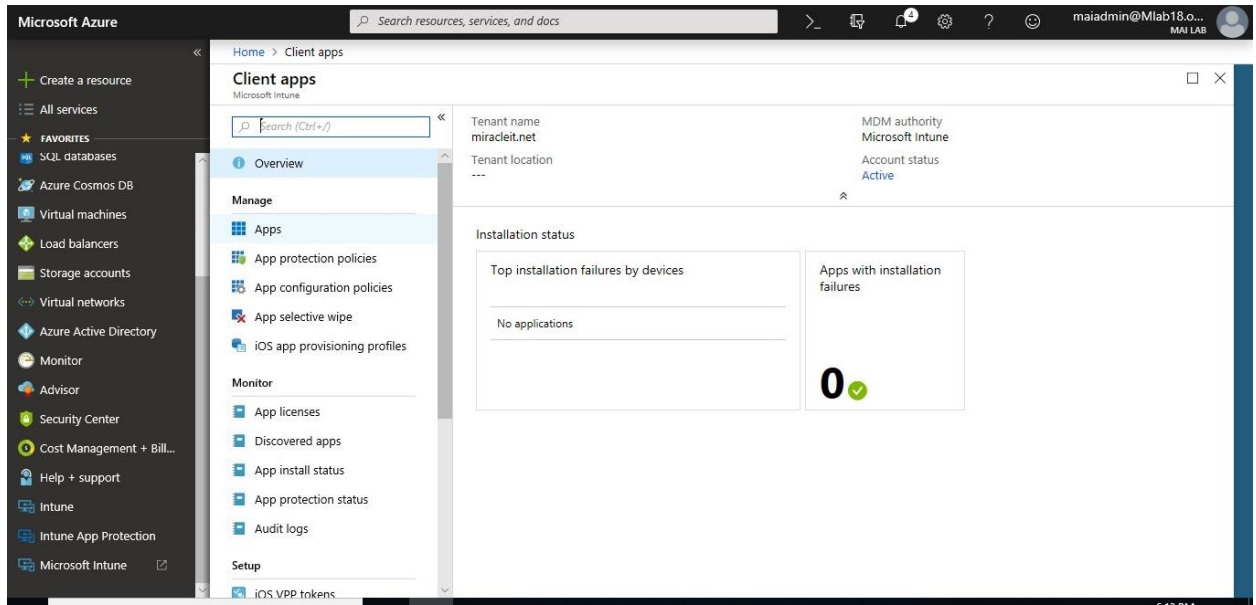
There are three different places to monitor the compliance status:

- Summary view
- Detailed view
- Reporting view

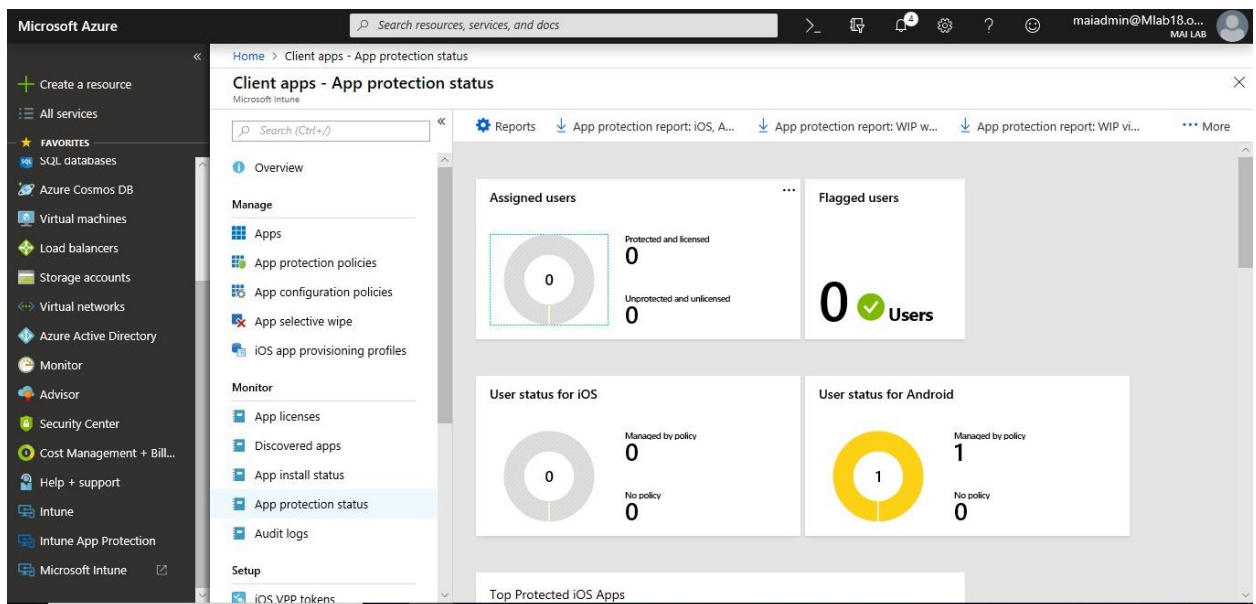
Summary view

1. Sign into the [Azure portal](#). Choose **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. On the **Intune** pane, choose **Client apps**.

Microsoft Intune step by step on Azure portal



3. In the **Client apps** workload, choose **Monitor** > **App protection status**, to see the summary view:



Detailed view

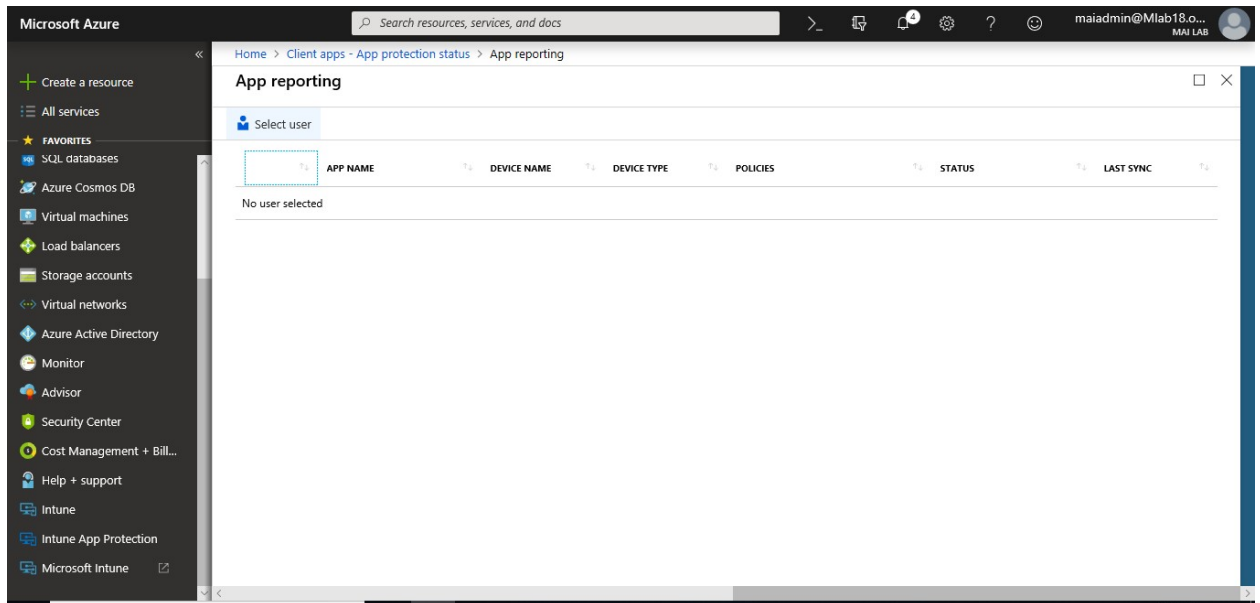
You can get to the detailed view of the summary by choosing the **User status** tile (based on device OS platform), and the **Flagged users** tile.

To see the reporting for a user, follow these steps:

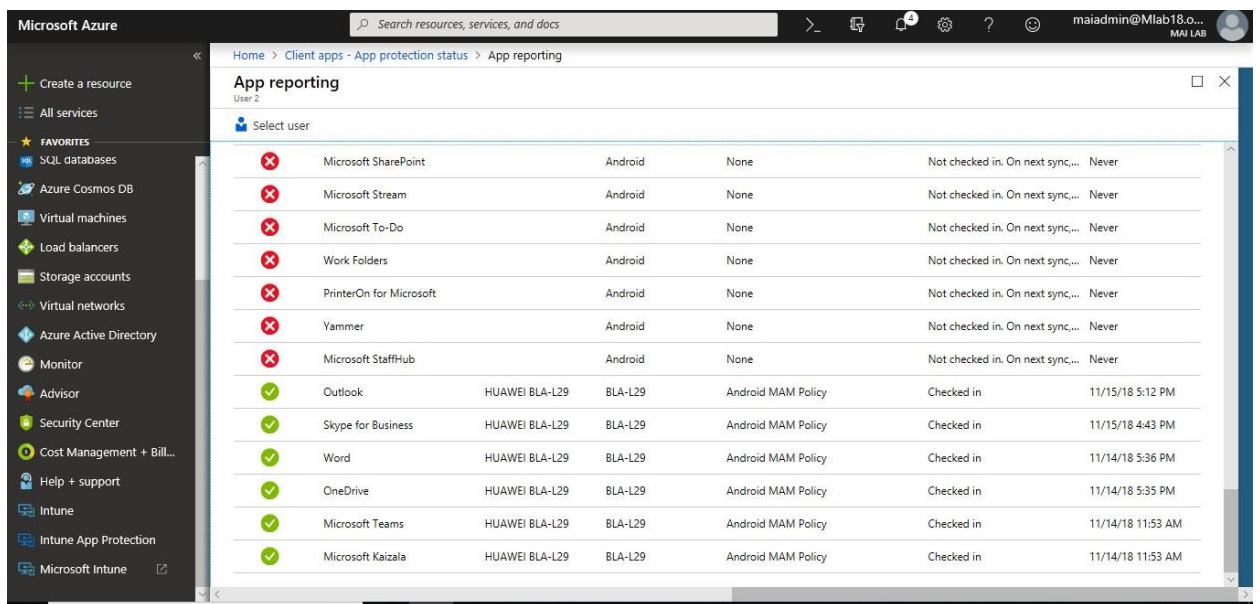
1. To select a user, choose the **Summary** tile and select **Assigned users** or **users status for iOS** or **users status for Android** Dashboard.

Microsoft Intune step by step on Azure portal

2. On the **App reporting** pane that opens, choose **Select user** to search for an Azure Active Directory user.



3. Select the user from the list. You can see the details of the compliance status for that user.

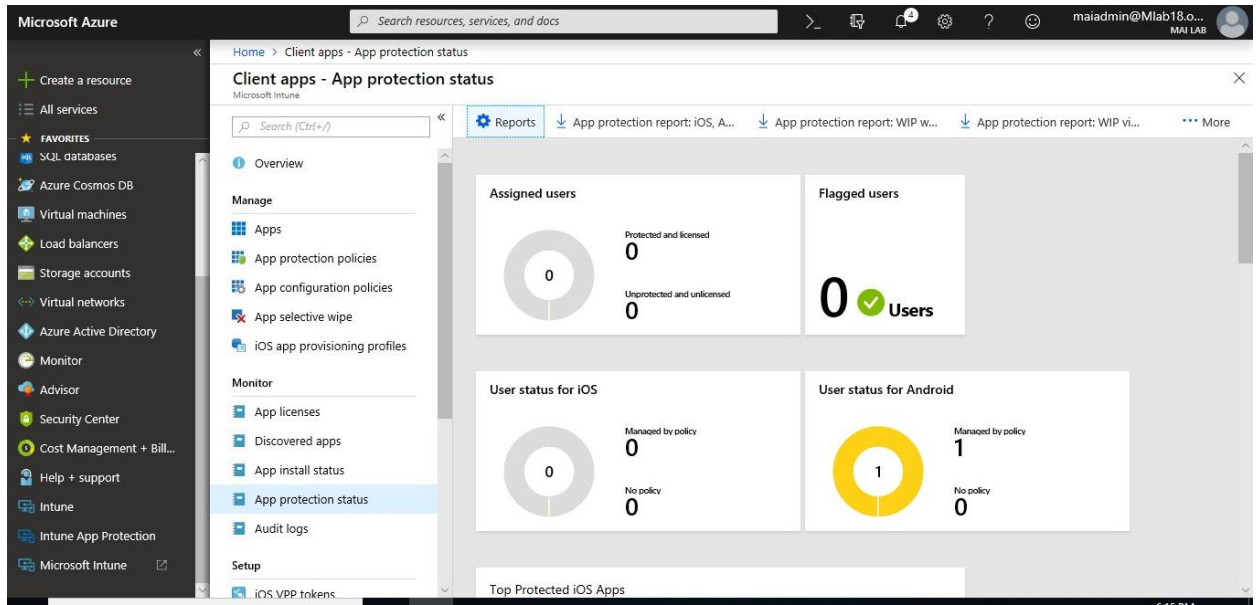


Reporting view

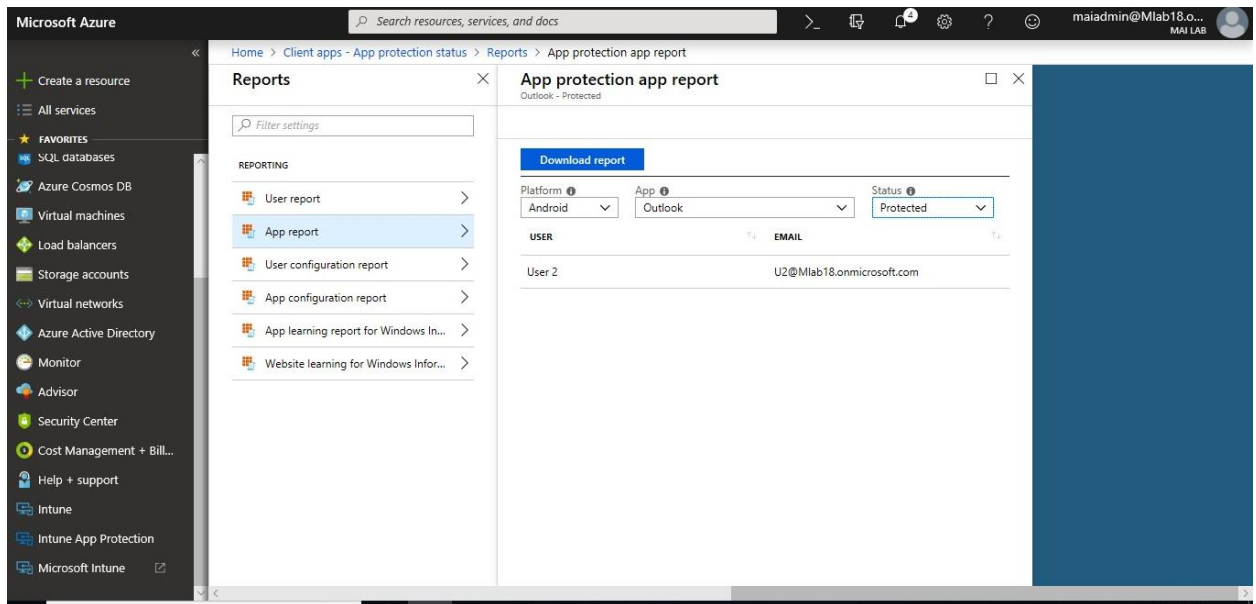
You can find the same reports from the Detailed view, and additional reports to help you with the MAM policy compliance status:

1. Sign in [Intune in the Azure Portal](#). Select **Client apps > App protection status**.
2. Select on **App protection status > Click Reports**.

Microsoft Intune step by step on Azure portal



3. **App protection user report:** It outlines the same information you can find at the **User status** report under the Detailed view section above.
4. **App protection app report:** It provides two different app protection statuses that admins can select before generating the report. The statuses can be protected or unprotected.

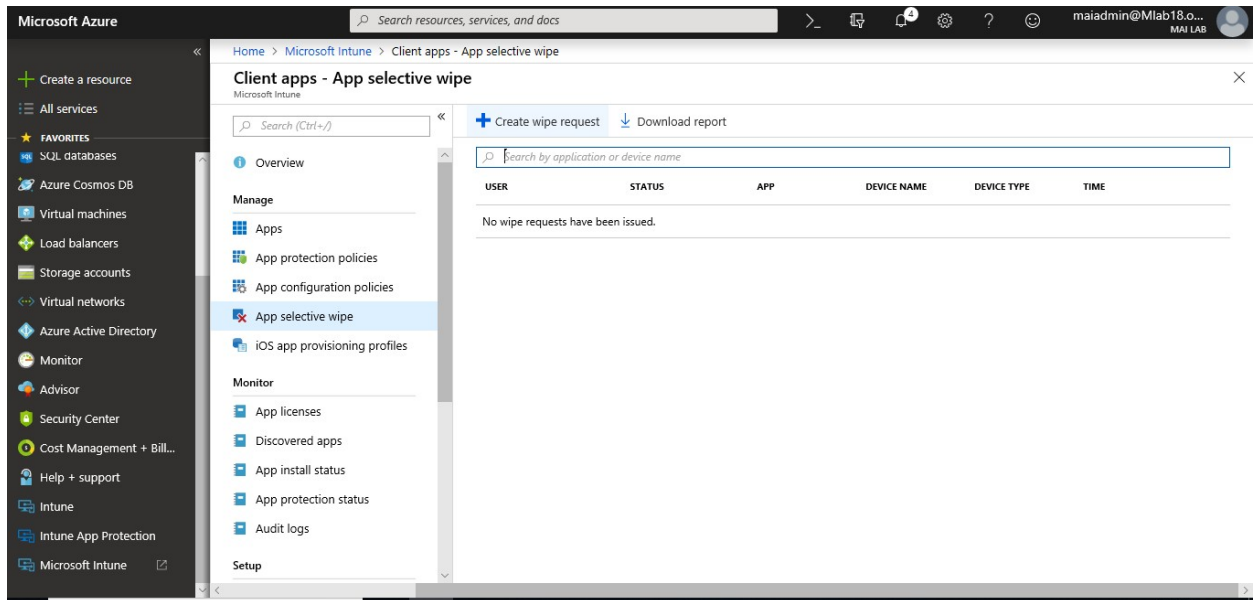


App Selective Wipe

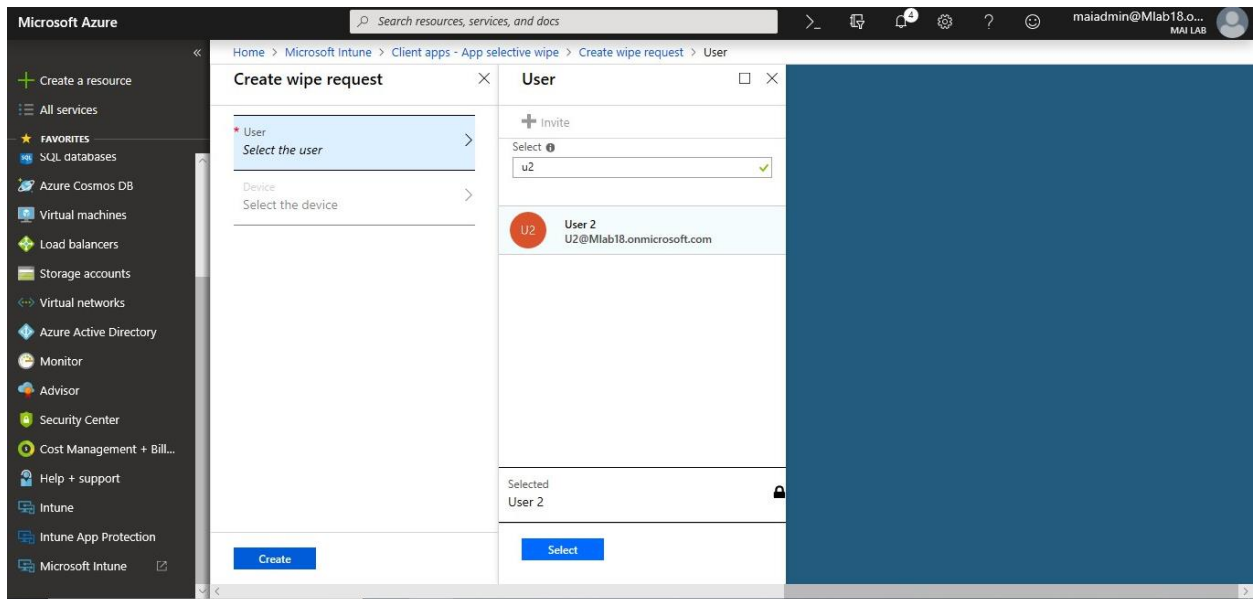
When a device is lost or stolen, or if the employee leaves your company, you want to make sure company app data is removed from the device. But you might not want to remove personal data on the device, especially if the device is an employee-owned device.

Create a wipe request

1. Sign in to the [Azure portal](#). Choose **All services**, type **Intune** in the filter textbox, and select **Intune**. The Intune pane opens, choose the **Client apps** pane.
2. On the **Client apps** pane, choose **App selective wipe**.
3. Choose **Create wipe request**. The **New wipe request** pane opens.



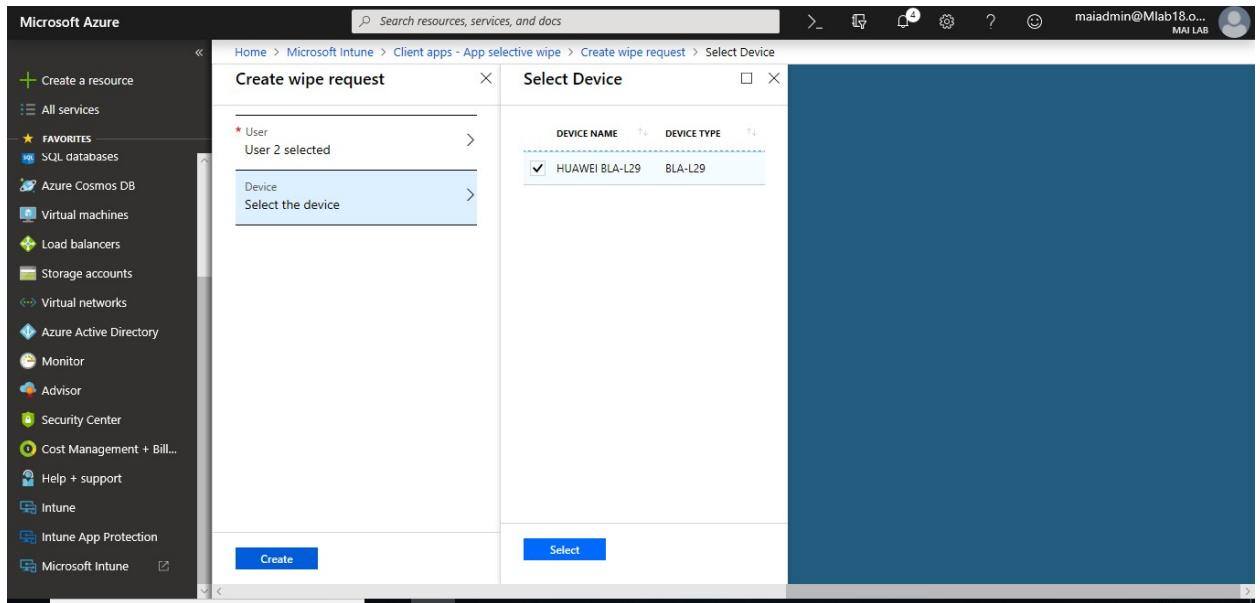
4. Choose a user and then choose **Select** to select the user whose app data you want to wipe.



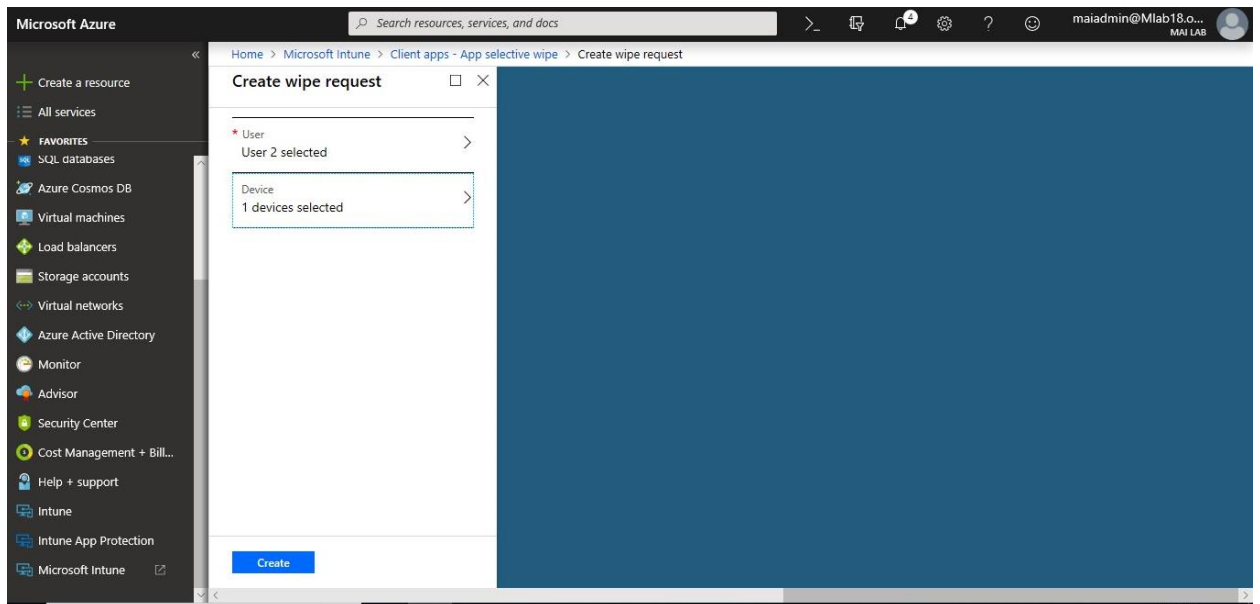
5. Next, choose **Device** from the **New wipe request** pane. This opens the **Select Device** pane that lists all the devices associated with the selected user, and provides two columns,

Microsoft Intune step by step on Azure portal

the device name, which is a friendly name defined by the user, and the device type, its device platform. Select the device you want to wipe.



6. You are now back on the **Create wipe request** pane. Click **Create** to make a wipe request.



7. The service creates and tracks a separate wipe request for each protected app on the device, and the user associated with the wipe request.

Monitor wipe requests

You can have a summarized report that shows the overall status of the wipe request and includes the number of pending requests and failures. To get more details, follow these steps:

1. On the **Client Apps - App selective wipe** pane, you can see the list of your requests grouped by users. Because the system creates a wipe request for each protected app running on the device, you might see multiple requests for a user. The status indicates whether a wipe request is **pending**, **failed**, or **successful**.

USER	STATUS	APP	DEVICE NAME	DEVICE TYPE	TIME
▼ User 2					
	Pending	OneDrive	HUAWEI BLA-L29	BLA-L29	11/15/18 6:37 PM
	Pending	Microsoft Kaizala	HUAWEI BLA-L29	BLA-L29	11/15/18 6:37 PM
	Pending	Microsoft Teams	HUAWEI BLA-L29	BLA-L29	11/15/18 6:37 PM
	Pending	Skype for Business	HUAWEI BLA-L29	BLA-L29	11/15/18 6:37 PM
	Pending	Outlook	HUAWEI BLA-L29	BLA-L29	11/15/18 6:37 PM
	Pending	Word	HUAWEI BLA-L29	BLA-L29	11/15/18 6:37 PM

USER	STATUS	APP	DEVICE NAME	DEVICE TYPE	TIME
▼ User 2					
	Complete	OneDrive	HUAWEI BLA-L29	BLA-L29	11/15/18 6:46 PM
	Complete	Skype for Business	HUAWEI BLA-L29	BLA-L29	11/15/18 6:46 PM
	Complete	Outlook	HUAWEI BLA-L29	BLA-L29	11/15/18 6:46 PM
	Complete	Microsoft Teams	HUAWEI BLA-L29	BLA-L29	11/15/18 6:45 PM
	Complete	Word	HUAWEI BLA-L29	BLA-L29	11/15/18 6:45 PM

Additionally, you are able to see the device name, and its device type, which can be helpful when reading the reports.

Note: The user must open the app for the wipe to occur, and the wipe may take up to 30 minutes after the request was made.

Delete a wipe request

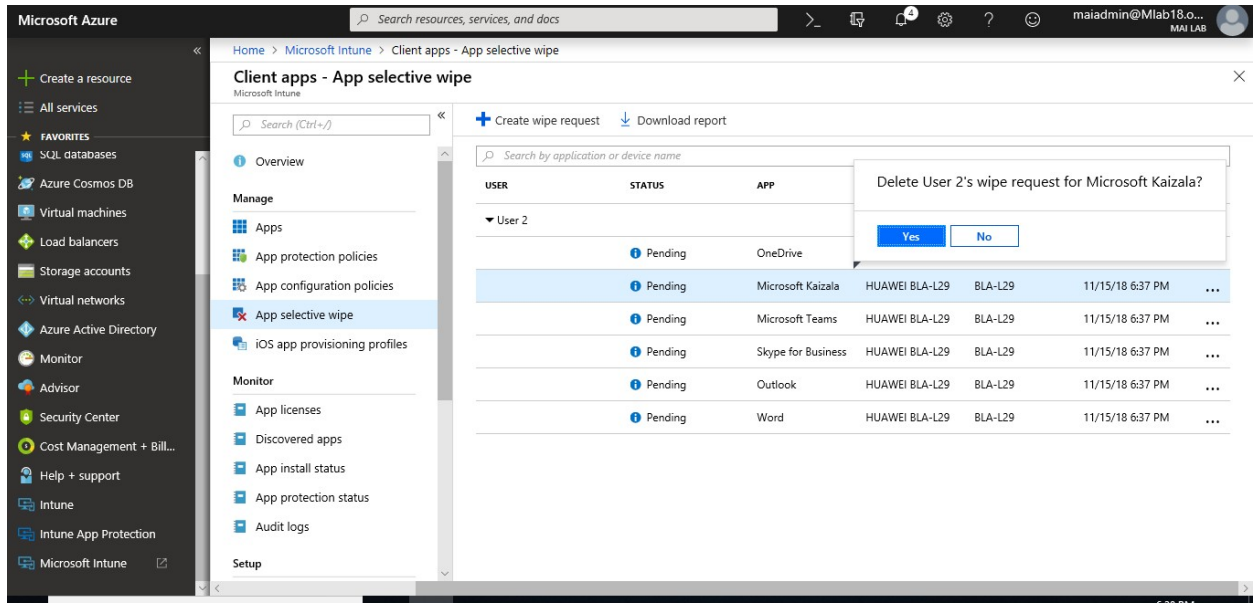
Wipes with pending status are displayed until you manually delete them. To manually delete a wipe request:

1. On the **Client Apps - App selective wipe** pane.
2. From the list, right-click on the wipe request you want to delete, then choose **Delete wipe request**.

The screenshot shows the Microsoft Azure portal interface. The main content area is titled 'Client apps - App selective wipe' under the 'Microsoft Intune' section. A search bar is present at the top of the content area. Below the search bar, there are buttons for 'Create wipe request' and 'Download report'. A table lists wipe requests for 'User 2'. The table has the following columns: USER, STATUS, APP, DEVICE NAME, DEVICE TYPE, and TIME. The 'Microsoft Kaizala' row is highlighted, and a context menu is open over it, showing the option 'Delete wipe request'.

USER	STATUS	APP	DEVICE NAME	DEVICE TYPE	TIME
User 2	Pending	OneDrive	HUAWEI BLA-L29	BLA-L29	11/15/18 6:37 PM
	Pending	Microsoft Kaizala	HUAWEI BLA-L29	BLA-L29	11/15/18 6:37 PM
	Pending	Microsoft Teams	HUAWEI BLA-L29	BLA-L29	11/15/18 6:37 PM
	Pending	Skype for Business	HUAWEI BLA-L29	BLA-L29	11/15/18 6:37 PM
	Pending	Outlook	HUAWEI BLA-L29	BLA-L29	11/15/18 6:37 PM
	Pending	Word	HUAWEI BLA-L29	BLA-L29	11/15/18 6:37 PM

3. You're prompted to confirm the deletion, choose **Yes** to confirm delete.



Wrap Android Apps with the Intune App Wrapping Tool for App protection policies

Use the Microsoft Intune App Wrapping Tool for Android to change the behavior of your in-house Android apps by restricting features of the app without changing the code of the app itself.

Note: The App Wrapping Tool does **not** support apps in the Apple App Store or Google Play Store. It also doesn't support [certain features](#) that require developer integration.

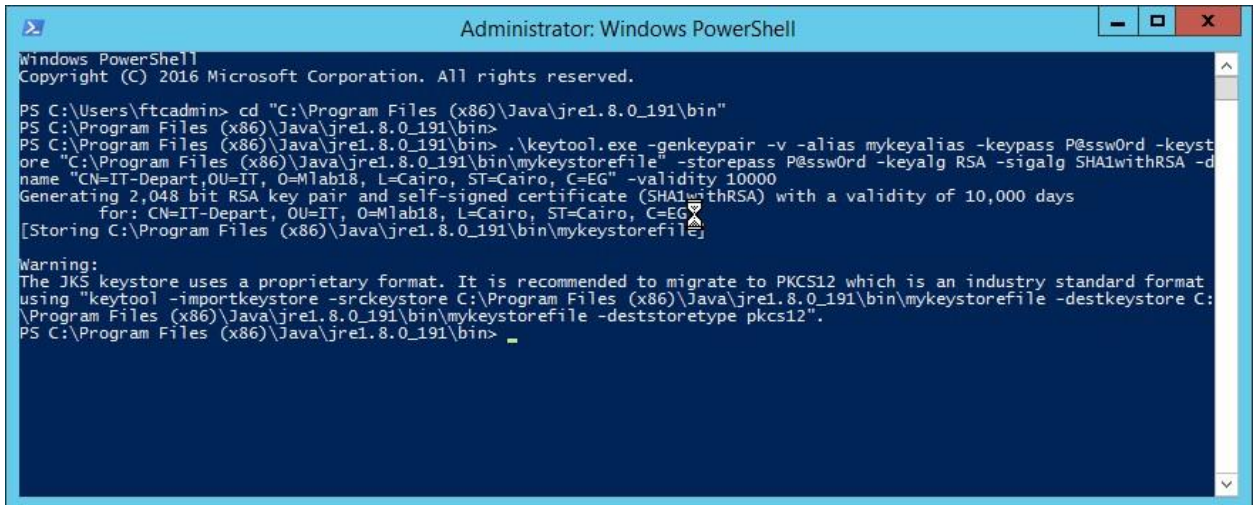
Install the App Wrapping Tool

1. To run the App Wrapping Tool, you must install the latest version of the [Java Runtime Environment](#)
2. The Java executable keytool.exe is used to generate **new** credentials needed to sign the wrapped output app. Any passwords that are set must be secure but make a note of them because they're needed to run the App Wrapping Tool.

```
cd "C:\Program Files (x86)\Java\jre1.8.0_191\bin"
```

```
.\keytool.exe -genkeypair -v -alias mykeyalias -keypass <enter new password> -keystore "C:\Program Files (x86)\Java\jre1.8.0_191\bin\mykeystorefile" -storepass <enter new password> -keyalg RSA -sigalg SHA1withRSA -dname "CN=IT-Depart,OU=IT,O=Mlab18,L=Cairo,ST=Cairo,C=EG" -validity 10000
```

Note: you need to verify the path for java folder because it will be change according to deploy version.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\ftcadmin> cd "C:\Program Files (x86)\Java\jre1.8.0_191\bin"
PS C:\Program Files (x86)\Java\jre1.8.0_191\bin>
PS C:\Program Files (x86)\Java\jre1.8.0_191\bin> .\keytool.exe -genkeypair -v -alias mykeyalias -keypass P@ssw0rd -keystore "C:\Program Files (x86)\Java\jre1.8.0_191\bin\mykeystorefile" -storepass P@ssw0rd -keyalg RSA -sigalg SHA1withRSA -dname "CN=IT-Depart,OU=IT,O=Mlab18,L=Cairo,ST=Cairo,C=EG" -validity 10000
Generating 2,048 bit RSA key pair and self-signed certificate (SHA1withRSA) with a validity of 10,000 days
for: CN=IT-Depart,OU=IT,O=Mlab18,L=Cairo,ST=Cairo,C=EG
[Storing C:\Program Files (x86)\Java\jre1.8.0_191\bin\mykeystorefile]

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format
using "keytool -importkeystore -srckeystore C:\Program Files (x86)\Java\jre1.8.0_191\bin\mykeystorefile -destkeystore C:\
\Program Files (x86)\Java\jre1.8.0_191\bin\mykeystorefile -deststoretype pkcs12".
PS C:\Program Files (x86)\Java\jre1.8.0_191\bin> _
```

- From the [GitHub repository](#), download the installation file **InstallAWT.exe** for the Intune App Wrapping Tool for Android to a Windows computer. Open the installation file.
- Click **Accept the license agreement** and click **Next**.



- Then click close finish the installation.

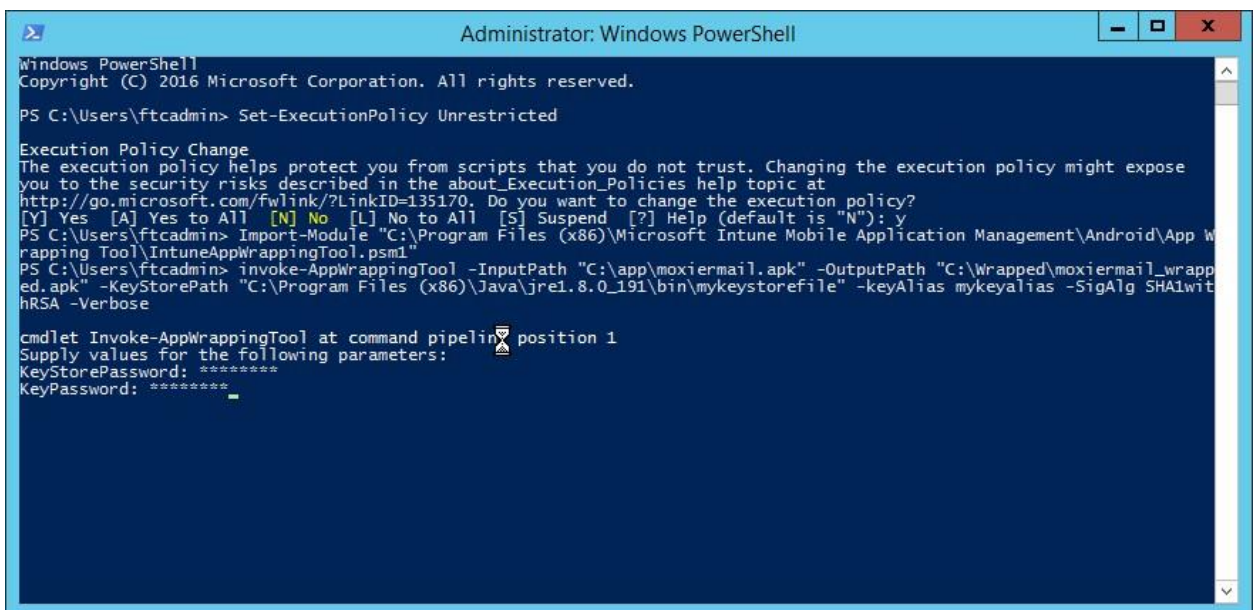
Run the App Wrapping Tool

- On the Windows computer where you installed the App Wrapping Tool, open a PowerShell window. Run this command ***Set-ExecutionPolicy Unrestricted***

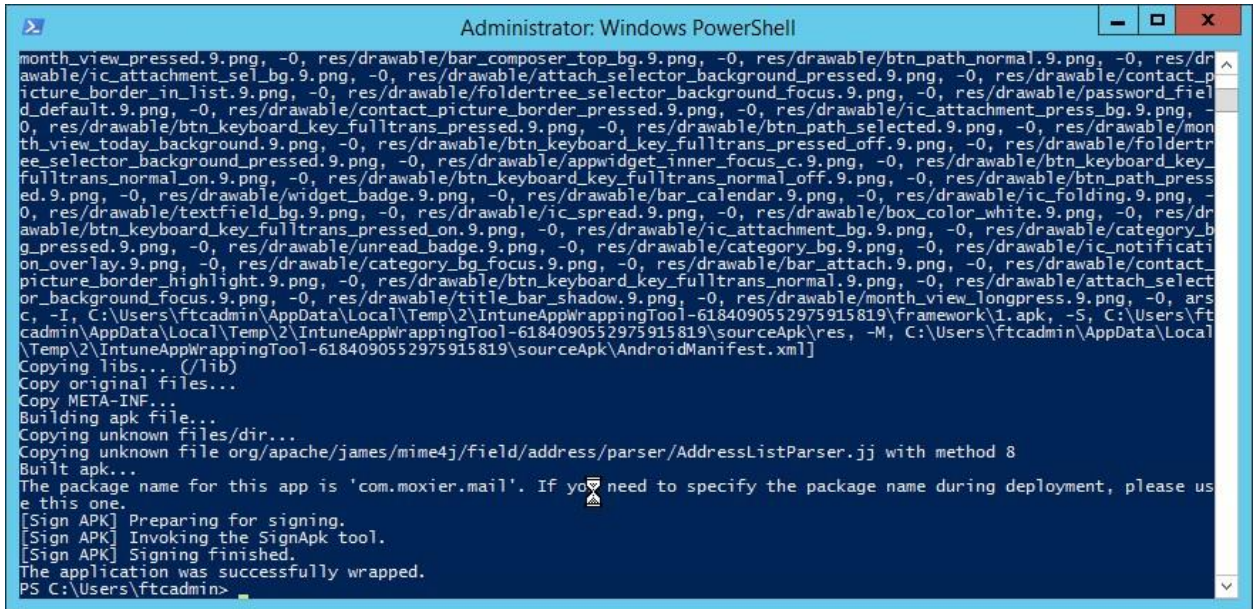


2. Run this command ***Import-Module "C:\Program Files (x86)\Microsoft Intune Mobile Application Management\Android\App Wrapping Tool\IntuneAppWrappingTool.psm1"***
3. Run the tool by using the ***invoke-AppWrappingTool*** command, which has the following usage syntax: Run the App Wrapping Tool on the app MoxierMail.apk.

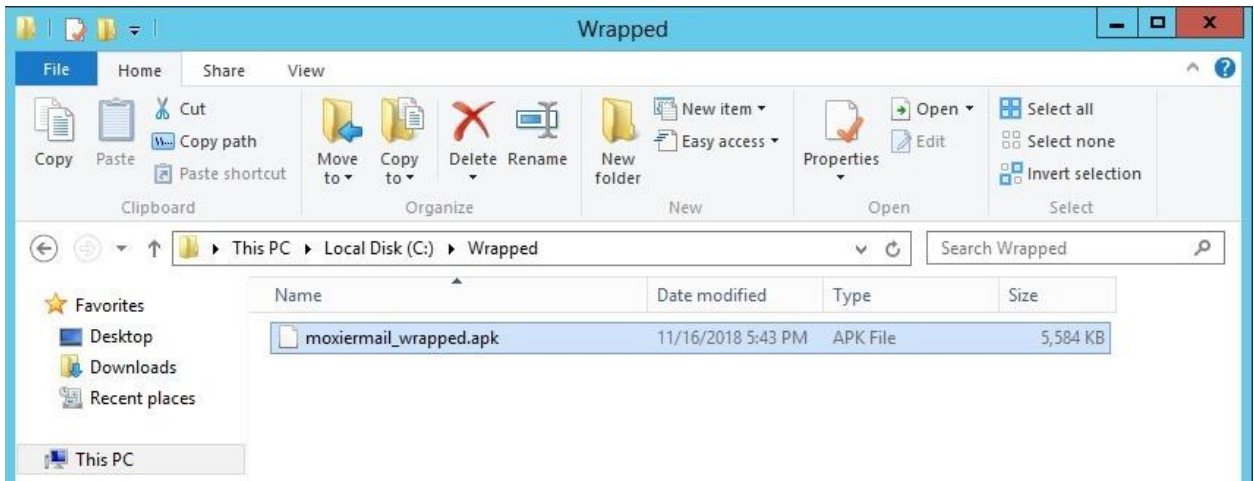
Invoke-AppWrappingTool -InputPath "c:\app\MoxierMail.apk" -OutputPath "c:\wrapped\MoxierMail_wrapped.apk -KeyStorePath "C:\Program Files (x86)\Java\jre1.8.0_191\bin\mykeystorefile" -keyAlias mykeyalias -SigAlg SHA1withRSA -Verbose



4. You will then be prompted for **KeyStorePassword** and **KeyPassword**. Enter the credentials you used to create the key store file.
5. The wrapped app and a log file are generated and saved in the output path you specified.



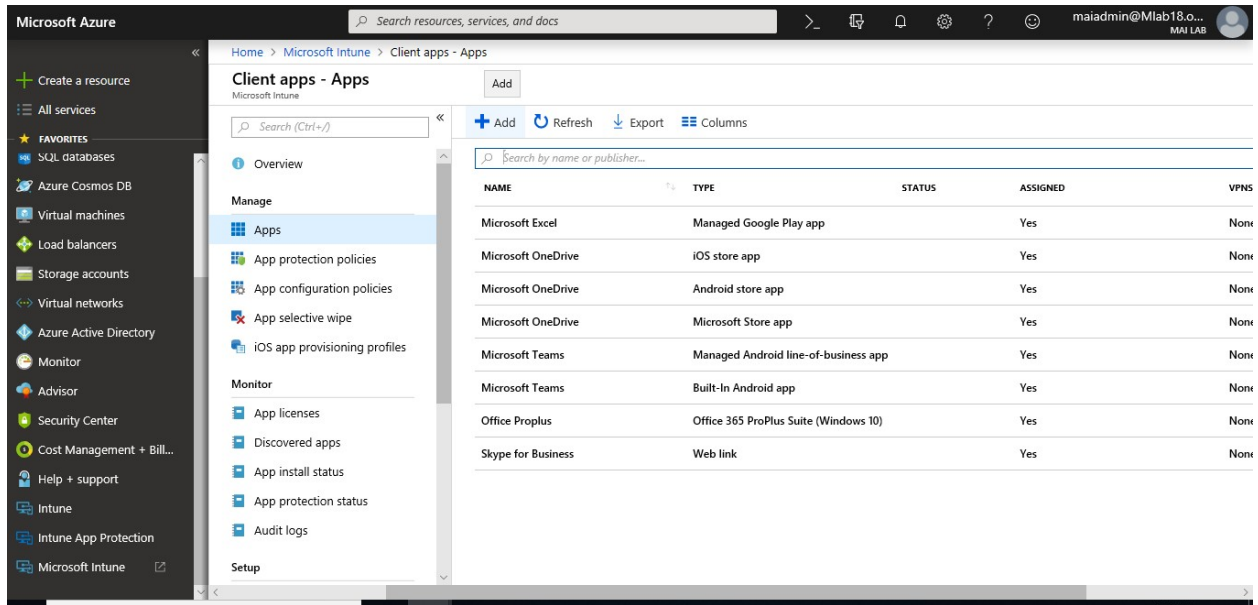
```
Administrator: Windows PowerShell
month_view_pressed.9.png, -0, res/drawable/bar_composer_top_bg.9.png, -0, res/drawable/btn_path_normal.9.png, -0, res/drawable/ic_attachment_sel_bg.9.png, -0, res/drawable/attach_selector_background_pressed.9.png, -0, res/drawable/contact_picture_border_in_list.9.png, -0, res/drawable/foldertree_selector_background_focus.9.png, -0, res/drawable/password_field_default.9.png, -0, res/drawable/contact_picture_border_pressed.9.png, -0, res/drawable/ic_attachment_press_bg.9.png, -0, res/drawable/btn_keyboard_key_fulltrans_pressed.9.png, -0, res/drawable/btn_path_selected.9.png, -0, res/drawable/month_view_today_background.9.png, -0, res/drawable/btn_keyboard_key_fulltrans_pressed_off.9.png, -0, res/drawable/foldertree_selector_background_pressed.9.png, -0, res/drawable/appwidget_inner_focus_c.9.png, -0, res/drawable/btn_keyboard_key_fulltrans_normal_on.9.png, -0, res/drawable/btn_keyboard_key_fulltrans_normal_off.9.png, -0, res/drawable/btn_path_pressed.9.png, -0, res/drawable/widget_badge.9.png, -0, res/drawable/bar_calendar.9.png, -0, res/drawable/ic_folding.9.png, -0, res/drawable/textfield_bg.9.png, -0, res/drawable/ic_spread.9.png, -0, res/drawable/box_color_white.9.png, -0, res/drawable/btn_keyboard_key_fulltrans_pressed_on.9.png, -0, res/drawable/ic_attachment_bg.9.png, -0, res/drawable/category_bg_pressed.9.png, -0, res/drawable/unread_badge.9.png, -0, res/drawable/category_bg.9.png, -0, res/drawable/ic_notification_overlay.9.png, -0, res/drawable/category_bg_focus.9.png, -0, res/drawable/bar_attach.9.png, -0, res/drawable/contact_picture_border_highlight.9.png, -0, res/drawable/btn_keyboard_key_fulltrans_normal.9.png, -0, res/drawable/attach_selector_background_focus.9.png, -0, res/drawable/title_bar_shadow.9.png, -0, res/drawable/month_view_longpress.9.png, -0, ars c, -I, C:\Users\ftcadmin\AppData\Local\Temp\2\IntuneAppWrappingTool-6184090552975915819\framework\1.apk, -S, C:\Users\ftcadmin\AppData\Local\Temp\2\IntuneAppWrappingTool-6184090552975915819\sourceApk\res, -M, C:\Users\ftcadmin\AppData\Local\Temp\2\IntuneAppWrappingTool-6184090552975915819\sourceApk\AndroidManifest.xml]
Copying libs... (/lib)
Copy original files...
Copy META-INF...
Building apk file...
Copying unknown files/dir...
Copying unknown file org/apache/james/mime4j/field/address/parser/AddressListParser.jj with method 8
Built apk...
The package name for this app is 'com.moxier.mail'. If you need to specify the package name during deployment, please use this one.
[Sign APK] Preparing for signing.
[Sign APK] Invoking the SignApk tool.
[Sign APK] Signing finished.
The application was successfully wrapped.
PS C:\Users\ftcadmin>
```



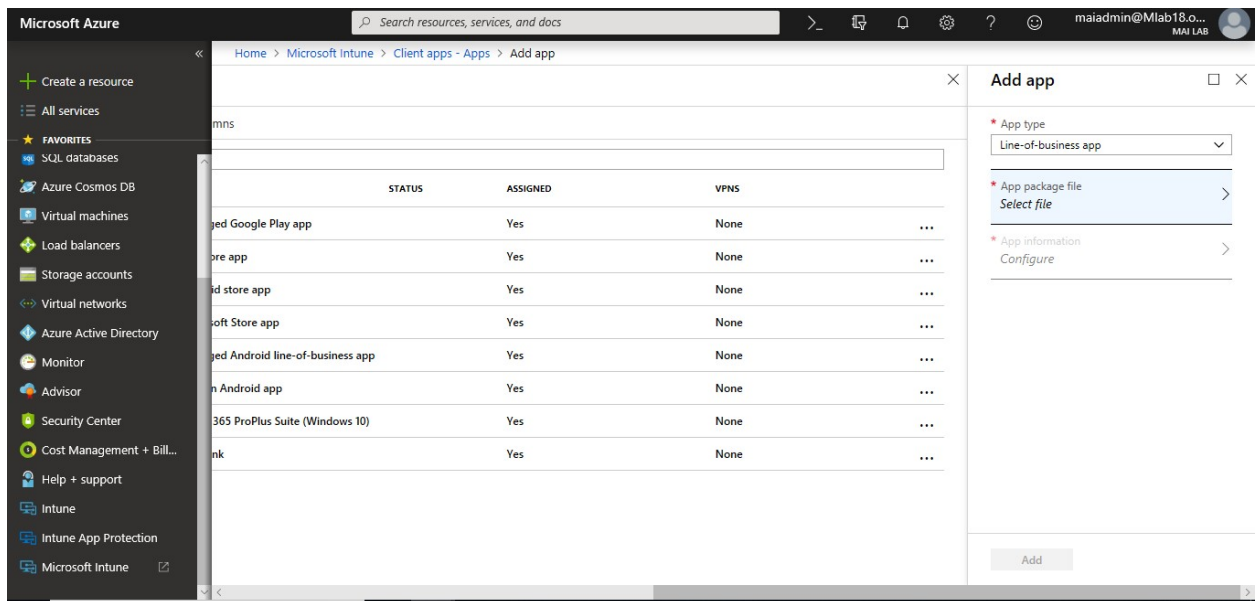
Configure Wrapped Line of Business App

To add a line of business app to your available apps in Microsoft Intune, do the following:

1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is in the **Monitoring + Management** section.
2. In the **Intune** pane, select **Client apps**.
3. In the **Client apps** workload, select **Manage** > **Apps**.
4. Above the list of apps, select **Add**.



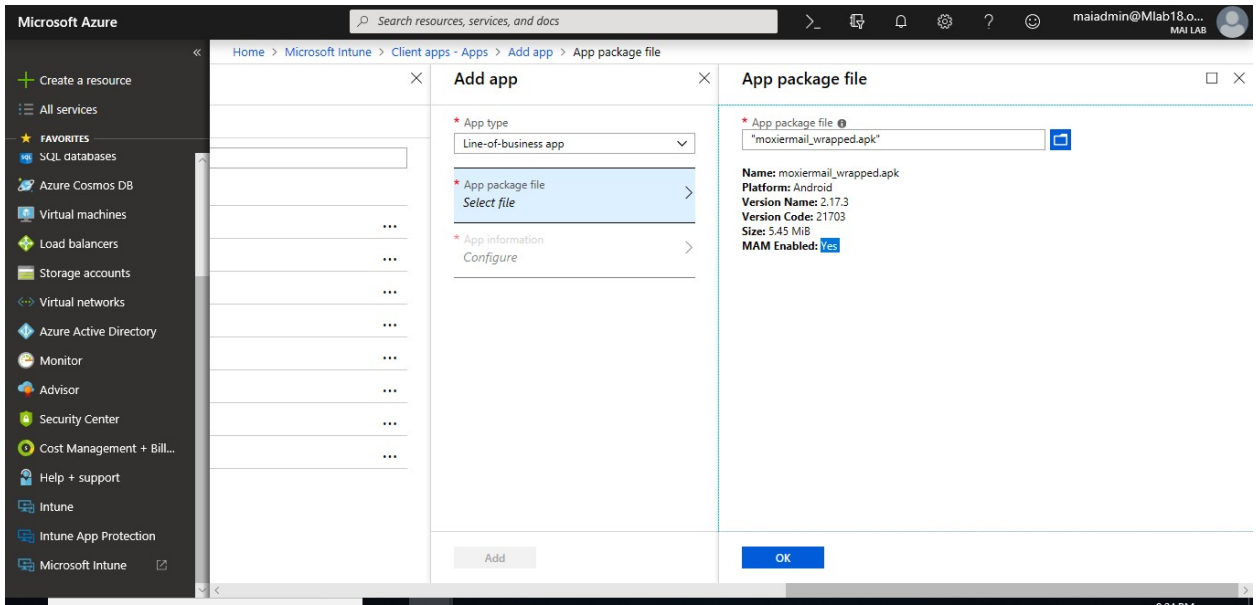
5. In the **Add app** pane, select **Line-of-business app**.



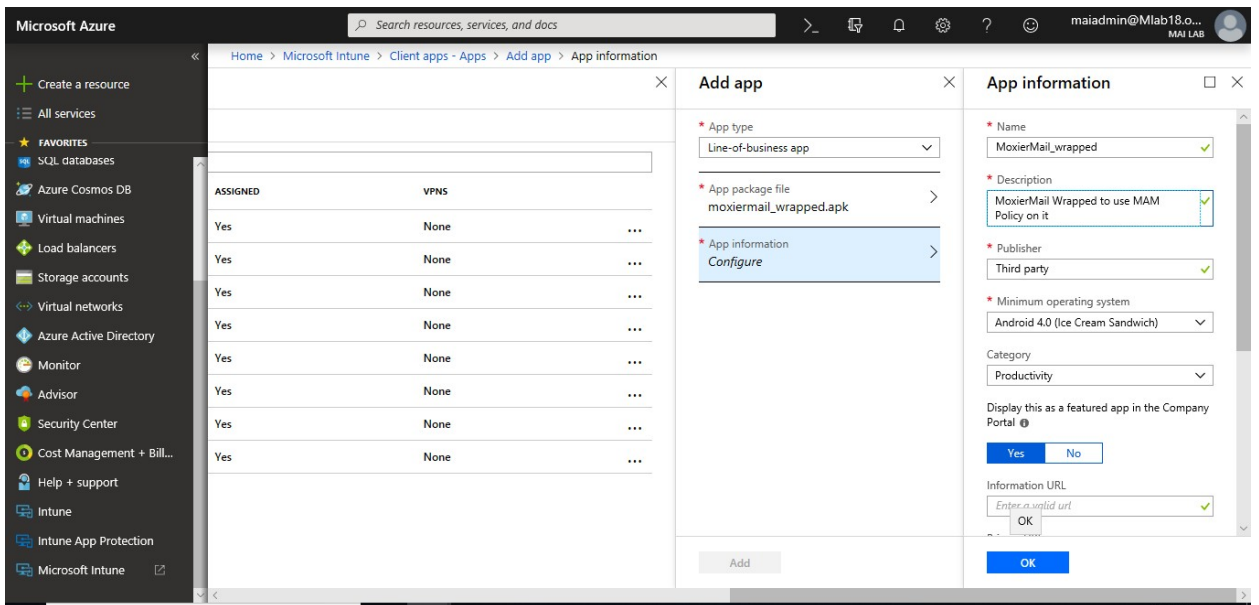
6. In the **Add app** pane, select **App package file**.

7. In the **App package file** pane, select the browse button. Then select an Android installation file with the extension **.apk**. You will find **MAM Enabled**. When you're finished, select **OK**.

Microsoft Intune step by step on Azure portal

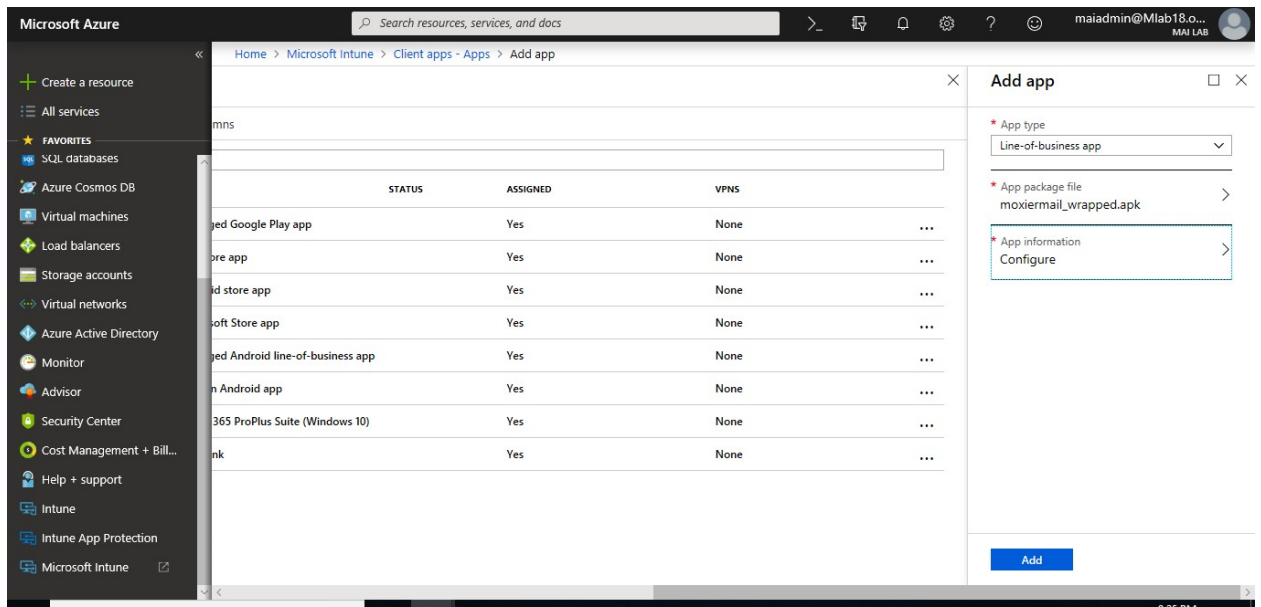


8. In the **App information** pane, add the details for your app.



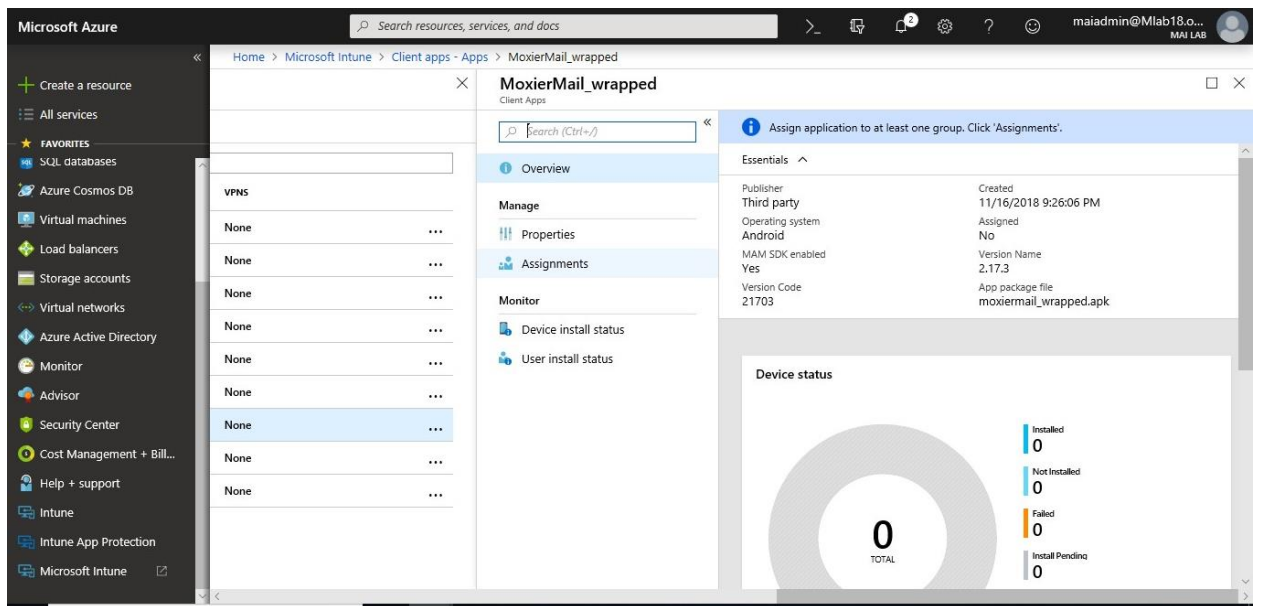
9. When you're finished, select **OK**.

10. In the **Add app** pane, verify that the details of your app are correct. Select **Add** to upload the app to Intune.

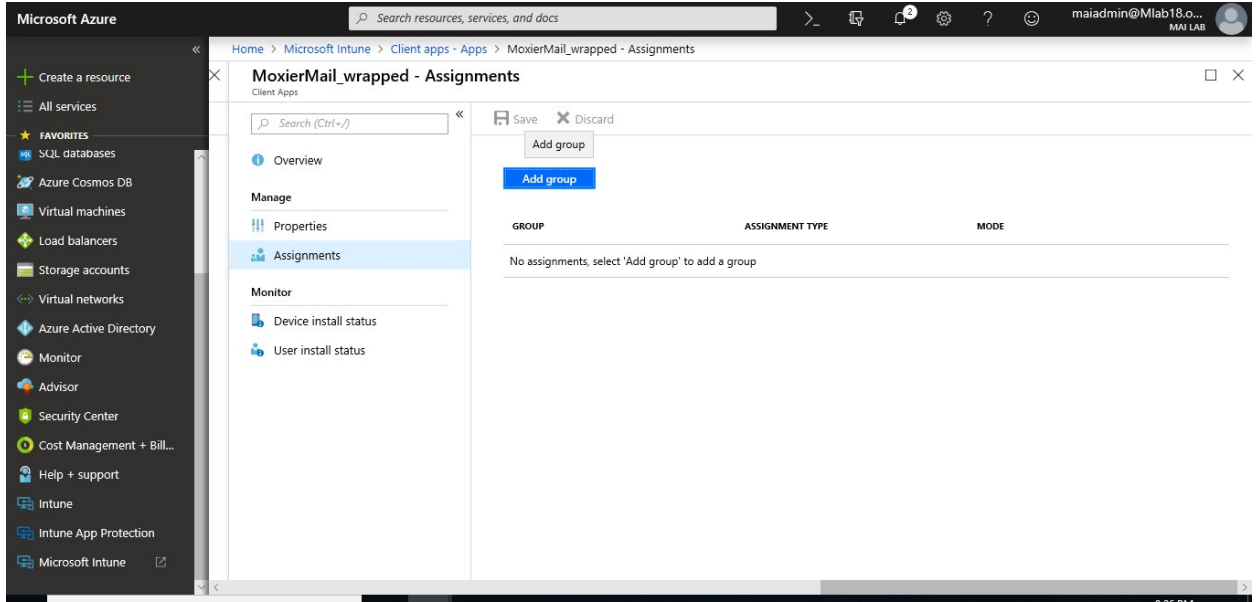


To assign specific group on Wrapped Line of Business App

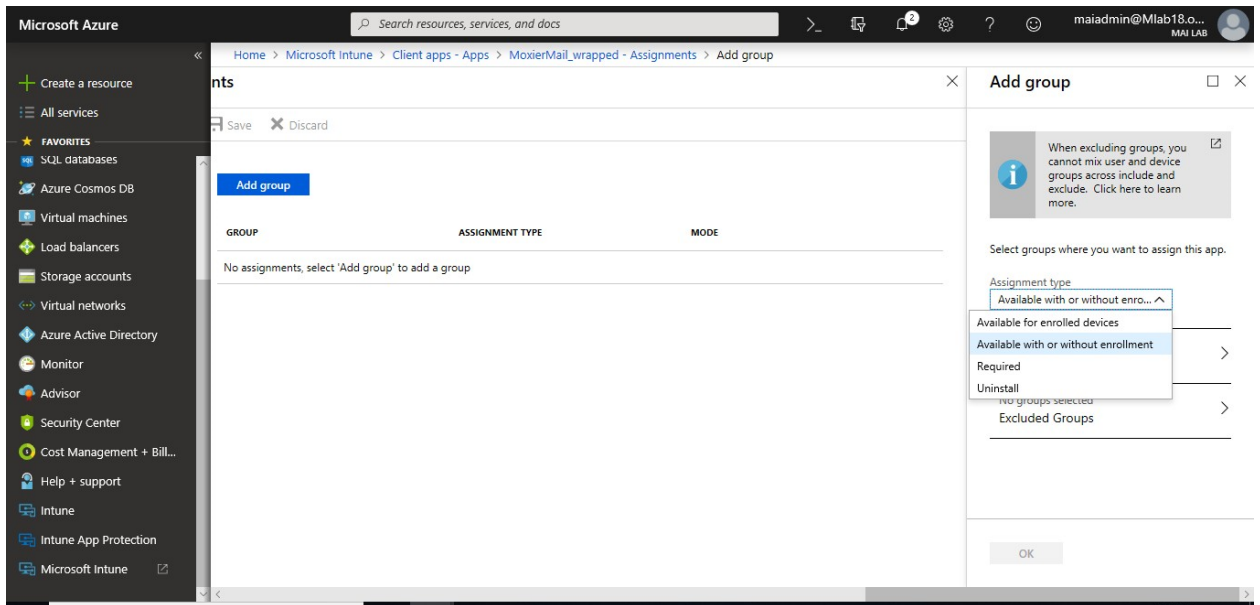
1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** menu, select **Client apps**.
3. In the **Manage** section of the menu, select **Apps**.
4. In the **Apps** pane, select the app you want to assign.
5. In the **Manage** section of the menu, select **Assignments**.



6. Select **Add Group** to open the **Add group** pane that is related to the app.



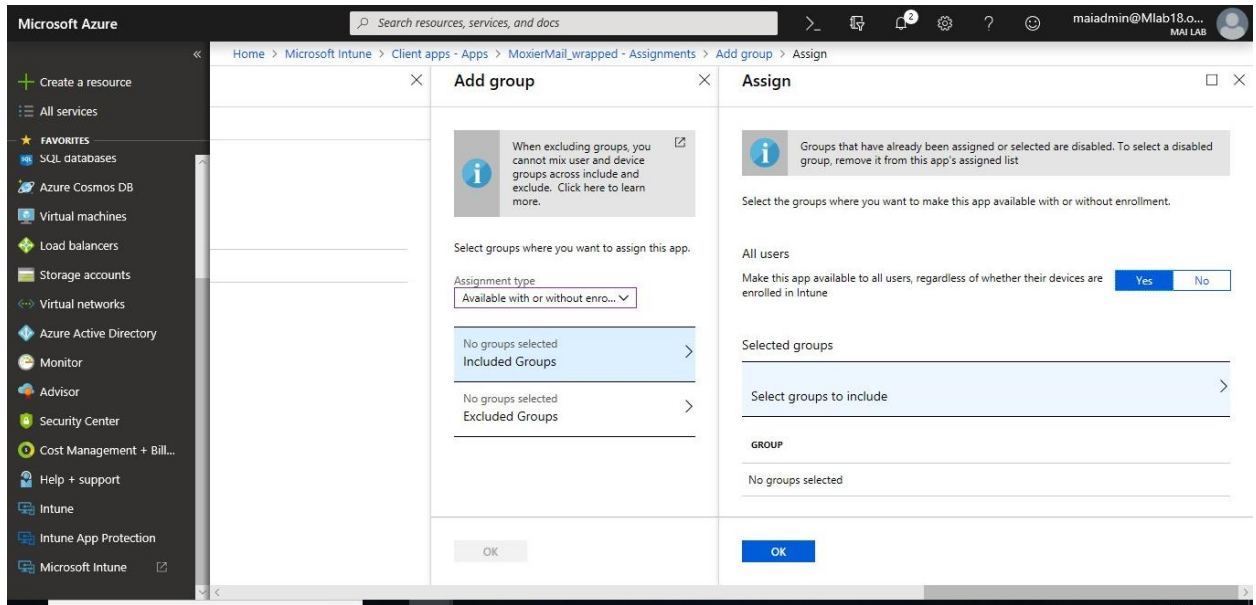
7. For the specific app, select an **assignment type**: Available with or without enrollment.



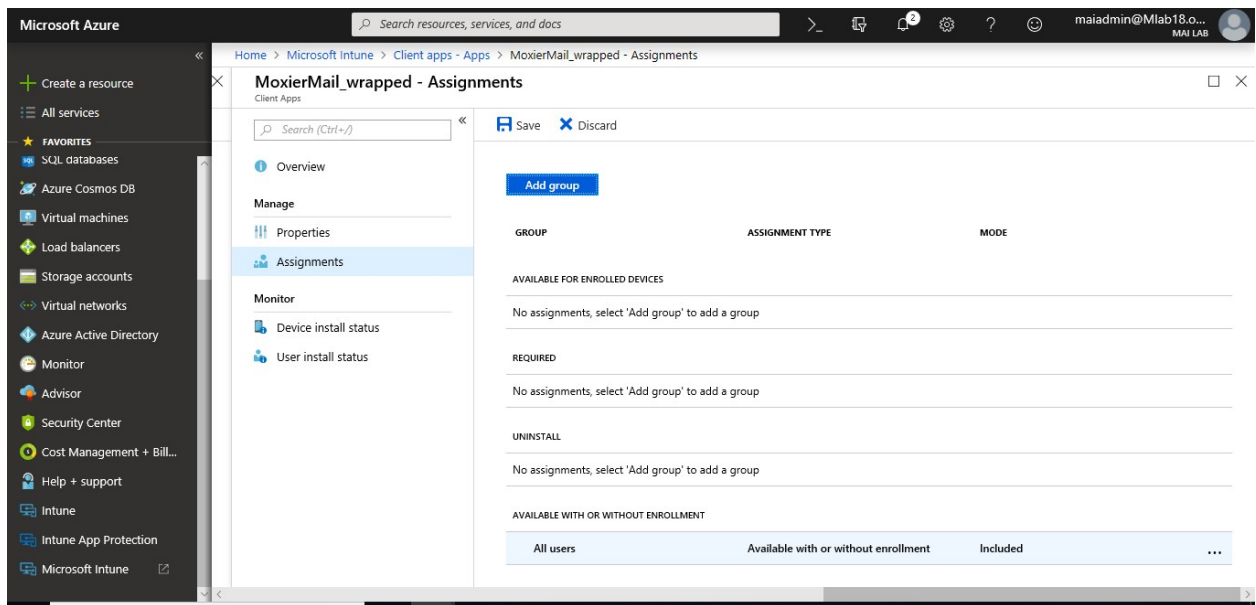
8. To select the groups of users that are affected by this app assignment, select **Included Groups**. After you have selected one or more groups to include, Click **Select**.

9. In the **Assign** pane, select **OK** to complete the included groups selection.

Microsoft Intune step by step on Azure portal



10. In the app **Assignments** pane, select **Save**.

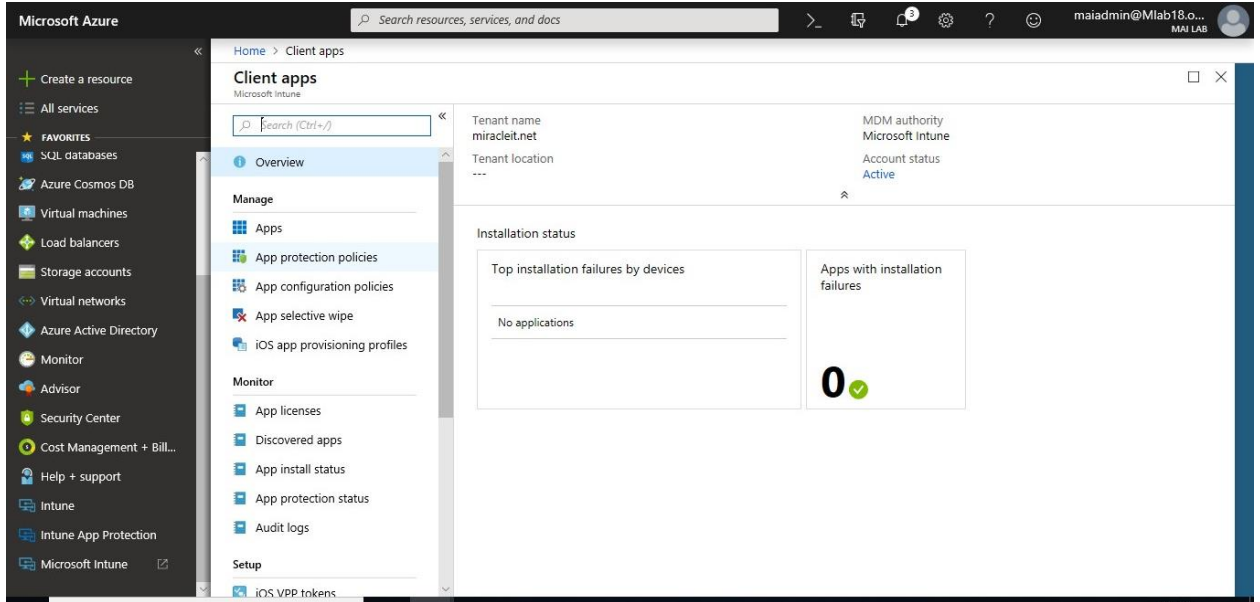


Note: End user need to trust developer app on Android Phone. Go to **Settings > Security >** Check the option **"Unknown sources"** > Tap **OK** on the prompt message > Select **"Trust"**. Once application become **trust**, End User will be able to install it from **Company portal**.

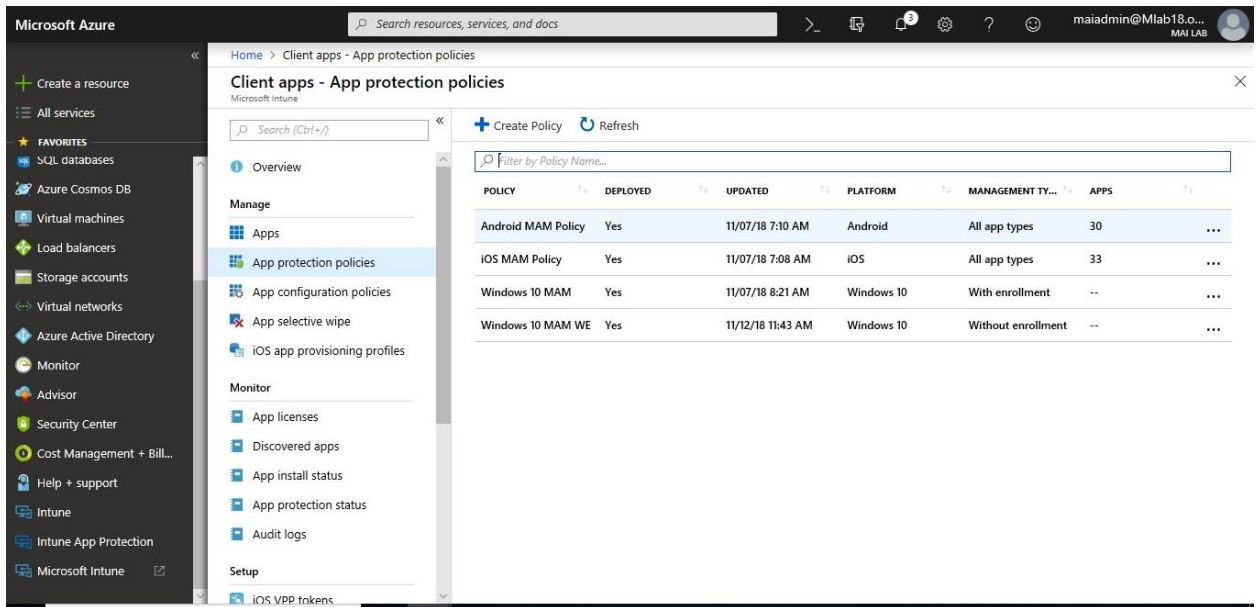
To apply MAM Policy, you need to follow below steps:

1. Sign in to the [Azure portal](#). Select **All services > Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** menu, select **Client apps**.
3. In the **Manage** section of the menu, select **App protection policies**.

Microsoft Intune step by step on Azure portal

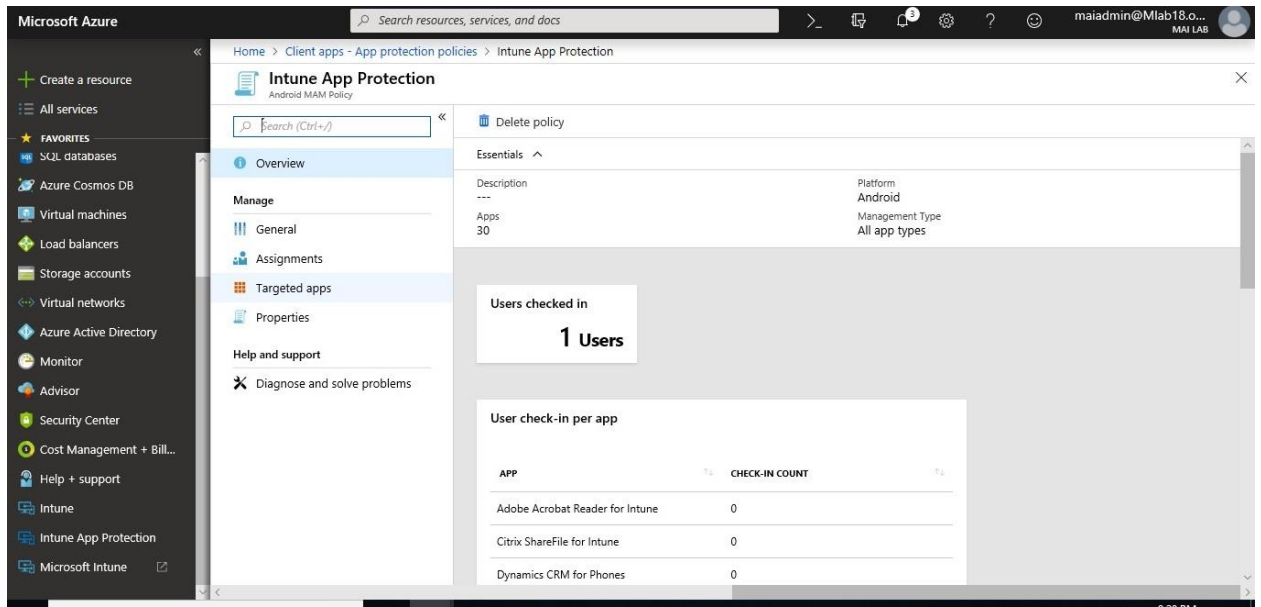


4. In the **App protection policies** pane, select the Android app policy you want to assign.

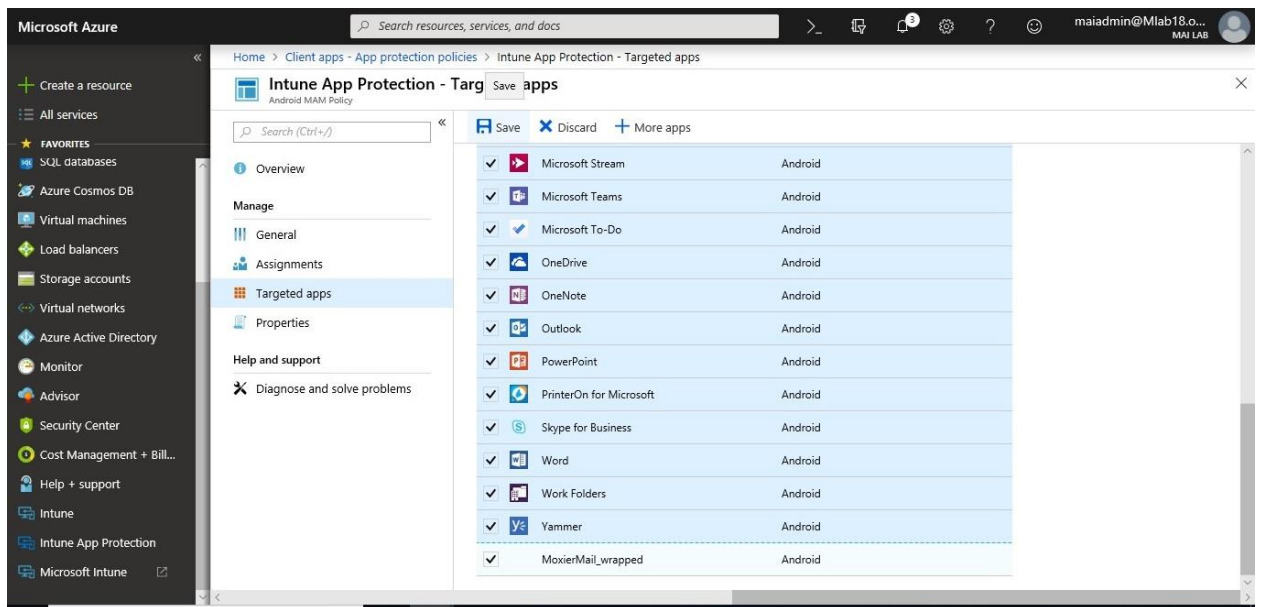


5. In the **Manage** section of the menu, select **Targeted Apps**.

Microsoft Intune step by step on Azure portal



6. Select wrapped app that you create it. Select **Save**.



Wrap iOS Apps with the Intune App Wrapping Tool for App protection policies

Use the Microsoft Intune App Wrapping Tool for iOS to enable Intune app protection policies for in-house iOS apps without changing the code of the app itself.

General prerequisites for the App Wrapping Tool

Before you run the App Wrapping Tool, you need to fulfill some general prerequisites:

Microsoft Intune step by step on Azure portal

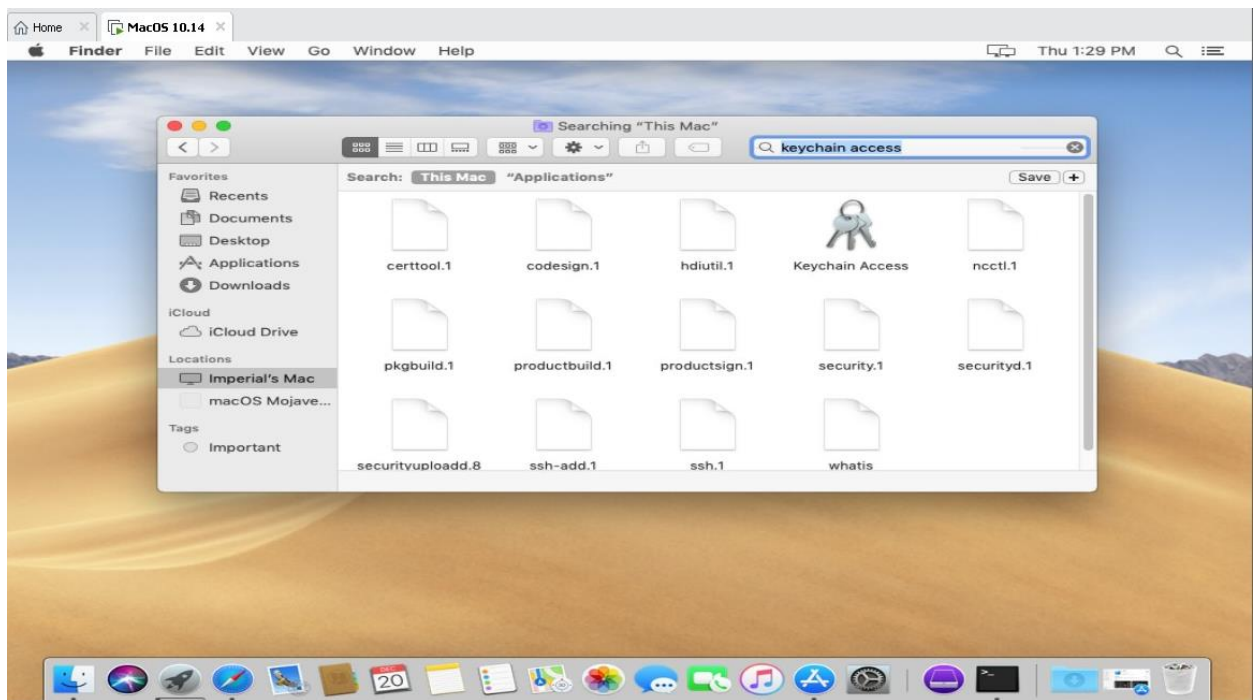
- Download the [Microsoft Intune App Wrapping Tool for iOS](#) from GitHub.
- A macOS computer that runs OS X 10.8.5 or later and has the [Xcode](#) toolset version 9 or later installed.
- The input iOS app must be developed and signed by your company or an independent software vendor (ISV).
 - The input app file must have the extension **.ipa** or **.app**.
 - The input app must be compiled for iOS 10 or later.
 - The input app cannot be encrypted.
 - The input app cannot have extended file attributes.
 - The input app must have entitlements set before being processed by the Intune App Wrapping Tool.

Note: Below Steps show configuration within Individual Developer Apple account as it's lab but within Organization, you will use [Apple Developer Enterprise Account](#).

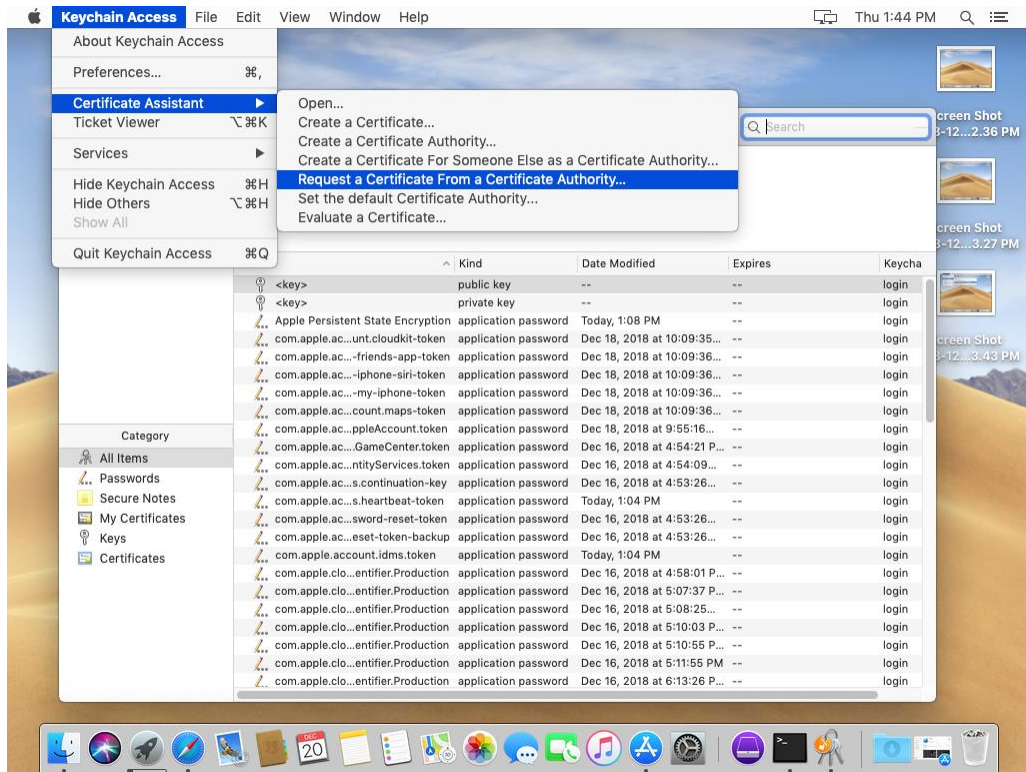
Create an Apple signing certificate

To create a Certificate Signing Request follow below steps:

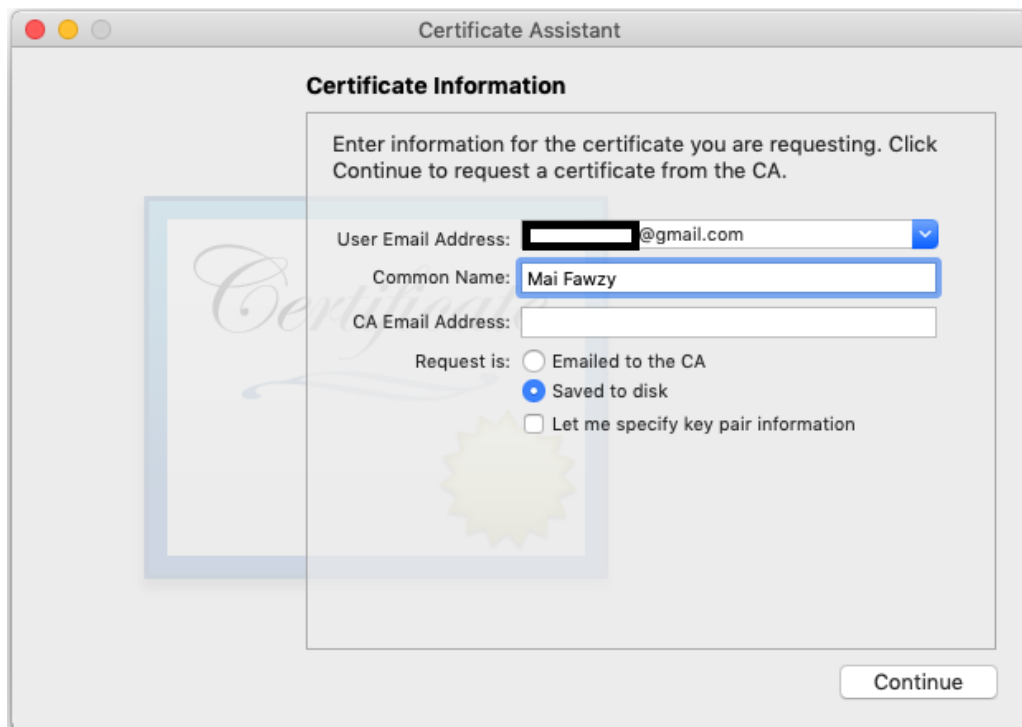
1. On your macOS computer, launch the **Keychain Access** application.



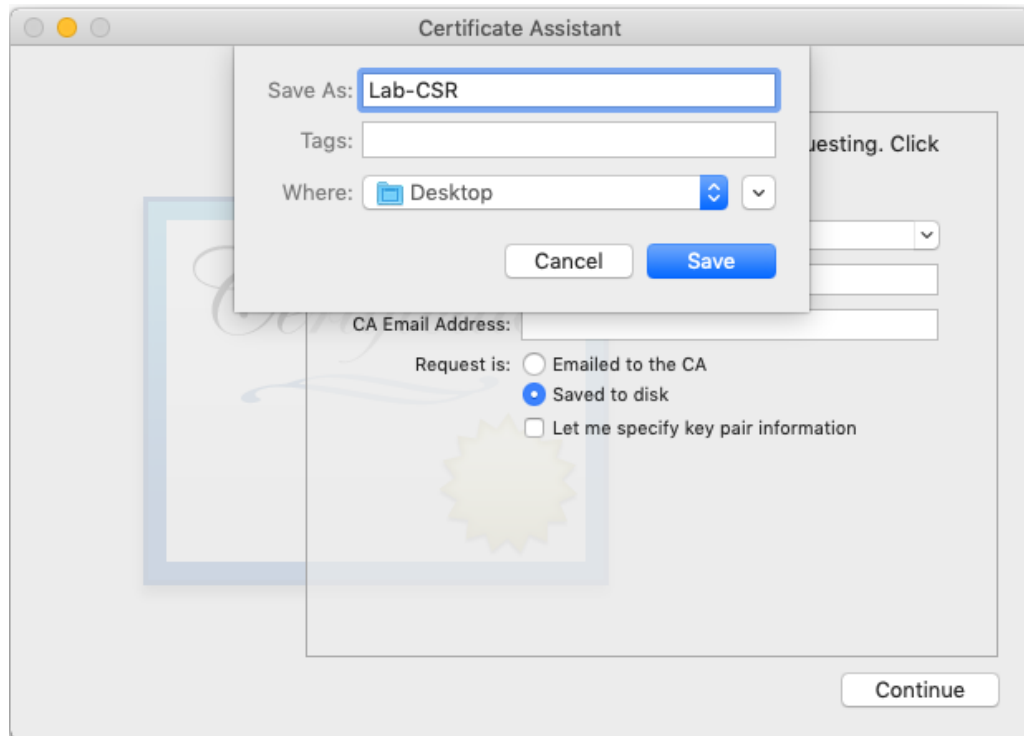
2. On the macOS menu at the top of the screen, go to **Keychain Access > Certificate Assistant > Request a Certificate from a Certificate Authority**.



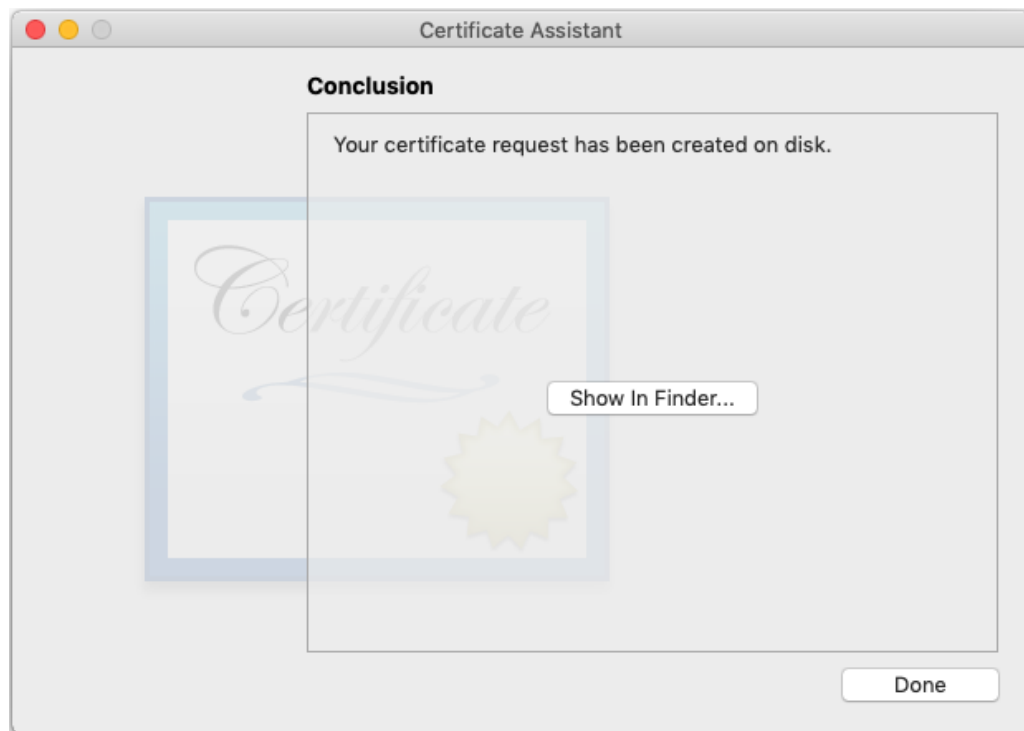
3. Follow the instructions from the Apple developer site above on how to create a CSR file. Save the CSR file to your macOS computer.



4. Save CSR file.



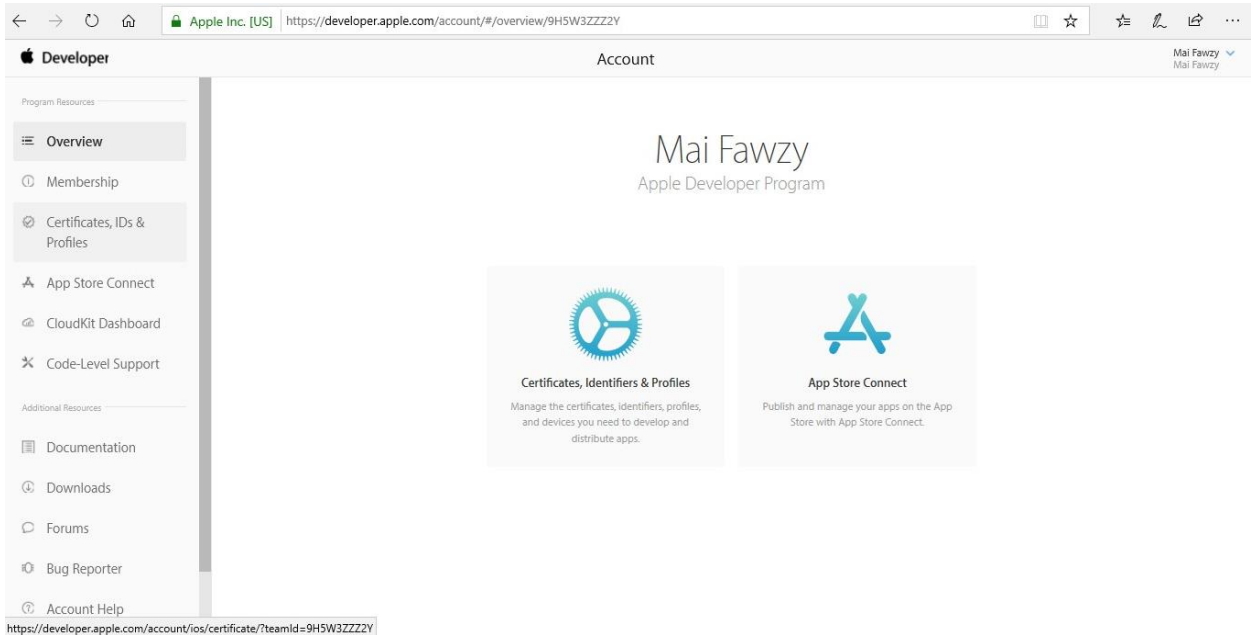
5. Click **Done**.



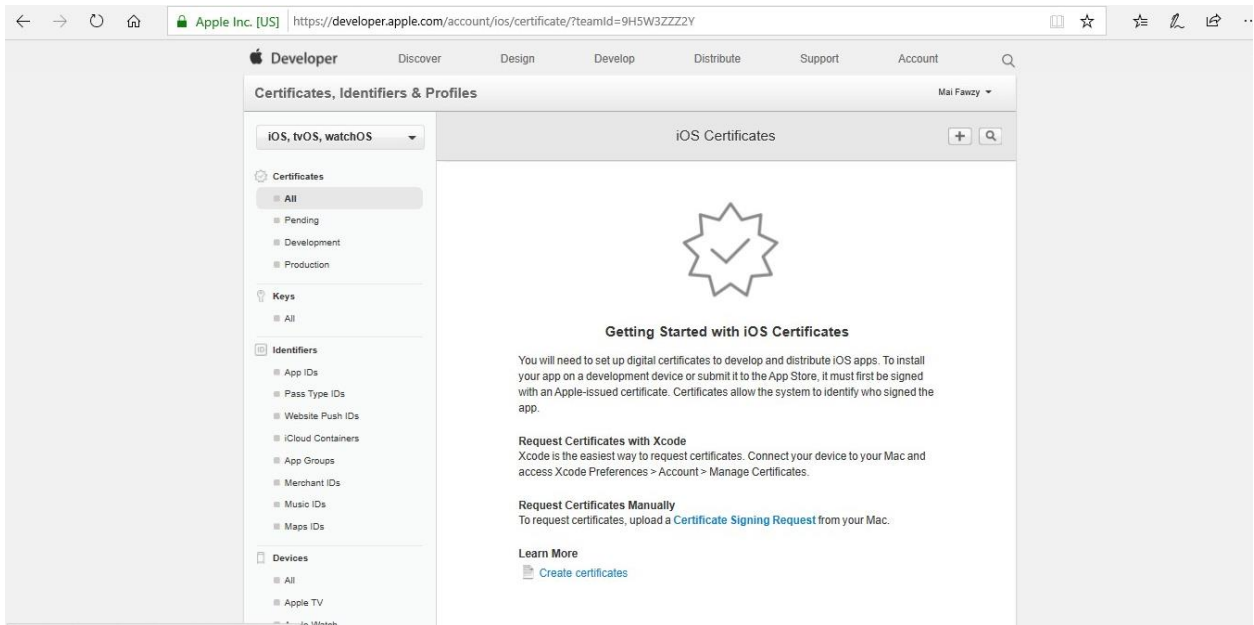
To create Apple Certificate Signing, follow below steps:

1. Go to the [Apple Developer portal](#). In the top right of the page, click **Account**.

2. **Sign in** with your organizational Apple ID. Click **Certificates, IDs & Profiles**.

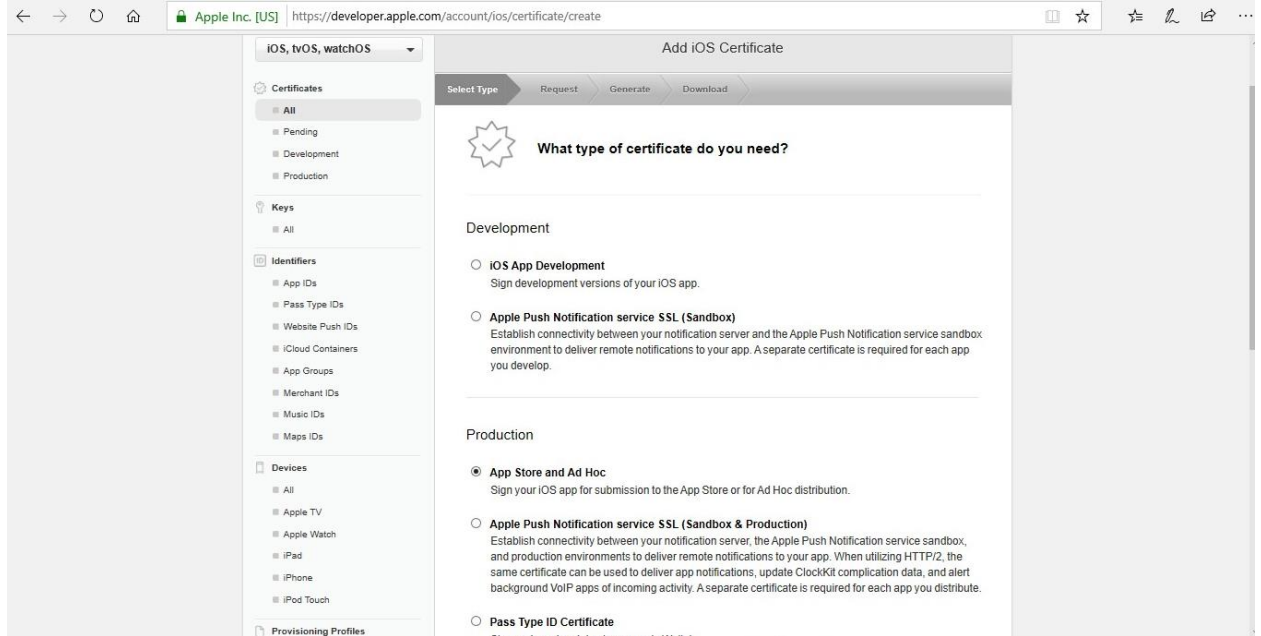


3. Click the + in the top right corner to add an iOS certificate.



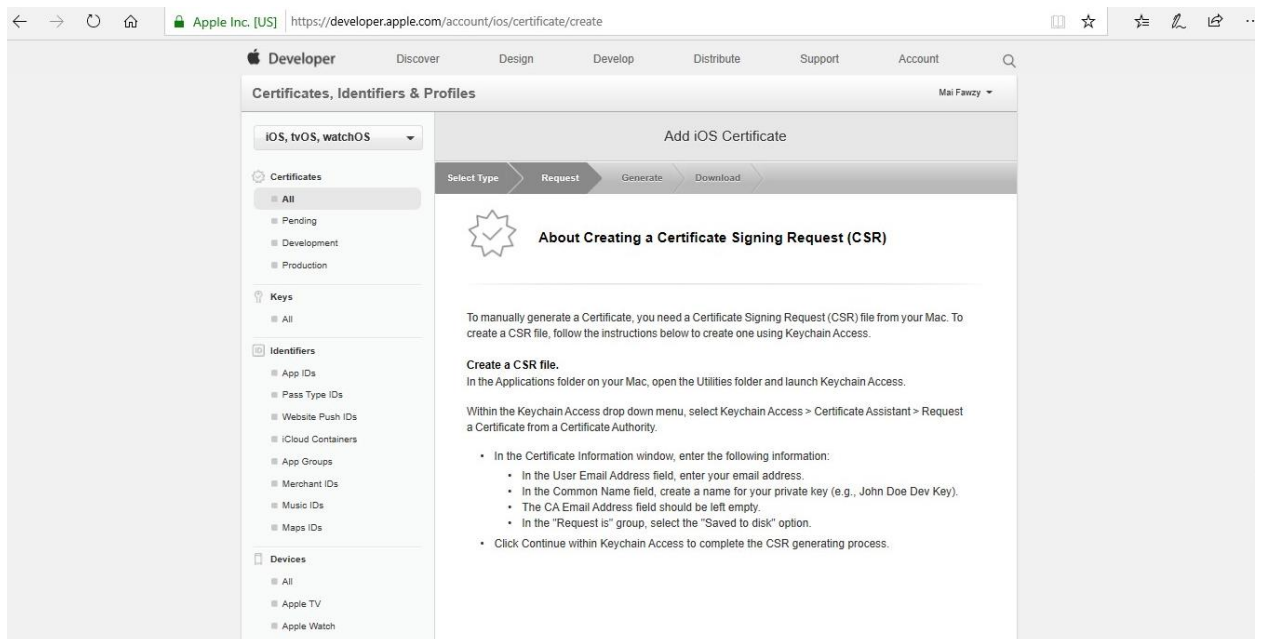
4. Choose to create an **App Store and Ad Hoc** certificate under **Production**.

Note: In case you deploy it within your organization, you will create **In-House and Ad Hoc** certificate because you will use [Apple Developer Enterprise Account](#).

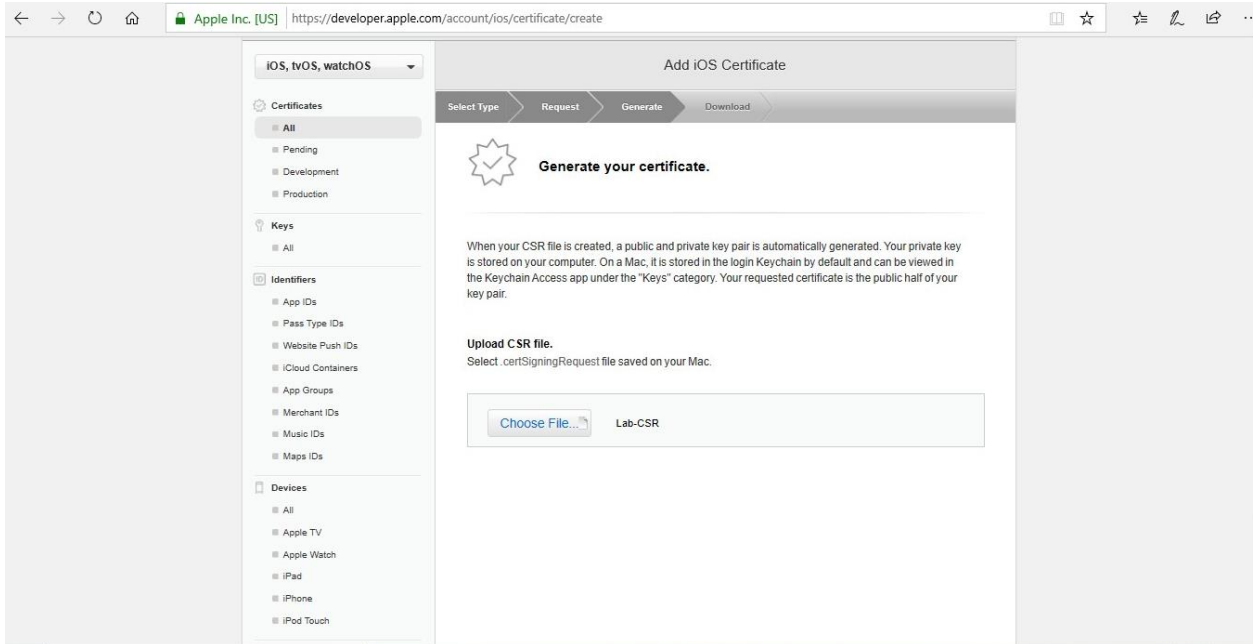


Note: If do not plan to distribute the app, and only want to test it internally, you can use an iOS App Development certificate instead of a certificate for Production. If you use a development certificate, make sure the mobile provisioning profile references the devices on which the app will be installed.

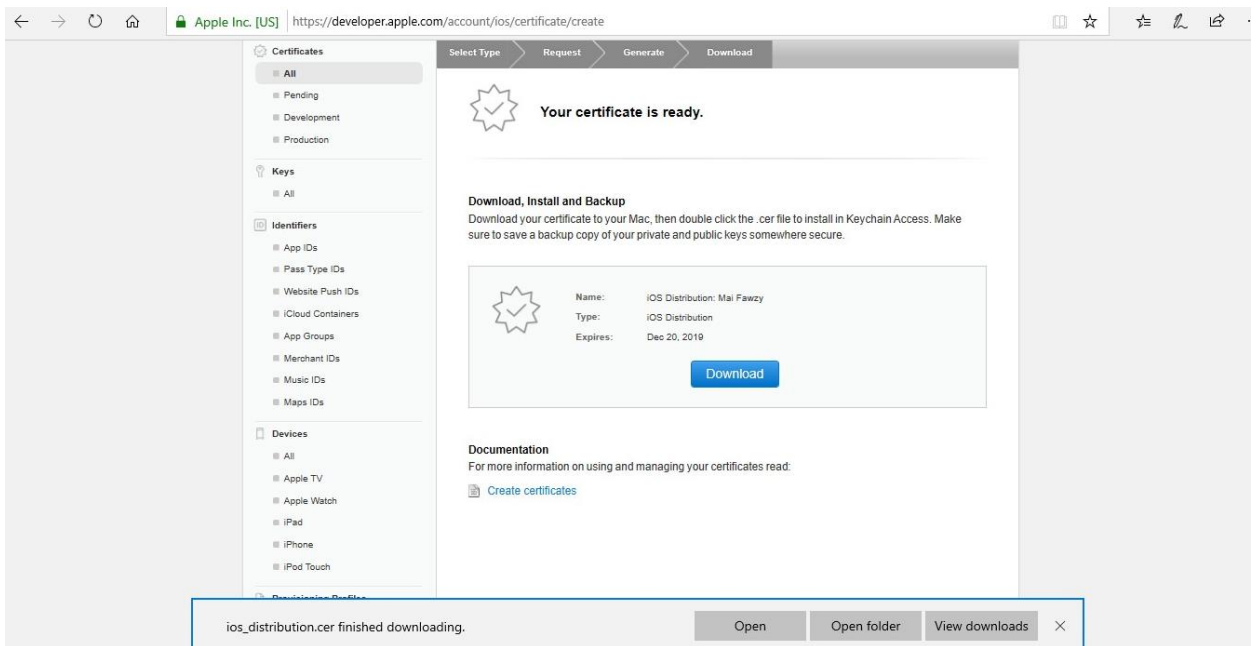
5. Click **Continue** at the bottom of the page.
6. Read the instructions on creating a **Certificate Signing Request (CSR)** using the Keychain Access application on your macOS computer. Click **Continue**.



7. Return to the Apple developer site. Click **Continue**. Then upload the CSR file.

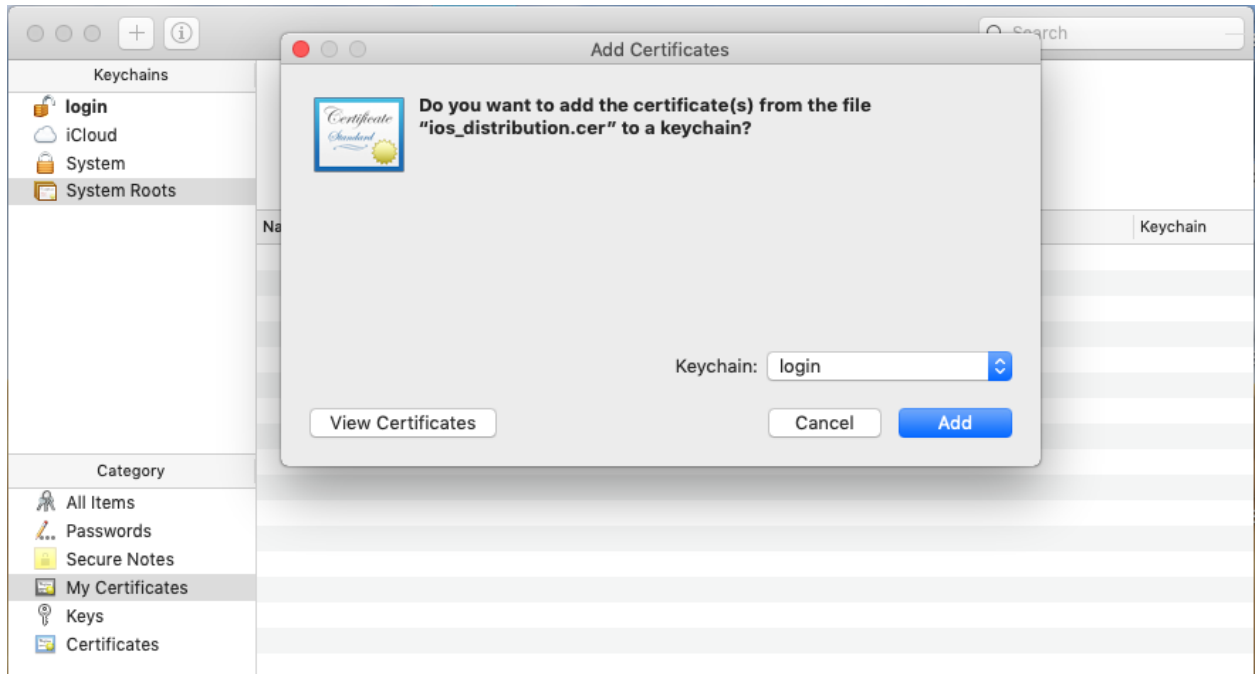


8. Apple generates your signing certificate. **Download** and save it to a memorable location on your macOS computer.



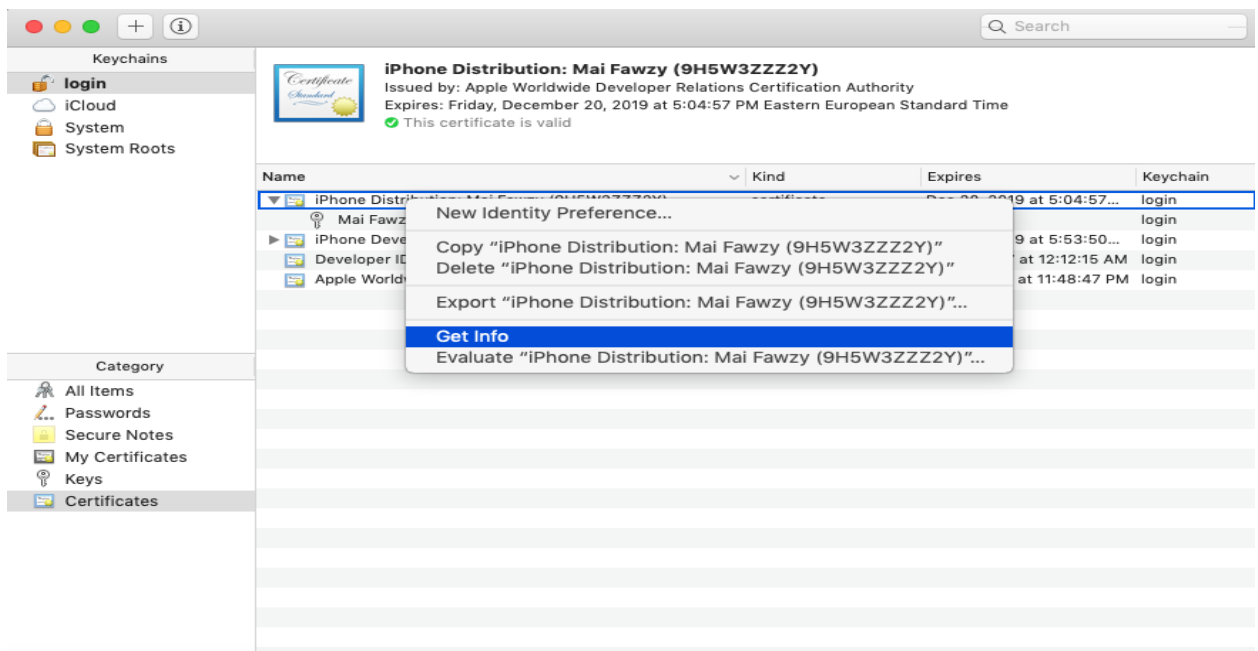
To add signing certificate, follow below steps:

1. On your macOS computer, Double-click the certificate file you just downloaded to add the certificate to a keychain.

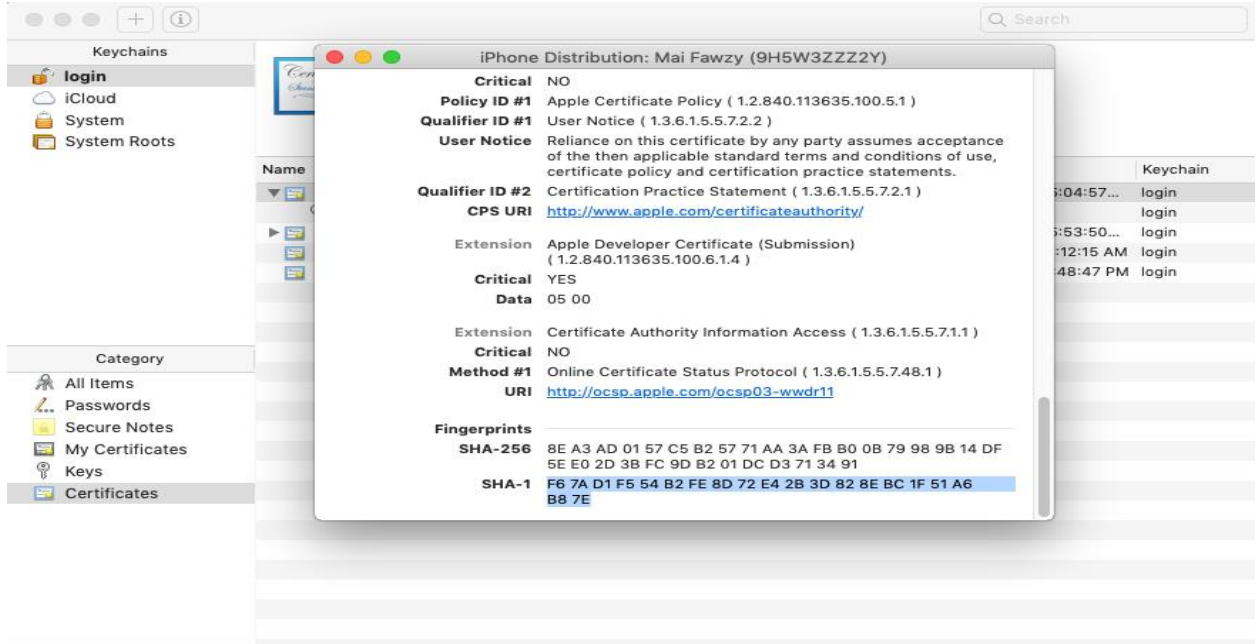


Note: In my lab, I add the signing certificate on System & login.

2. Open **Keychain Access** again. Locate your certificate by searching for its name in the top right search bar. Right-click on the item to bring up the menu and click **Get Info**.

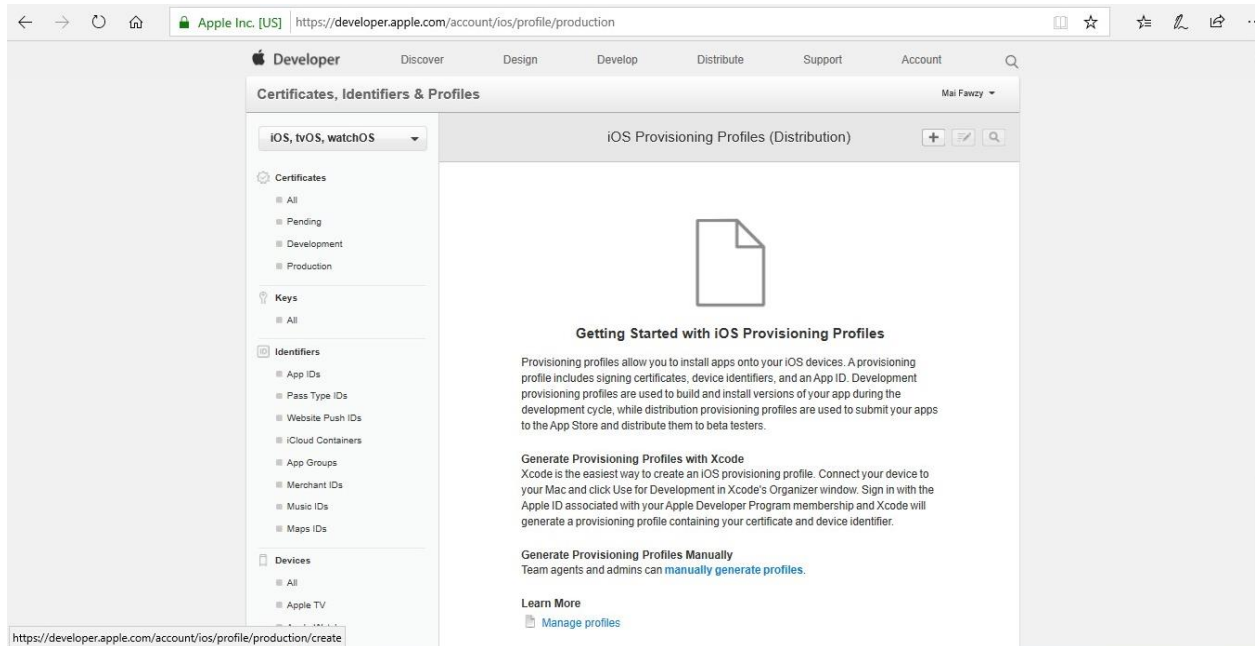


3. An informational window appears. Scroll to the bottom and look under the **Fingerprints** label. Copy the **SHA1** string (blurred out) to use as the argument for "-c" for the App Wrapping Tool.

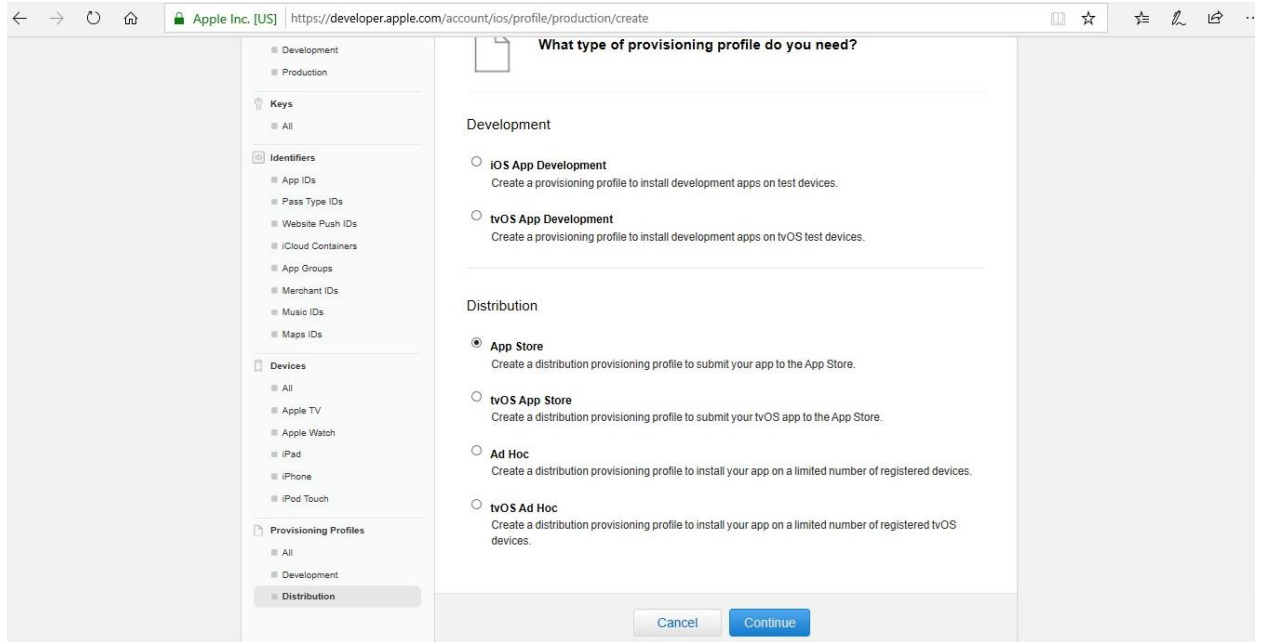


Create Distribution Provisioning profile

1. Go back to the [Apple Developer account portal](#) .**sign in** with your organizational Apple ID. Click **Certificates, IDs & Profiles** > Click **Distribution** under Provisioning Profile.
2. Click the + in the top right corner to add an iOS provisioning profile.

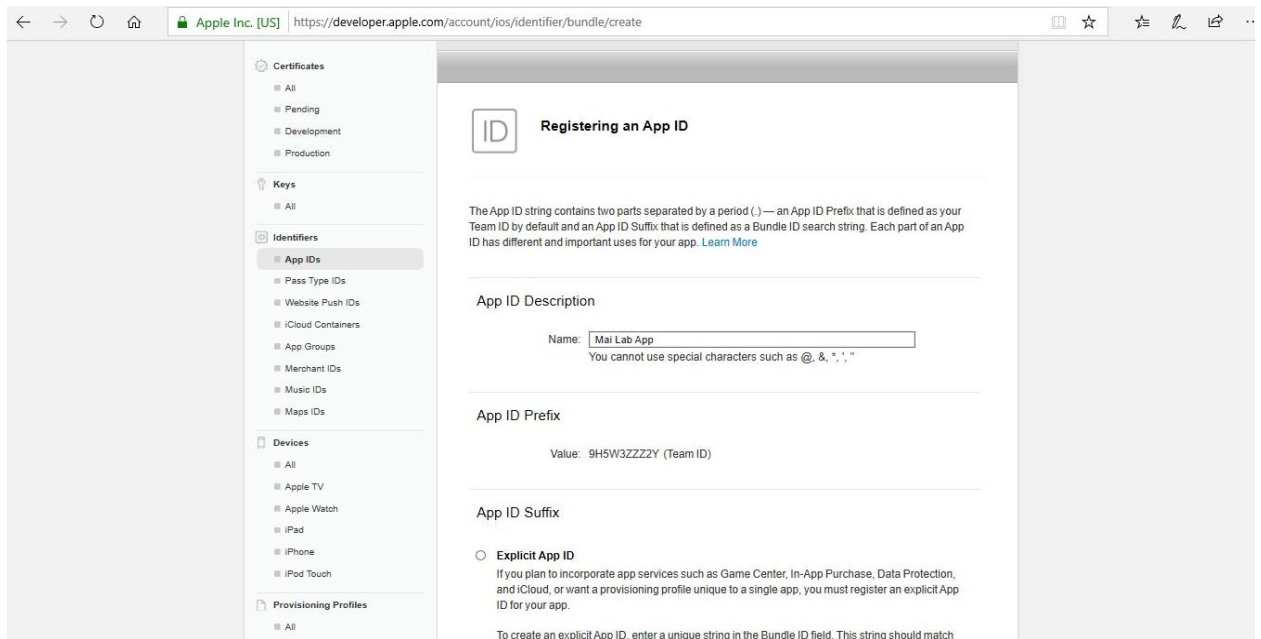


3. Choose to create an **App Store** provisioning profile under **Distribution**. Click **Continue**.

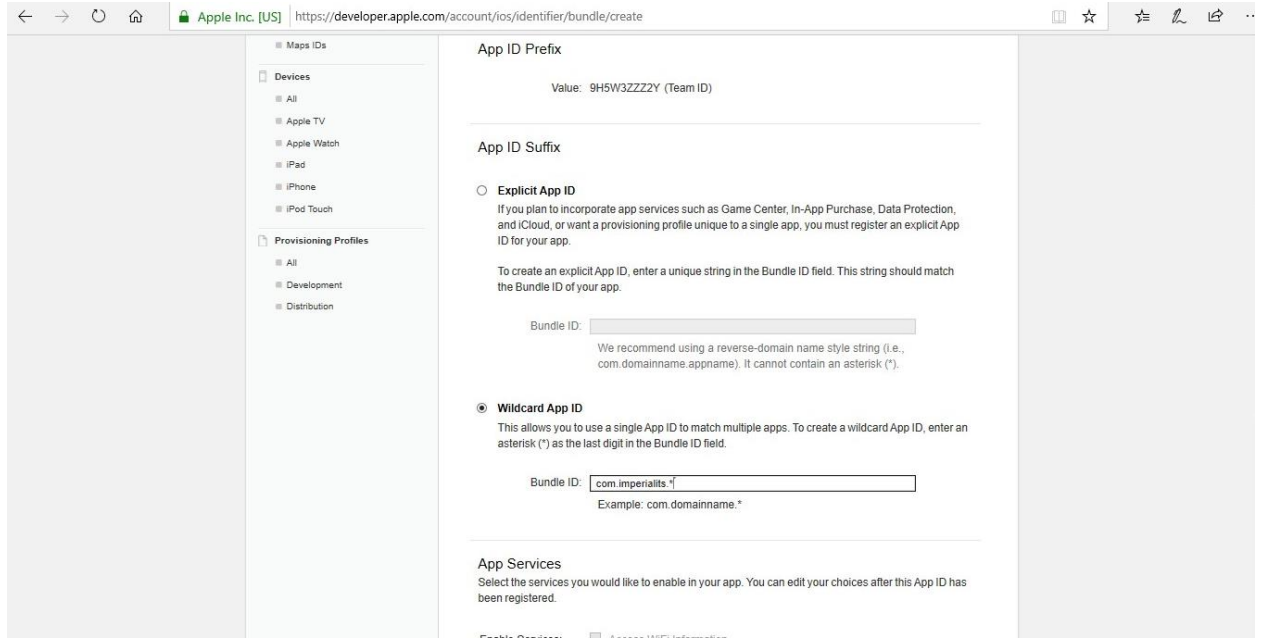


Note: In your organization, you will create **In-House** Distribution Profile.

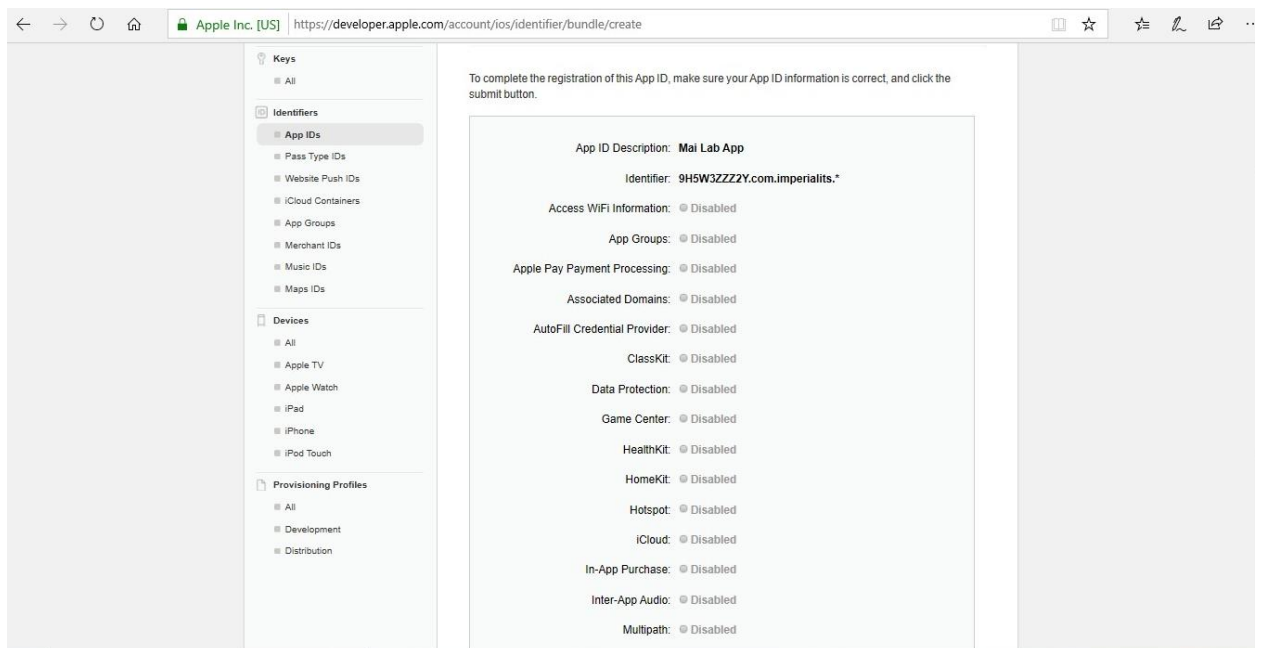
4. On **App ID** Page, Click **Registering an App ID**, Type Name for App ID.



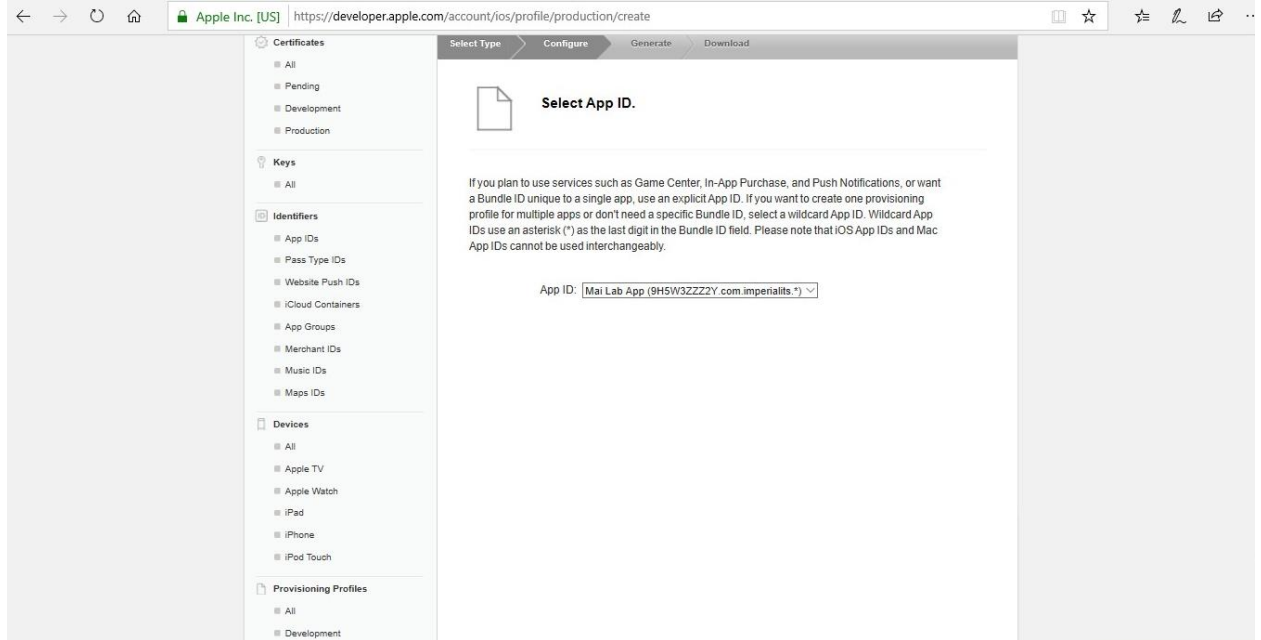
5. Select **Wildcard App ID**, Type Bundle ID.



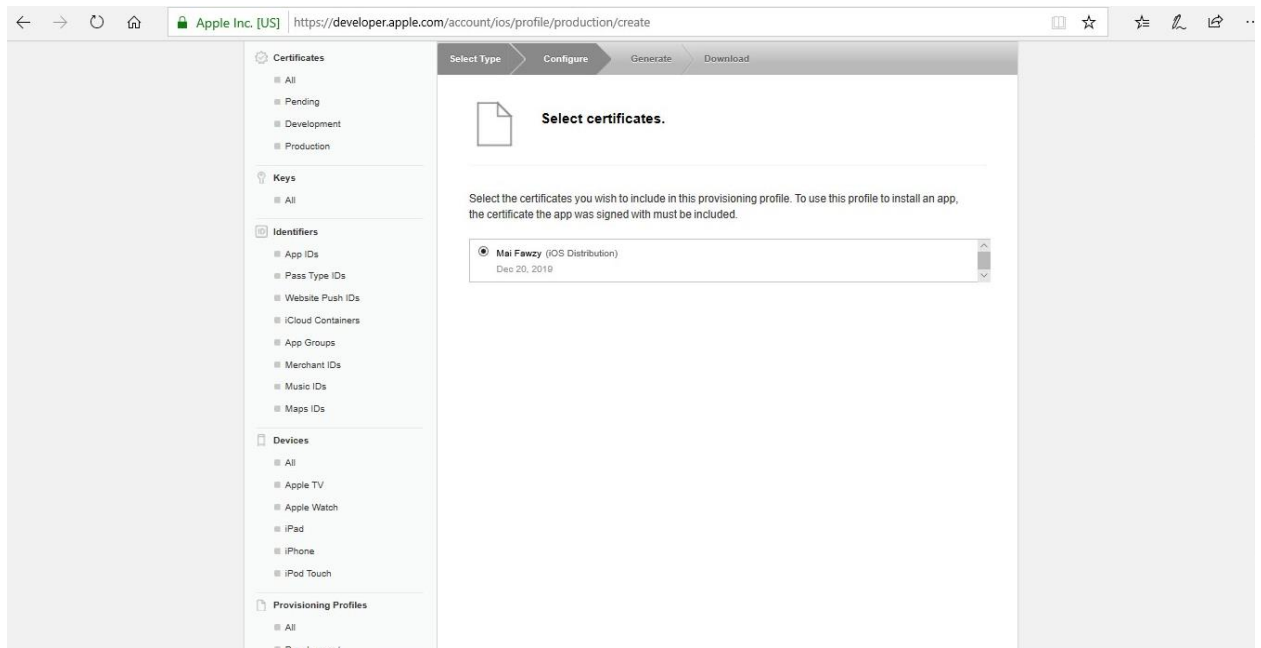
6. Click **Continue**.



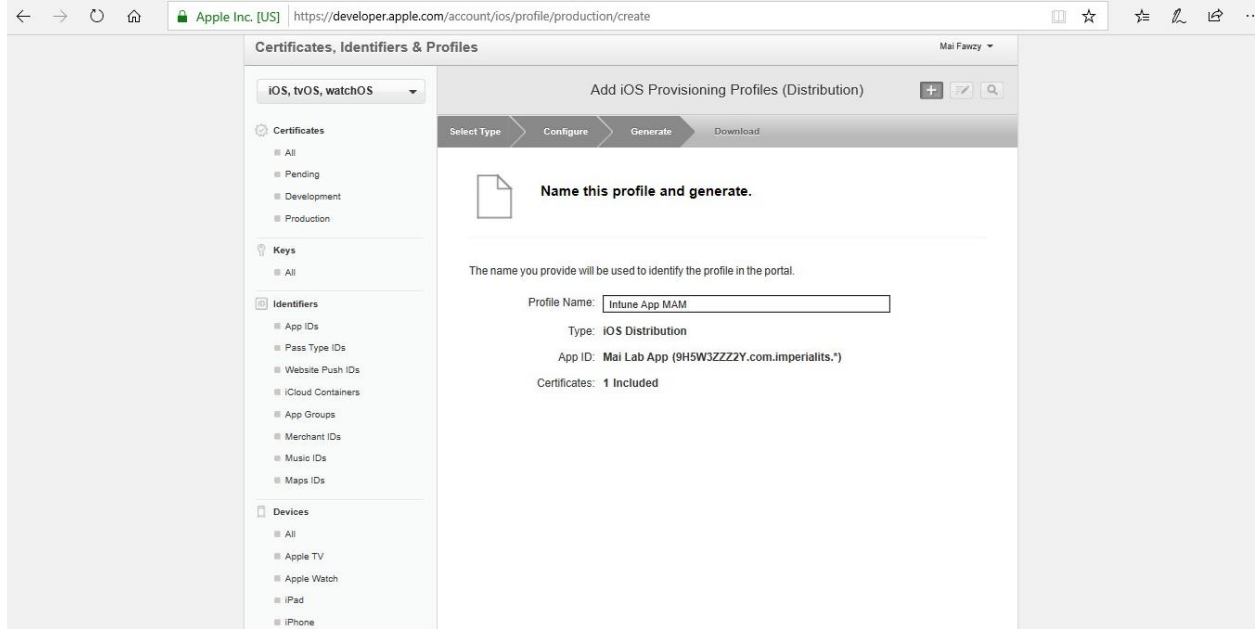
7. Select **App ID**. Click **Continue**.



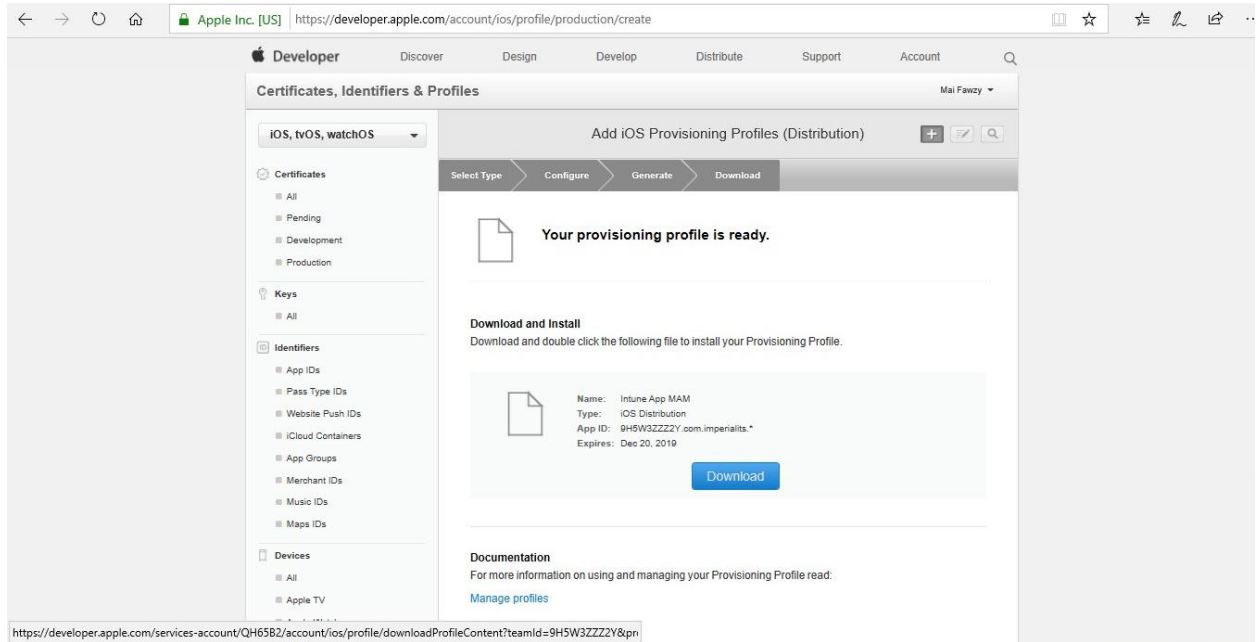
8. Make sure to link the previously generated signing certificate to the provisioning profile.



9. Type **Profile Name**.

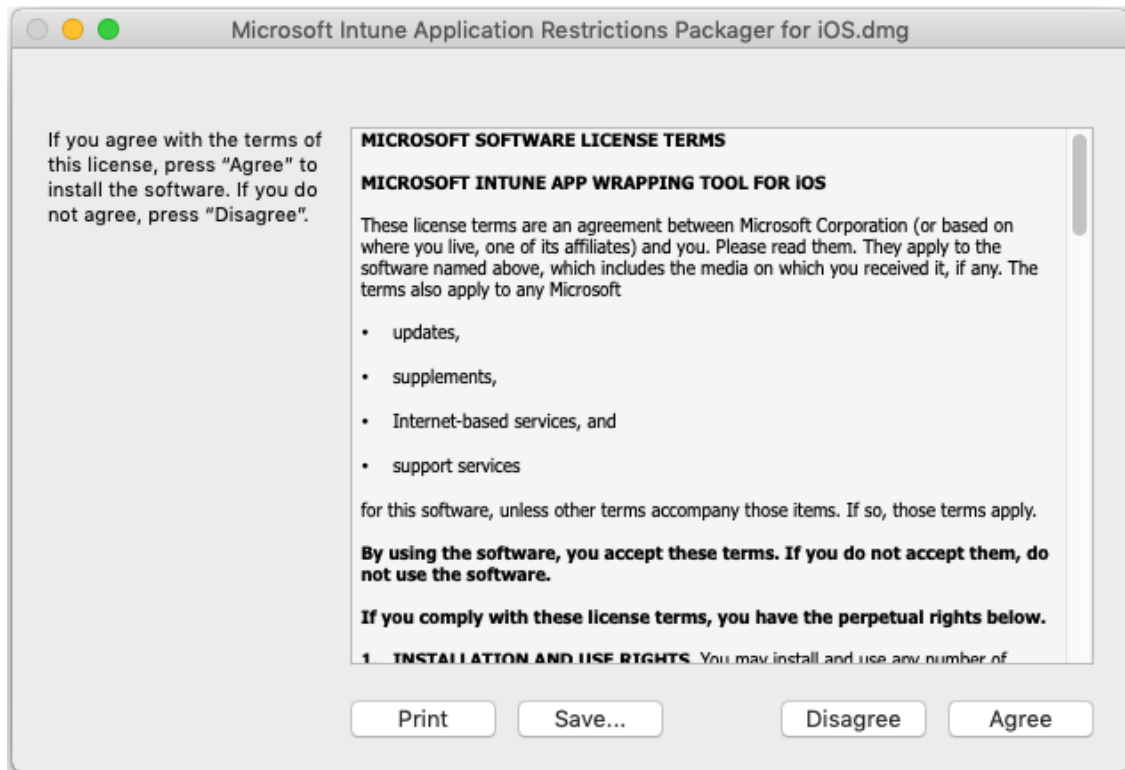


10. Download your profile (with extension .mobileprovision) to your macOS computer. Save the file in a memorable location. This file will be used for the -p parameter while using the App Wrapping Tool.



Configure the App Wrapping Tool

1. Download the files for the App Wrapping Tool from [GitHub](#) to a macOS computer.
2. Double-click **Microsoft Intune App Wrapping Tool for iOS.dmg**. A window with the End User License Agreement (EULA) will appear. Choose **Agree** to accept EULA.



3. After Installation finished, you will find **IntuneMAMPackager** & contain **contents**.



Run the App Wrapping Tool

Open the macOS Terminal and run the following command:

```
Cd "/Volumes/IntuneMAMPackager/Contents/MacOS/"
```

```
./IntuneMAMPackager -i /Users/imperialit/Desktop/Mai-App.ipa -o  
/Users/imperialit/Desktop/Mai-App_Wrapped.ipa -p  
/Users/imperialit/Desktop/LAB/Intune_APP_MAM.mobileprovision -c "F6 7A D1 F5 54 B2  
FE 8D 72 E4 2B 3D 82 8E BC 1F 51 A6 B8 7E" -v true
```

Microsoft Intune step by step on Azure portal

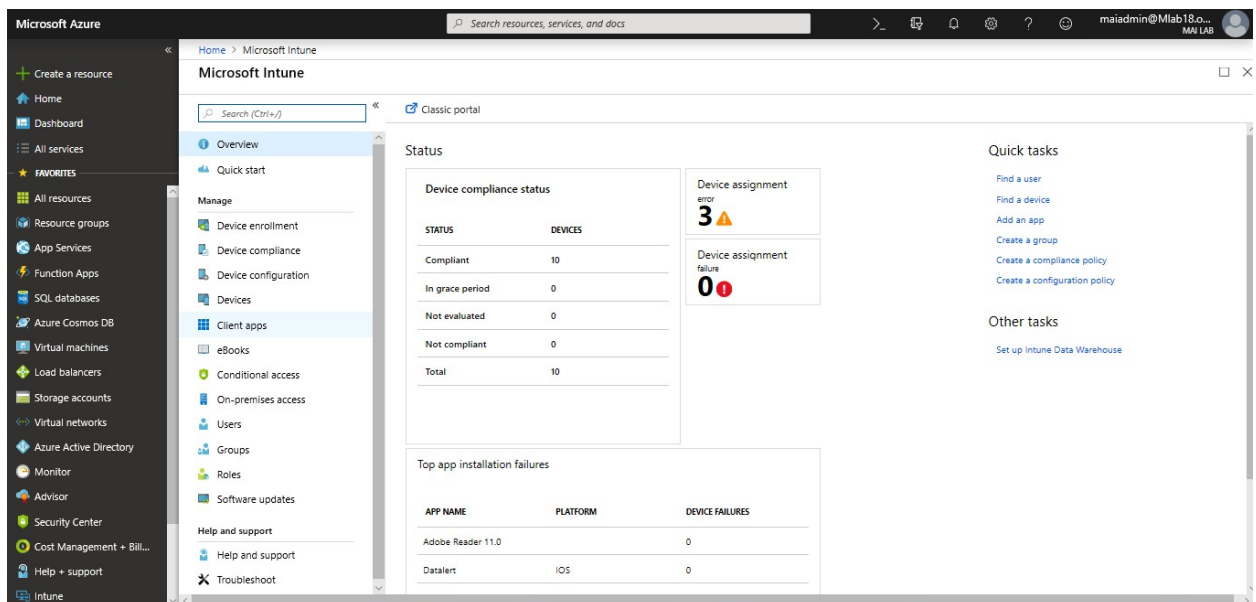
```
MacOS — -bash — 80x24
Last login: Thu Dec 20 19:52:11 on ttys000
[Imperialism-Mac:~ imperialism$ cd "/Volumes/IntuneMAMPackager/Contents/MacOS"
Imperialism-Mac:MacOS imperialism$ ./IntuneMAMPackager -i /Users/imperialism/Desktop
/Mai-App.ipa -o /Users/imperialism/Desktop/Mai-App_Wrapped.ipa -p /Users/imperial
it/Desktop/LAB/Intune_APP_MAM.mobileprovision -c "F6 7A D1 F5 54 B2 FE 8D 72 E4
2B 3D 82 8E BC 1F 51 A6 B8 7E" -v true
```

After you run above command, you should find wrap application created. The application was successfully packaged.

Configure Wrapped Line of Business App

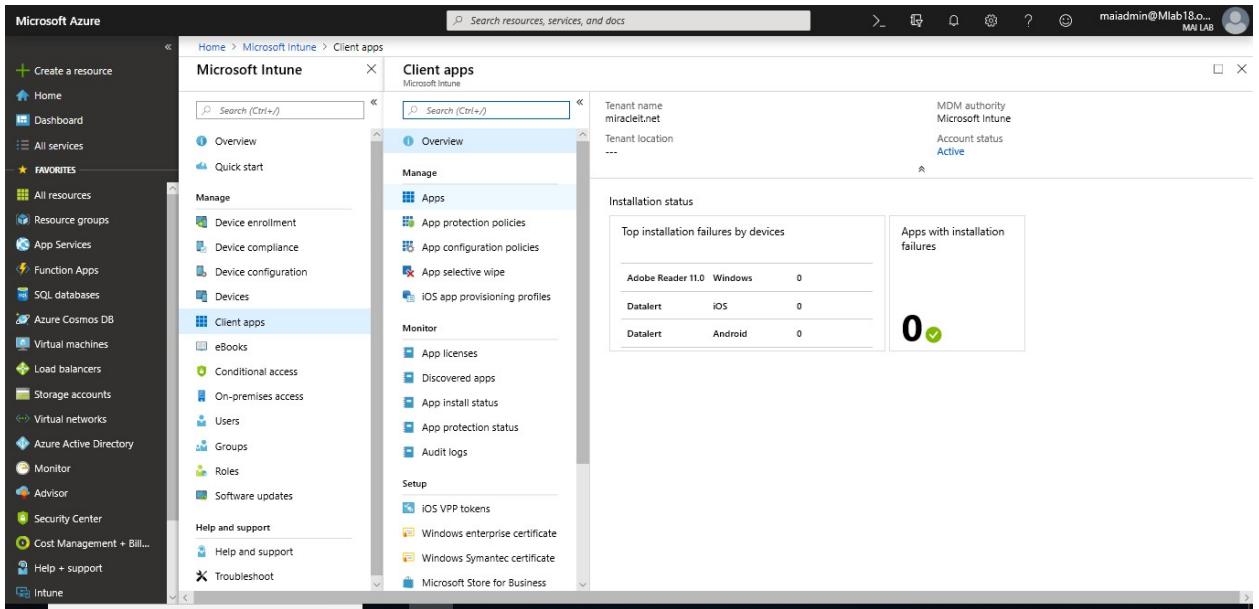
To add a line of business app to your available apps in Microsoft Intune, do the following:

1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is in the **Monitoring + Management** section.
2. In the **Intune** pane, select **Client apps**.

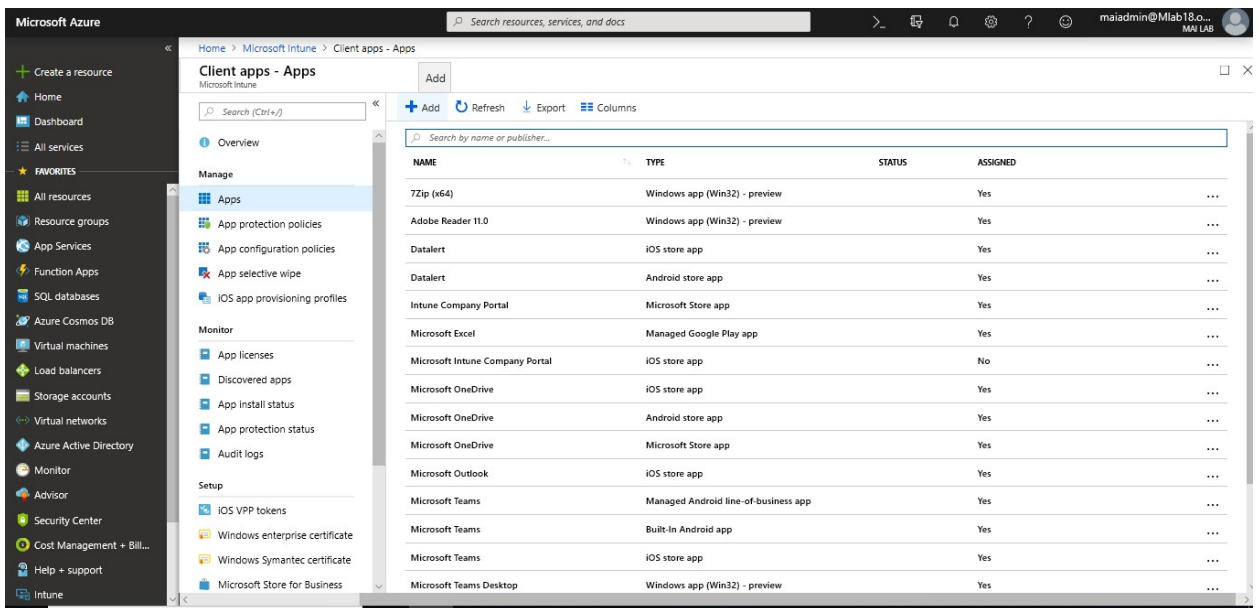


3. In the **Client apps** workload, select **Manage** > **Apps**.

Microsoft Intune step by step on Azure portal

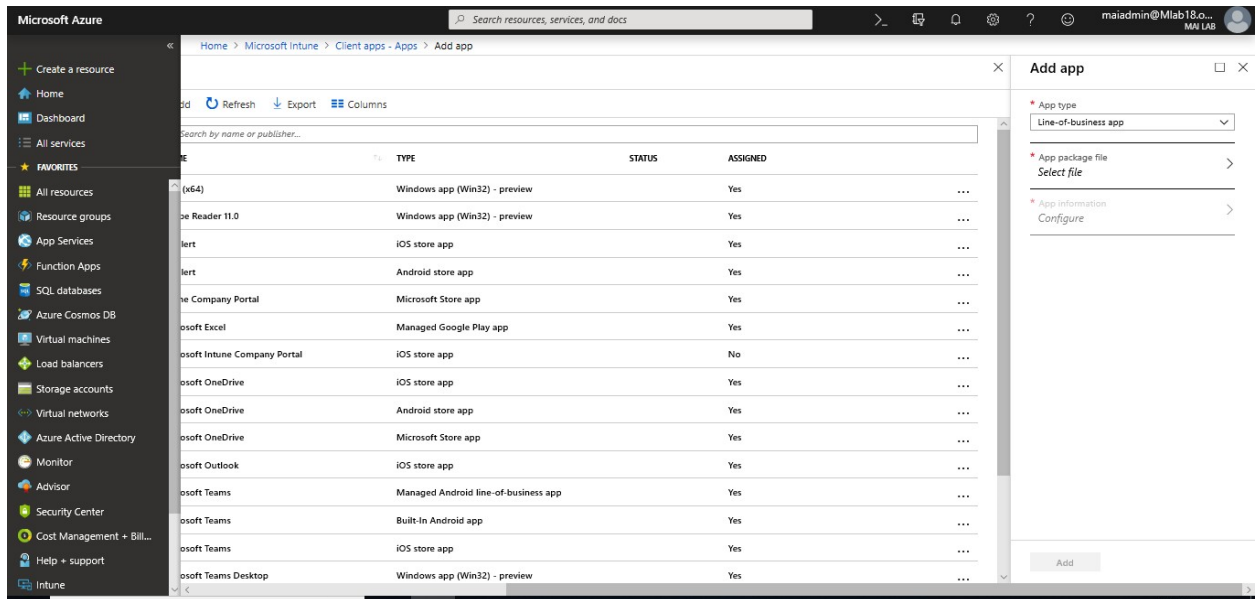


4. Above the list of apps, select **Add**.

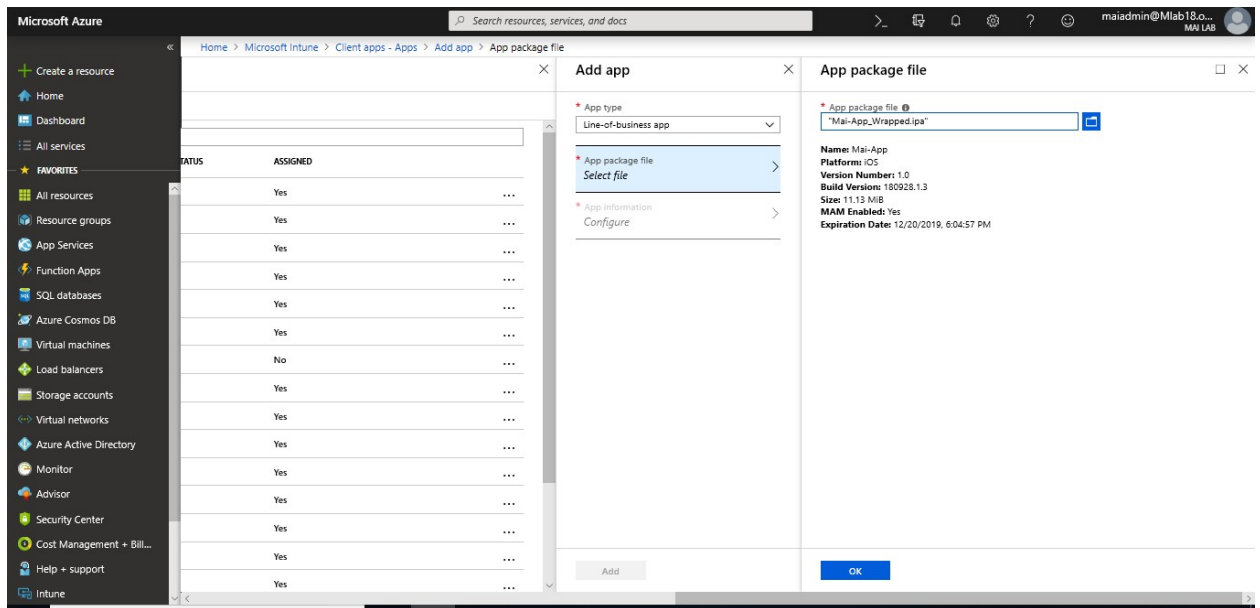


5. In the **Add app** pane, select **Line-of-business app**.

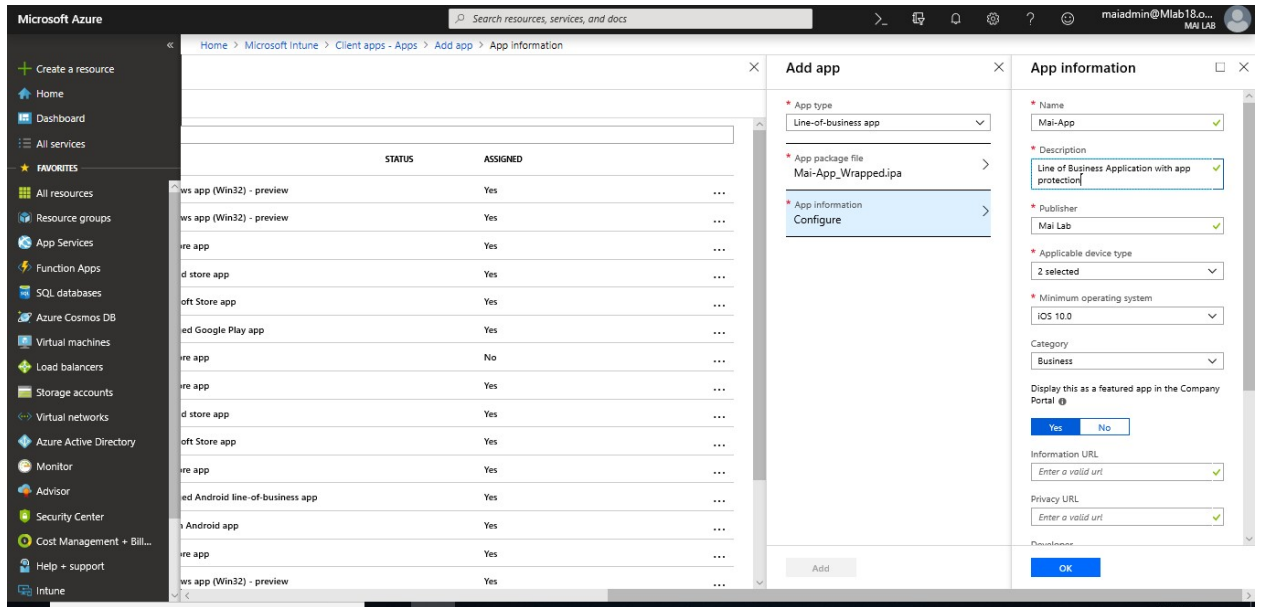
Microsoft Intune step by step on Azure portal



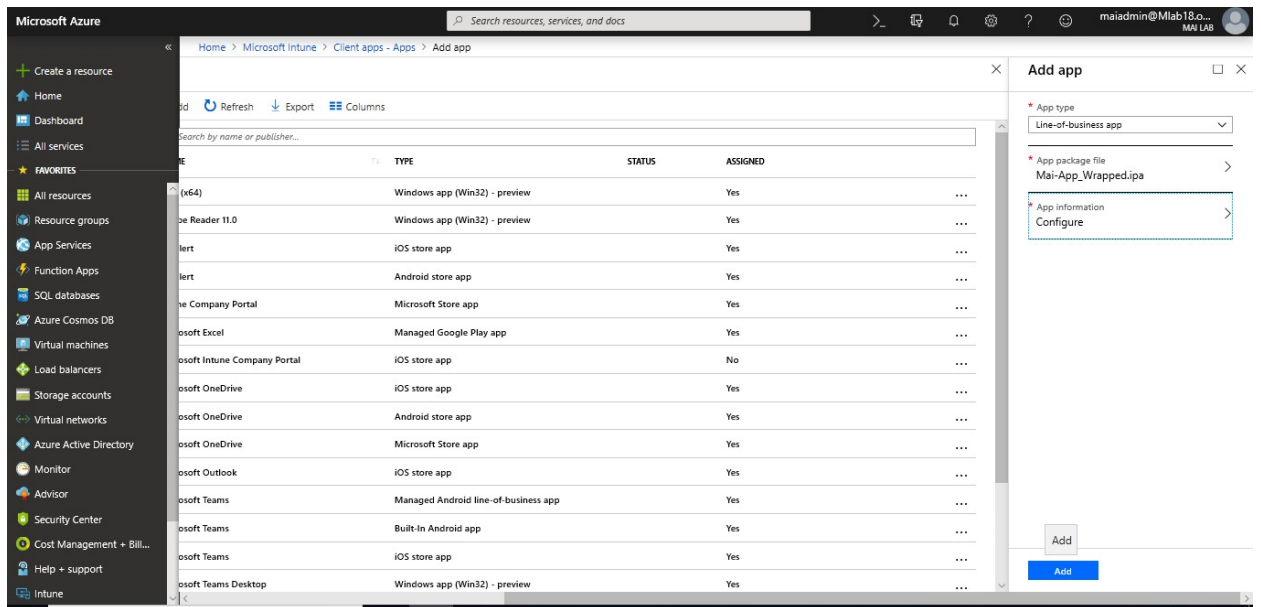
6. In the **Add app** pane, select **App package file**.
7. In the **App package file** pane, select the browse button. Then select an iOS installation file with the extension **.ipa**. You will find **MAM Enabled**. When you're finished, select **OK**.



8. In the **App information** pane, add the details for your app.
9. When you're finished, select **OK**.



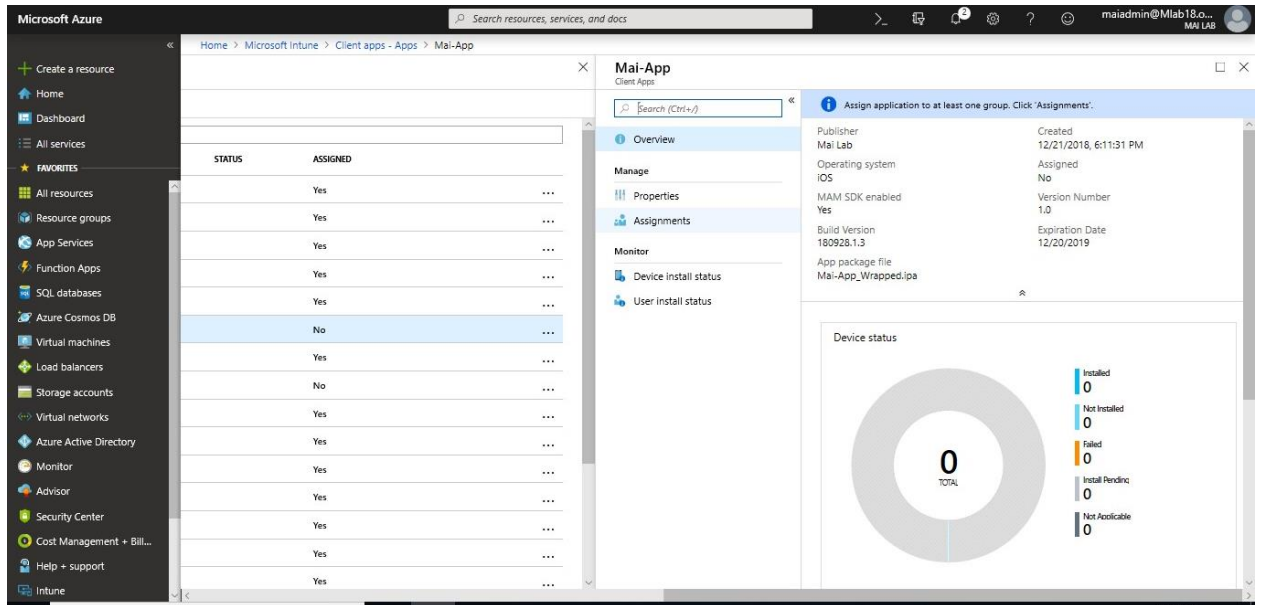
10. In the **Add app** pane, verify that the details of your app are correct. Select **Add** to upload the app to Intune.



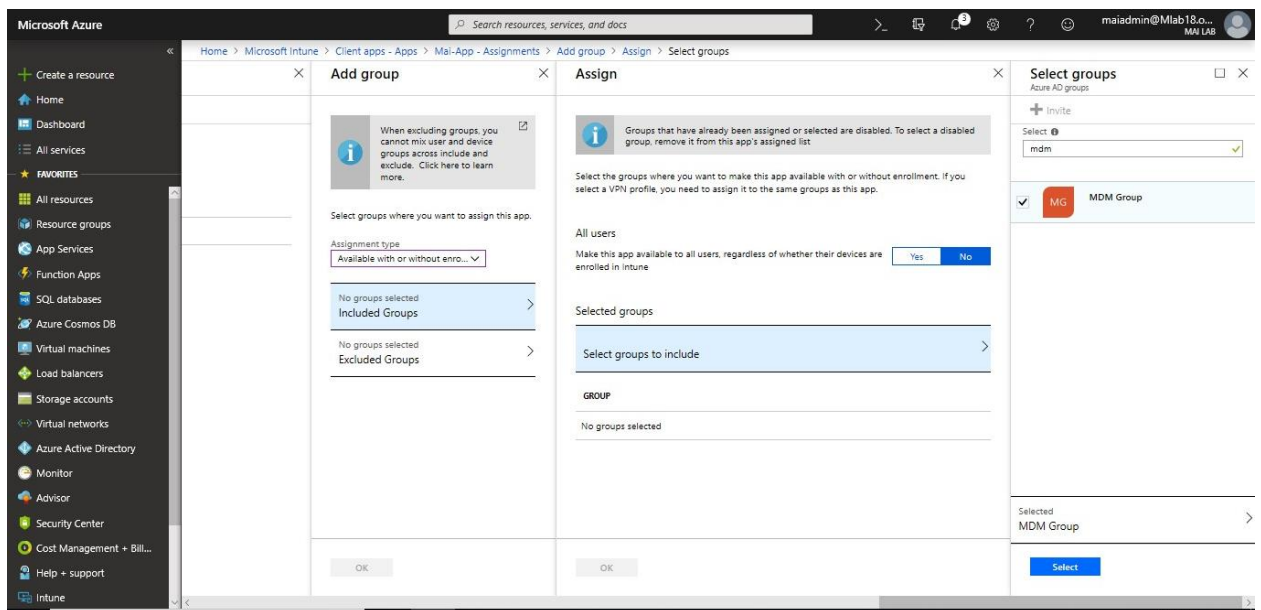
To assign specific group on Wrapped Line of Business App

1. Sign in to the [Azure portal](#). Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. In the **Intune** menu, select **Client apps**.
3. In the **Manage** section of the menu, select **Apps**.
4. In the **Apps** pane, select the app you want to assign.
5. In the **Manage** section of the menu, select **Assignments**.

Microsoft Intune step by step on Azure portal

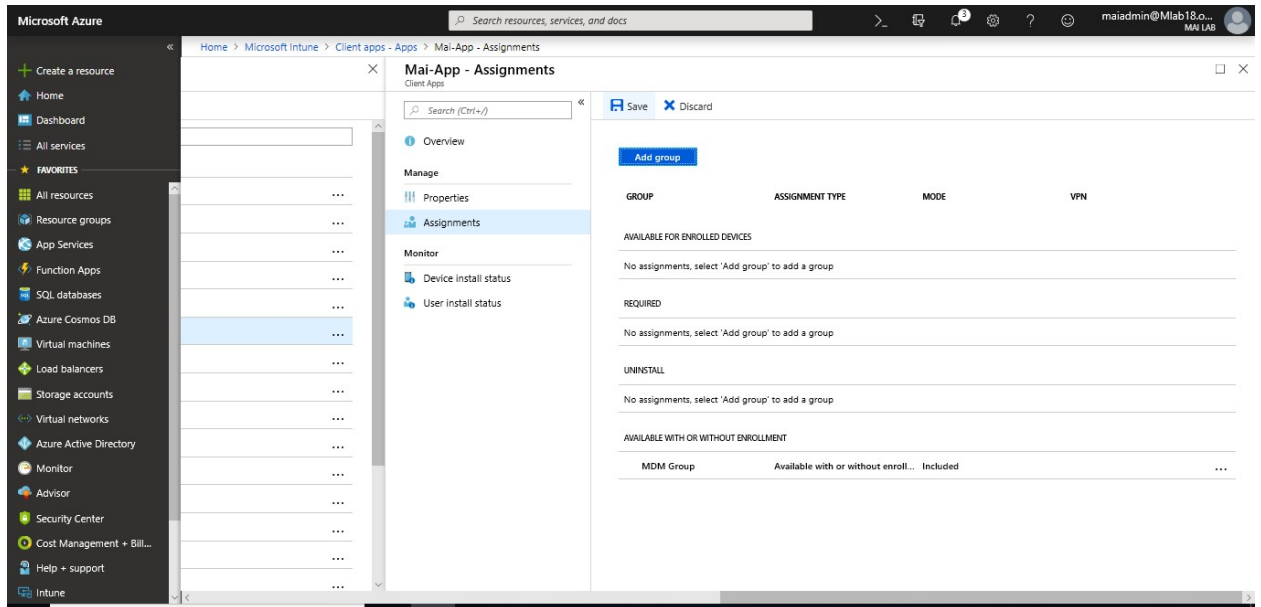


6. Select **Add Group** to open the **Add group** pane that is related to the app.
7. For the specific app, select an **assignment type**: Available with or without enrollment.
8. To select the groups of users that are affected by this app assignment, select **Included Groups**. After you have selected one or more groups to include, Click **Select**.



9. In the **Assign** pane, select **OK** to complete the included groups selection.
10. In the app **Assignments** pane, select **Save**.

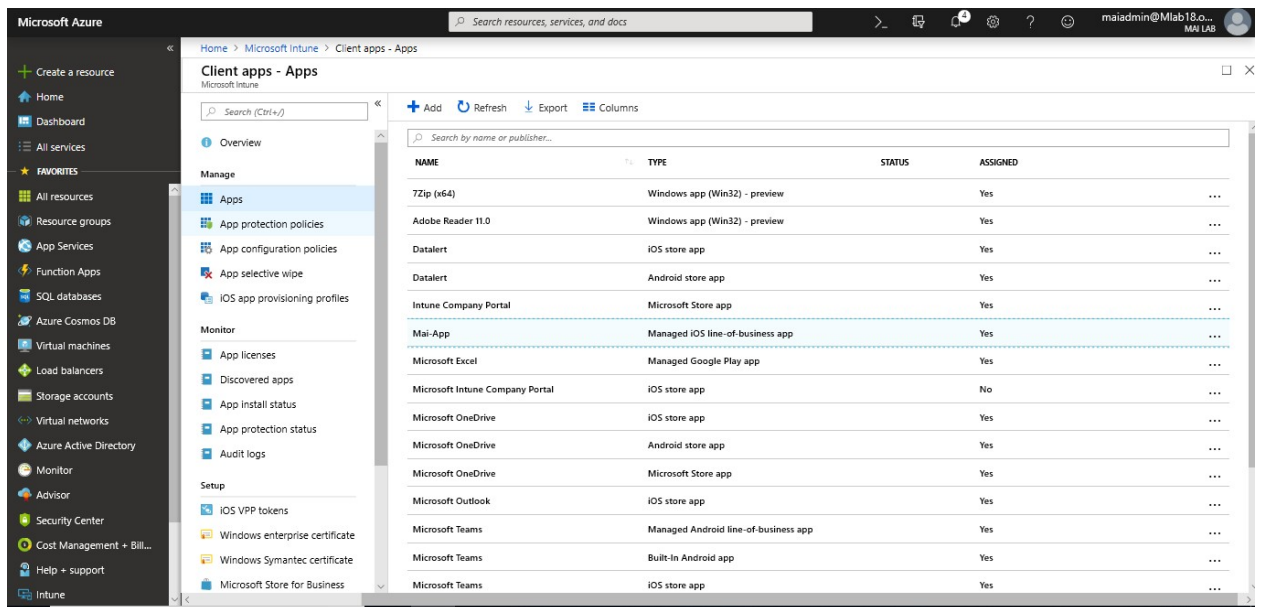
Microsoft Intune step by step on Azure portal



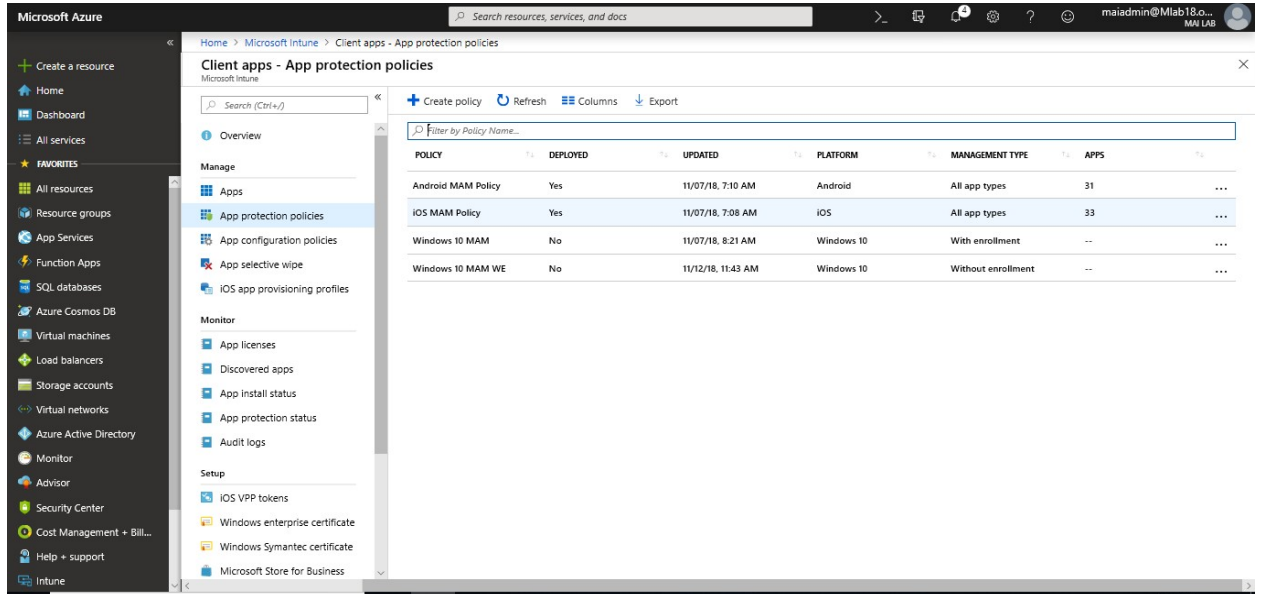
Note: If you install an app by Mobile Device Management (MDM), trust is automatically established. If you manually install an app, you must also manually establish trust. End user will need to **Manually trust a developer on iOS**. go to **Settings > General > Device Management > Under Enterprise App, Tap Trust "[Organization Name]"**. Once application become **trust**, End User will be able to install it from **Company portal**.

To apply MAM Policy, you need to follow below steps:

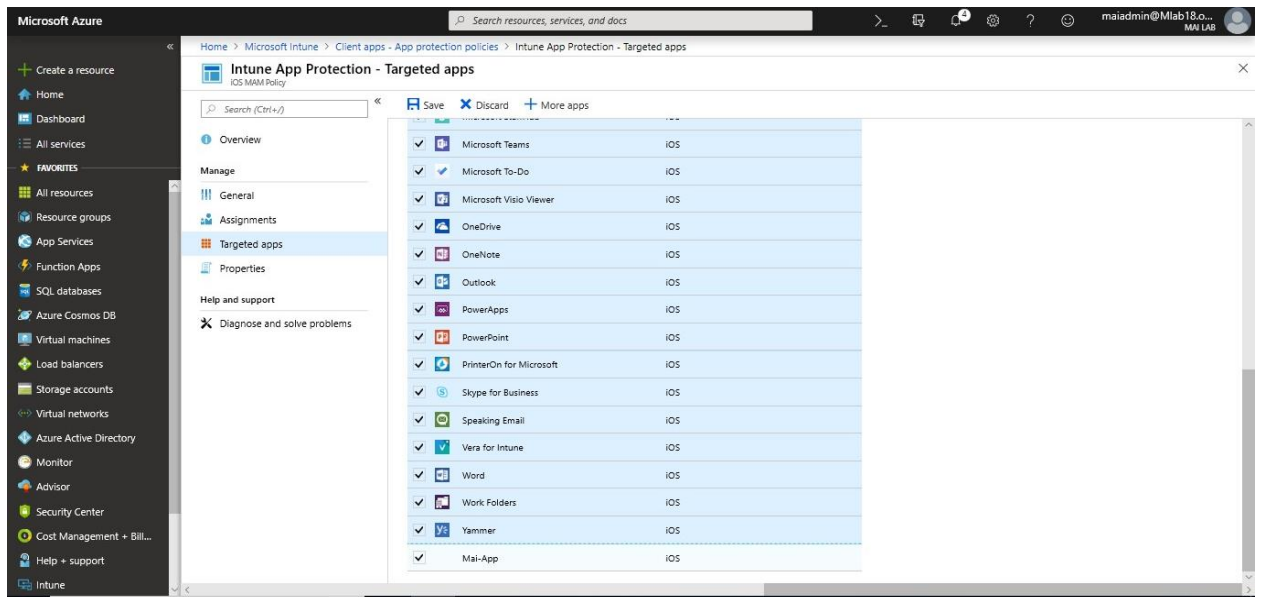
1. Sign in to the [Azure portal](#). Select **All services > Intune**. Intune is located in the **Monitoring + Management** section. Select **Client apps > App protection policies**.



2. In the **App protection policies** pane, select the iOS app policy you want to assign.



3. In the **Manage** section of the menu, select **Targeted Apps**.



4. Select wrapped app that you add it. Select **Save**.

Chapter 8

Integrate between Microsoft Intune & Other Products

Telecom expense management service in Intune

Intune enables you to manage telecom expenses incurred from data usage on corporate-owned mobile devices. To enable this capability, Intune has integrated with the third-party software developer Saaswedo's [Datalert telecom expense management](#) solution. Datalert is real-time telecom expense management software that lets you manage telecom data usage. It helps you avoid costly and unexpected data and roaming overages for your Intune-managed devices.

Intune's integration with Datalert enables you centrally set, monitor, and enforce roaming and domestic data usage limits. Automated alerts are triggered when the limits exceed defined thresholds. You can configure the service to apply different actions to individuals or groups of end users (like disabling roaming or exceeding the threshold). Reports that provide data usage and monitoring information are available from the Datalert management console.

Supported platforms

- Samsung Knox
- iOS 8.0 and later

Prerequisites

- A subscription to Microsoft Intune, and access to the Azure portal.
- A subscription to the Datalert telecom expense management service

List of telecom expense management providers

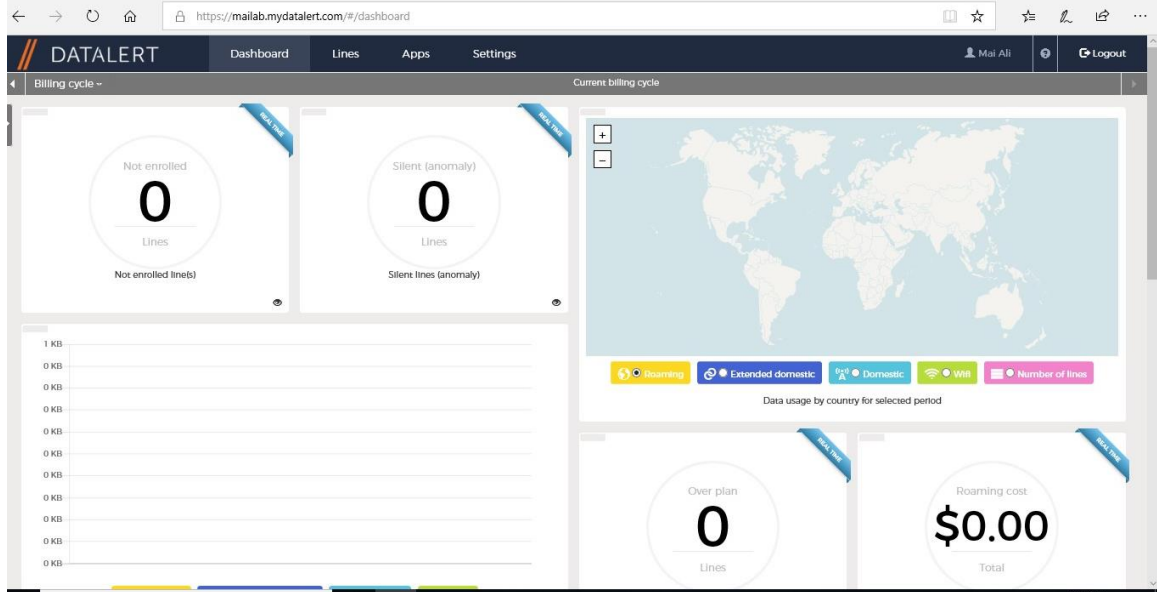
Intune currently integrates with the following telecom expense management providers: [Saaswedo Datalert telecom expense management service](#)

Deploy the Intune and Datalert integrated solution

Before you start, make sure that you already have an Intune and a Datalert telecom expense management service subscription.

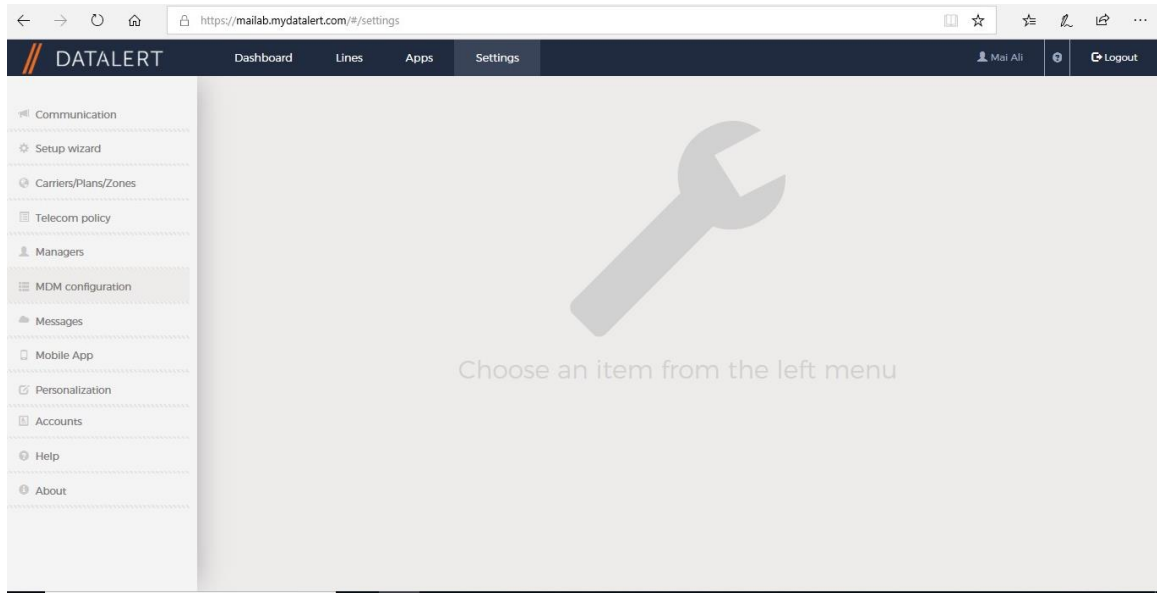
Step 1: Connect the Datalert service to Microsoft Intune

1. Sign into the Datalert management console with your administrator credentials.



Note: Once you create account on Datalert, you will receive an email with URL & credential.

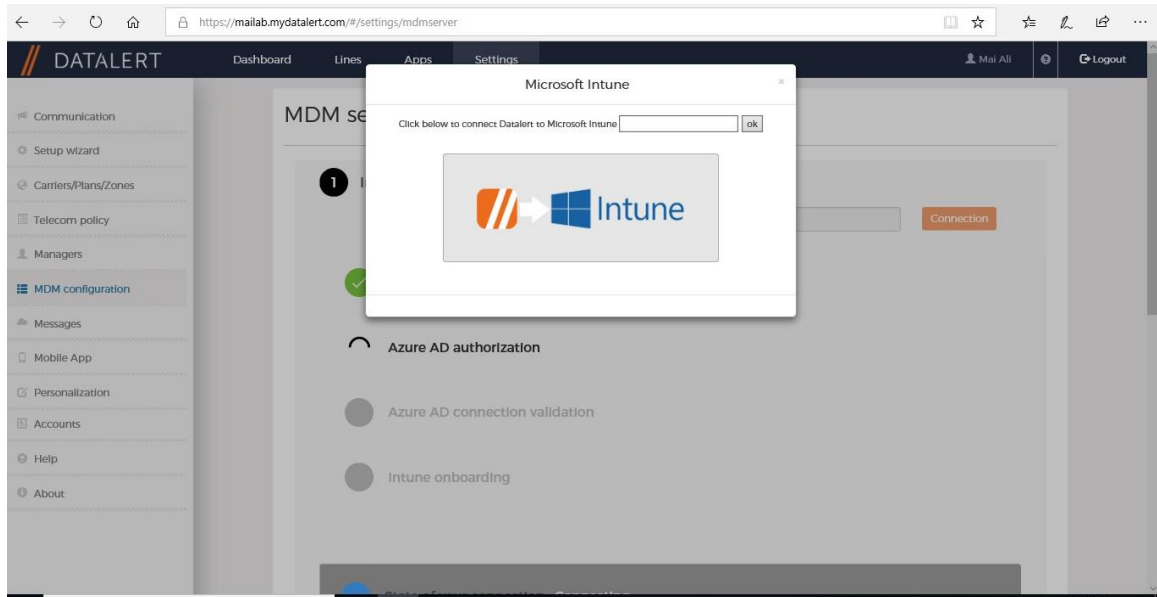
2. On the Datalert management console, go to the **Settings** tab, and then to **MDM configuration**.



3. In the **Intune / Datalert Connection** section, choose **Microsoft Intune** for **Server MDM**. For **Azure AD domain**, enter your Azure tenant ID, and then select **Connection**.

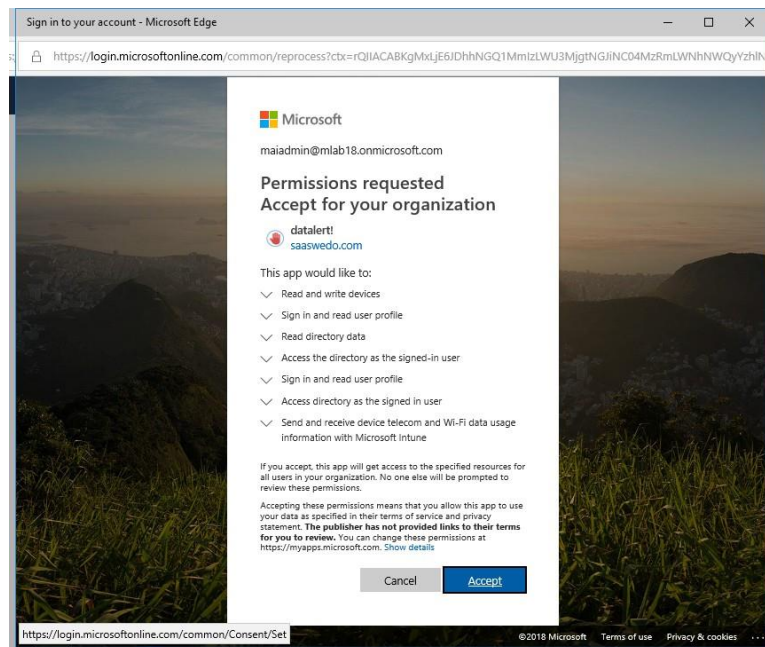
Note: Select **Unblock** at the bottom of the page, which enables you to modify settings on the page.

Microsoft Intune step by step on Azure portal

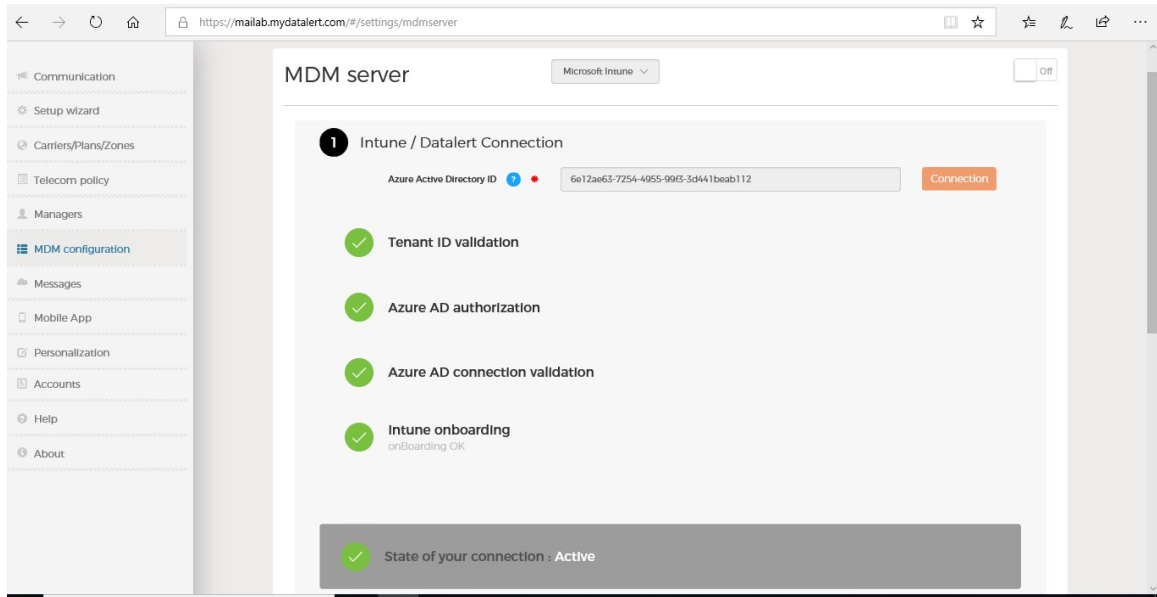


Note: To get tenant ID, Login to [Azure portal](#) > **Azure Active Directory** > **Properties** > Copy **Directory ID**

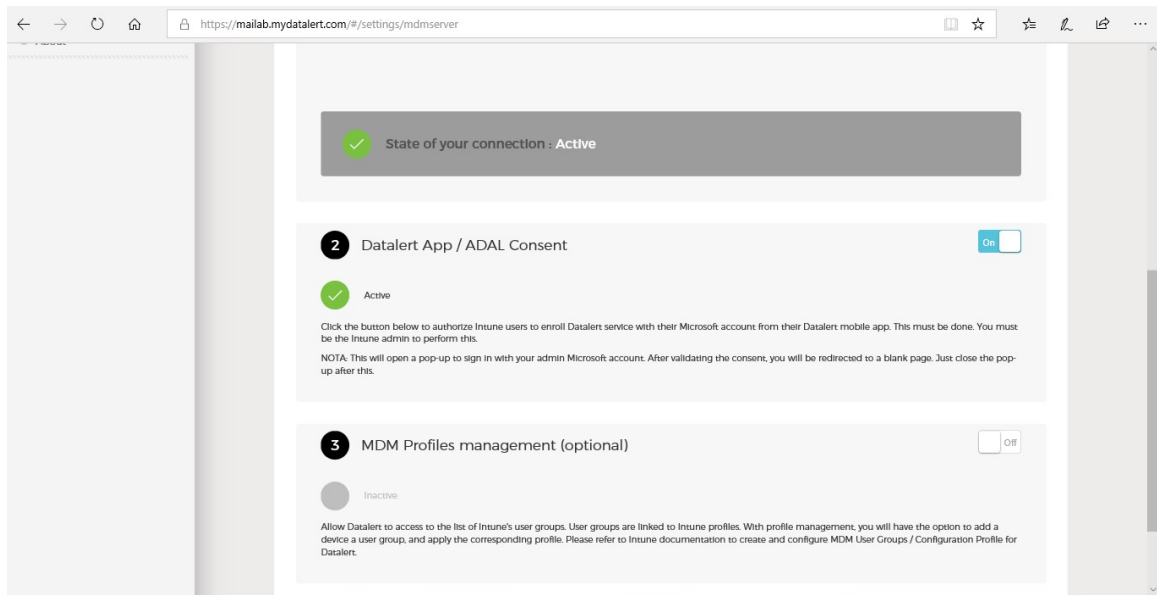
4. When you select **Connection**, the Datalert service checks in with Intune to ensure there are no pre-existing Datalert connections with Intune. After a few seconds, a Microsoft login page appears, enter global admin account for your tenant.



5. On the Microsoft authentication page, select **Accept**. You are redirected to a Datalert **thank you** page, which closes after a few seconds. Datalert validates the connection and displays green check marks next to a list of items that it validated. If the validation fails, you see a message in red and should contact Datalert Support for help.

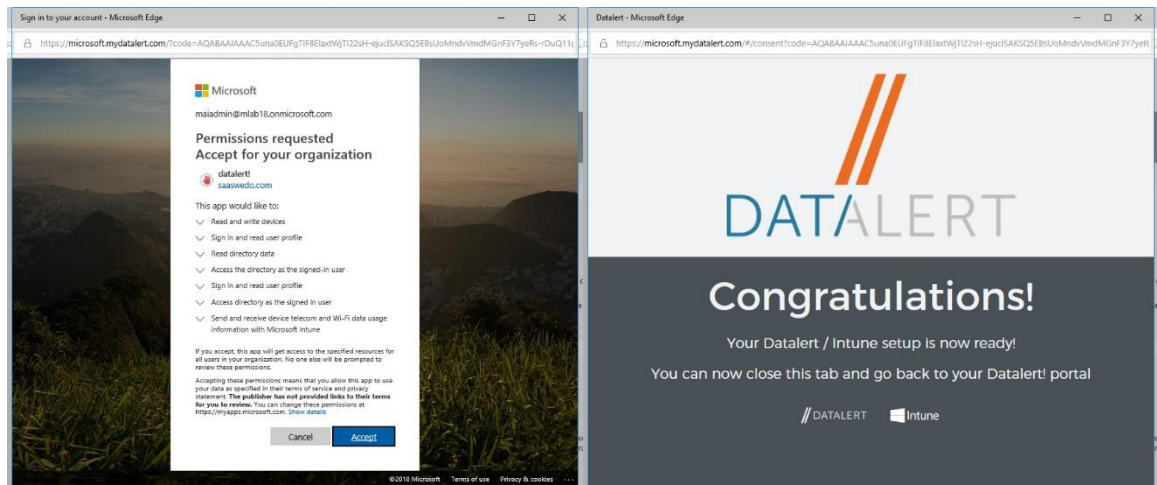
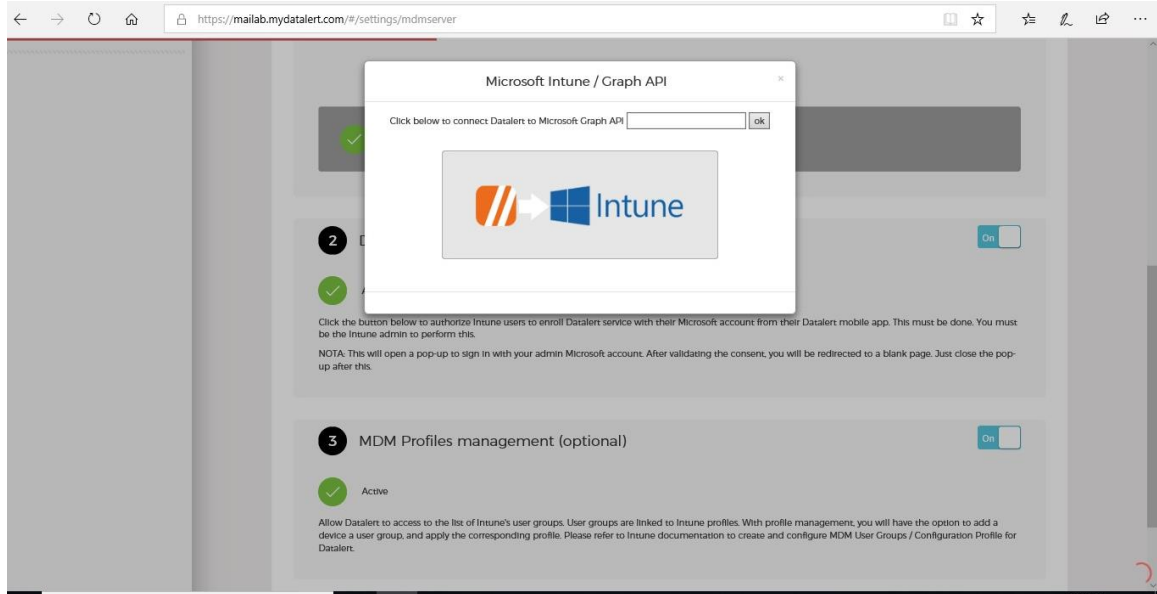


6. In the **Datalert App / ADAL Consent** section, set the switch to **On**. On the Microsoft authentication page, select **Accept**. You are redirected to a Datalert **thank you** page, which closes after a few seconds. Datalert validates the connection and displays green check marks next to a list of items that it validated. If the validation fails, you see a message in red and should contact Datalert Support for help.



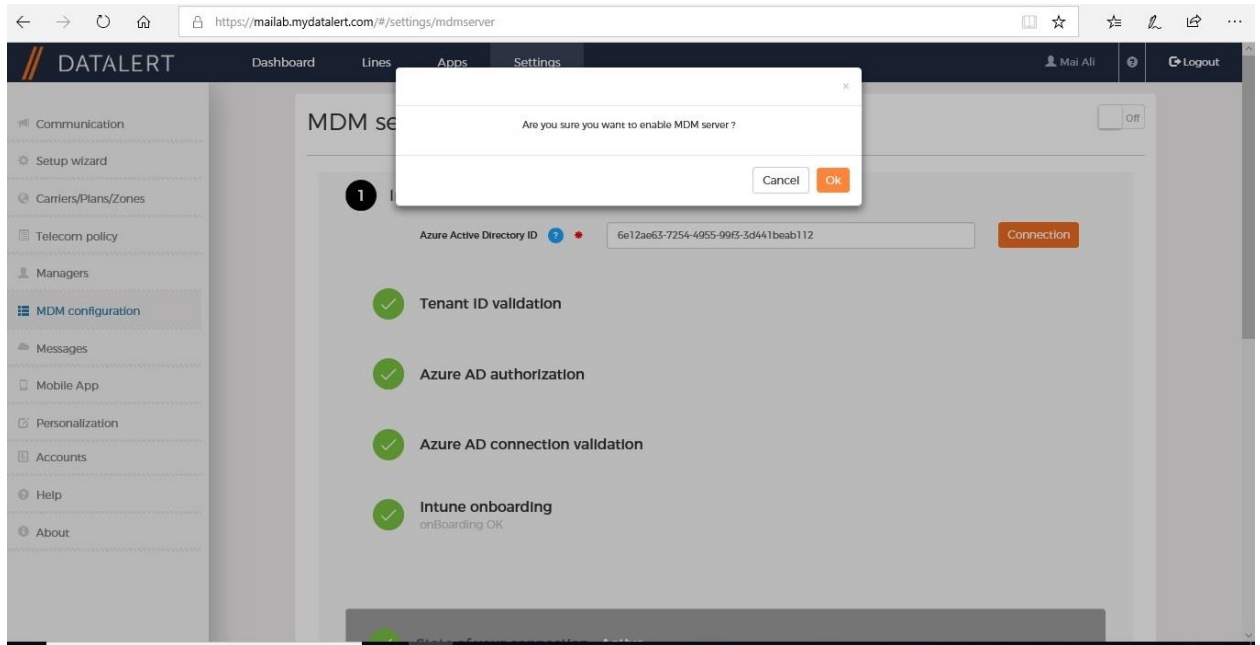
7. In the **MDM Profiles management (optional)** section, set the switch to **On** to allow Datalert to read the available profiles in Intune to help you to setup policies. On the Microsoft authentication page, select **Accept**. You are redirected to a Datalert **thank you** page, which closes after a few seconds. Datalert validates the connection and displays green check marks next to a list of items that it validated. If the validation fails, you see a message in red and should contact Datalert Support for help.

Microsoft Intune step by step on Azure portal



8. In the **MDM Server** section, set the switch to **On** to allow Connection for the Datalert service and for Intune. Intune receives the communication. Then Click Yes to confirm enable MDM.

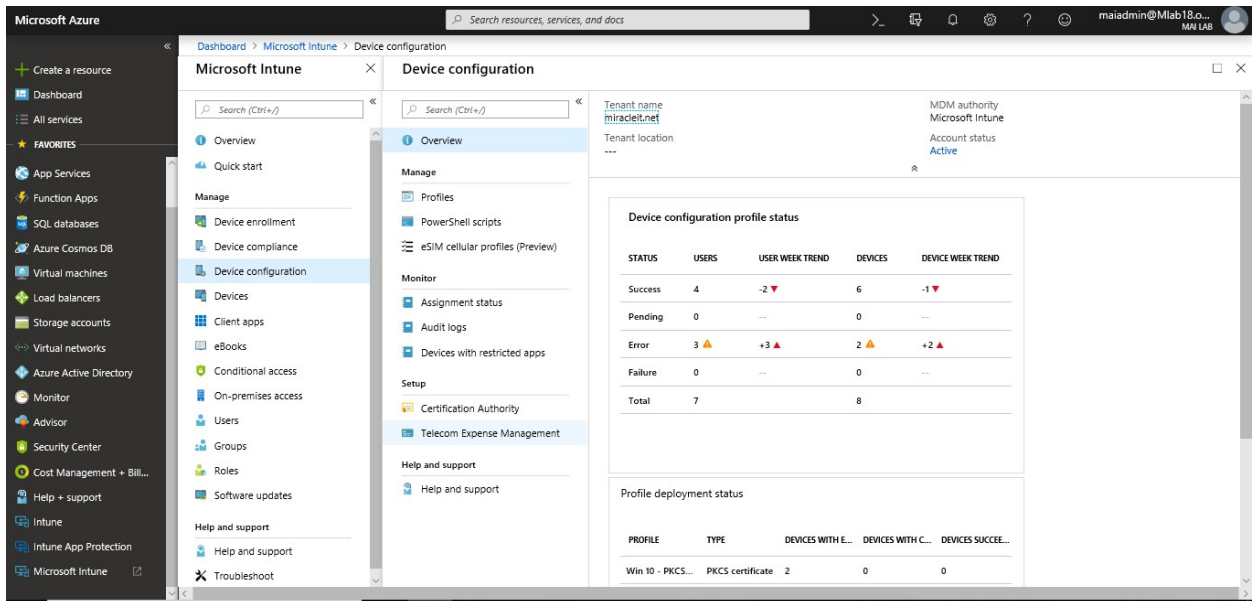
Microsoft Intune step by step on Azure portal



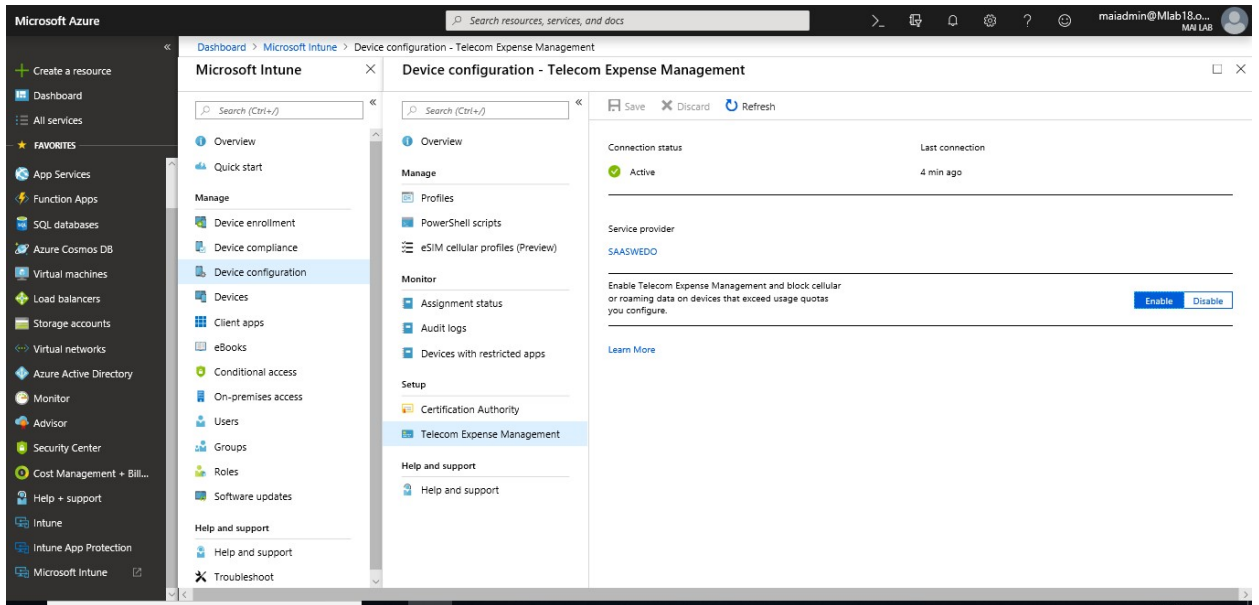
Step 2: Check that the telecom expense management feature is Active in Intune

After you complete Step 1 above, your connection should be automatically enabled, and a connection status of **Active** should be showing in the Azure portal. These steps show you how to check for the **Active** status.

1. Sign into the [Azure portal](#). Choose **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.
2. On the **Intune** pane, choose **Device configuration**.



3. On the **Device configuration** pane, choose **Setup** > **Telecom Expense Management**. Look for the **Active** connection status at the top of the page.



Step 3: Deploy the Datalert app to corporate enrolled devices

To ensure that data usage from only corporate-owned lines is collected, you must do two things:

- Create device categories in Intune
- Target the Datalert app to only corporate phones.

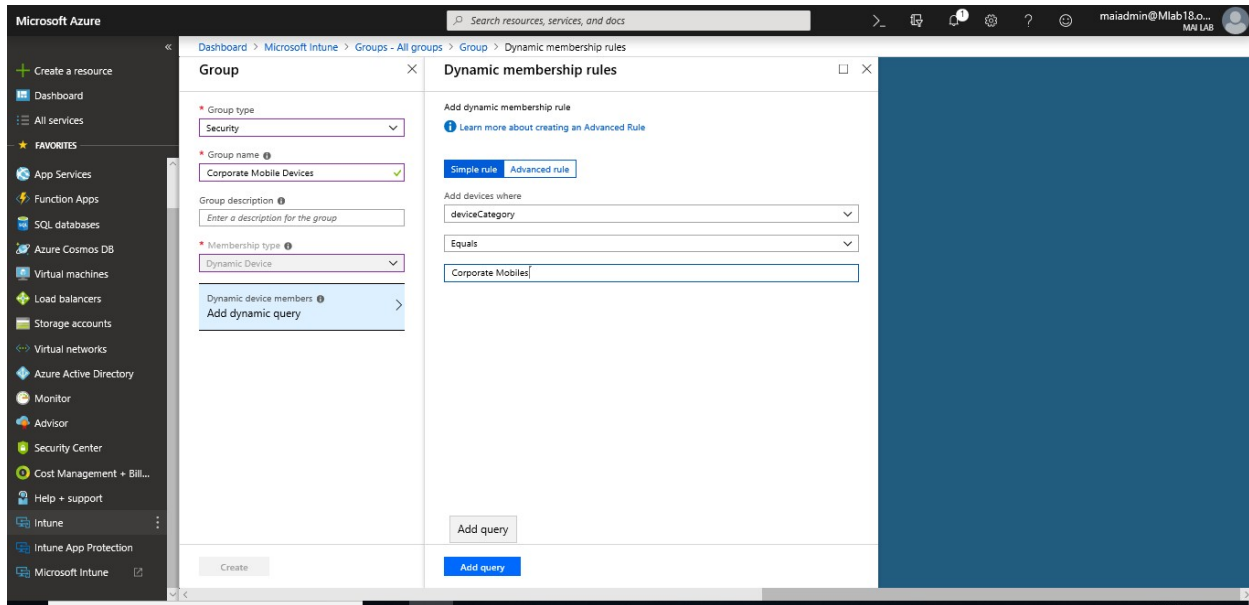
Define device categories and device groups mapped to the categories

Depending on your organizational needs, create at least two device categories (for example, Corporate and Personal). Then, create dynamic device groups for each category. You can create more categories for your organization, as needed.

These categories will be shown to users during enrollment. Depending on which category users choose, the enrolled device will be moved to the corresponding device group. For steps on to create [Device Category](#), you need to check chapter 3.

To create dynamic device group based on category, you need to create dynamic query as following (*device.deviceCategory -eq "Name for caterogy"*)

Microsoft Intune step by step on Azure portal

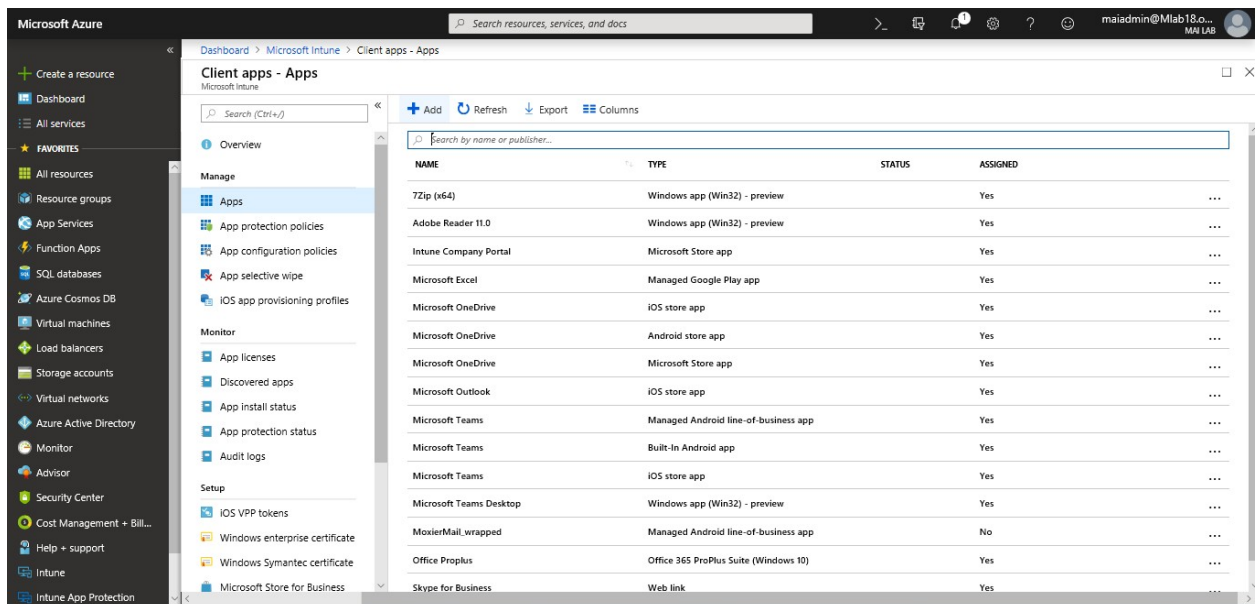


Note: If you already configured corporate identifier on your organization, you won't need to create category & you can create dynamic group based on ownership. In this case dynamic query will be *(device.deviceOwnership -eq "Corporate")*

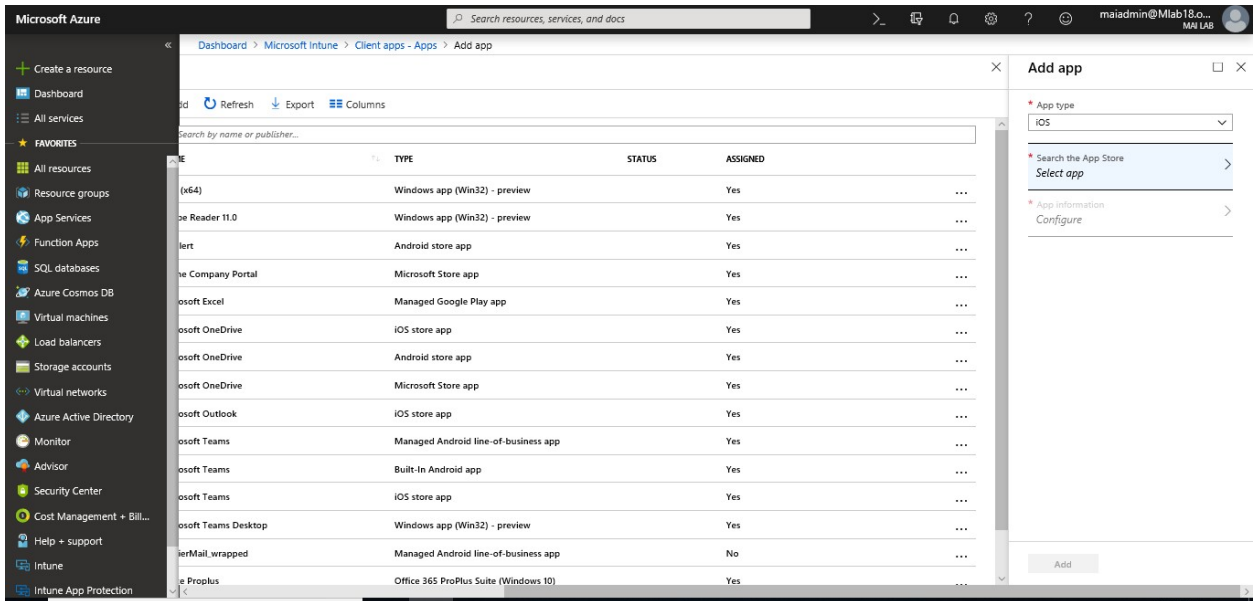
Create the Datalert app in Intune

Follow these steps to create the Datalert app in Intune for each platform. iOS is used as an example in these steps.

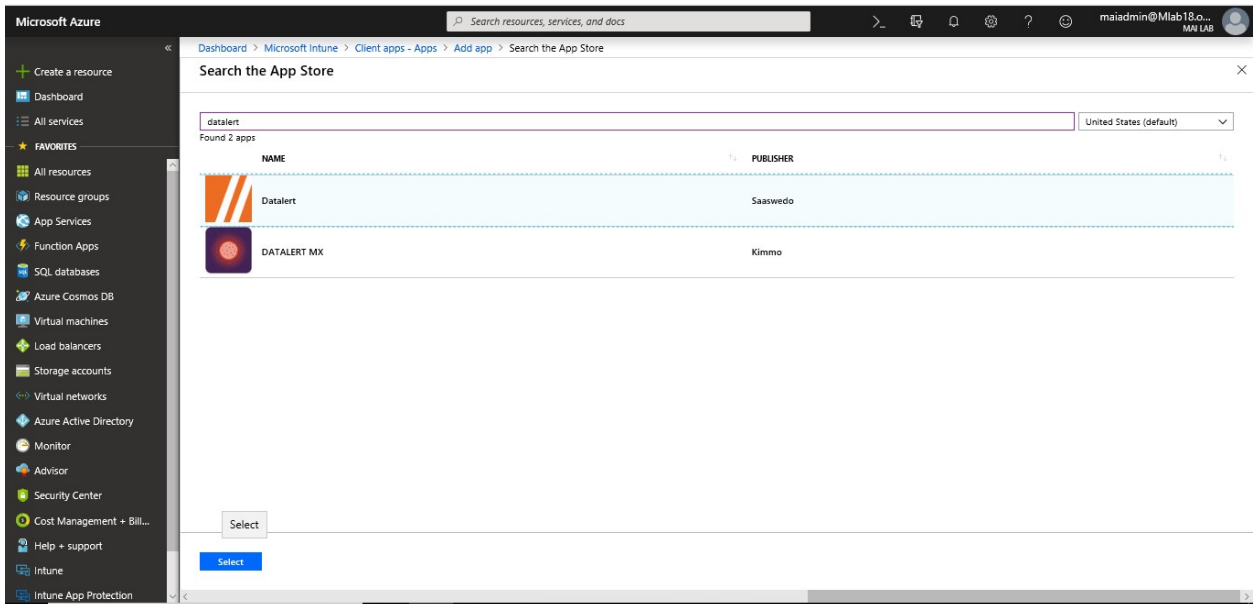
1. On the **Intune** pane of the [Azure portal](#), choose **Client apps**.
2. On the **Client apps** pane, choose **Manage > Apps**.
3. Select **Add** to add an app.



4. Select the app type. For example, for iOS, you would select **iOS Store App**.

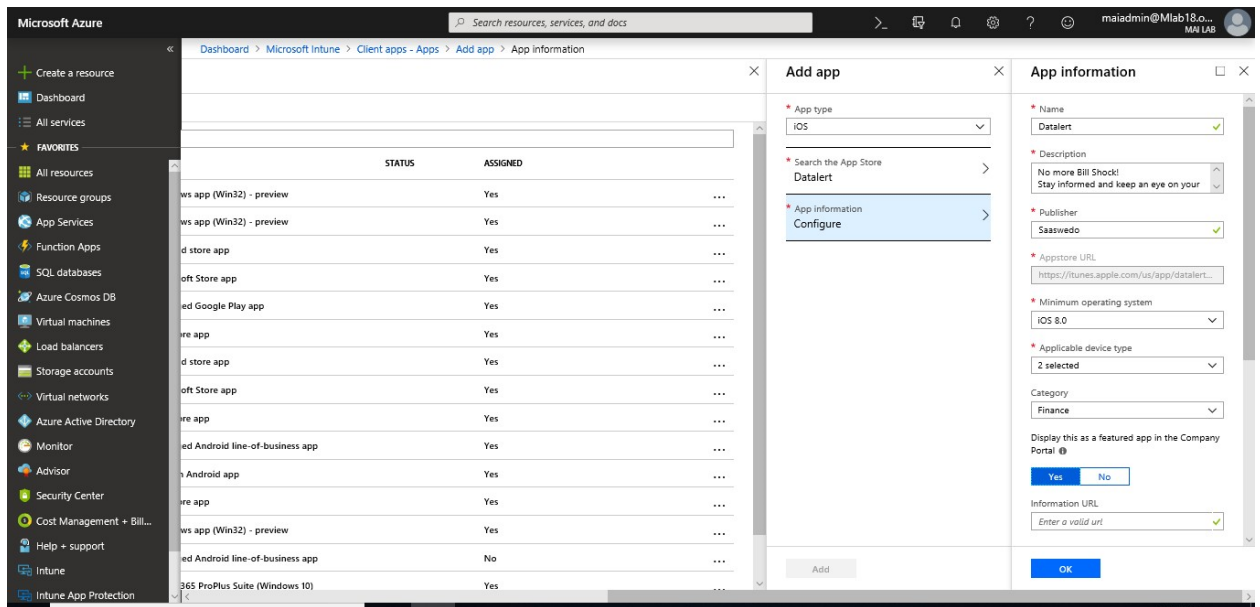


5. In **Search the App Store**, look for the Datalert app by typing **Datalert** in the search window. Select the **Datalert** app and choose **Select**.



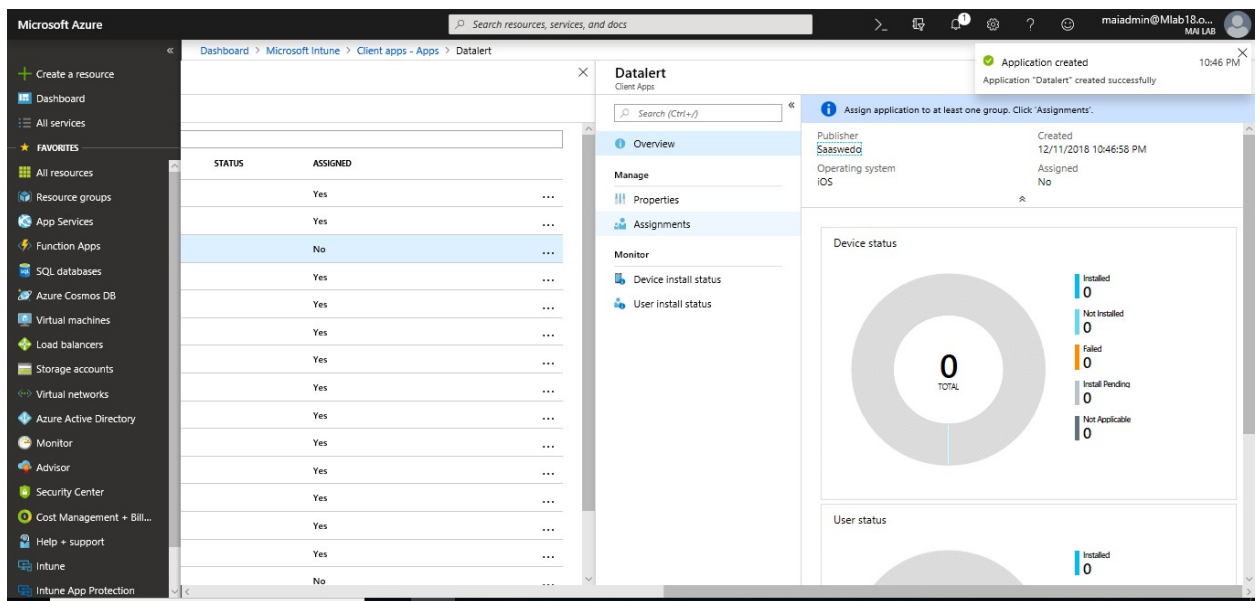
6. Complete the remaining steps to create an app for iOS.

Microsoft Intune step by step on Azure portal

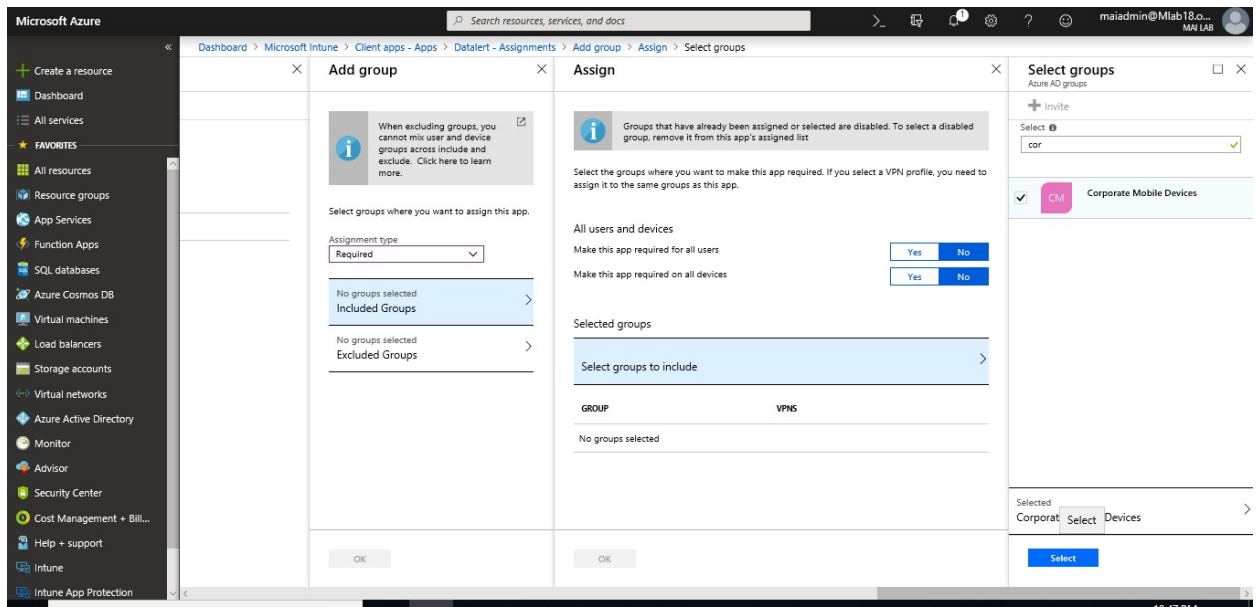


Assign the Datalert app to the corporate device group

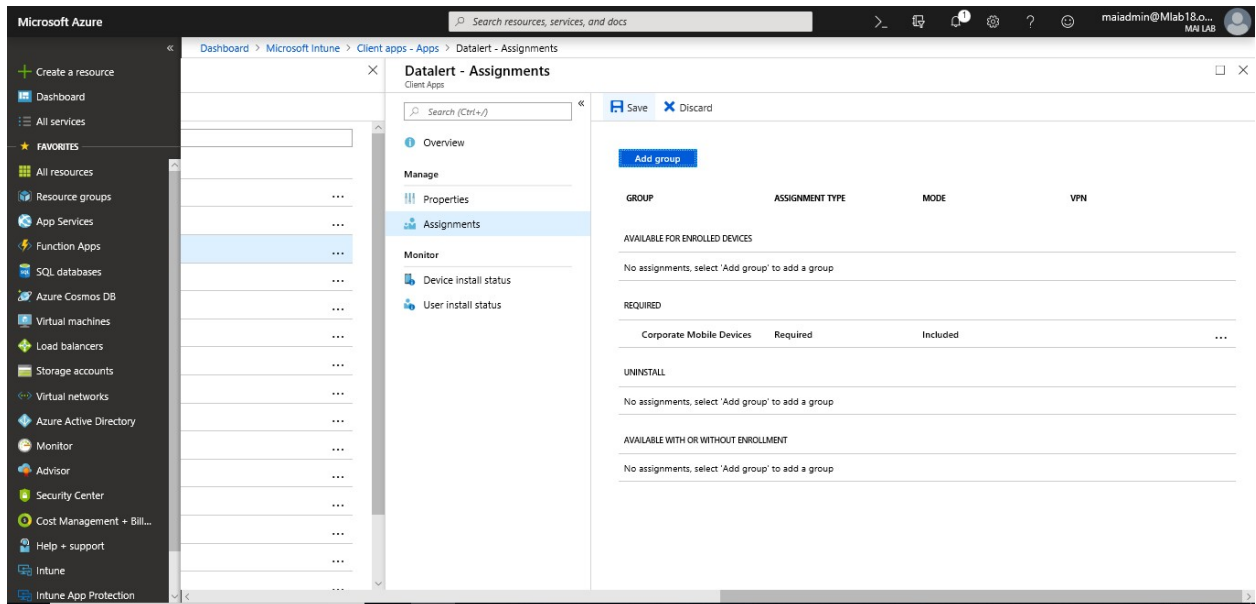
1. From the **Client apps - Apps** pane, select the iOS Datalert app that you created in the previous step.
2. On the **Apps** pane, choose **Manage > Assignments**.



3. Choose **Add group** and follow the steps to select the corporate device group.



4. Choose whether to make the app installation required or optional for the group. The following example screenshot shows the installation as required, which means that users must install the Datalert app installation after enrolling their device.

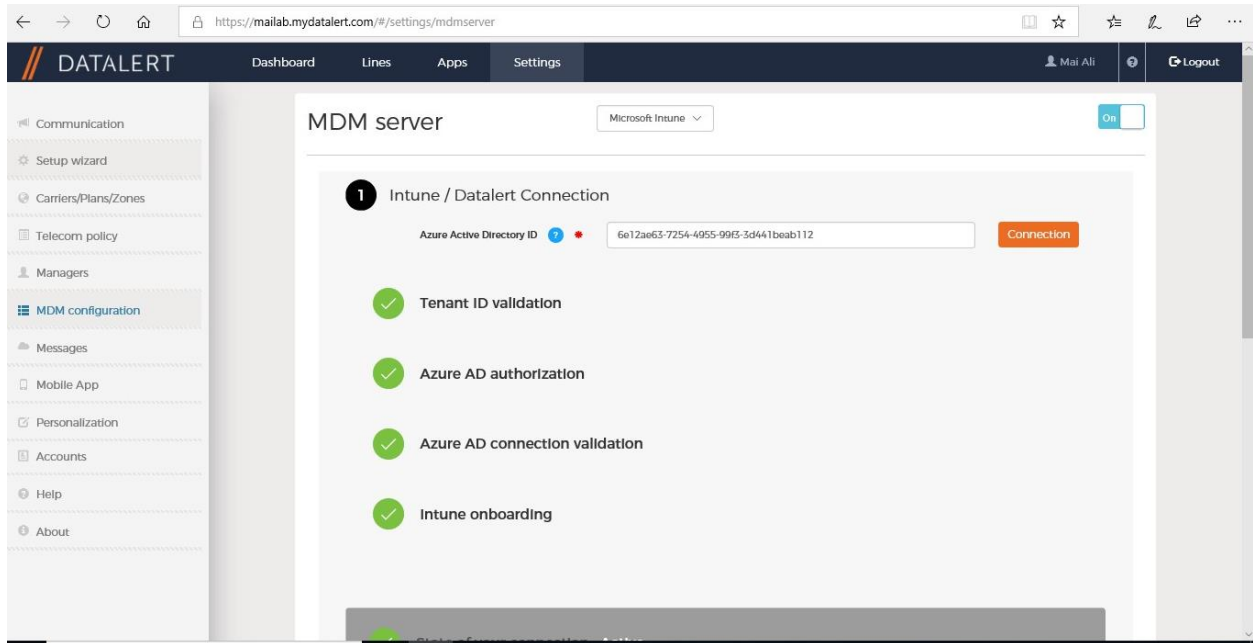


Step 4: Add corporate paid phone lines to the Datalert console

You now have configured the Intune and Datalert services to communicate with each other. You now need to add your corporate paid phone lines to the Datalert console and define thresholds and actions for any cellular or roaming usage violations. You can manually add corporate paid phone lines to the Datalert console or automatically add them after the device is enrolled into Intune.

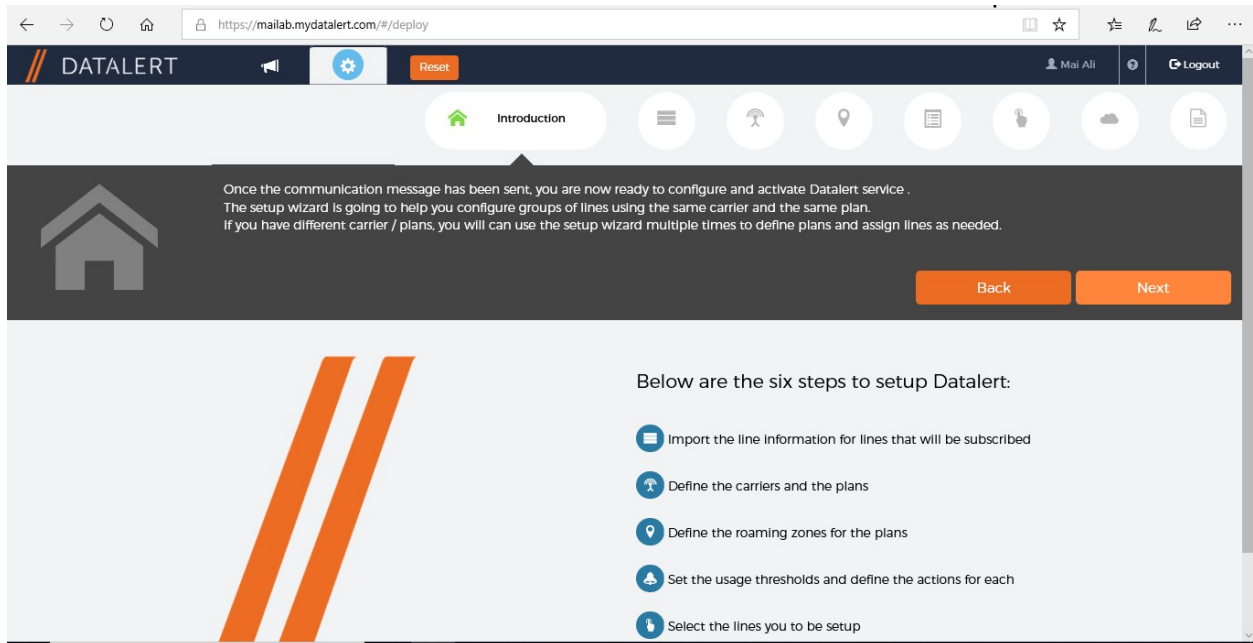
To set these items, follow the steps in the setup wizard under the **Settings** tab

Microsoft Intune step by step on Azure portal



Step 1 - Start the wizard setup in "Settings / Wizard setup"

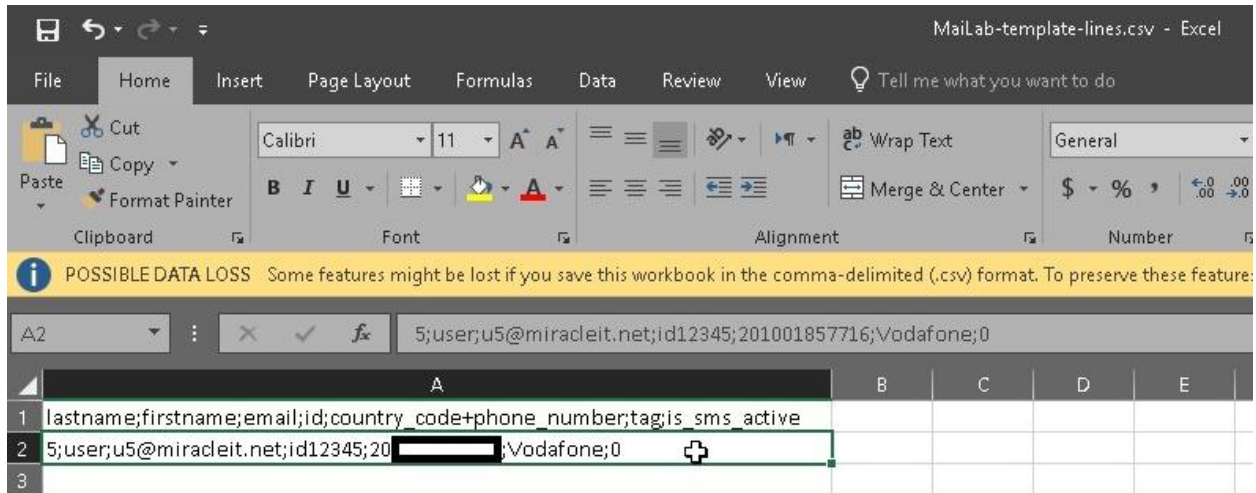
The first screen summarizes the 6 different steps of the setup. Click on "Next"



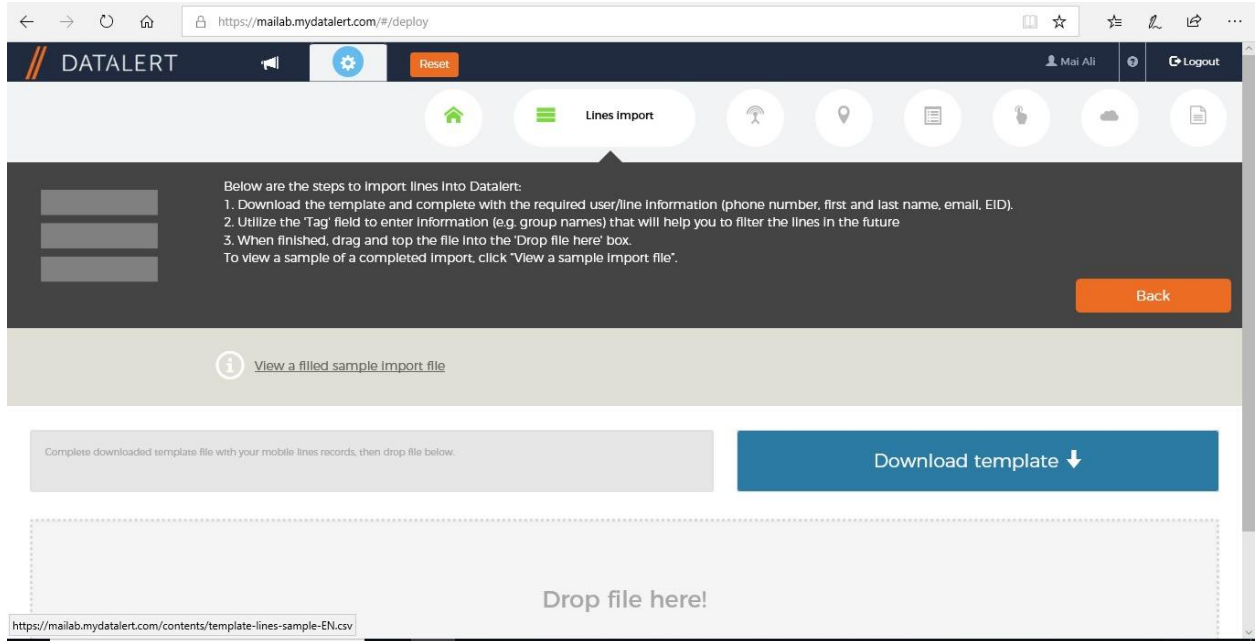
Step 2 - Line import

If it is not previously completed, you can import your lines using a downloadable template. For each line Datalert requires the following: First and last name, email, phone number. A "tag" field is also available and can be used to add other information about the line for sort capabilities (such as carrier, cost center...)

Microsoft Intune step by step on Azure portal



Note: From the lines menu at any time, you can add phone lines manually. Lines enrolled into Microsoft EMS Intune are also automatically added to Datalert and do not need to be imported.



Drag **template file** and Click on “Next”

Step 3 - Carrier / plan creation

In this step you can create the carrier plan or use an existing one. You define a name for the plan, the data allowance for domestic usage and the billing date (bill cycle). You can use the check box below to define the plan as a default plan for this carrier. Click “Next”.

Microsoft Intune step by step on Azure portal

You have selected the lines you want to setup.
The next step is to associate them to a carrier and a plan

- You can create a carrier / plan
- You can use a previously created carrier / plan
- Set the domestic data limit of the plan
- Specify the monthly billing date of the carrier (if you do not know the billing day, choose "1st" and you can update it later)

Back Next

Carrier selection and plan definition

Egypt

Vodafone

Create a new plan Use an existing plan

Vodafone Plan

50 MB

1 USD(S) / MB

Roaming data limit

Billing day

Set the billing day for the line(s)

30

This is the default plan for carrier Vodafone

Step 4 - Zones setup

In this step you create the different zones that are attached to the carrier plans. For each zone you select the countries that are part of the plan using the interactive map, the search engine or the preset continents and define the data allowance (if any) and the price per MB for overages. You can create as many zones as you need to.

You have created a plan for a selected carrier
Please define for each one

- A zone name
- How much data is part of the plan (roaming data limit)
- What is the cost of roaming data over the limit
- The countries to be included in the zone

Back Skip this step Next

Zones for the plan

Vodafone/Vodafone Plan

MEA
50 MB
\$1.00 / MB
0 countries

+ Add

MEA

Egypt(+20) Vodafone

Vodafone Plan

50 MB / KB

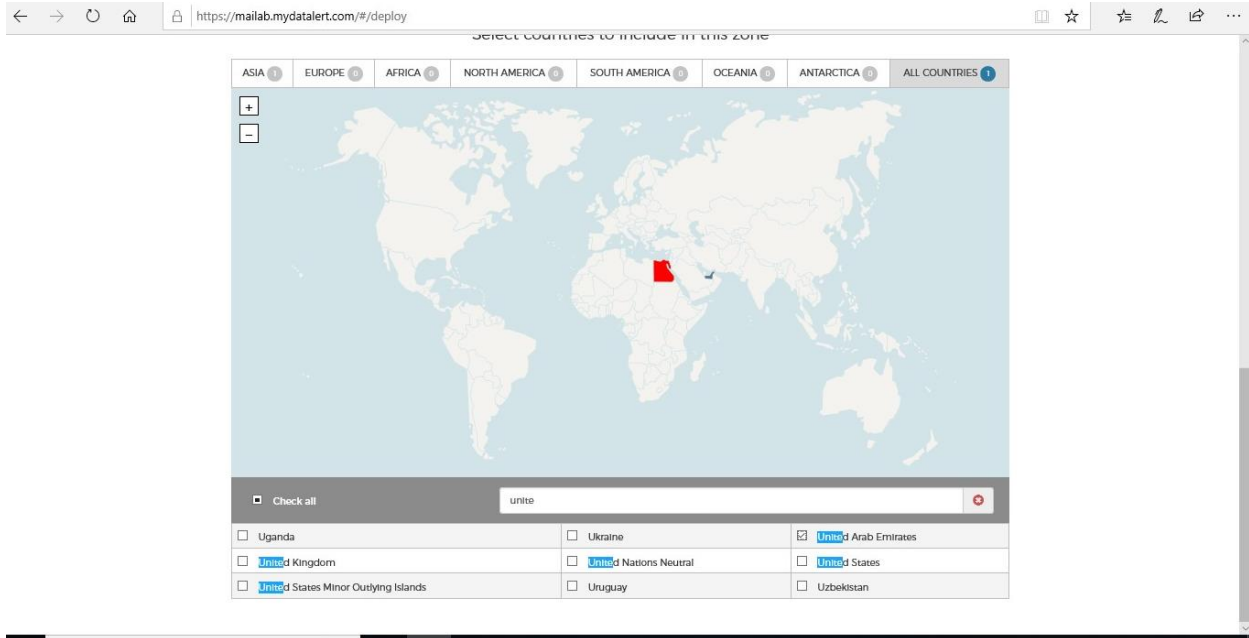
Set domestic limit ↑

1 USD(S) / MB

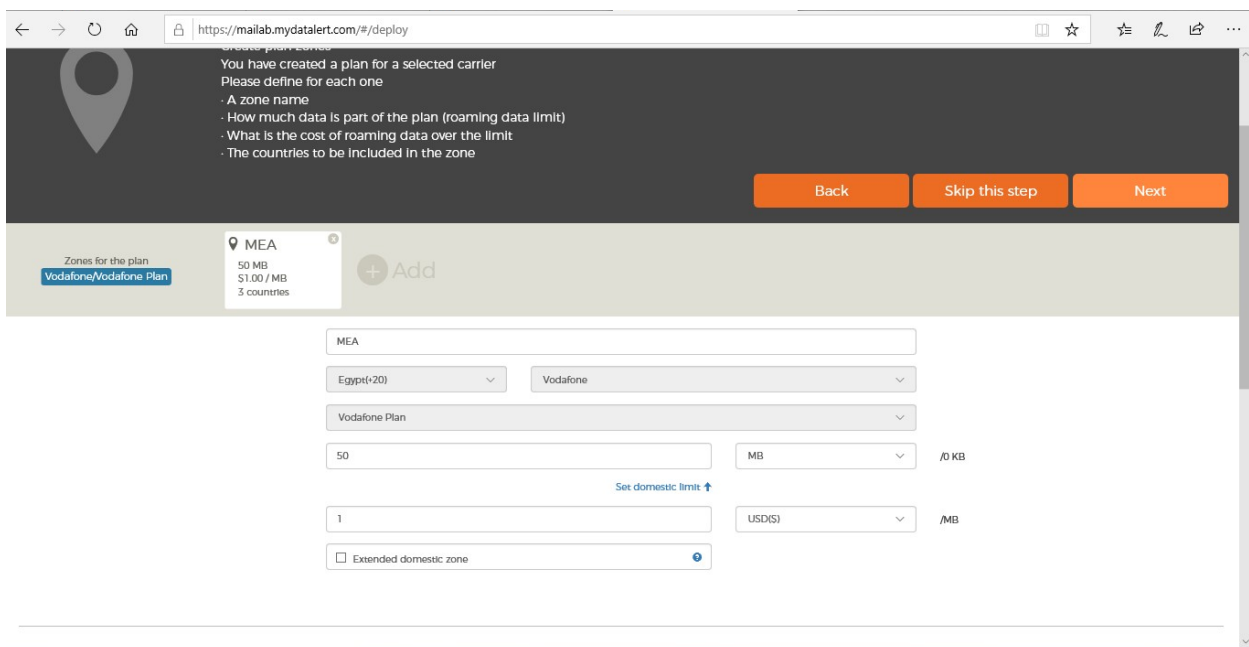
Extended domestic zone

Select **Countries** that are part of the plan

Microsoft Intune step by step on Azure portal



Click Next



Step 5 - Thresholds and actions setup

Either for domestic usage as for roaming usage per zone, you can define the different thresholds and the related actions you want to be taken when they are hit. Messages can be choosing and customized in this step.

Microsoft Intune step by step on Azure portal

← → ↻ 🏠 🔒 https://mailab.mydataalert.com/#/deploy

🛠️ Add domestic data threshold

🛠️ Add Roaming threshold

Month - % ⏪ 🗑️

25 %
of 100 MB

0% 25% 200%

When threshold has been reached.

Message

Send message

English Domestic warning L1

[Add message](#)

Send message to manager

MDM ?

Disable data

On Connection Status page, Check settings

← → ↻ 🏠 🔒 https://mailab.mydataalert.com/#/deploy

Send a notification

Immediately

After hours days

By

Email

Push notif

And repeat action until app is ok

No

Every hours days

Online degraded / Low power mode / Background App Refresh off On

When device state is not optimum

Send a notification

Immediately

After hours days

By

Email

Push notif

And repeat action until app is ok

No

Every hours days

Offline / Force closed / Device off / Network off On

App stopped by the user or device out of network

Send a notification

After hours days

By

Email

And repeat action until app is ok

No

Every hours days

Offline / App deleted On

When an app is deleted by the user

Send a notification

Immediately

After hours days

By

Email

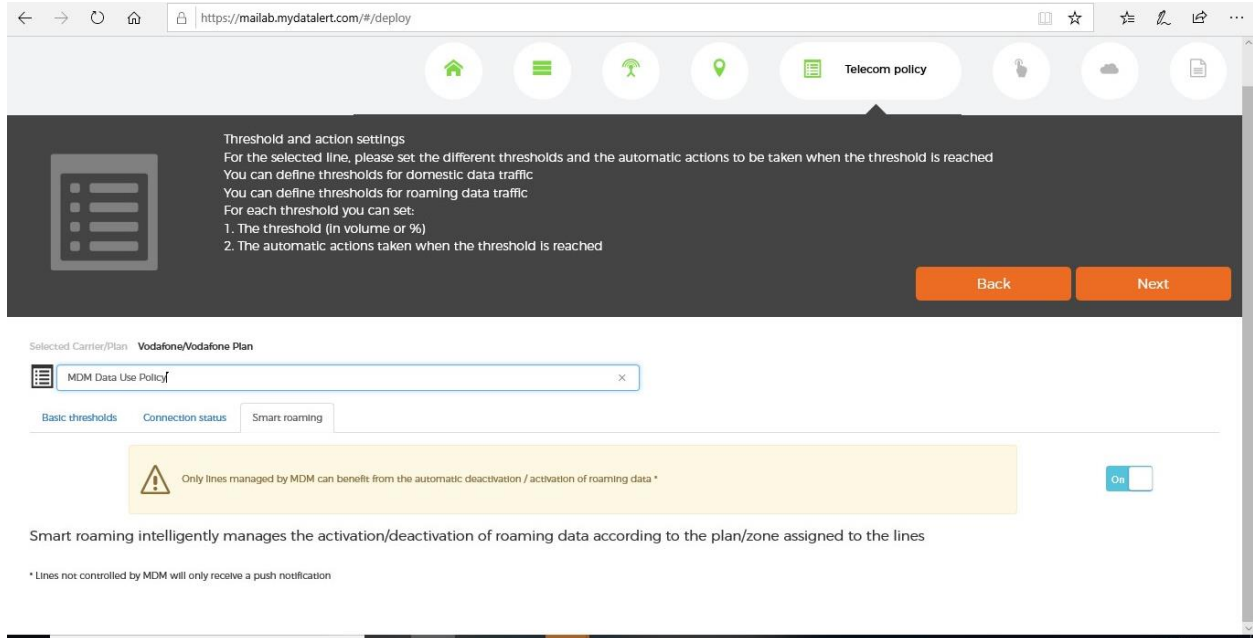
And repeat action until app is ok

No

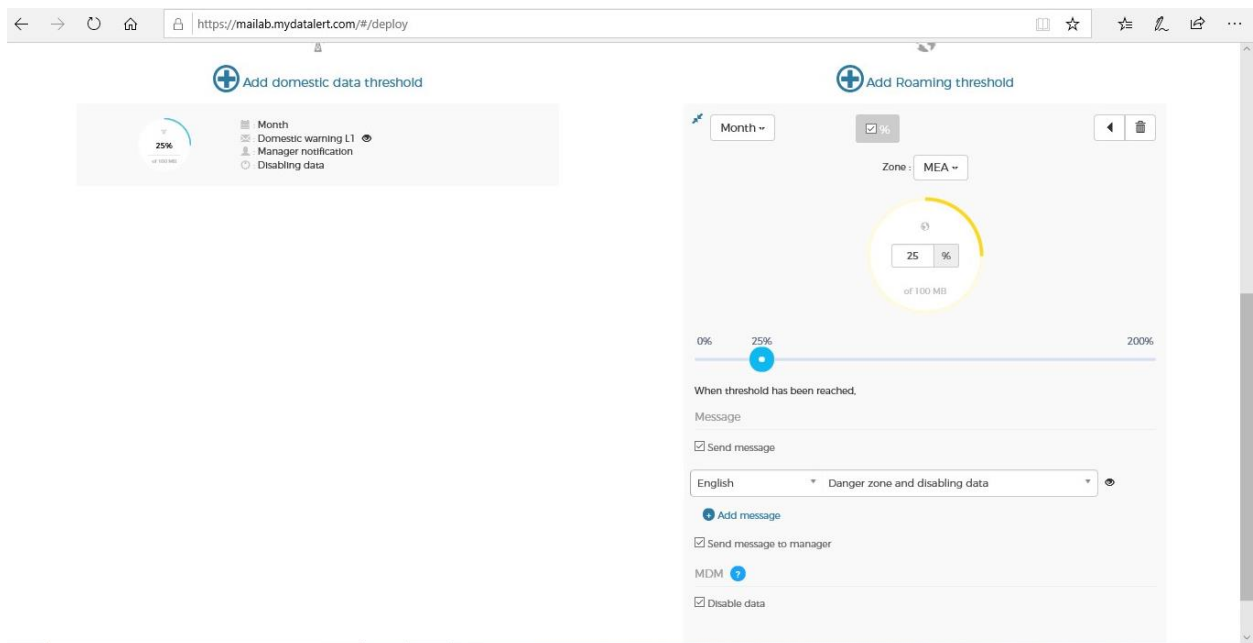
Every hours days

Turn on "Smart roaming"

Microsoft Intune step by step on Azure portal



Add Roaming threshold



By giving a name to those settings you can create a "Policy" that can be applied to different lines and can be modify at any moment. The policy created is linked to the carrier plan it had been created under and can be applied per default for the lines having this carrier plan. Click "Next"

Microsoft Intune step by step on Azure portal

Threshold and action settings
For the selected line, please set the different thresholds and the automatic actions to be taken when the threshold is reached
You can define thresholds for domestic data traffic
You can define thresholds for roaming data traffic
For each threshold you can set:
1. The threshold (in volume or %)
2. The automatic actions taken when the threshold is reached

Selected Carrier/Plan: Vodafone/Vodafone Plan
MDM Data Use Policy

Basic thresholds | Connection status | Smart roaming

+ Add domestic data threshold

- Month
- Domestic warning L1
- Manager notification
- Disabling data

+ Add Roaming threshold

Month: [dropdown]
Zone: MEA
25 MB

Step 6 - Selection of the lines

Select the lines you want the previous configured settings to apply to. The selected line(s) need to have the same billing cycle day and of course the same carrier. A search engine allows a quick search and selection using the “tag” field. Click “Next”

Lines export | Display costs | Percentage (%) | Search by name

Display lines: On | Off | Datalens service | Only over plan | Only roaming | Not enrolled | Without plan | Silent | Selected lines

1 line(s) selected / 2 line(s)

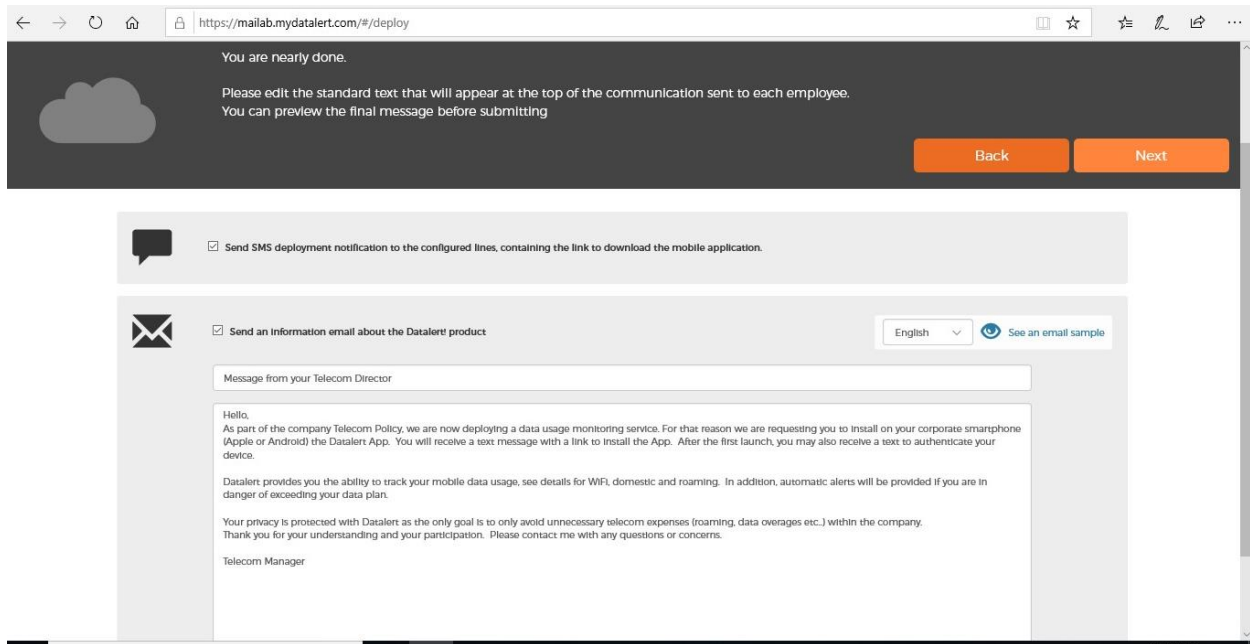
User/Line	Roaming	Domestic	No. of threshold(s)	Last connection
<input type="checkbox"/> USER 4 [redacted] u4@miracleit.net Wataraiya Telecom Ooredoo Nov 30, 2018 - Dec 30, 2018	0 KB	0 KB of 10 MB	2 MDM Data Use Policy	7 days ago Offline App uninstalled
<input checked="" type="checkbox"/> USER 5 +20 10 [redacted] u5@miracleit.net Unknown Carrier No plans set Dec 1, 2018 - Dec 31, 2018	0 KB	0 KB	0	No connection Offline Ready to enroll

Step 7 - Sending messages for deployment (optional)

This is the final step in the setup. The admin can send to the end user(s) either or both of the following messages. Of course, the preferred way is to deploy the app using Intune.

Microsoft Intune step by step on Azure portal

- If the Datalert App has not been previously installed on the device with the Intune enrollment or by the user from the App store, the admin can send a text message to the mobile device with a "one tap" link to finalize the enrollment. The link will walk the user through the installation prior to the last step of enrollment.
- If the Datalert App has been installed on the device already, an email message can be sent to the end user that explains the benefits of Datalert solution for the company and for him/her. This editable communication provides information about data privacy as well.



The screenshot shows a web browser window with the URL <https://mailab.mydatalert.com/#/deploy>. The page has a dark header with a cloud icon and the text: "You are nearly done. Please edit the standard text that will appear at the top of the communication sent to each employee. You can preview the final message before submitting." Below this are "Back" and "Next" buttons.

The main content area has two sections:

- Send SMS deployment notification to the configured lines, containing the link to download the mobile application.
- Send an information email about the Datalert product. This section includes a language dropdown set to "English" and a "See an email sample" link.

A preview of the email content is shown below:

Message from your Telecom Director

Hello,
As part of the company Telecom Policy, we are now deploying a data usage monitoring service. For that reason we are requesting you to install on your corporate smartphone (Apple or Android) the Datalert App. You will receive a text message with a link to install the App. After the first launch, you may also receive a text to authenticate your device.

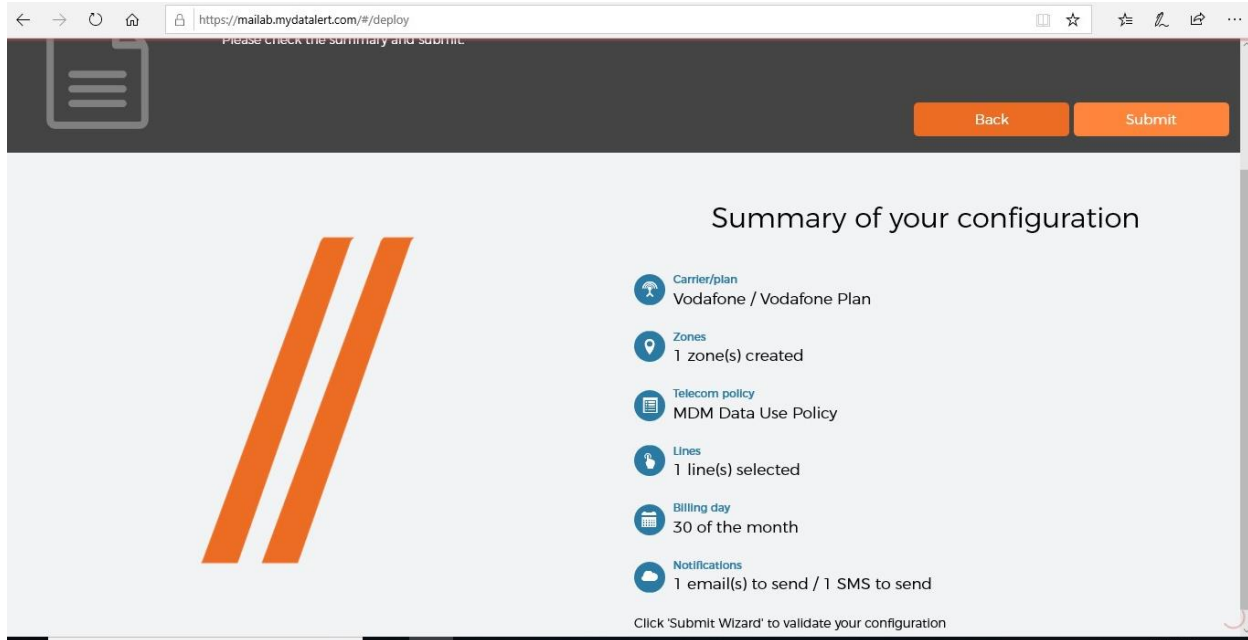
Datalert provides you the ability to track your mobile data usage, see details for WFL, domestic and roaming. In addition, automatic alerts will be provided if you are in danger of exceeding your data plan.

Your privacy is protected with Datalert as the only goal is to only avoid unnecessary telecom expenses (roaming, data overages etc.) within the company. Thank you for your understanding and your participation. Please contact me with any questions or concerns.

Telecom Manager

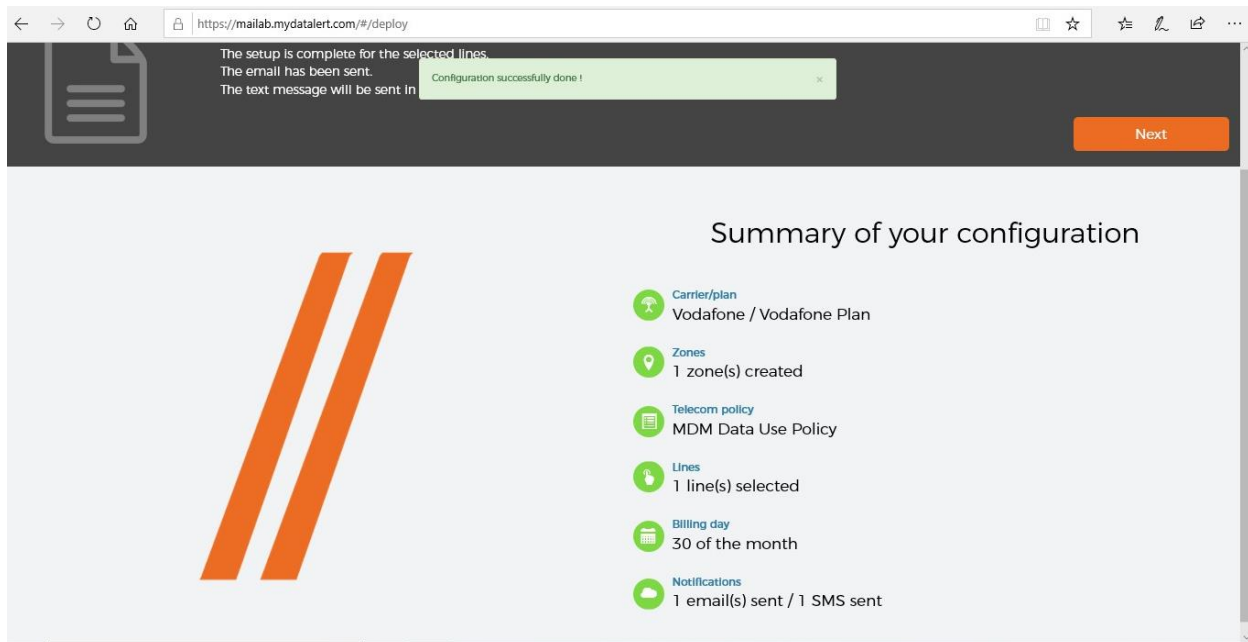
Click "**Submit**" to finish.

Microsoft Intune step by step on Azure portal



Note: At any time after the initial setup, you can launch the wizard to add or manage your deployment.

The Datalert service is now active, and it starts monitoring data usage and disabling cellular and roaming data on devices that exceed the configured usage limits.

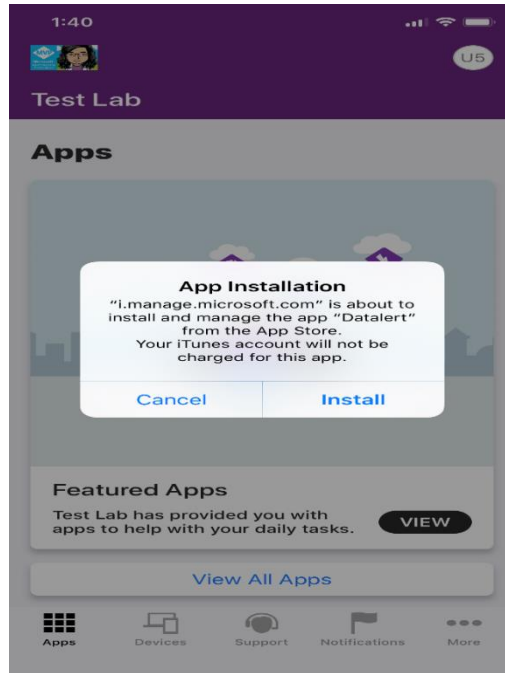


Note: When you enable Datalert with Intune, it will disable roaming data when you exceed threshold for iPhone & Samsung Knox, but it will **disable domestic data** if you exceed threshold, **only exist on Samsung Knox** until now.

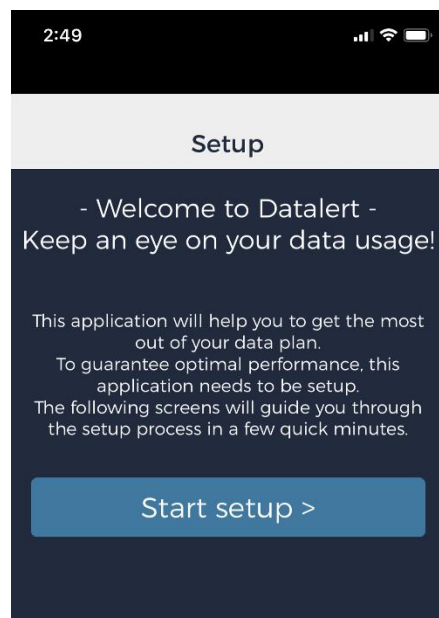
Step 5: Client enrollment experience

For the client enrollment experience, see the following:

You will receive a notification to install the [Datalert](#) app from the App Store.

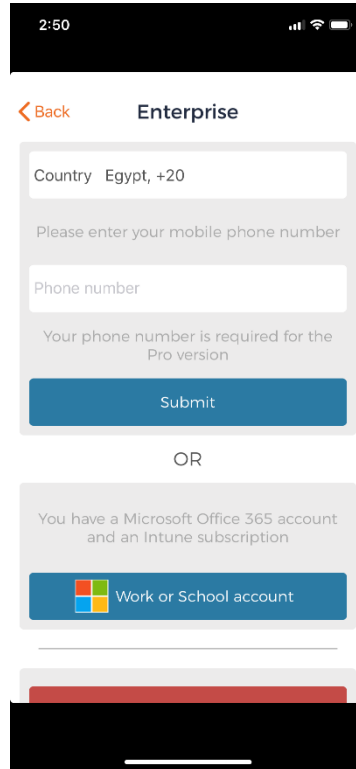


Select **Start Setup**.

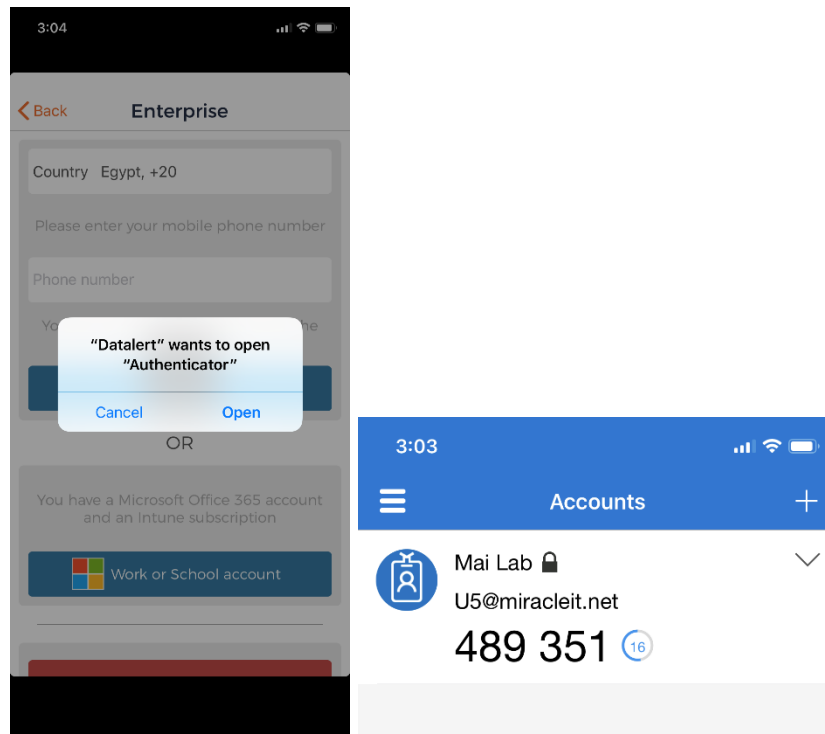


To Enroll into Datalert using your Microsoft work or school account

1. Select **Enroll with Microsoft account**.

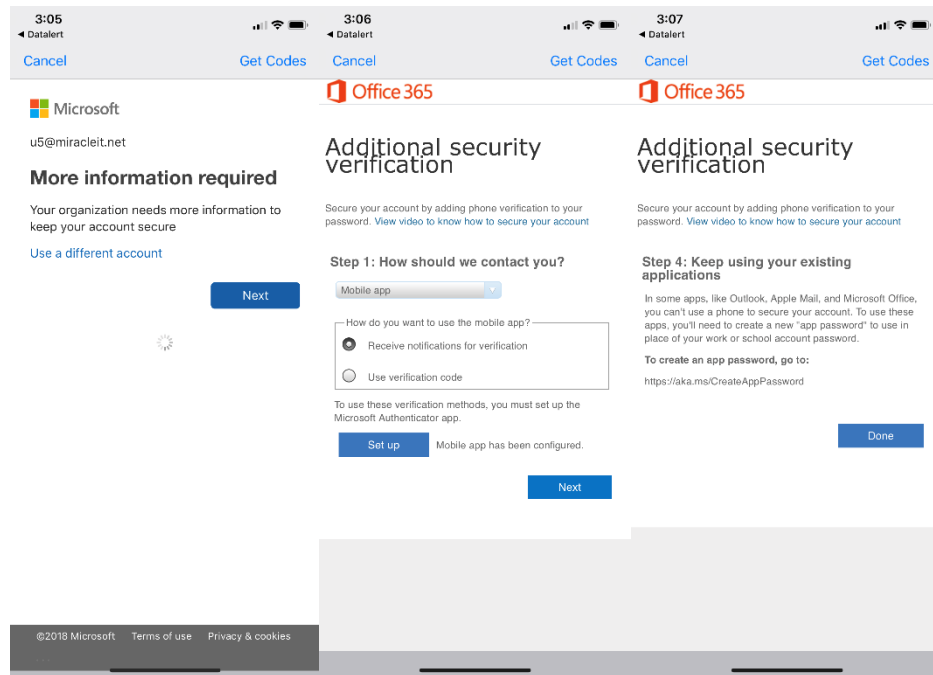


2. You'll receive a notification that **"Dataalert"** wants to open **"Authenticator"**. Select **Open**.

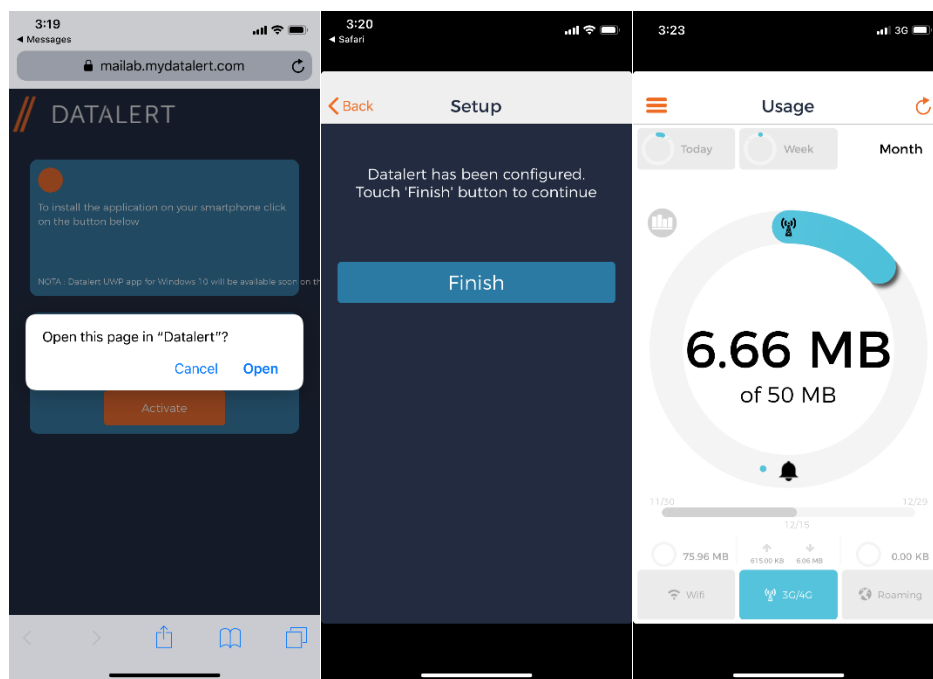


Note: You need to have the Microsoft Authenticator app installed and active on your phone to enroll this way.

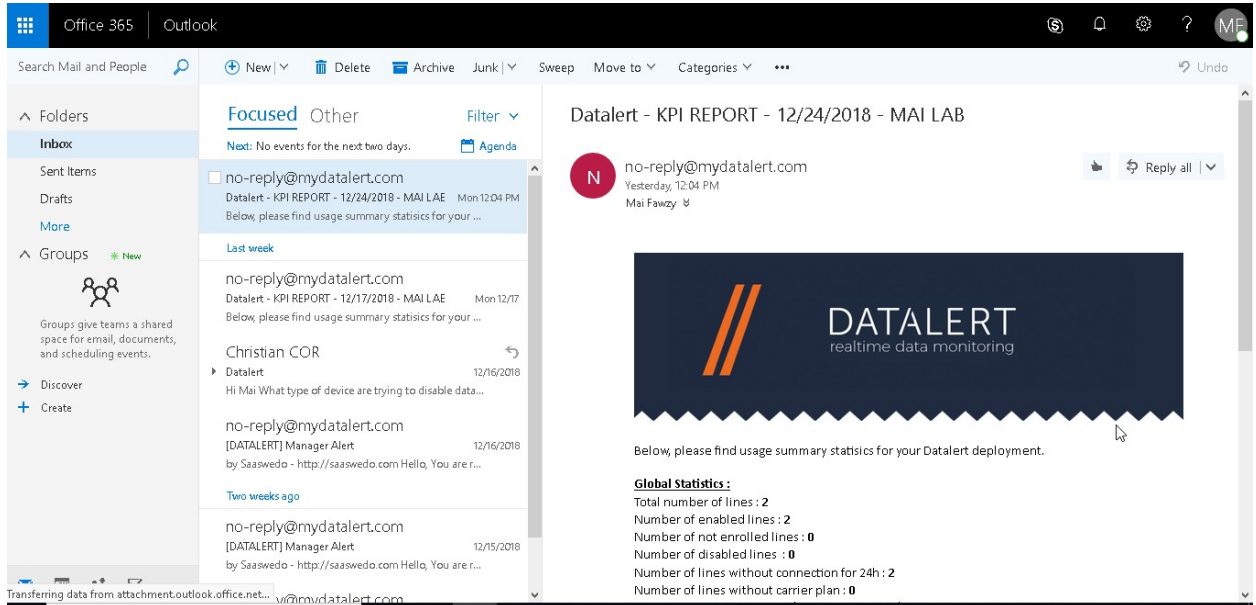
3. Sign in with your **Microsoft school or work account**. Datalert setup will work for a few moments, then should complete.



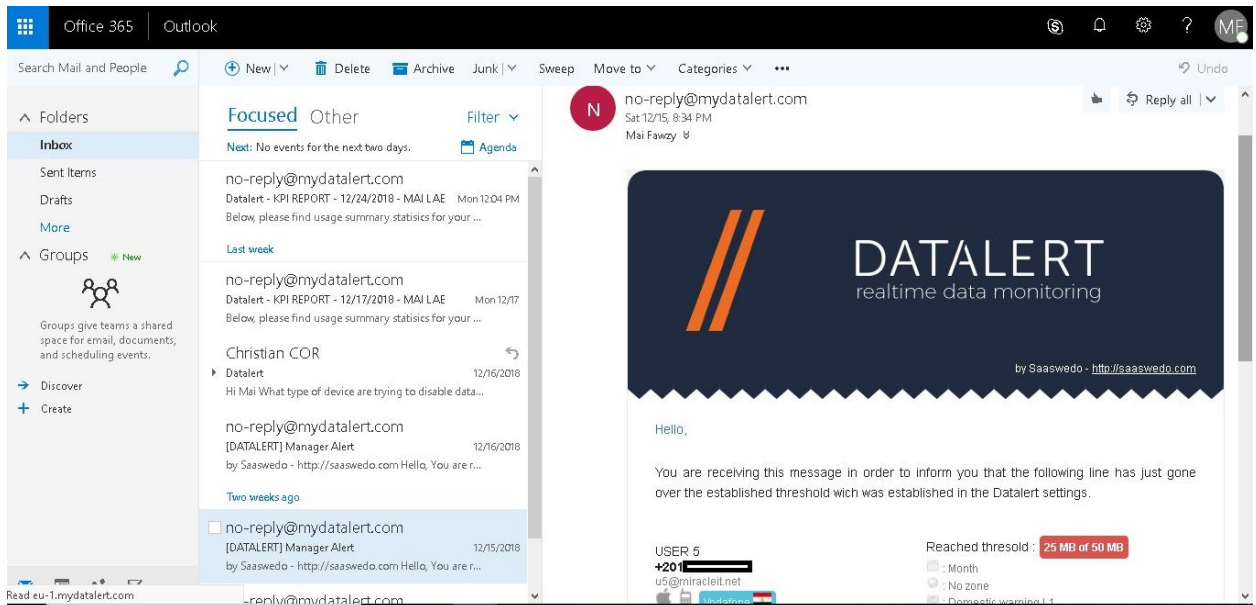
4. Tap **Finish** when it completes.



5. Admin will receive weekly report as mention on configuration.



6. When end user exceed threshold, admin will receive warning mail as below.



Note: The Datalert app is how your organization can measure data usage. If your organization has configured the Microsoft work or school enrollment option, you will be required to log in with your work or school account. If this hasn't been enabled, you will need to provide information such as your phone number and verify your device using a code to enroll into the Datalert service from the app.

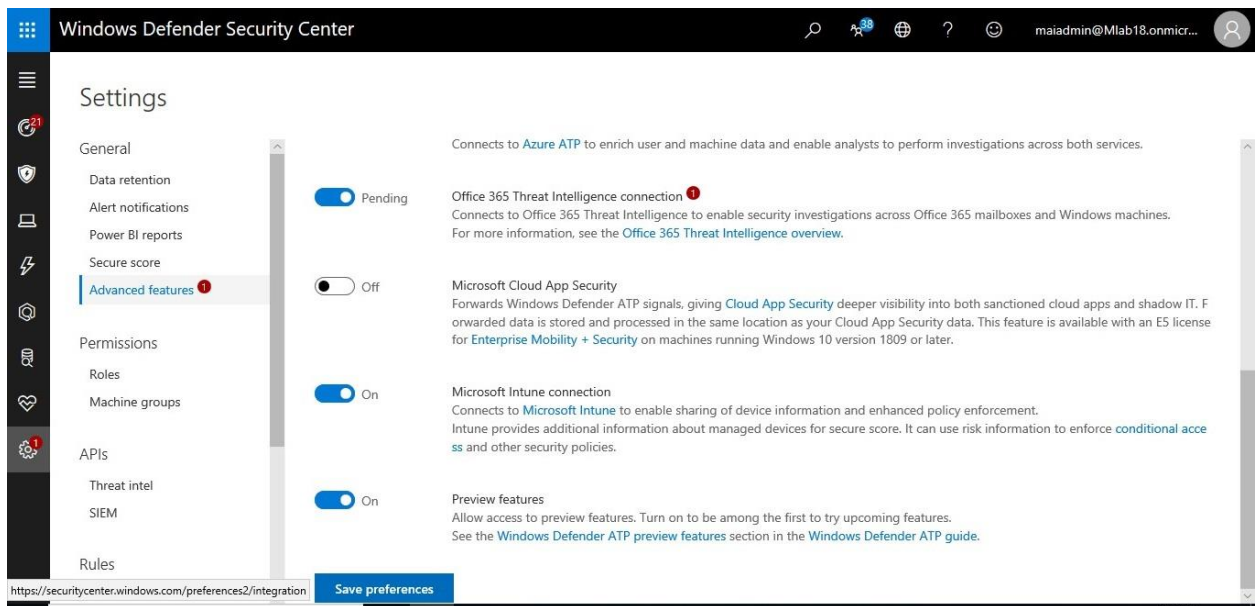
Integrate between Microsoft Intune & Windows Defender ATP

Microsoft Intune step by step on Azure portal

In this scenario, All Windows 10 Pcs with high risk block access to corporate data. You need to make sure that all your devices are enrolled in Intune.

Step 1: Turn on the Microsoft Intune connection

1. Sign in to the [Azure portal](#). Select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device compliance** > **Windows Defender ATP** > **Open the Windows Defender Security Center**.
3. In **Windows Defender Security Center**, select **Settings** > **Advanced features** > **Microsoft Intune connection**. Toggle the Microsoft Intune setting to **On**.

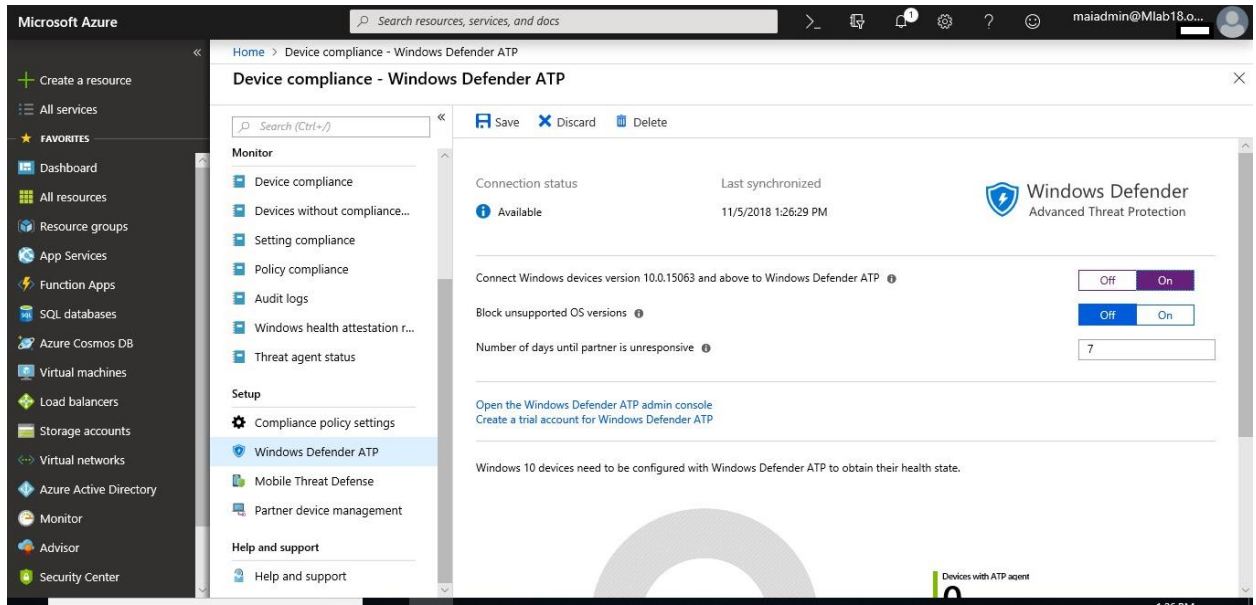


4. Click **Save preferences**.

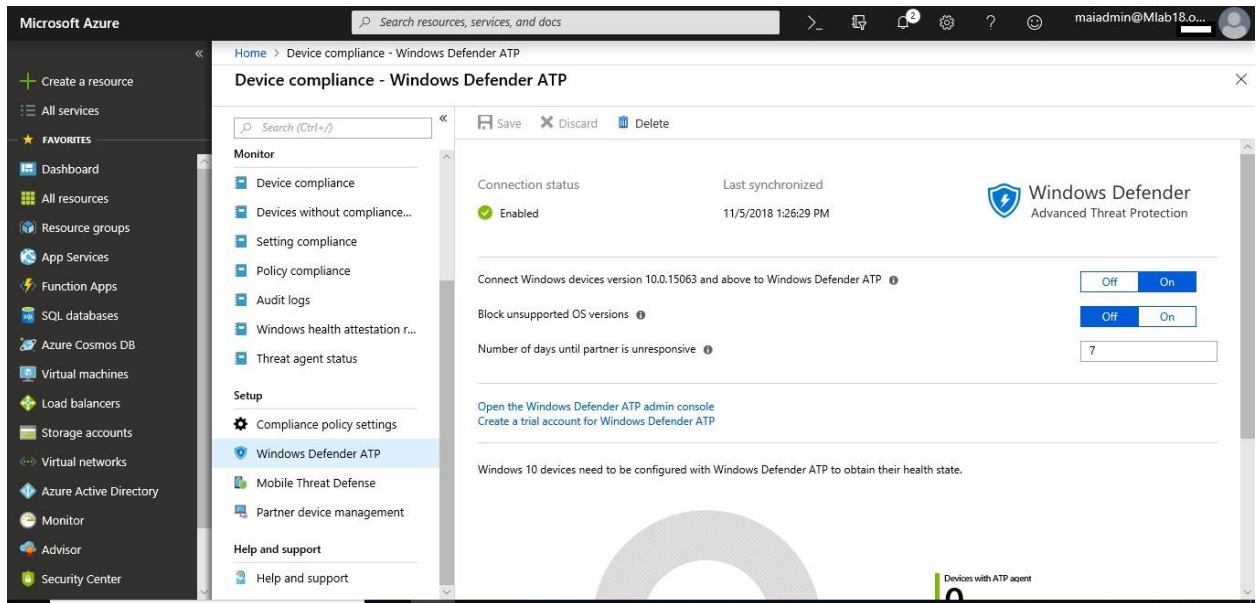
Step 2: Turn on the Windows Defender ATP integration in Intune

1. Sign in to the [Azure portal](#).
2. Select **Device compliance** > **Windows Defender ATP**.
3. Set **Connect Windows 10.0.15063+ devices to Windows Defender Advanced Threat Protection** to **On**.

Microsoft Intune step by step on Azure portal



4. Click Save.



Step 3: Onboard devices using a configuration profile

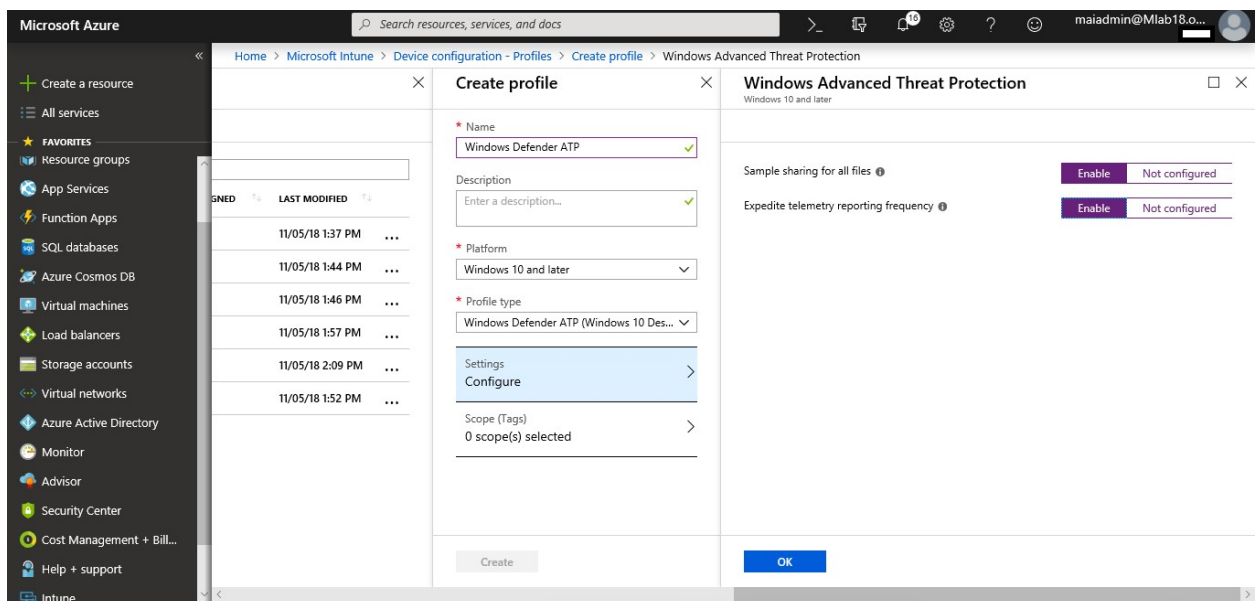
When you onboard, Intune gets an auto-generated configuration package from Windows Defender ATP. When the profile is pushed or deployed to the device, this configuration package is also pushed to the device. This allows Windows Defender ATP to monitor the device for the threats.

To Create the configuration profile, you can follow below steps

1. In the [Azure portal](#), select **All services**, filter on **Intune**, and select **Microsoft Intune**.

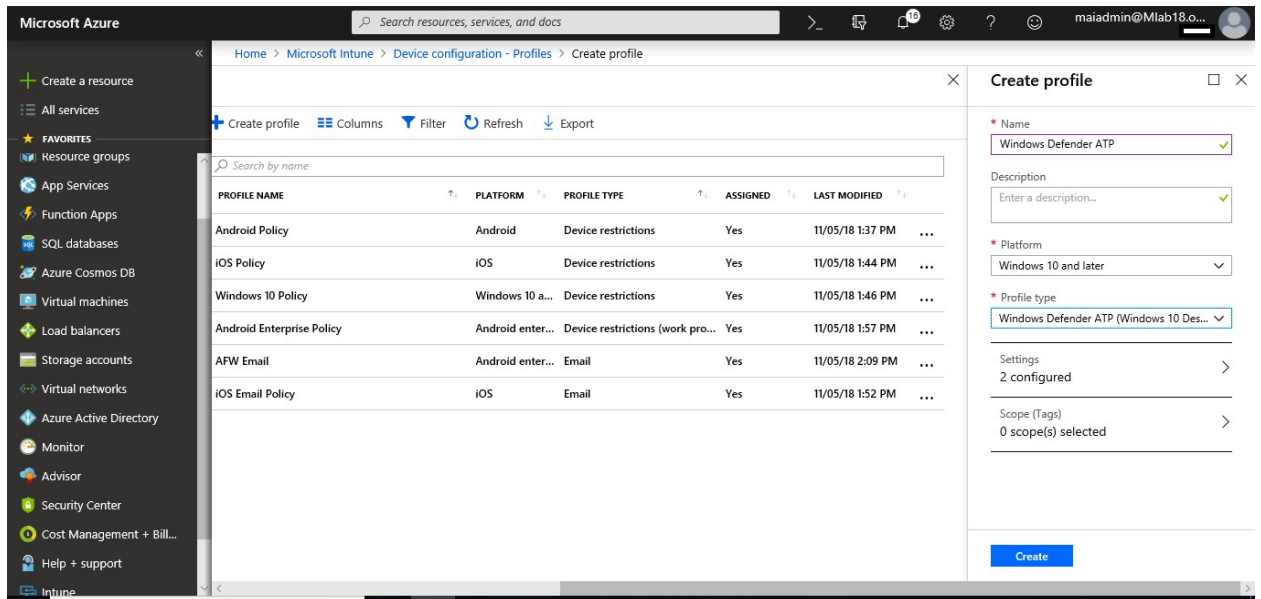
2. Select **Device Configuration > Profiles > Create profile**.
3. Enter a **Name** and **Description**.
4. For **Platform**, select **Windows 10 and later**
5. For **Profile type**, select **Windows Defender ATP (Windows 10 Desktop)**.
6. Configure the settings:
 - **Sample sharing for all files: Enable** allows samples to be collected and shared with Windows Defender ATP. For example, if you see a suspicious file, you can submit it to Windows Defender ATP for deep analysis. **Not configured** doesn't share any samples to Windows Defender ATP.
 - **Expedite telemetry reporting frequency:** For devices that are at high risk, **enable** this setting so it reports telemetry to the Windows Defender ATP service more frequently.

Note: If you've properly established a connection with Windows Defender ATP, Intune will automatically **Onboard** the configuration profile for you.

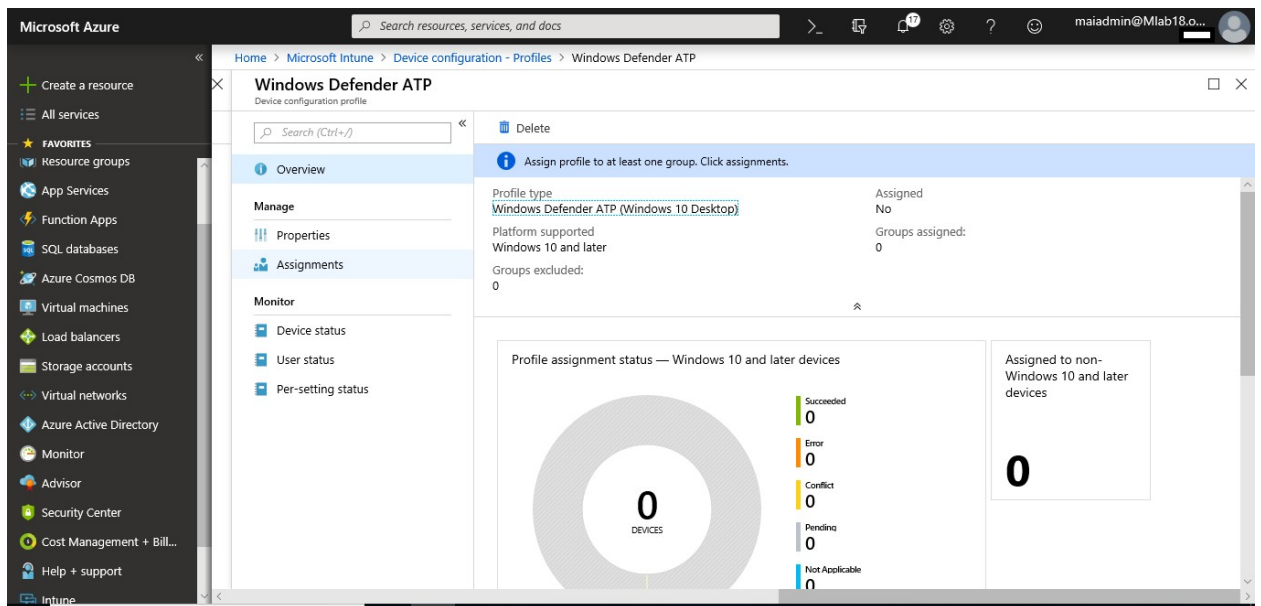


7. Select **OK**, and **Create** to save your changes, which creates the profile.

Microsoft Intune step by step on Azure portal

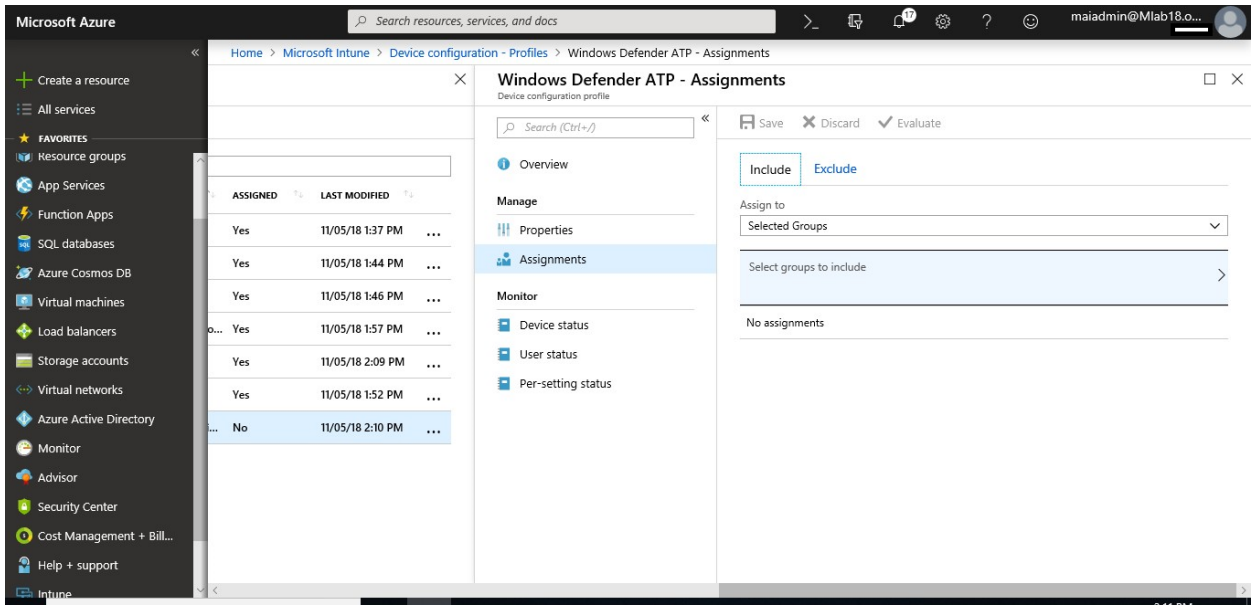


8. In the **Manage** section of the menu, select **Assignments**.

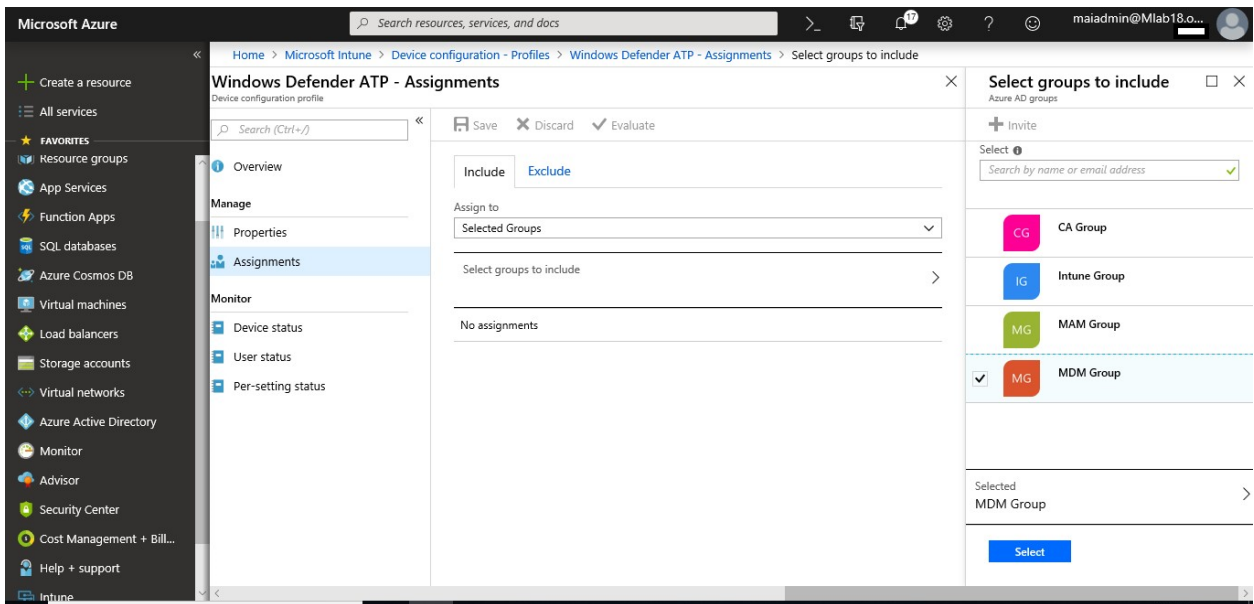


9. Select **Add Group** to open the **Add group** pane that is related to the app.

Microsoft Intune step by step on Azure portal

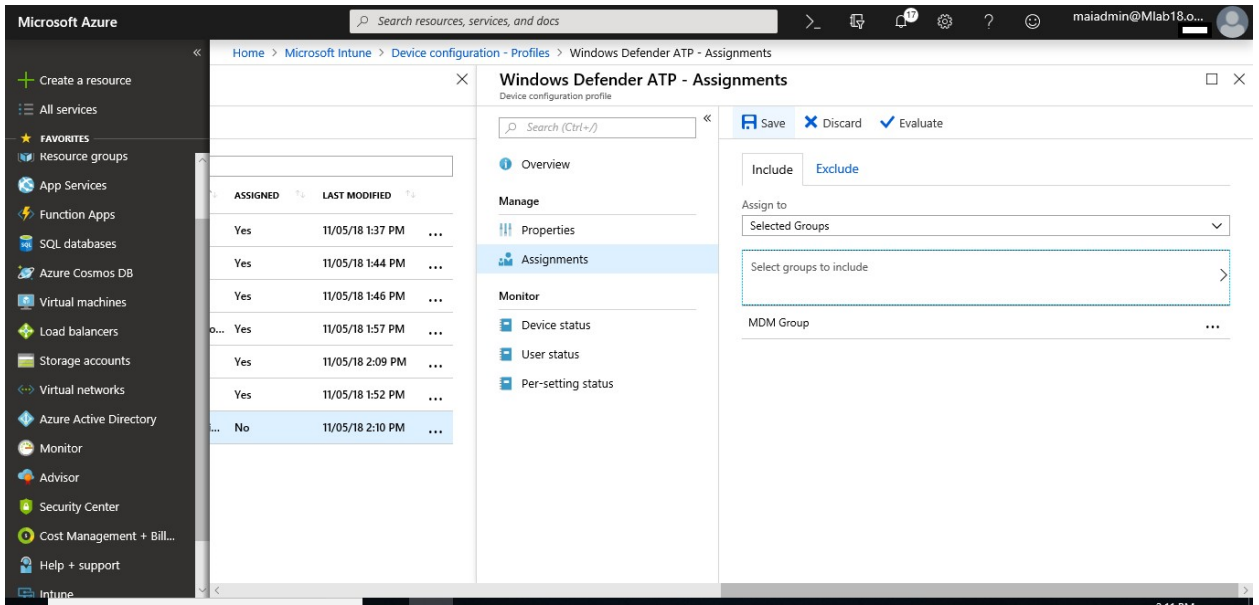


- To select the groups of users that are affected by this app assignment, select **Included Groups**. After you have selected one or more groups to include, Click **Select**.

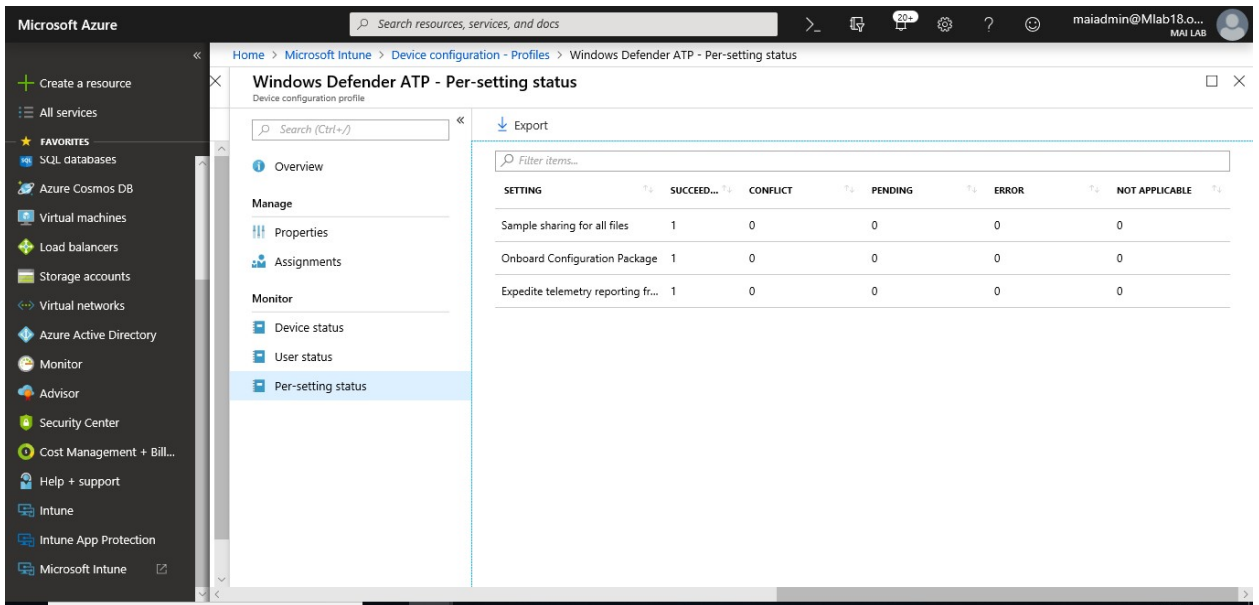


- In the app **Assignments** pane, select **Save**.

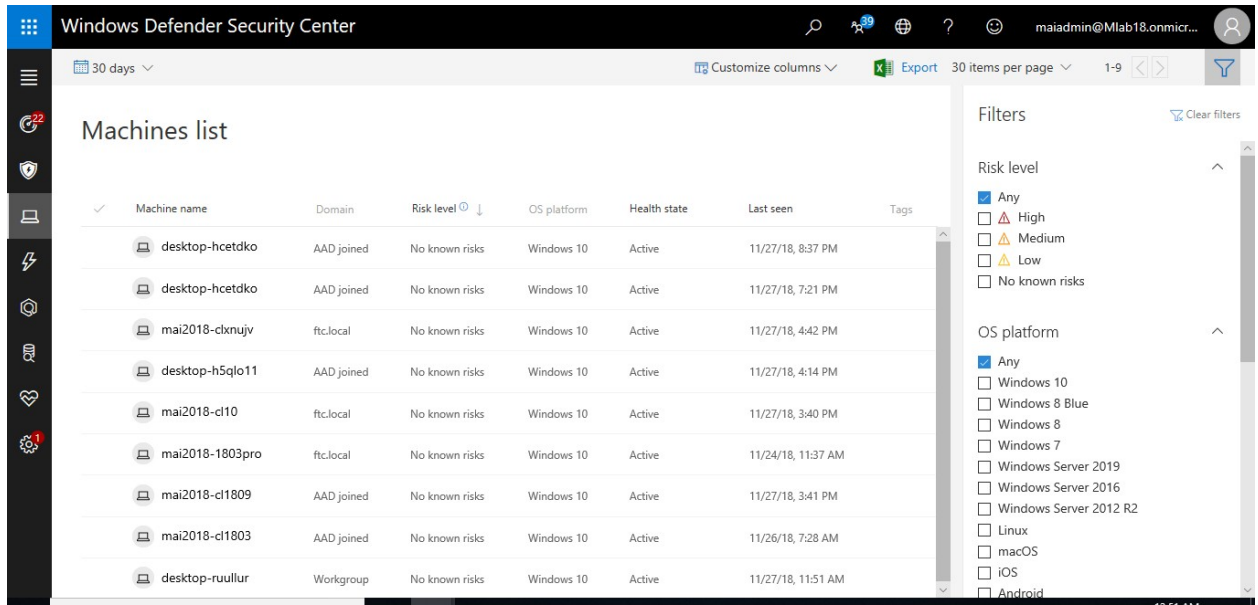
Microsoft Intune step by step on Azure portal



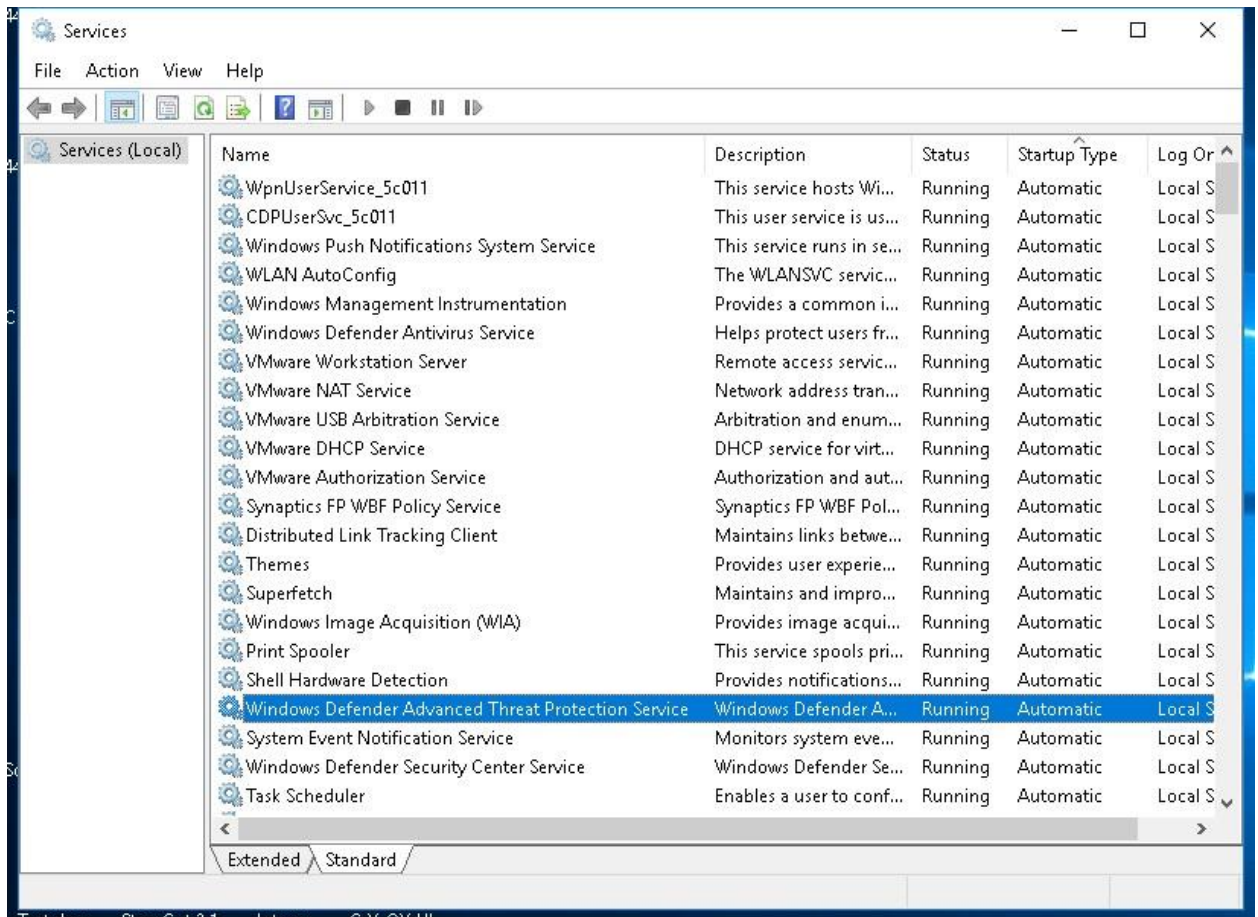
12. Once it's deployed on machine, you can check monitoring per setting status.



13. You should find PC appear on [windows defender ATP console](#).

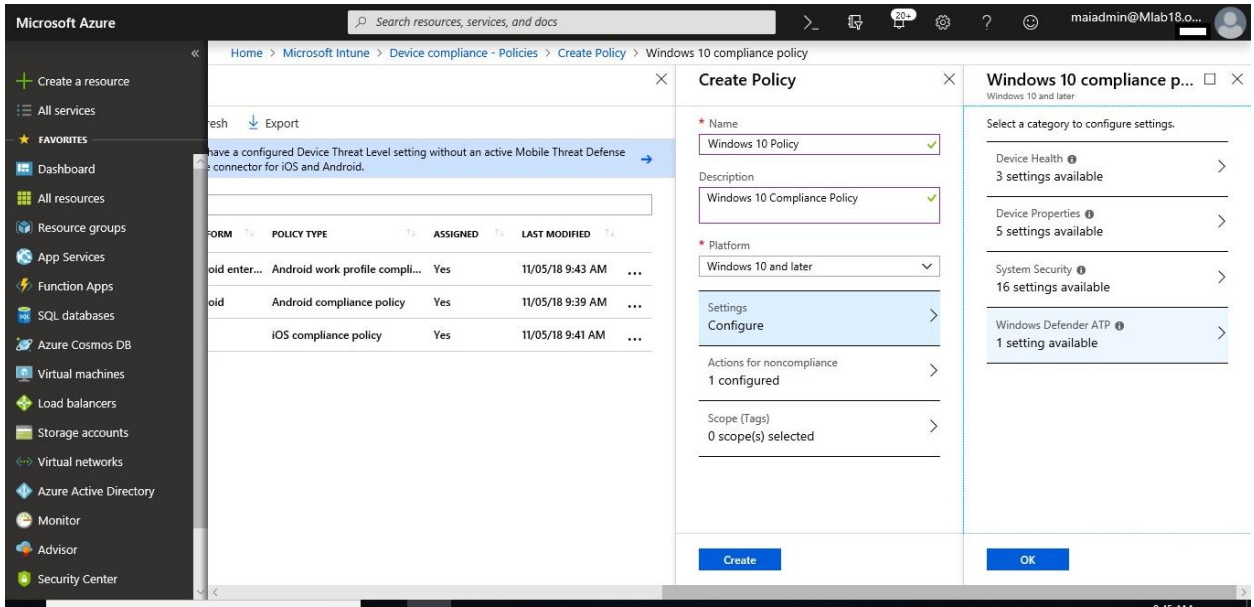


14. On Client PC, you can find on services, **Windows Defender Advanced Threat Protection** service exist & running.



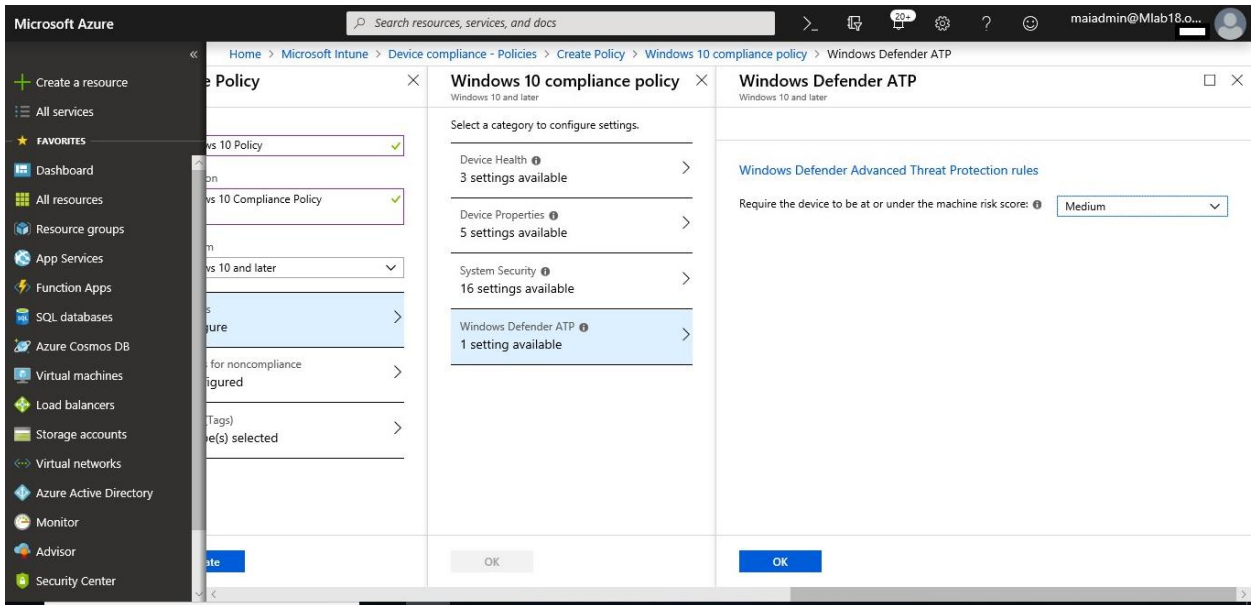
Step 4: Create the compliance policy in Intune

1. In the [Azure portal](#), select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device compliance > Policies > Create policy**.
3. Enter a **Name** and **Description**.
4. In **Platform**, select **Windows 10 and later**.

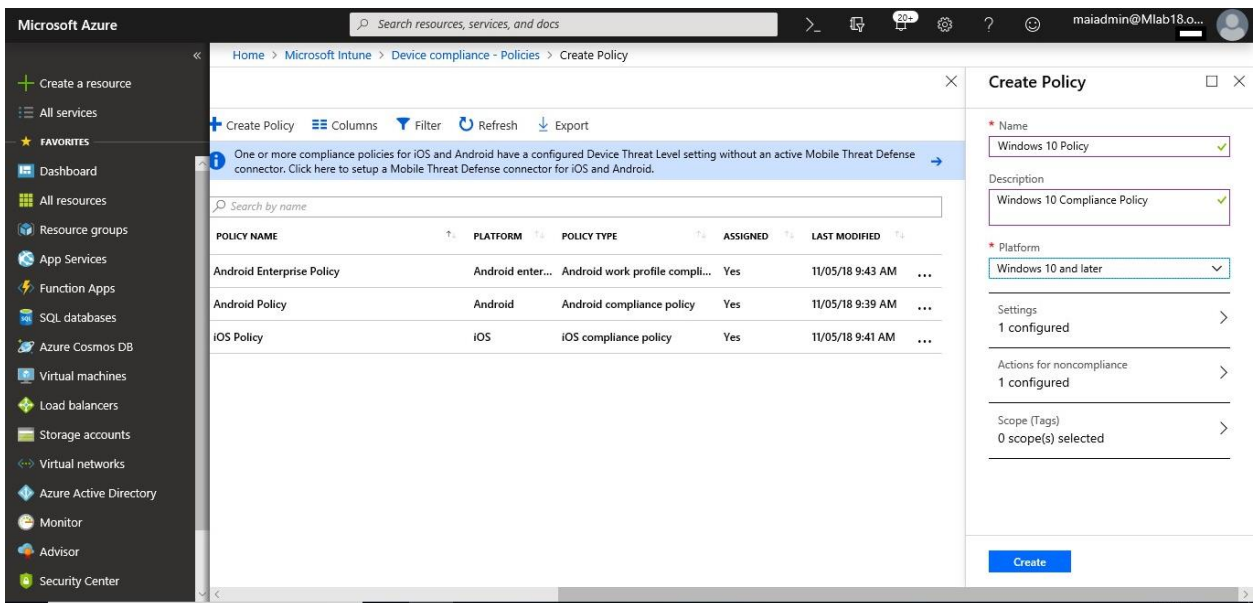


5. In the **Device Health** settings, set **Require the device to be at or under the Device Threat Level** to your preferred level:
 - **Secured:** This level is the most secure. The device cannot have any existing threats and still access company resources. If any threats are found, the device is evaluated as noncompliant.
 - **Low:** The device is compliant if only low-level threats exist. Devices with medium or high threat levels are not compliant.
 - **Medium:** The device is compliant if the threats found on the device are low or medium. If high-level threats are detected, the device is determined as noncompliant.
 - **High:** This level is the least secure and allows all threat levels. So, devices that with high, medium or low threat levels are considered compliant.

Microsoft Intune step by step on Azure portal



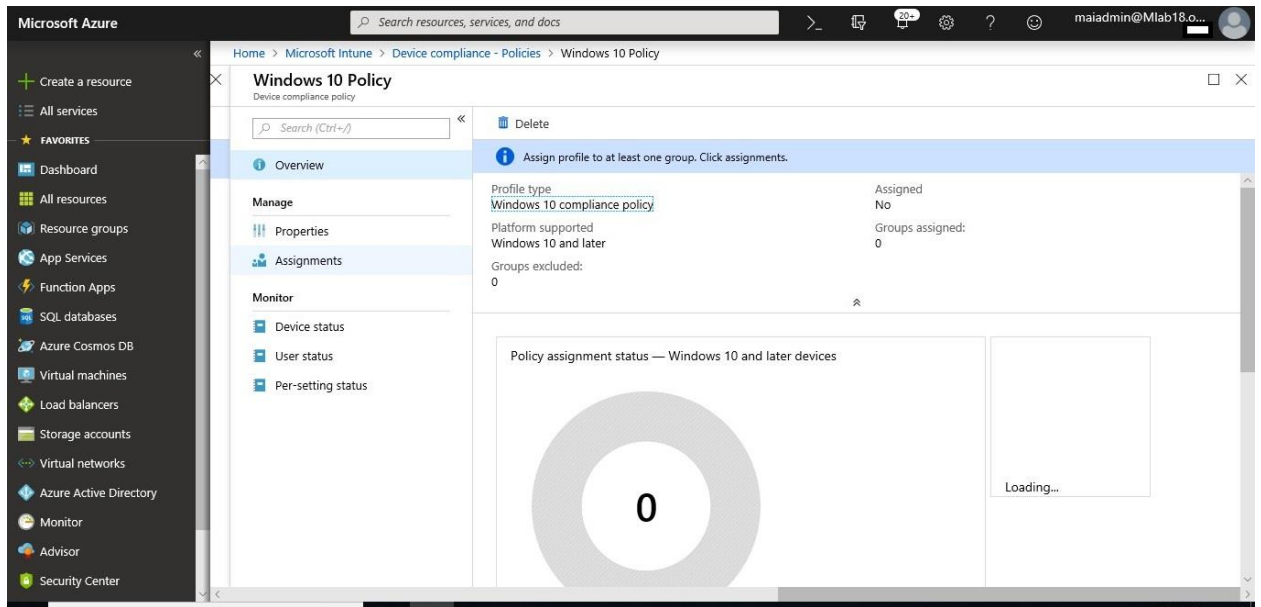
6. Select **OK** and **Create** to save your changes (and create the policy).



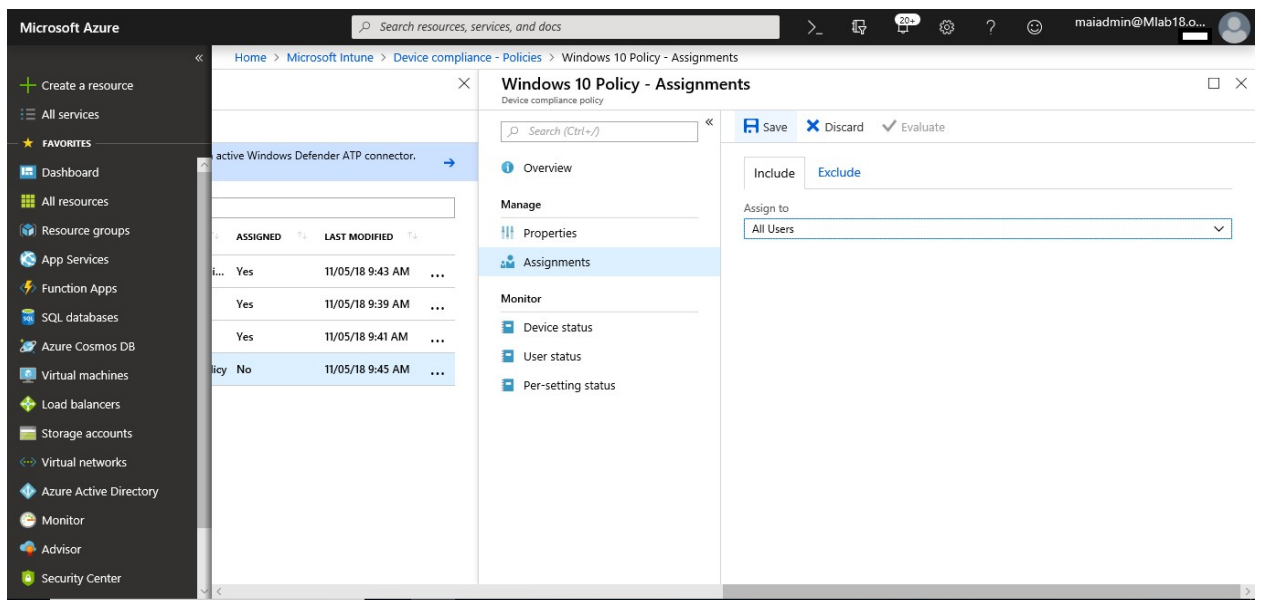
Step 5: Assign the policy

1. In the [Azure portal](#), select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device compliance** > **Policies** > select your Windows Defender ATP compliance policy.
3. Select **Assignments**.

Microsoft Intune step by step on Azure portal



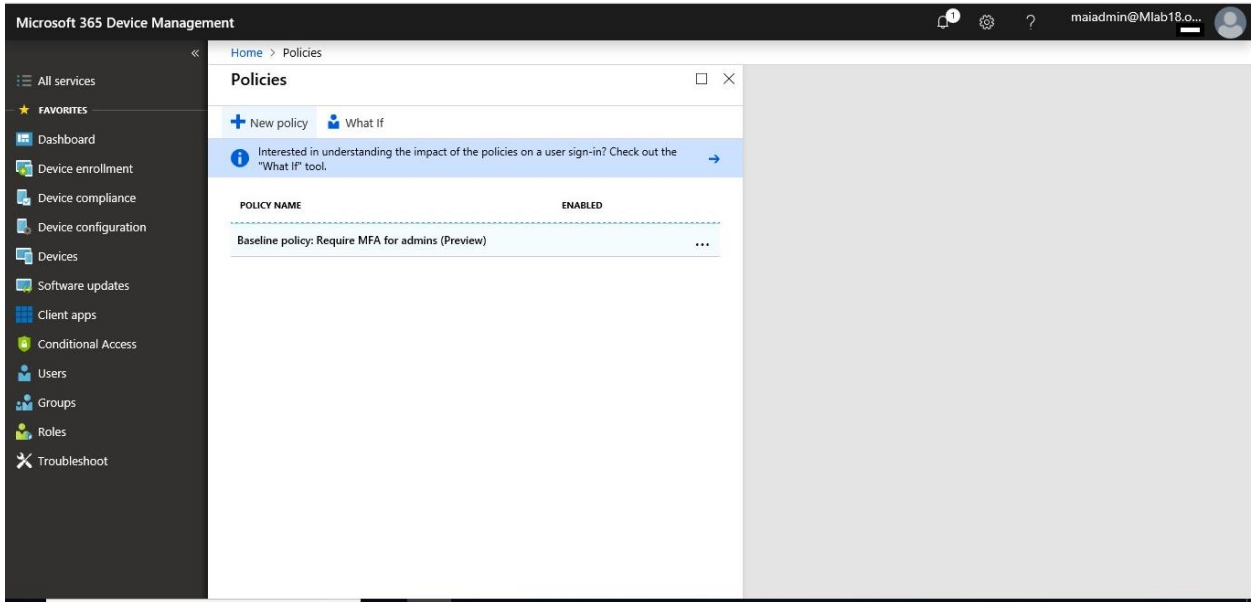
4. Include or exclude your Azure AD groups to assign them the policy.



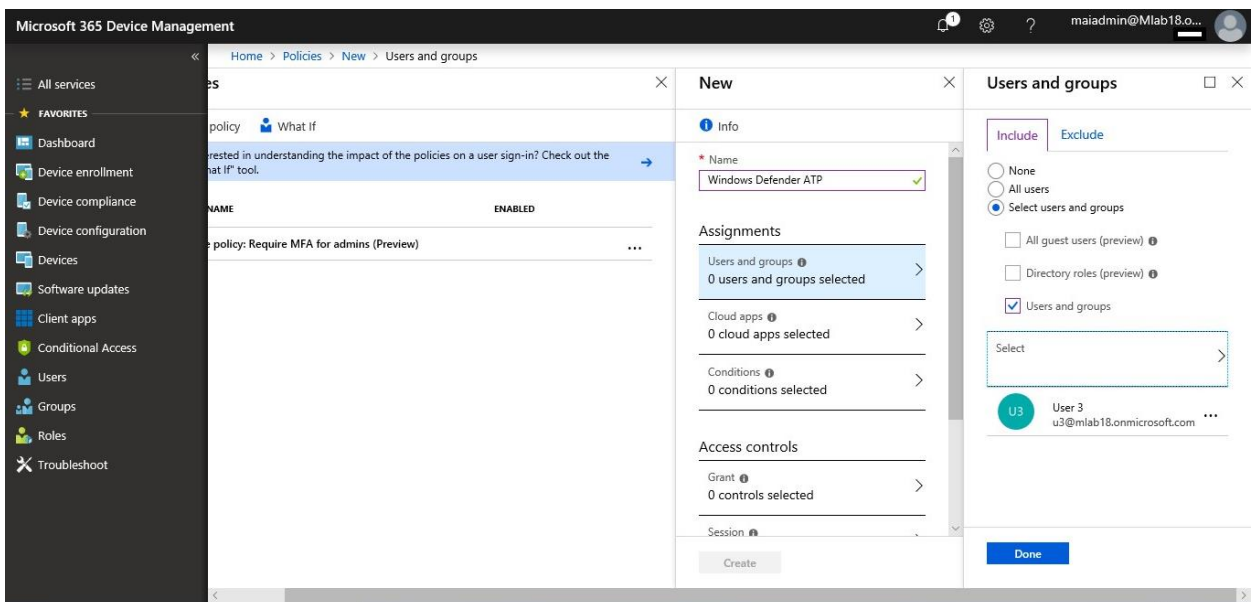
5. To deploy the policy to the groups, select **Save**. The user devices targeted by the policy are evaluated for compliance.

Step 6: Create an Azure AD conditional access policy

1. In the [Azure portal](#), open **Azure Active Directory** > **Conditional access** > **New policy**.

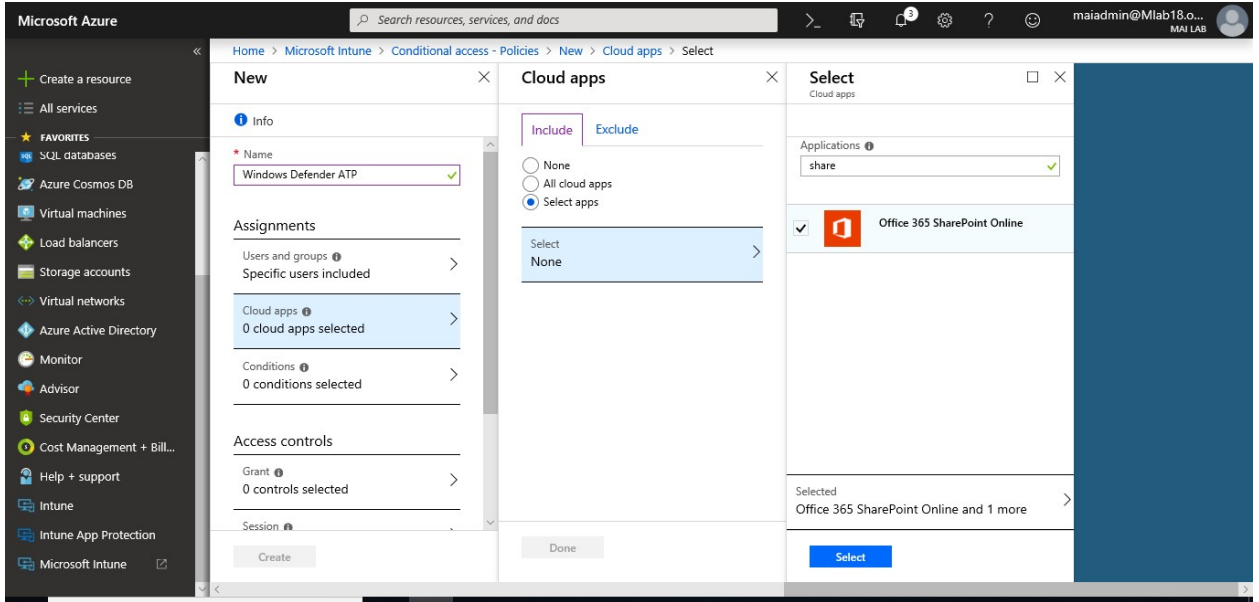


2. Enter a policy **Name** and select **Users and groups**. Use the Include or Exclude options to add your groups for the policy and select **Done**.

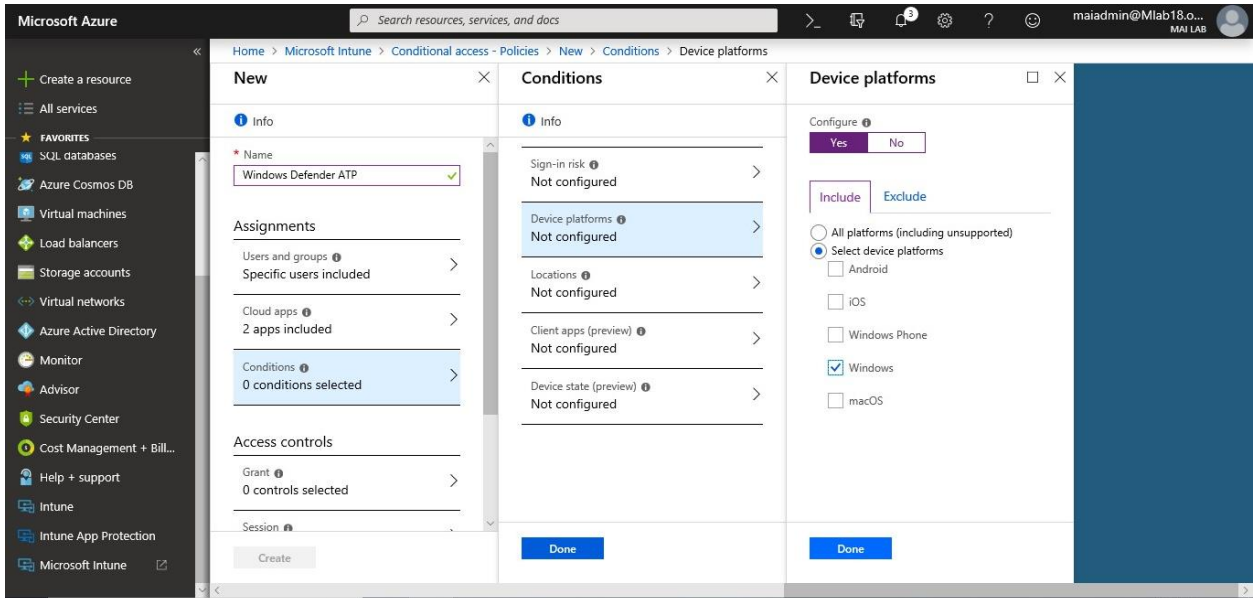


3. Select **Cloud apps** and choose which apps to protect. For example, choose **Select apps**, and select **Office 365 SharePoint Online** and **Office 365 Exchange Online**. Select **Done** to save your changes.

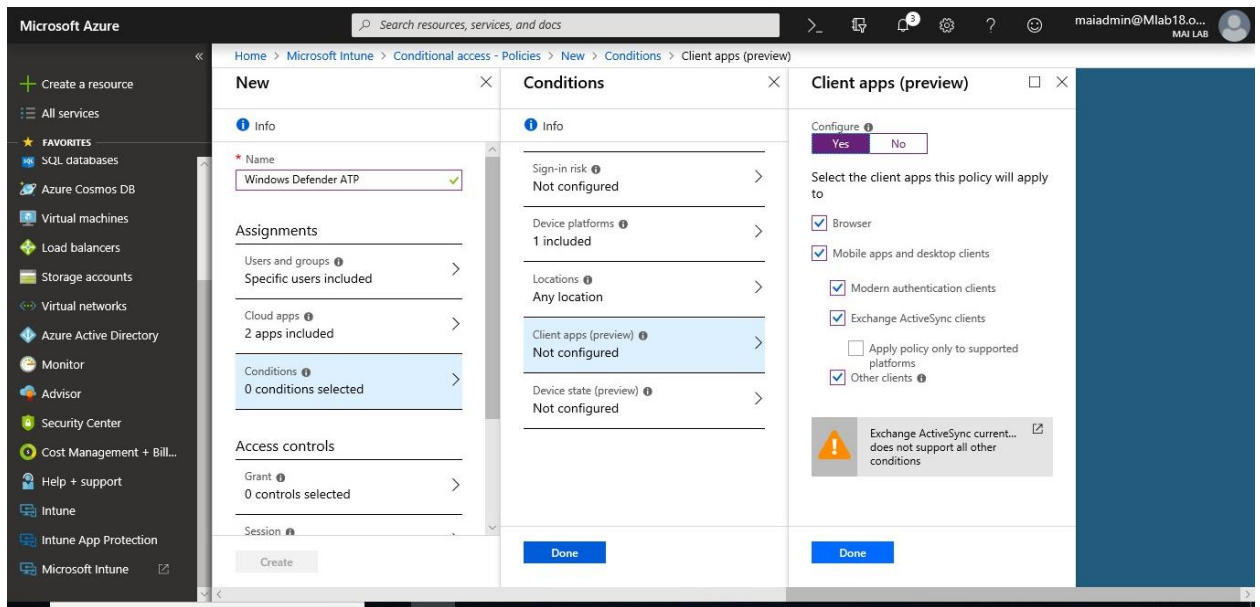
Microsoft Intune step by step on Azure portal



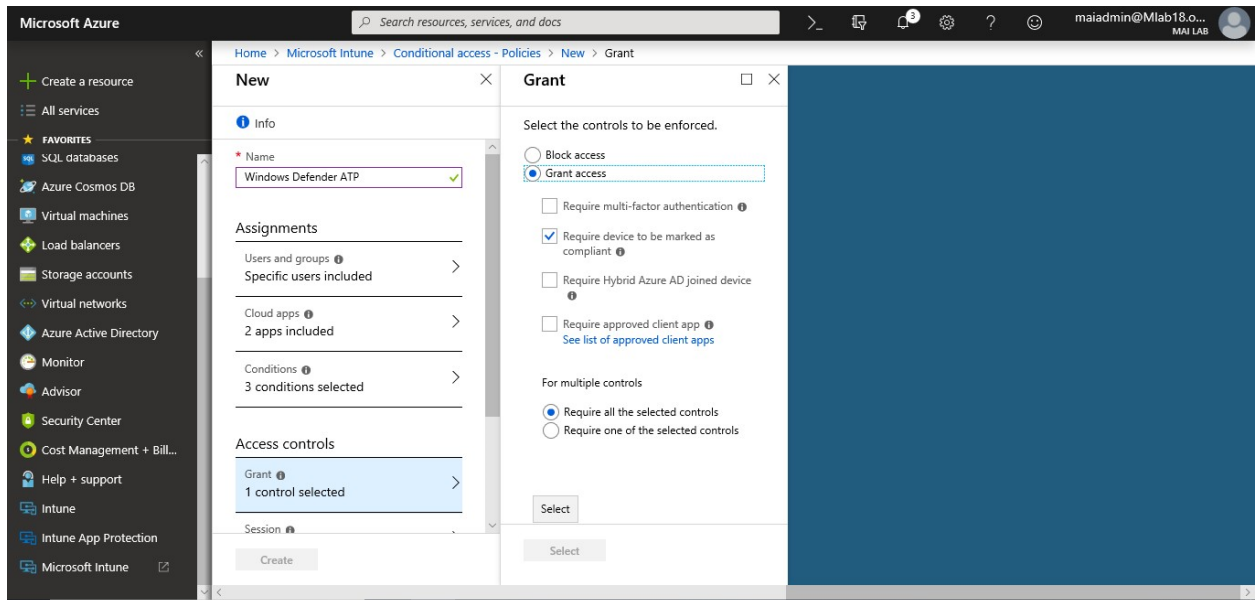
4. Select **Conditions** > **Client apps** to apply the policy to apps and browsers. For example, select **Yes**, and then enable **Browser** and **Mobile apps and desktop clients**. Select **Done** to save your changes.



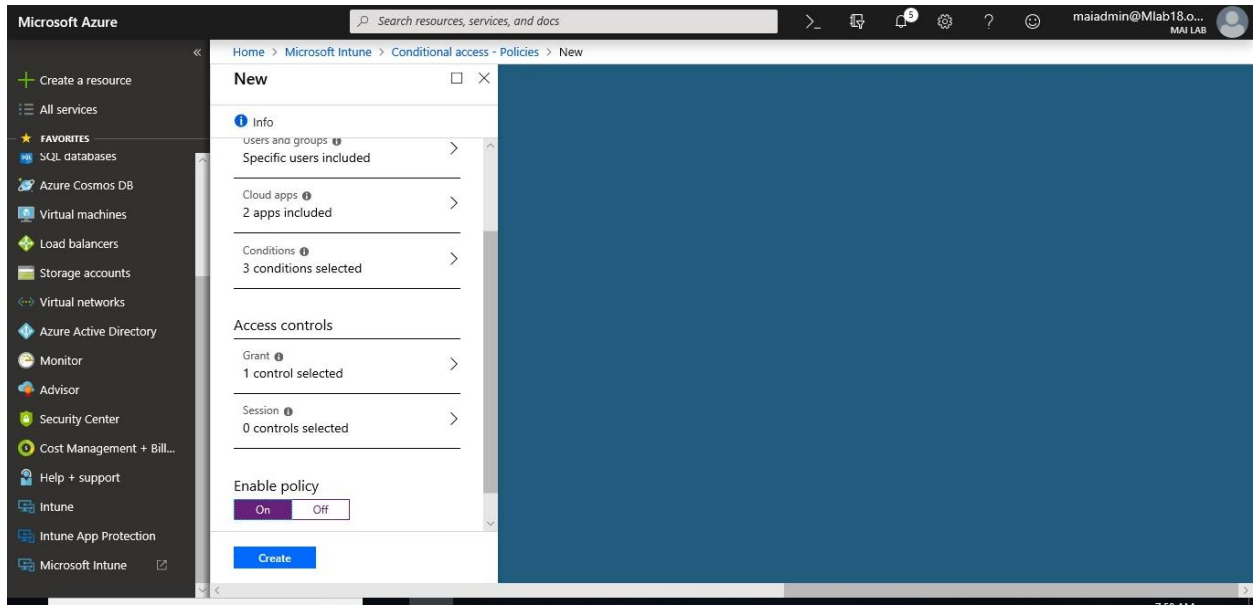
Microsoft Intune step by step on Azure portal



5. Select **Grant** to apply conditional access based on device compliance. For example, select **Grant access > Require device to be marked as compliant**. Choose **Select** to save your changes.



6. Select **Enable policy**, and then **Create** to save your changes.



Integrate between Microsoft Intune & Lookout Mobile Threat Defense

You can control mobile device access to corporate resources based on risk assessment conducted by Lookout, a Mobile Threat Defense solution integrated with Microsoft Intune. Risk is assessed based on telemetry collected from devices by the Lookout service including:

- Operating system vulnerabilities
- Malicious apps installed
- Malicious network profiles

You can configure conditional access policies based on Lookout's risk assessment enabled through Intune compliance policies. Settings let you allow or block noncompliant devices based on detected threats.

Step 1: Collect Azure AD information

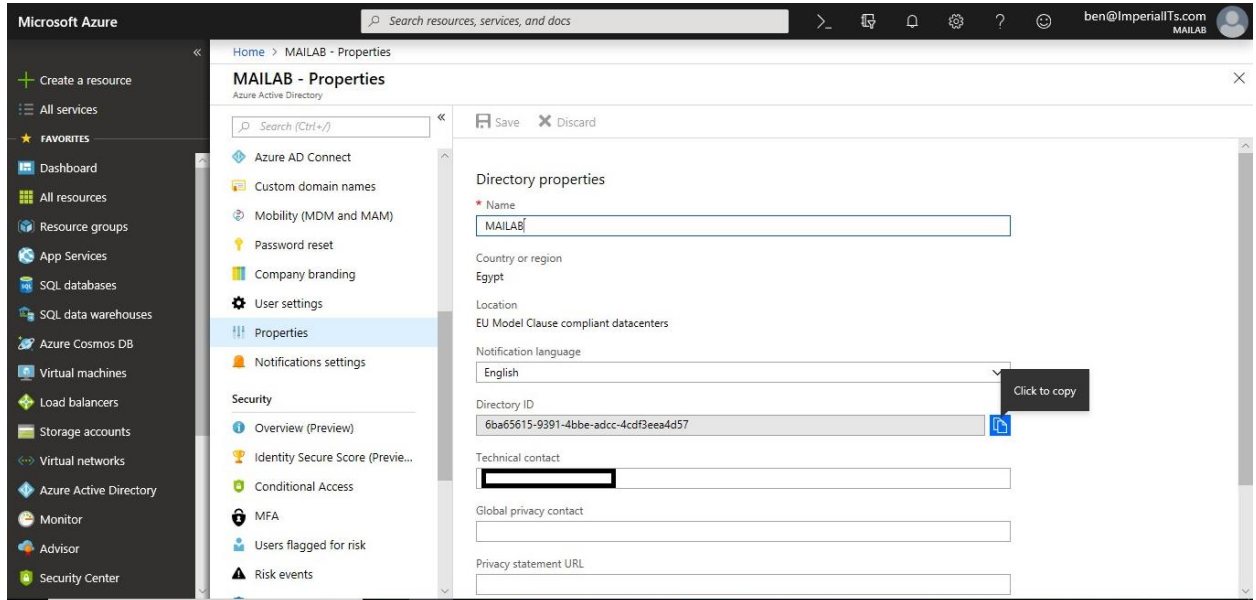
Your Lookout Mobility Endpoint Security tenant will be associated with your Azure AD subscription to integrate Lookout with Intune. To enable your Lookout Mobile Threat Defense service subscription, Lookout support (enterprisesupport@lookout.com) needs the following information:

- **Azure AD Tenant ID**
- **Azure AD Group Object ID** for full Lookout console access
- **Azure AD Group Object ID** for restricted Lookout console access (optional)

Use the following steps to gather the information you need to give to the Lookout support team.

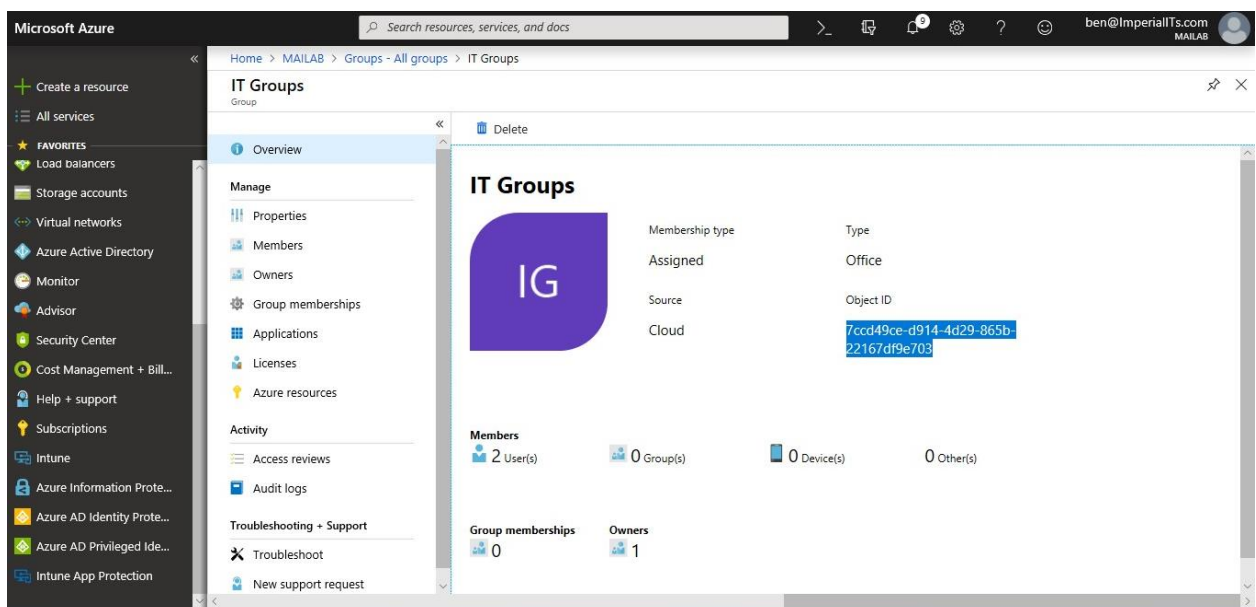
1. Sign in to the [Azure portal](#) and click **Azure Active Directory**.

2. Under **Manage**, click **Properties**. The tenant ID is shown in the **Directory ID** box.



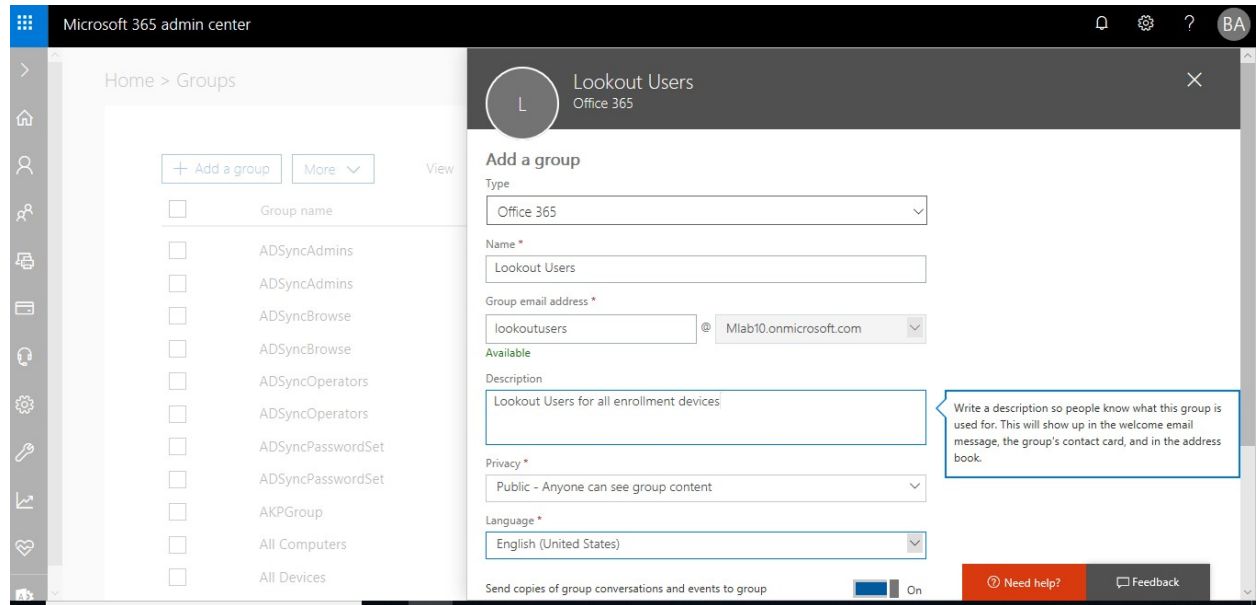
3. Find your Azure AD Group ID. The Lookout console supports 2 levels of access:
 1. **Full Access:** The Azure AD admin can create a group for users that have Full Access and optionally create a group for users that will have Restricted Access. Only users in these groups will be able to login to the **Lookout console**.
 2. **Restricted Access:** The users in this group will have no access to several configuration and enrollment-related modules of the Lookout console and have read-only access to the **Security Policy** module of the Lookout console.

Note: The **Group Object ID** is on the **Properties** page of the group in the **Azure AD management portal**.



Create the following groups, those groups can be created in your local Active Directory or directly in Azure AD. The following groups need to be created.

Group name	Purpose
Lookout Administrators	All Administrators for the Lookout Service
Lookout Restricted Administrators	Restricted Admin access to the Lookout service
Lookout Users	All users that need Lookout for Work (enrollment group)

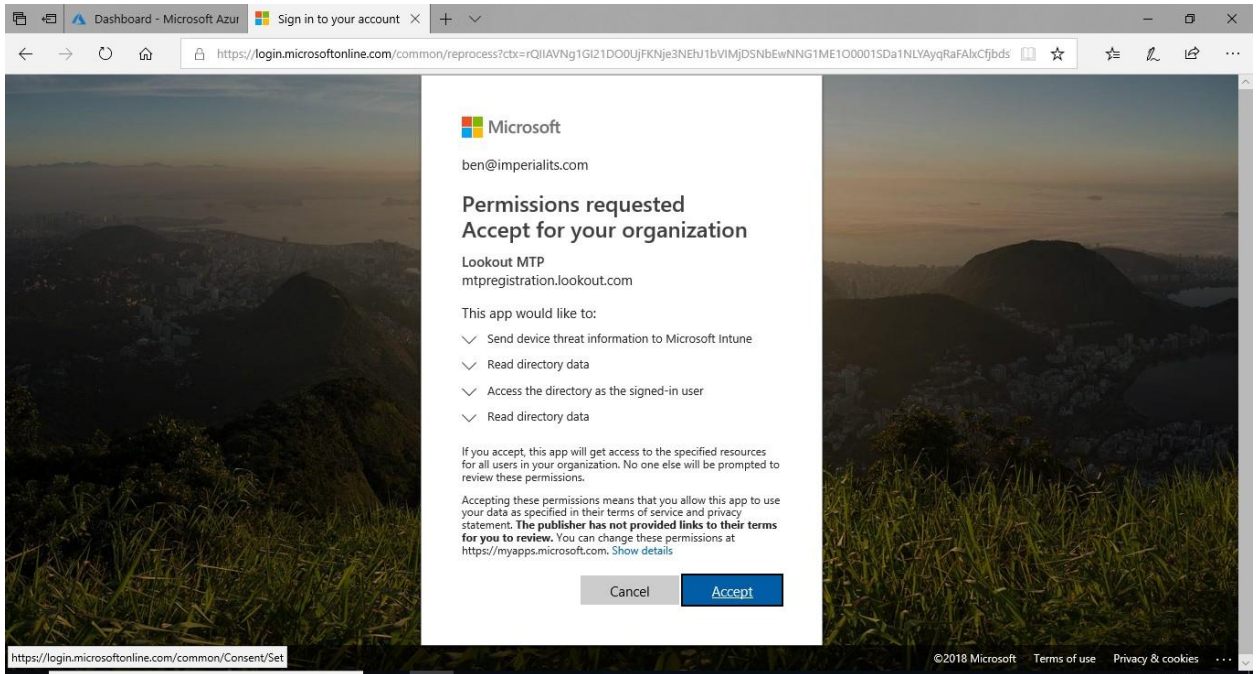


4. Once you have gathered this information, contact Lookout support (email: enterprisesupport@lookout.com). Lookout Support will work with your primary contact to onboard your subscription and create your Lookout Enterprise account, using the information that you collected.

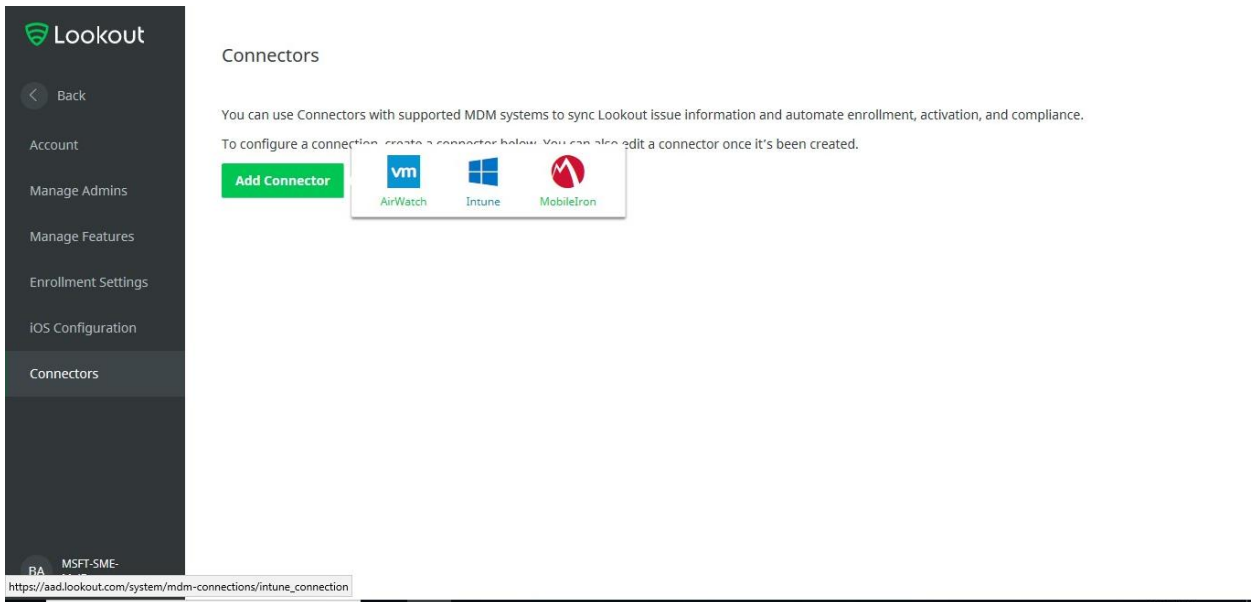
Step 2: Configure your subscription

1. After Lookout support creates your Lookout Enterprise account, an email from Lookout is sent to the primary contact for your company with a link to the login url: <https://aad.lookout.com/les?action=consent>.
2. The first login to the Lookout console must be by with a user account with the Azure AD role of Global Admin to register your Azure AD tenant. Later, sign in doesn't this level of Azure AD privilege. A consent page is displayed. Choose **Accept** to complete the registration. Once you have accepted and consented, you are redirected to the Lookout Console.

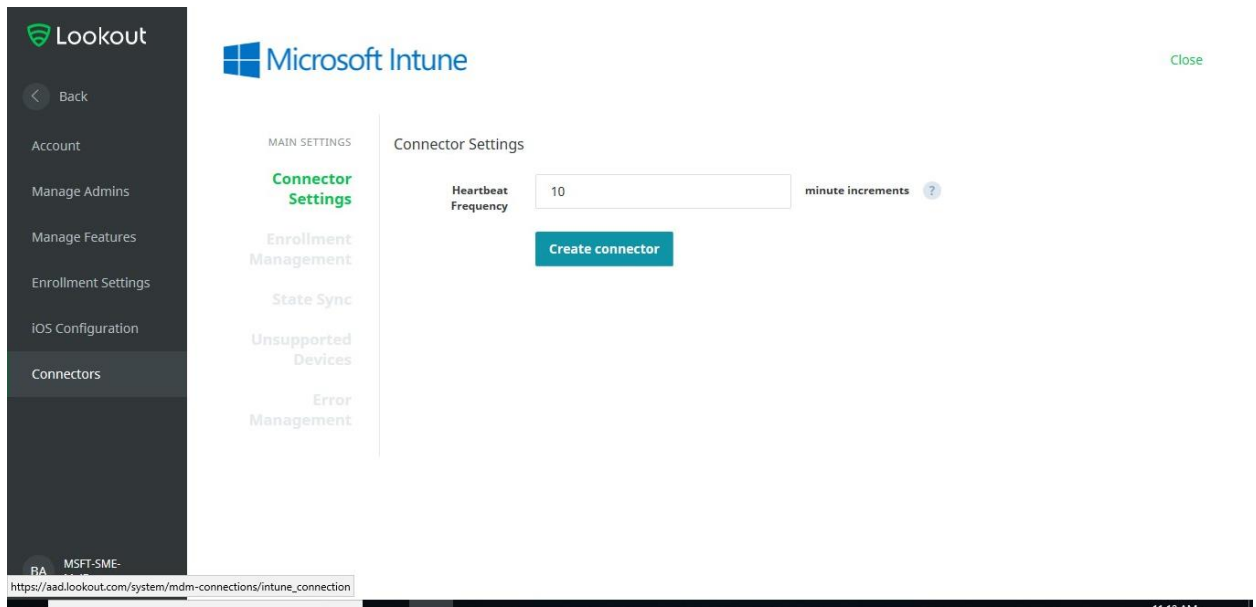
Microsoft Intune step by step on Azure portal



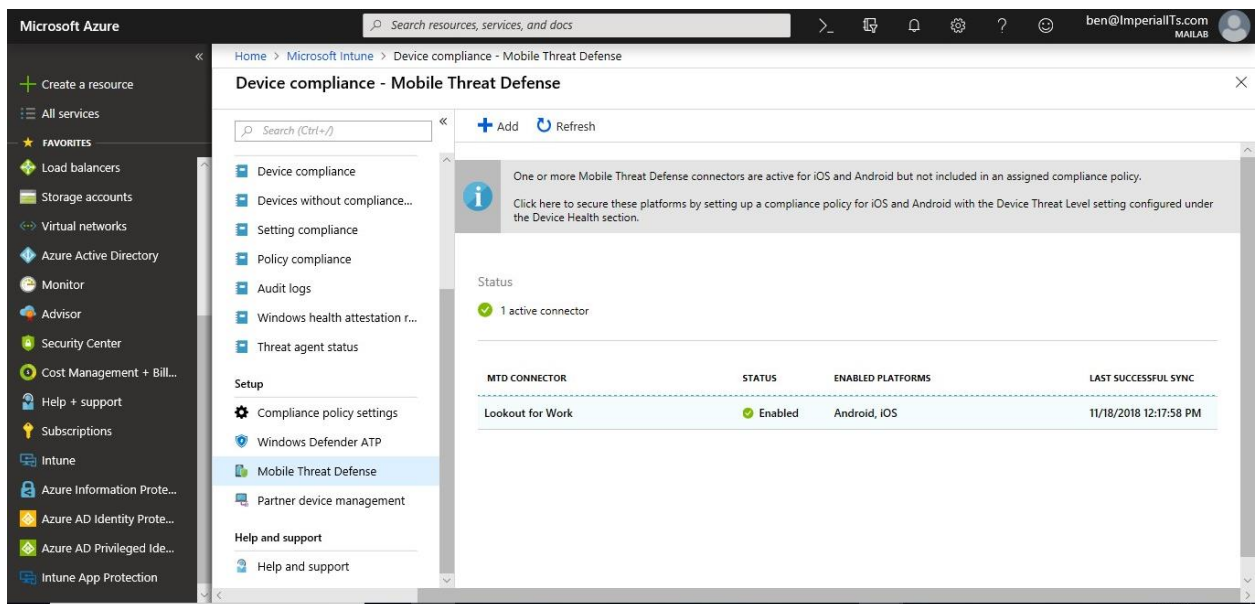
3. In the [Lookout Console](#), from the **System** module, choose the **Connectors** tab, and select **Intune**.



4. Go **Connectors > Connection Settings** and specify the **Heartbeat Frequency** in minutes.



5. If you login to [Intune in Azure Portal](#) > **Device Compliance** > **Mobile Threat Defense**, you should find that lookout connector is created.

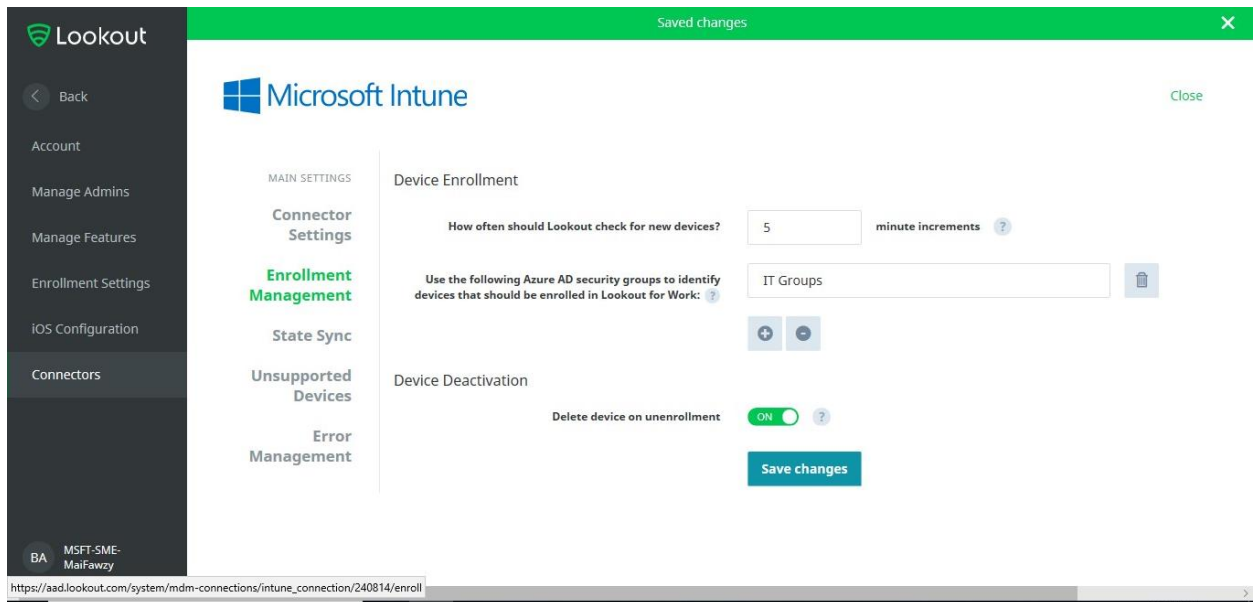


Step 3: Configure enrollment groups

1. As a best practice, create an Azure AD security group in the [Azure AD management portal](#) containing a small number of users to test Lookout integration.

Note: All the Lookout-supported, Intune-enrolled devices of users in an enrollment group in Azure AD that are identified and supported are enrolled and eligible for activation in Lookout MTD console.

2. In the [Lookout Console](#), from the **System** module, choose the **Connectors** tab, and select **Enrollment Management** to define a set of users whose devices should be enrolled with Lookout. Add the Azure AD security group **Display Name** for enrollment.



Note: The **Display Name** is case-sensitive as shown in the **Properties** of the security group in the Azure portal. As shown in the image, the **Display Name** of the security group is camel case while the title is all lower case. In the Lookout console match the **Display Name** case for the security group.

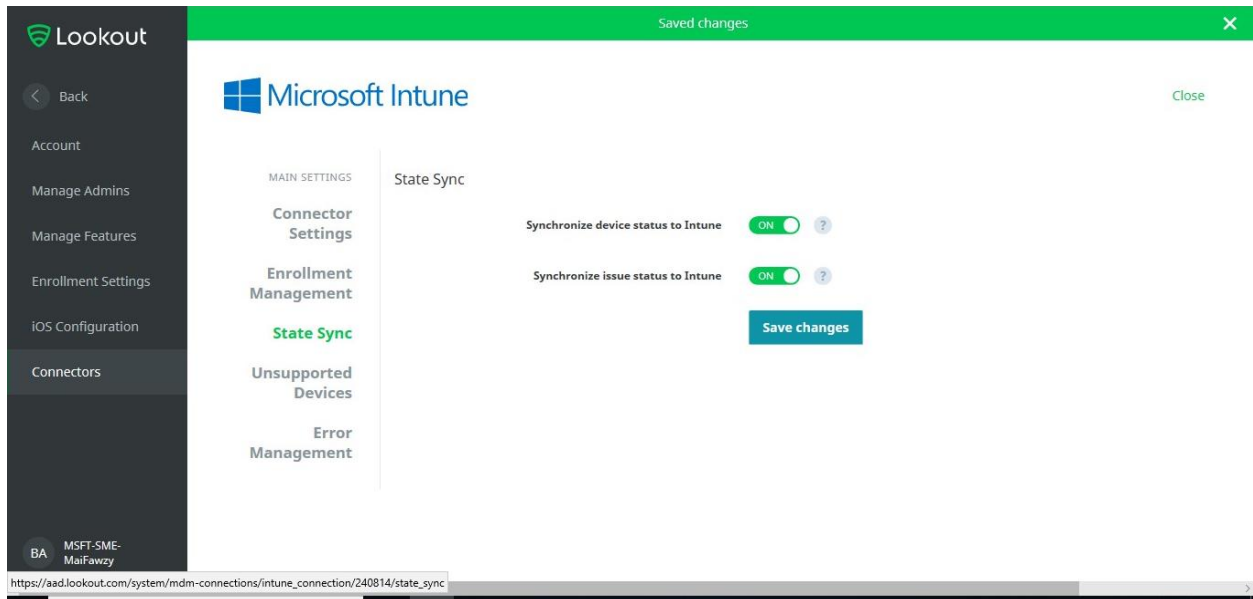
The best practice is to use the default (5 minutes) for the increment of time to check for new devices. Current limitations, **Lookout cannot validate group display names:** Ensure the **DISPLAY NAME** field in the Azure portal exactly matches the Azure AD security group. **Creating nest groups is not supported:** Azure AD security groups used in Lookout must contain users only. They cannot contain other groups.

3. Once a group is added, the next time a user opens the Lookout for Work app on their supported device, the device is activated in Lookout.
4. Once you are satisfied with your results, extend enrollment to additional user groups.

Step 4: Configure state sync

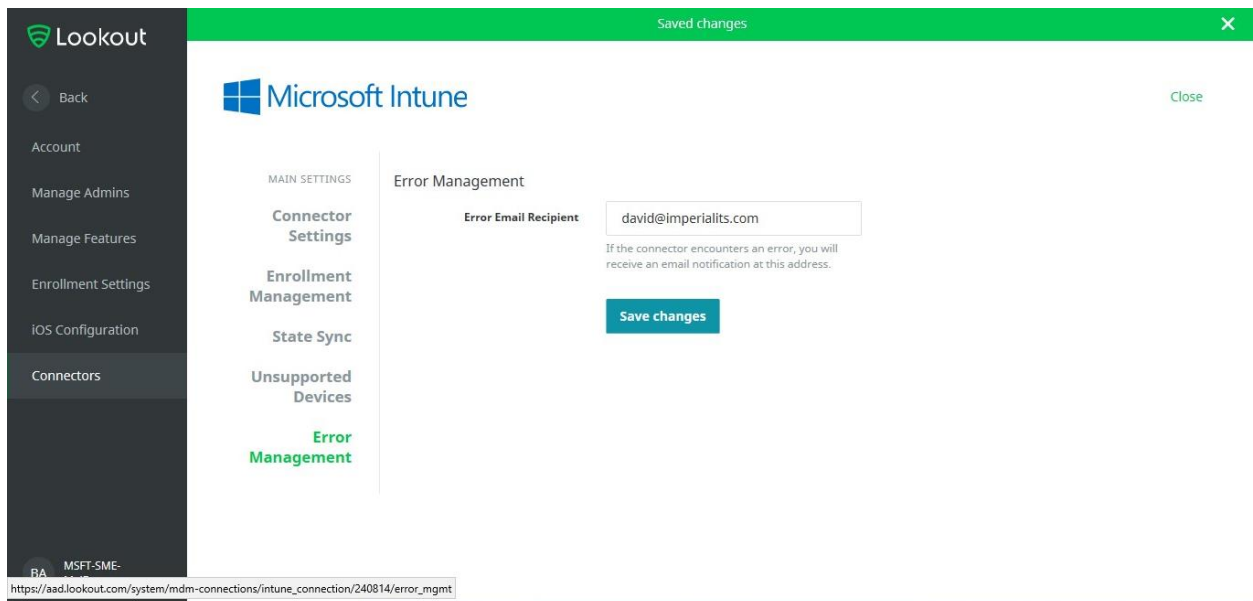
In the **State Sync** option, specify the type of data that should be sent to Intune. Both device status and threat status are required for the Lookout Intune integration to work correctly. These settings are enabled by default.

Microsoft Intune step by step on Azure portal



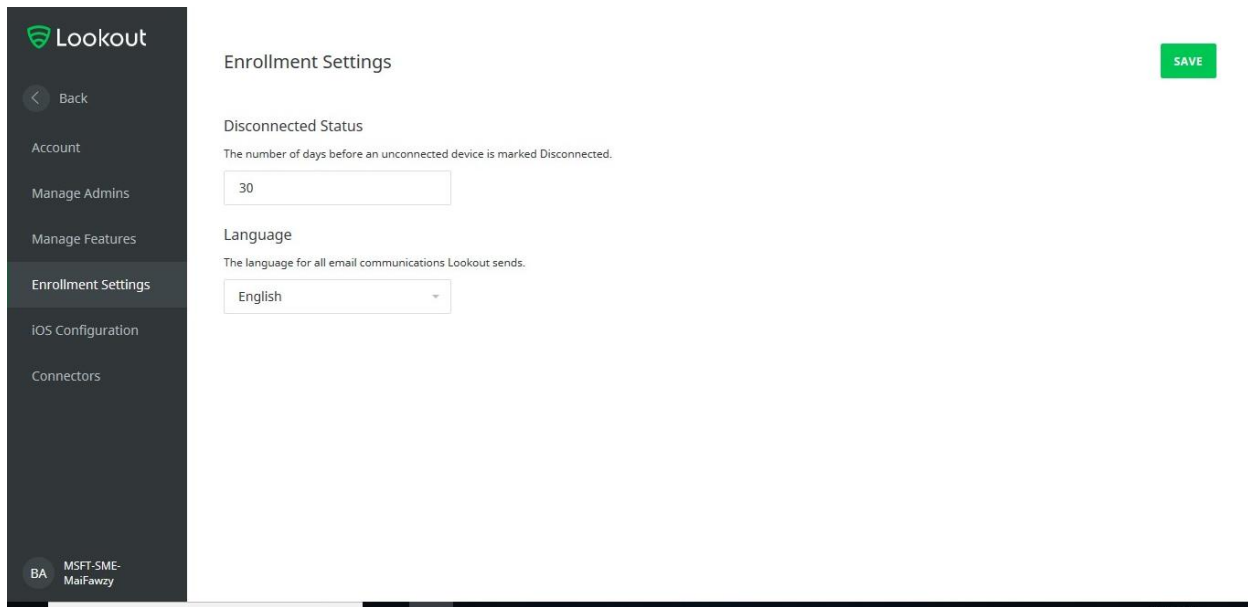
Step 5: Configure error report email recipient information

In the **Error Management** option, enter the email address that should receive the error reports.



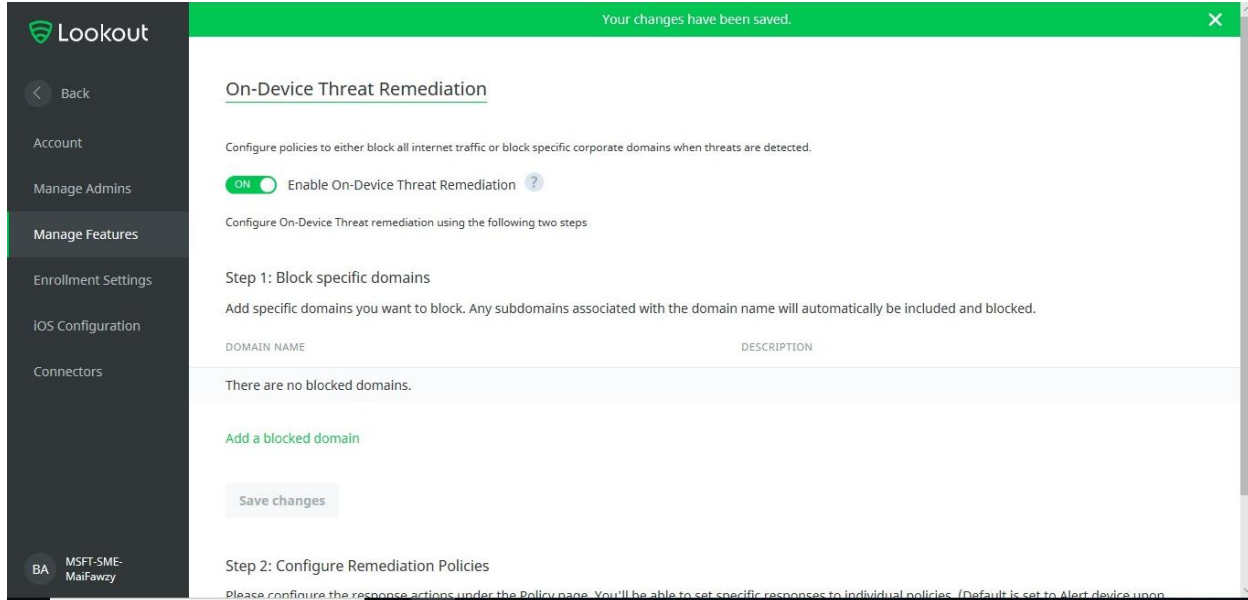
Step 6: Configure enrollment settings

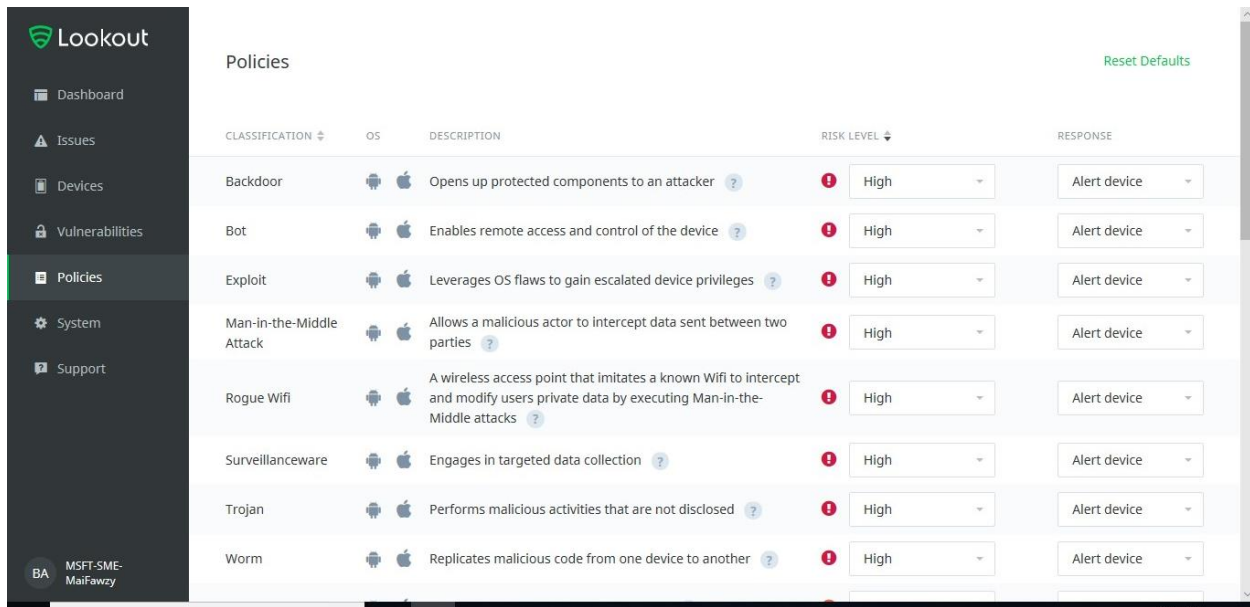
In the **System** module, on the **Connectors** page, specify the number of days before a device is considered as disconnected. Disconnected devices are considered as noncompliant and will be blocked from accessing your company applications based on the Intune conditional access policies. You can specify values between 1 and 90 days.



Step 7: Configure threat classification

Lookout Mobile Threat Defense classifies mobile threats of various types. The [Lookout threat classifications](#) have default risk levels associated with them. These can be changed at any time to suit your company requirements.





CLASSIFICATION	OS	DESCRIPTION	RISK LEVEL	RESPONSE
Backdoor	Android, iOS	Opens up protected components to an attacker ?	High	Alert device
Bot	Android, iOS	Enables remote access and control of the device ?	High	Alert device
Exploit	Android, iOS	Leverages OS flaws to gain escalated device privileges ?	High	Alert device
Man-in-the-Middle Attack	Android, iOS	Allows a malicious actor to intercept data sent between two parties ?	High	Alert device
Rogue Wifi	Android, iOS	A wireless access point that imitates a known Wifi to intercept and modify users private data by executing Man-in-the-Middle attacks ?	High	Alert device
Surveillanceware	Android, iOS	Engages in targeted data collection ?	High	Alert device
Trojan	Android, iOS	Performs malicious activities that are not disclosed ?	High	Alert device
Worm	Android, iOS	Replicates malicious code from one device to another ?	High	Alert device

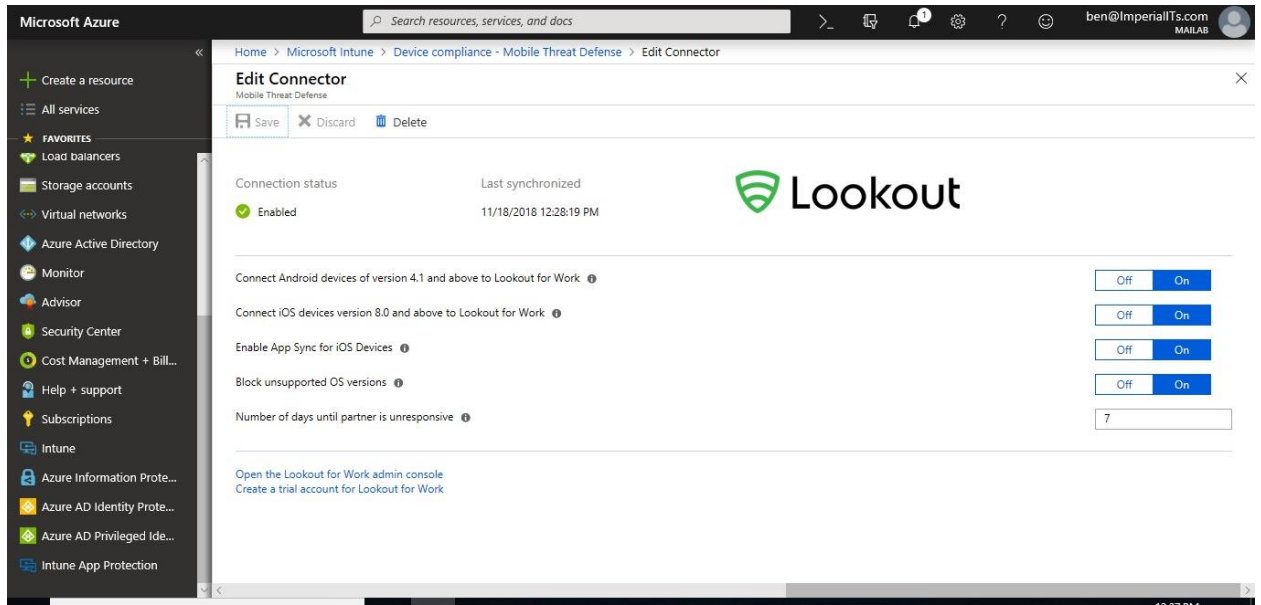
Note: Risk levels are an important aspect of Mobile Threat Defense because the Intune integration calculates device compliance according to these risk levels at runtime. The Intune administrator sets a rule in policy to identify a device as noncompliant if the device has an active threat with a minimum level of **High, Medium, or Low**. The threat classification policy in Lookout Mobile Threat Defense directly drives the device compliance calculation in Intune.

Step 8: Enable the Mobile Threat Defense connector in Intune

If you've already configured the Intune connector in the MTD partner console, you can now enable the MTD connection in Intune.

To enable the MTD connector

1. Go to the [Azure portal](#). On the **Azure Dashboard**, choose **All services** from the left menu, then type **Intune** in the text box filter.
2. Choose **Intune**; the **Intune Dashboard** opens.
3. On the **Intune Dashboard**, choose **Device compliance**, then choose **Mobile Threat Defense** under the **Setup** section.
4. On the **Mobile Threat Defense** pane, choose **Add**.
5. Choose your MTD solution as the **Mobile Threat Defense connector to setup** from the drop-down list.



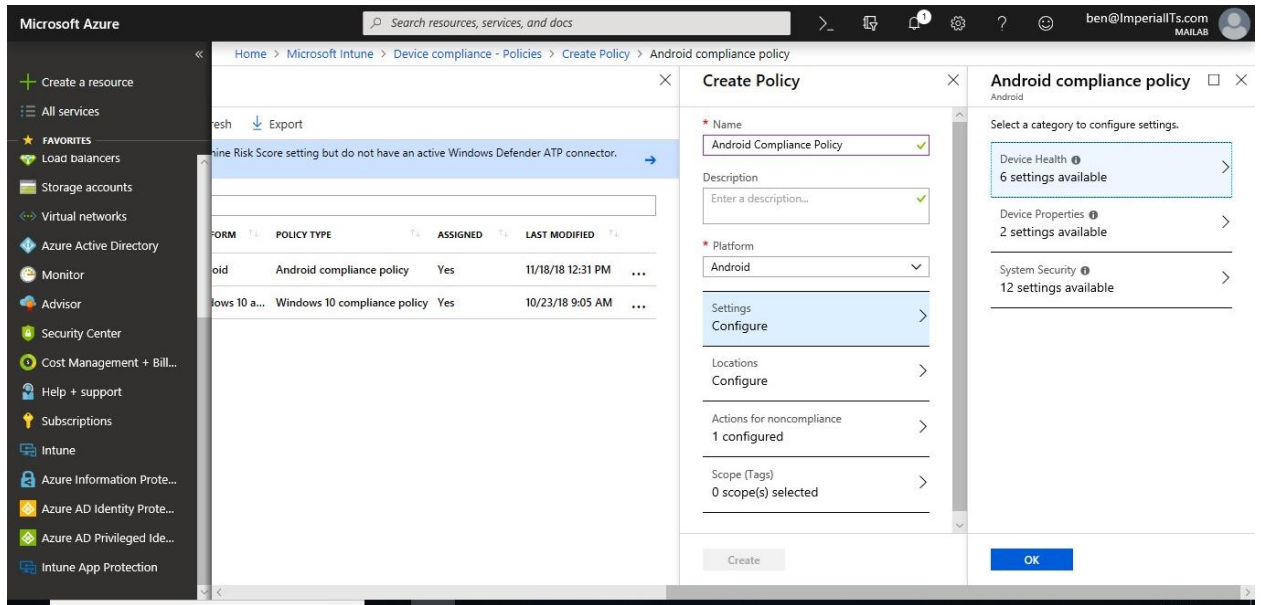
6. Enable the toggle options according to your organization's requirements. Toggle options visible will vary depending on the MTD partner.

Step 9: Create Mobile Threat Defense (MTD) device compliance policy

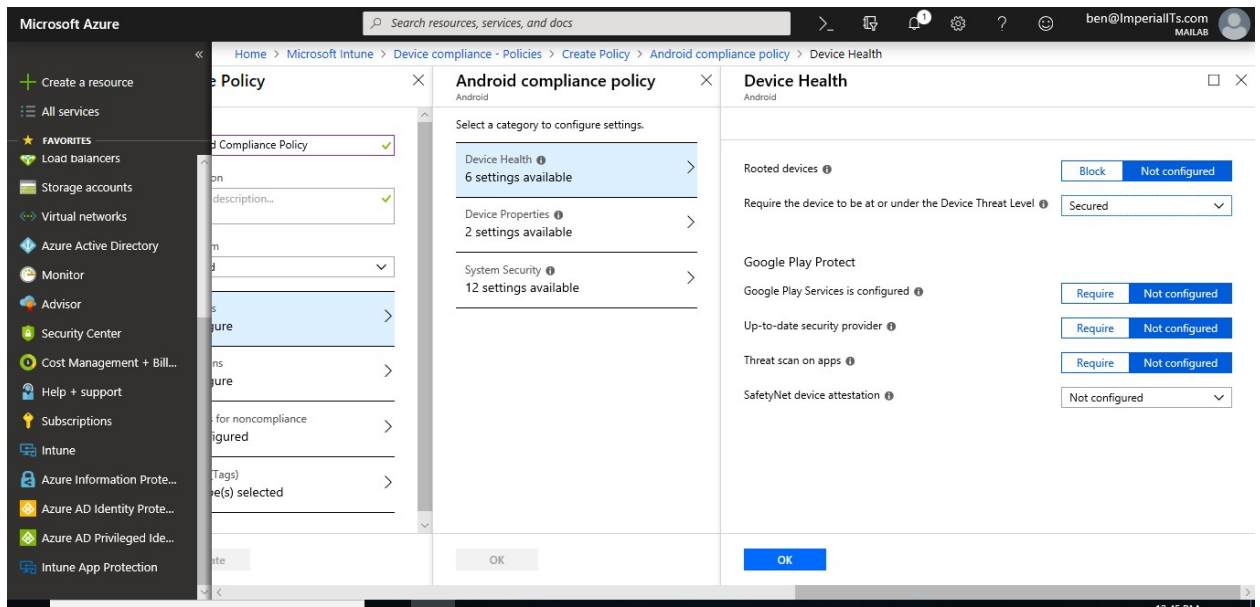
As part of the MTD setup, in the MTD partner console, you created a policy that classifies various threats as high, medium, and low. You now need to set the Mobile Threat Defense level in the Intune device compliance policy.

To create an MTD device compliance policy

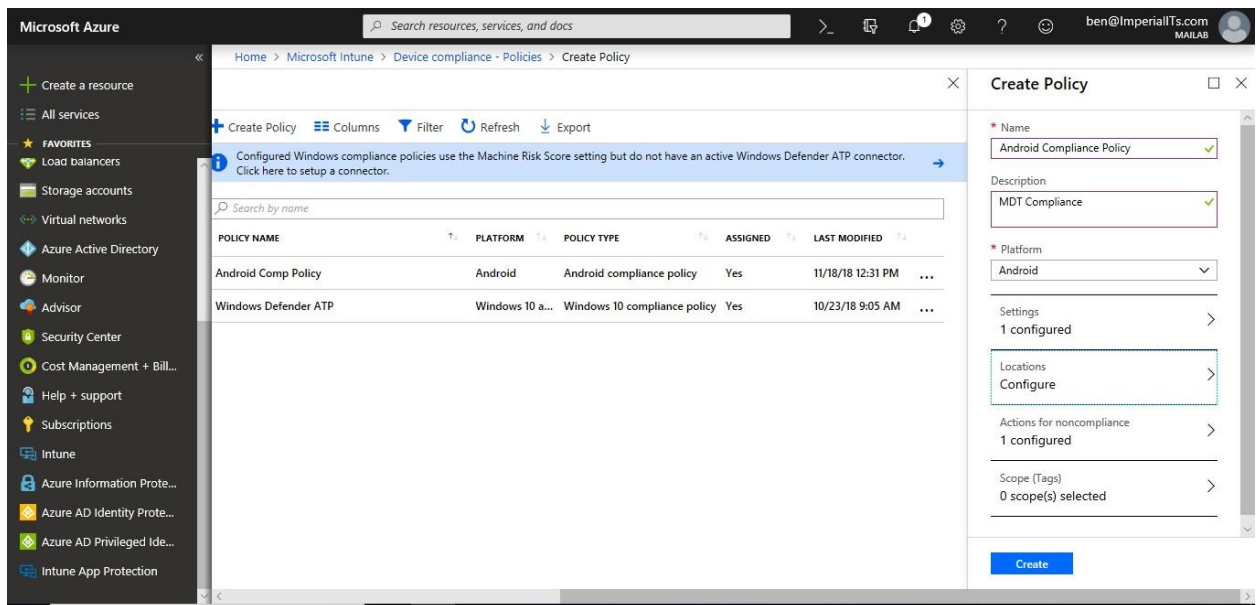
1. Go to the [Azure portal](#), and sign in with your Intune credentials.
2. On the **Azure Dashboard**, choose **All services** from the left menu, then type **Intune** in the text box filter.
3. Choose **Intune**, the **Intune Dashboard** opens.
4. On the **Intune Dashboard**, choose **Device compliance**, then choose **Policies** under the **Manage** section.
5. Choose **Create policy**, enter the device compliance **Name**, **Description**, select the **Platform**, then choose **Configure** under the **Settings** section.



6. On the **compliance policy** pane, choose **Device Health**.
7. On the **Device Health** pane, choose the Mobile Threat Level from the drop-down list under the **Require the device to be at or under the Device Threat Level**.
 - a. **Secured**: This level is the most secure. The device cannot have any threats present and still access company resources. If any threats are found, the device is evaluated as noncompliant.
 - b. **Low**: The device is compliant if only low-level threats are present. Anything higher puts the device in a noncompliant status.
 - c. **Medium**: The device is compliant if the threats found on the device are low or medium level. If high-level threats are detected, the device is determined as noncompliant.
 - d. **High**: This level is the least secure. This allows all threat levels and uses Mobile Threat Defense for reporting purposes only. Devices are required to have the MTD app activated with this setting.



8. Click **OK** twice, then choose **Create**.

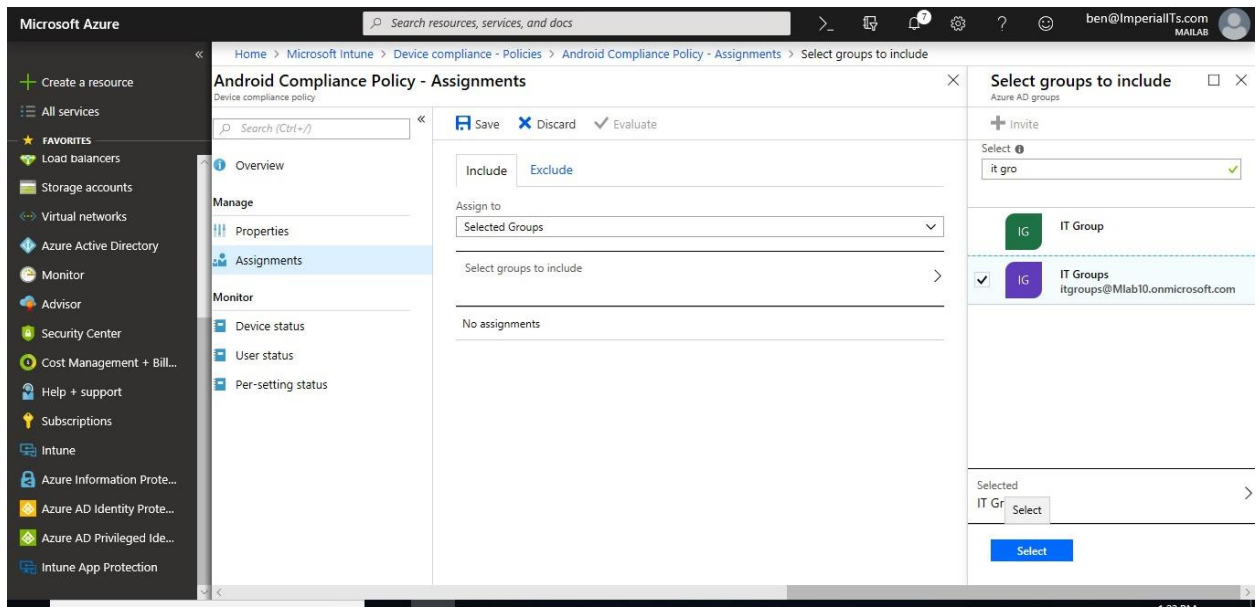


To assign an MTD device compliance policy

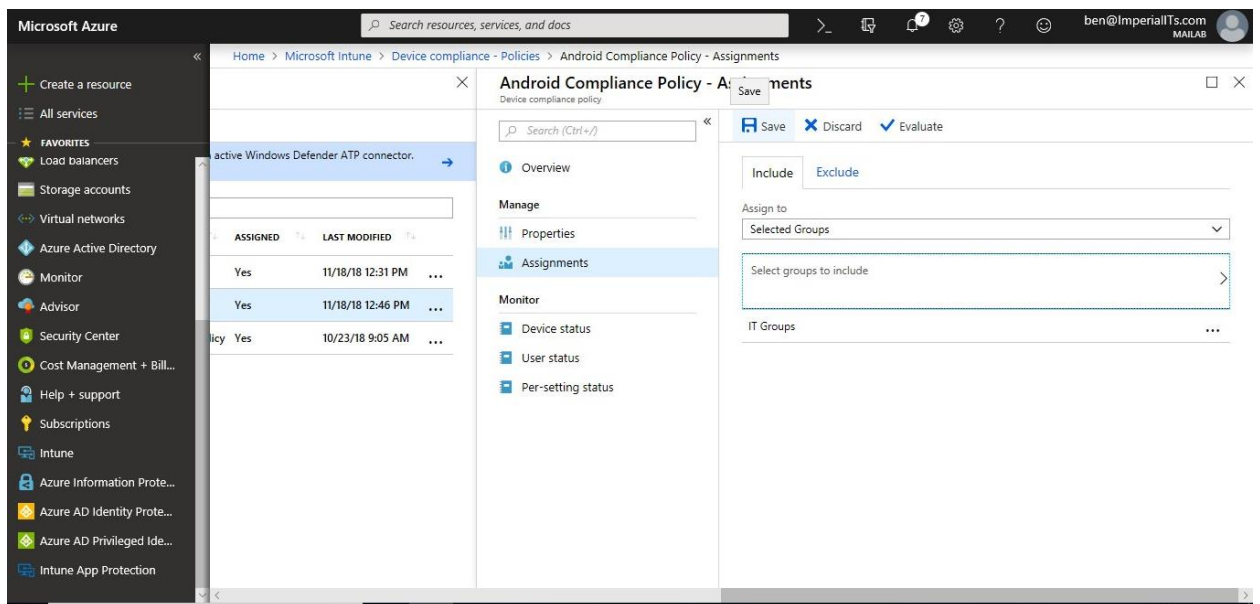
To assign a device compliance policy to users, choose a policy that you have previously configured. Existing policies can be found in the **Device compliance – policies** pane.

1. Choose the policy you want to assign to users and choose **Assignments**. This action opens the pane where you can select **Azure Active Directory security groups** and assign them to the policy.

Microsoft Intune step by step on Azure portal



2. Choose **Select groups to include** to open the pane that displays the Azure AD security groups. Choosing **Select** deploys the policy to users.

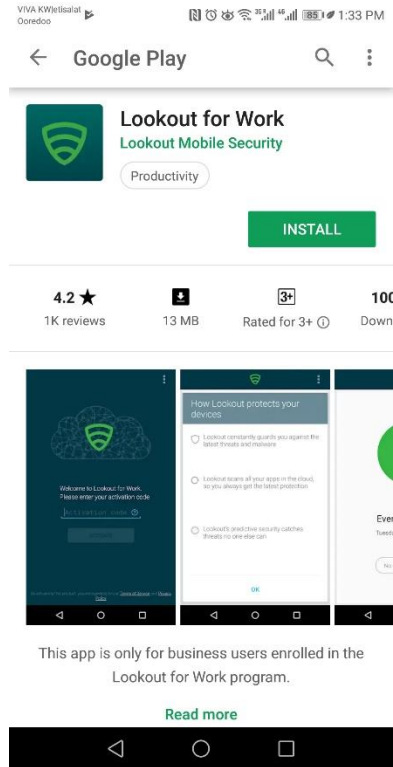


Note: You have applied the policy to users. The devices used by the users who are targeted by the policy are evaluated for compliance.

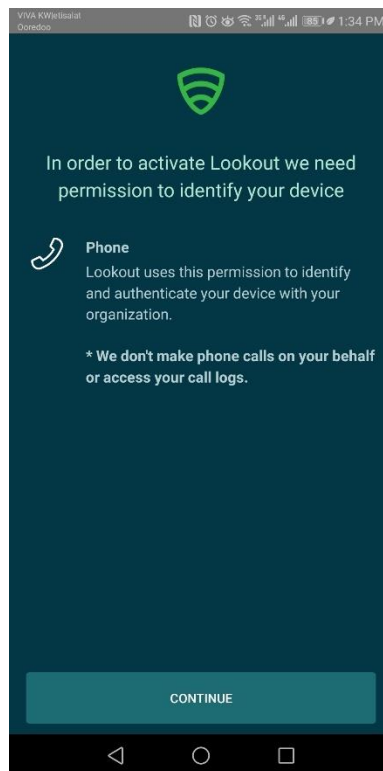
Once you applied Compliance policy, on Mobile device will ask you to install & configure lookout. To configure lookout on your Mobile device, you will need to follow below steps:

1. Drag down from the top of the screen to open the Notifications bar, and then tap **Required application – Install Lookout for Work from Play Store.**

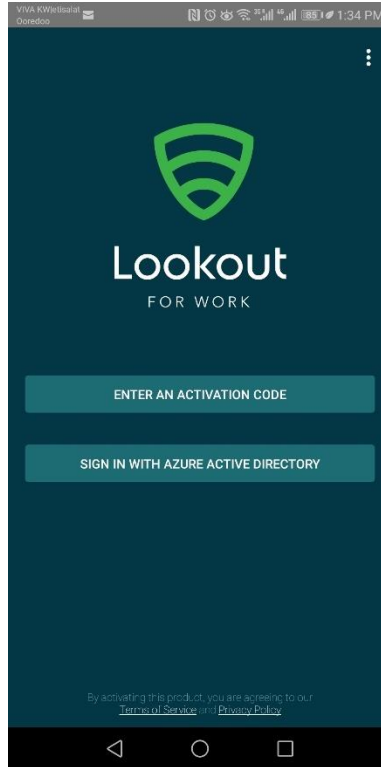
Microsoft Intune step by step on Azure portal



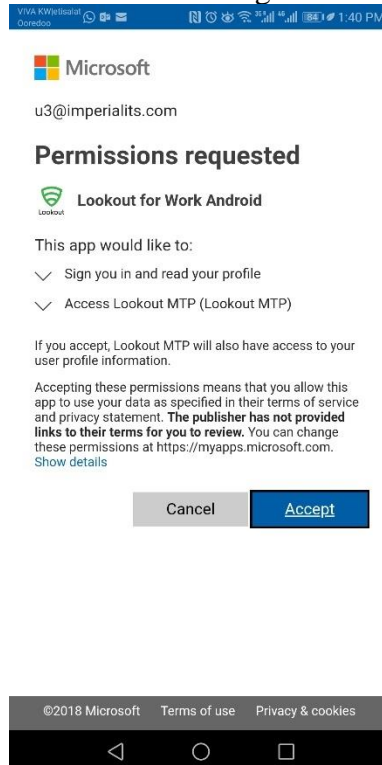
-
2. You are taken to the Lookout for Work installation page in the Play Store. Install Lookout for Work, and then tap **ACCEPT** to let Lookout for Work access your device.
3. Click **Continue**.



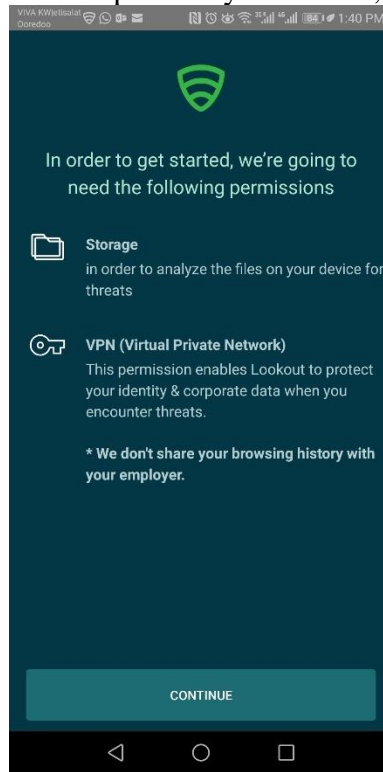
-
-
-
4. Tap **Sign in with Azure Active Directory**, and then enter the account that you use to access work or school email and files.



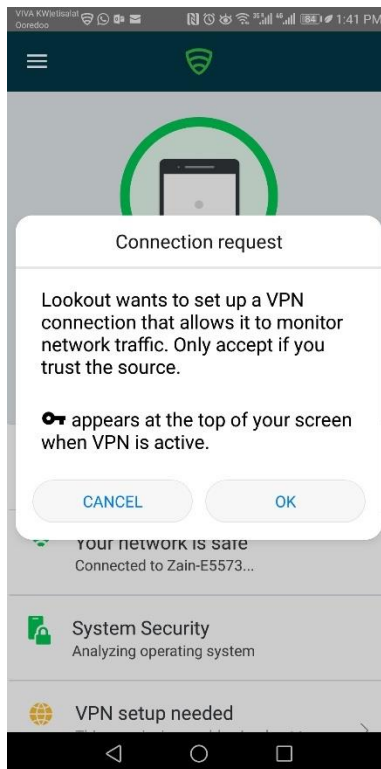
5. Select the account that you use to access work or school email and files, and then tap **ADD ACCOUNT**.
6. Tap **Accept** to give Lookout for Work permission to sign you in and read your profile. A screen shows that Lookout for Work is connecting to the Lookout Security Cloud.



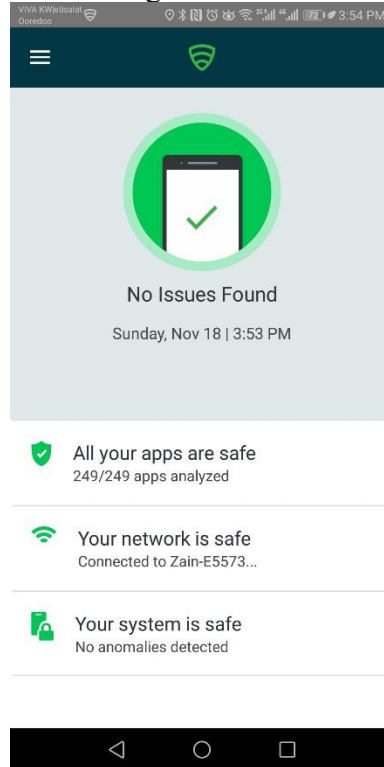
7. Review the items about how Lookout protects your device, and then tap **Continue**.



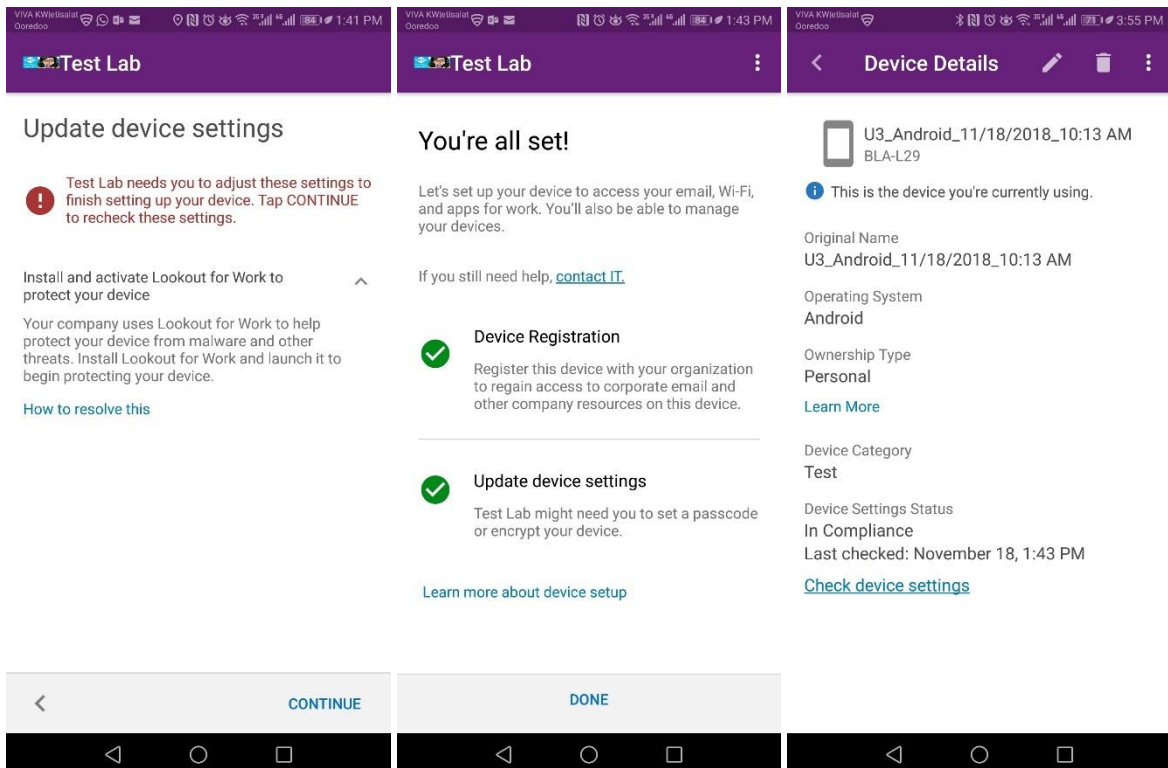
8. When you see the following screen, Lookout is now set up and connected.



9. Lookout for Work starts to check right away for security threats on your device. If no threats are found, you'll see the following screen.

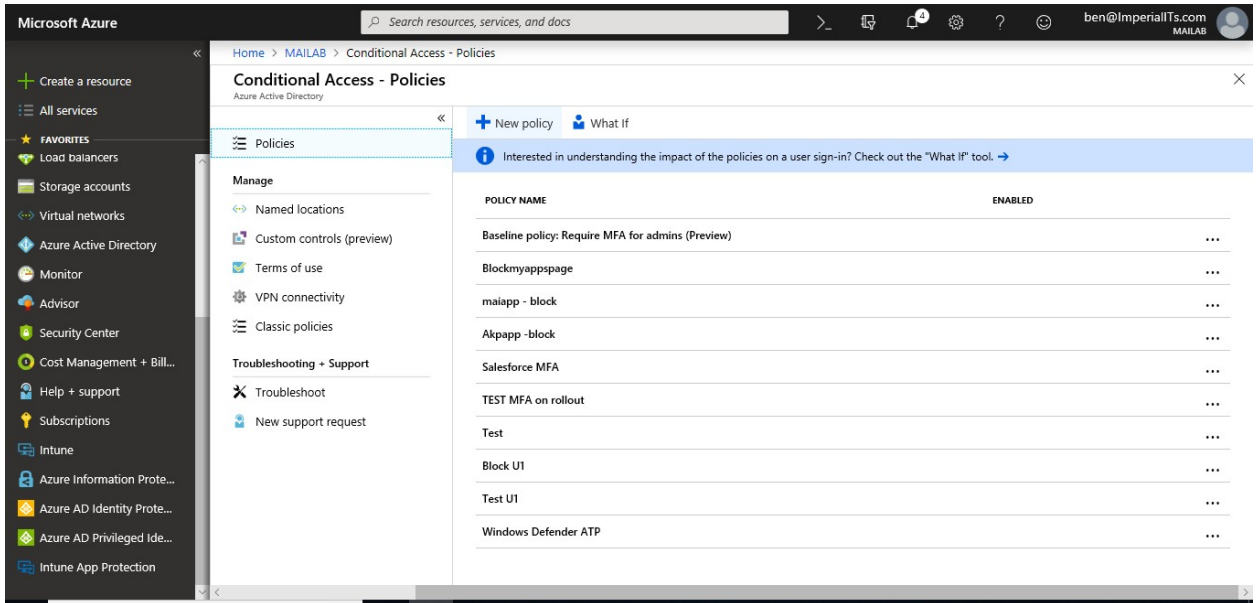


10. The Device Details screen in the Company Portal shows that you are now in compliance with your company's security requirements.

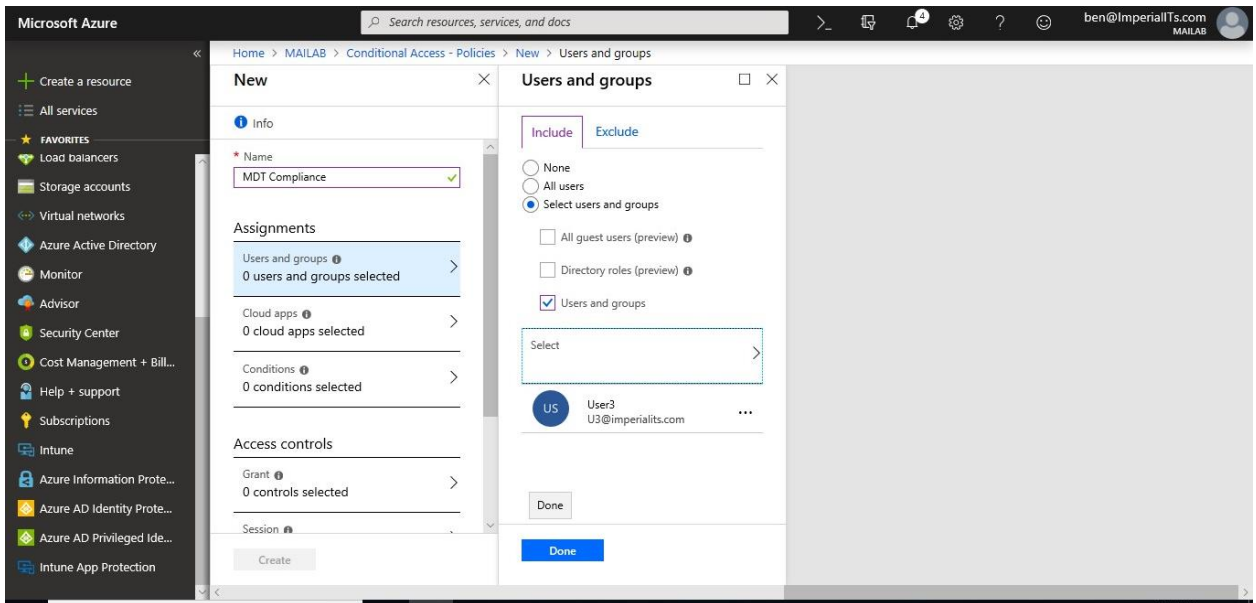


Step 10: Create an Azure AD conditional access policy

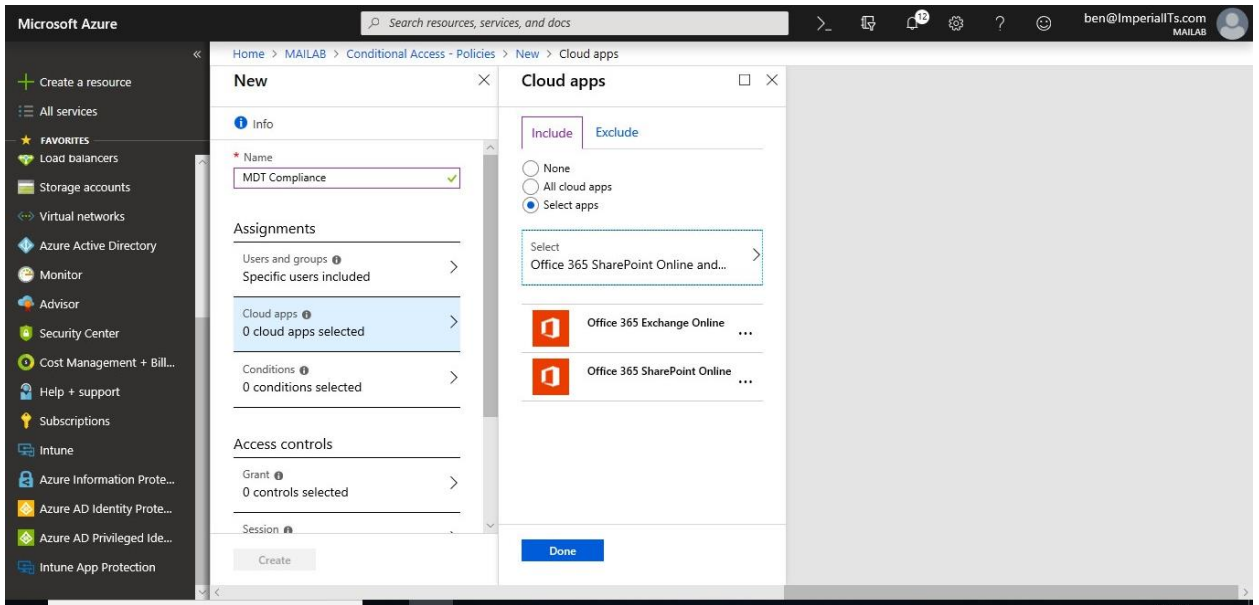
1. In the [Azure portal](#), open **Azure Active Directory** > **Conditional access** > **New policy**.



2. Enter a policy **Name** and select **Users and groups**. Use the Include or Exclude options to add your groups for the policy and select **Done**.

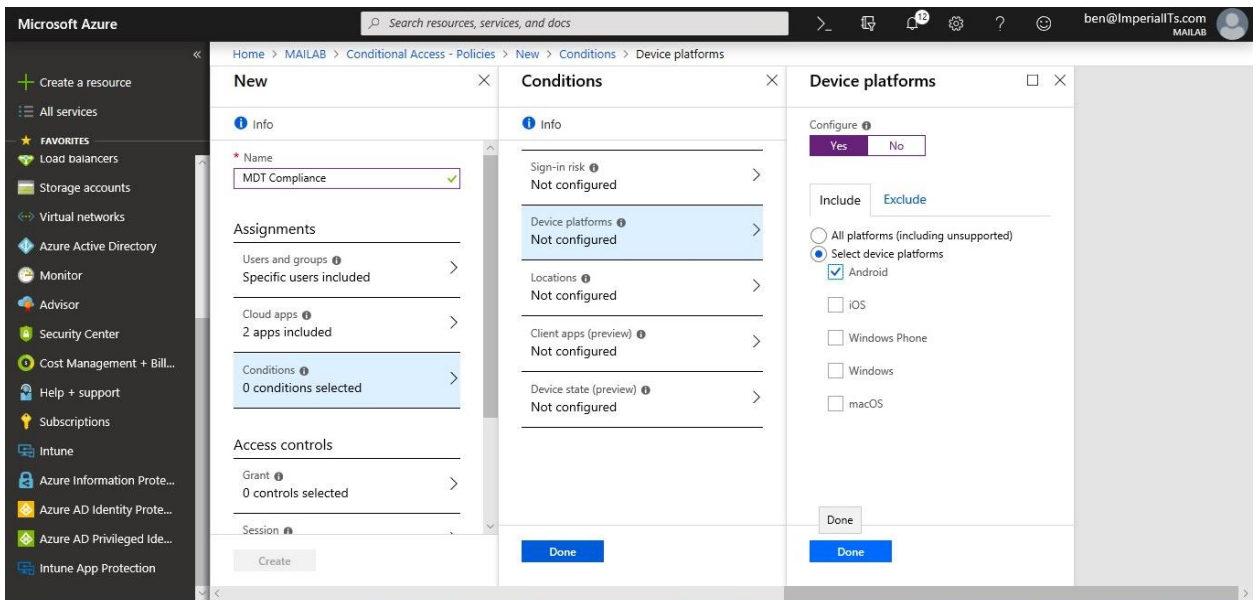


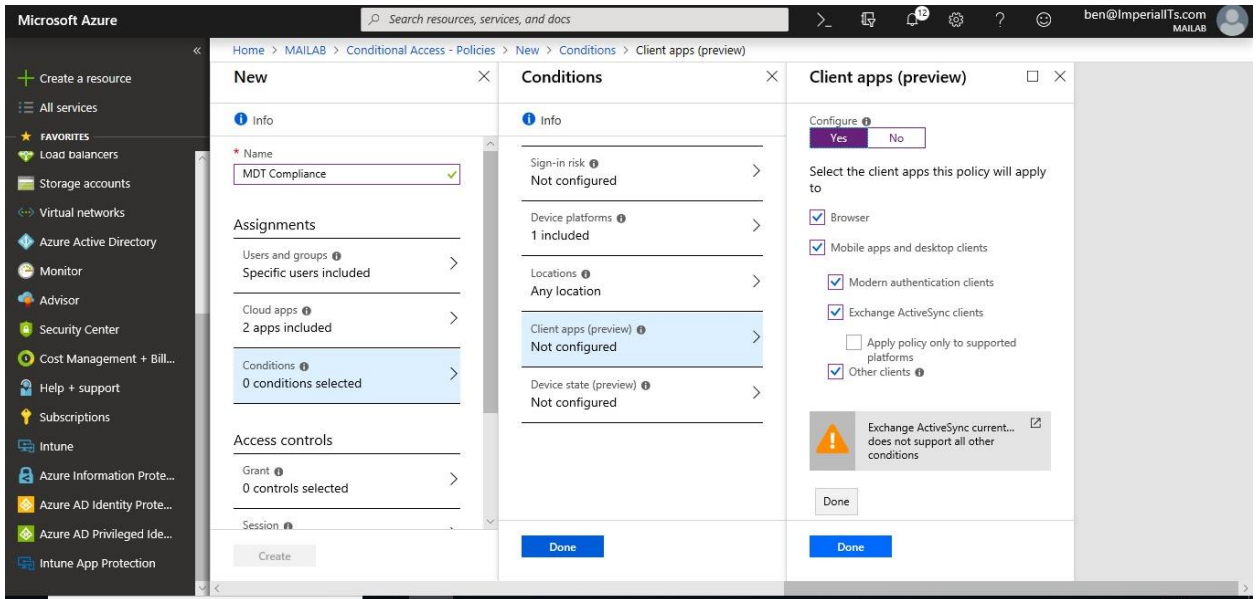
3. Select **Cloud apps** and choose which apps to protect. For example, choose **Select apps**, and select **Office 365 SharePoint Online** and **Office 365 Exchange Online**. Select **Done** to save your changes.



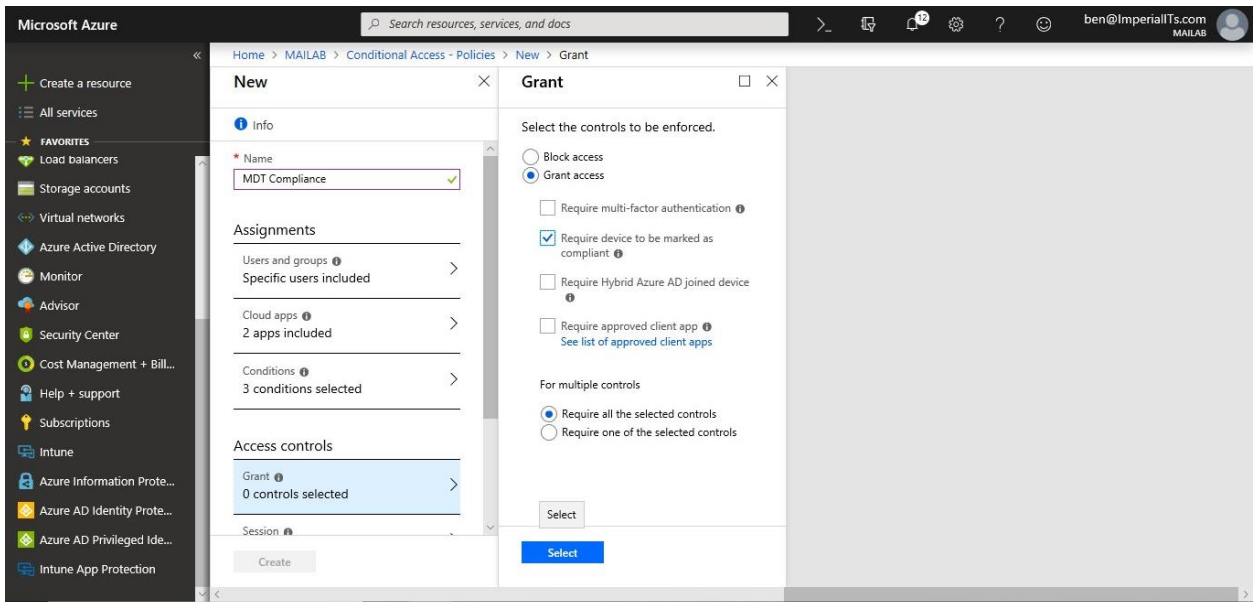
Note: Don't apply CA policy on all cloud apps, to be able to install & configure Lookout on your mobile phone without any issue because when you apply it to all cloud app, it will be applying on company portal and you won't be sign in on lookout & configure it.

4. Select **Conditions** > **Client apps** to apply the policy to apps and browsers. For example, select **Yes**, and then enable **Browser** and **Mobile apps and desktop clients**. Select **Done** to save your changes.



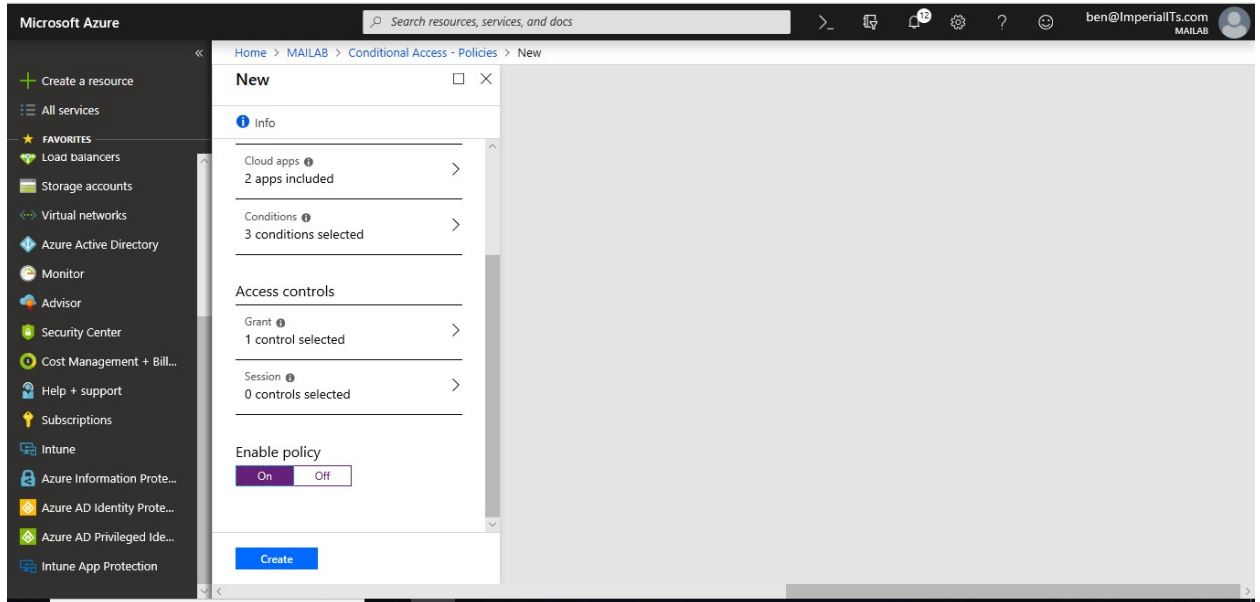


5. Select **Grant** to apply conditional access based on device compliance. For example, select **Grant access** > **Require device to be marked as compliant**. Choose **Select** to save your changes.



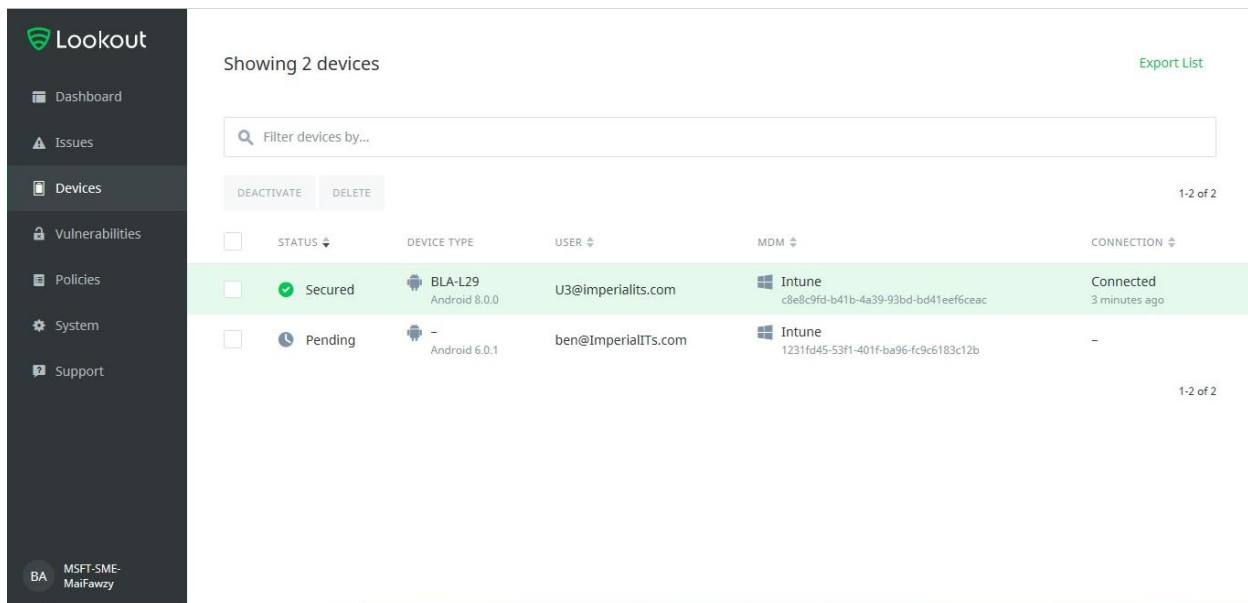
6. Select **Enable policy**, and then **Create** to save your changes.

Microsoft Intune step by step on Azure portal



Step 11: Watching enrollment

Once the setup is complete, Lookout Mobile Threat Defense starts to poll Azure AD for devices that correspond to the specified enrollment groups. You can find information about the devices enrolled on the Devices module. The initial status for devices is shown as pending. The device status changes once the Lookout for Work app is installed, opened, and activated on the device.



Chapter 9

Manage Windows 10 PCs Using Microsoft Intune

Windows 10 provides an enterprise management solution to help IT pros manage company security policies and business applications, while avoiding compromise of the users' privacy on their personal devices. A built-in management component can communicate with the management server. There are two parts to the Windows 10 management component:

- The enrollment client, which enrolls and configures the device to communicate with the enterprise management server.
- The management client, which periodically synchronizes with the management server to check for updates and apply the latest policies set by IT.

When you connect your device using mobile device management (MDM) enrollment, your organization may enforce certain policies on your device and pushing applications or some security policy.

Enroll Windows 10 MDM

We have one or more of the following methods to enroll windows 10

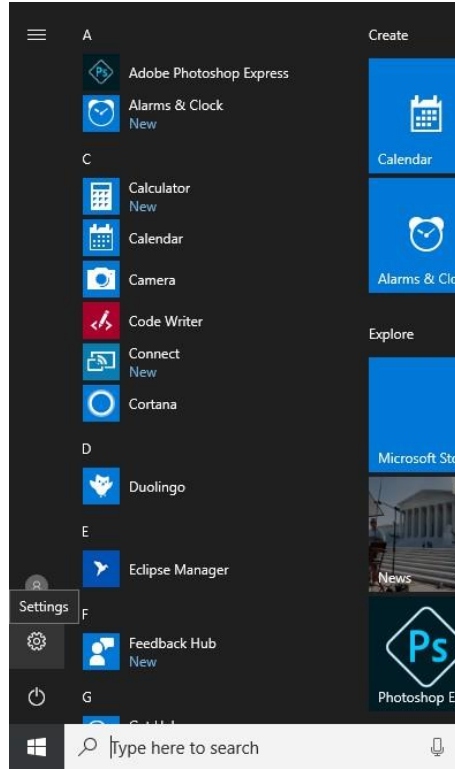
- [Manually enroll windows 10](#)
- [Automatically enroll Windows 10 using Azure AD.](#)
- [Automatically enroll Windows 10 using Group Policy.](#)
- [Enroll Windows 10 devices by using the Windows Autopilot.](#)

Manually Enroll Windows 10

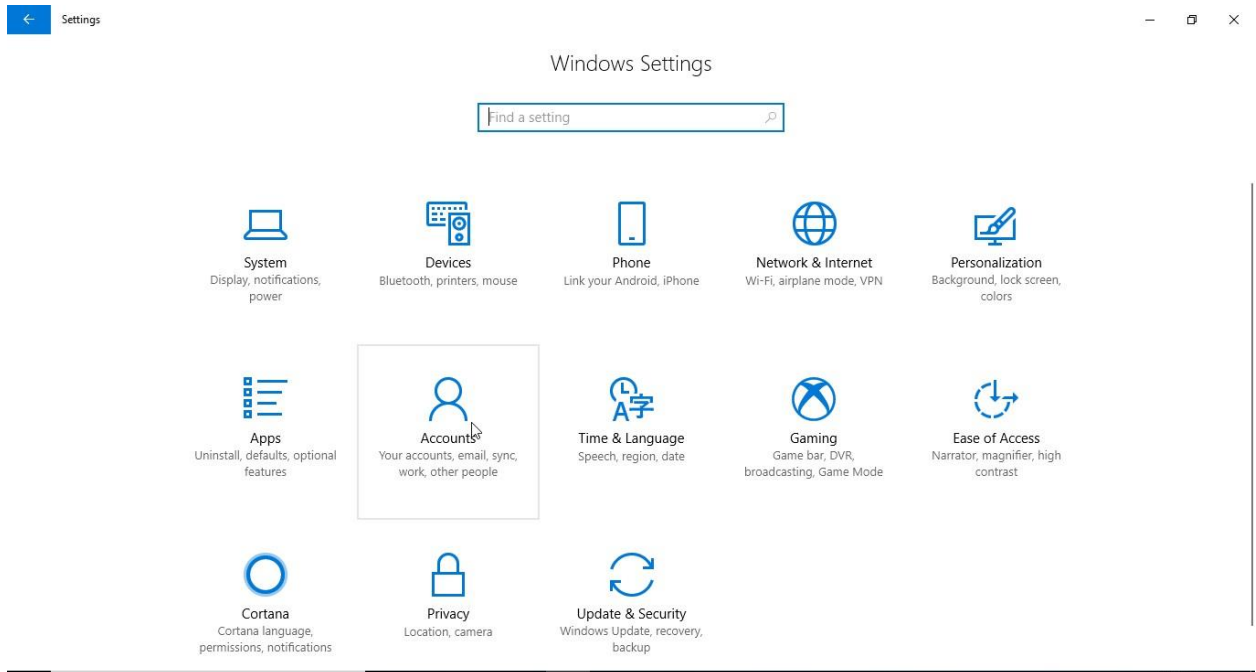
All Windows 10-based devices can be connected to an MDM. You can connect to an MDM through the Settings app.

1. Launch the Settings app.

Microsoft Intune step by step on Azure portal

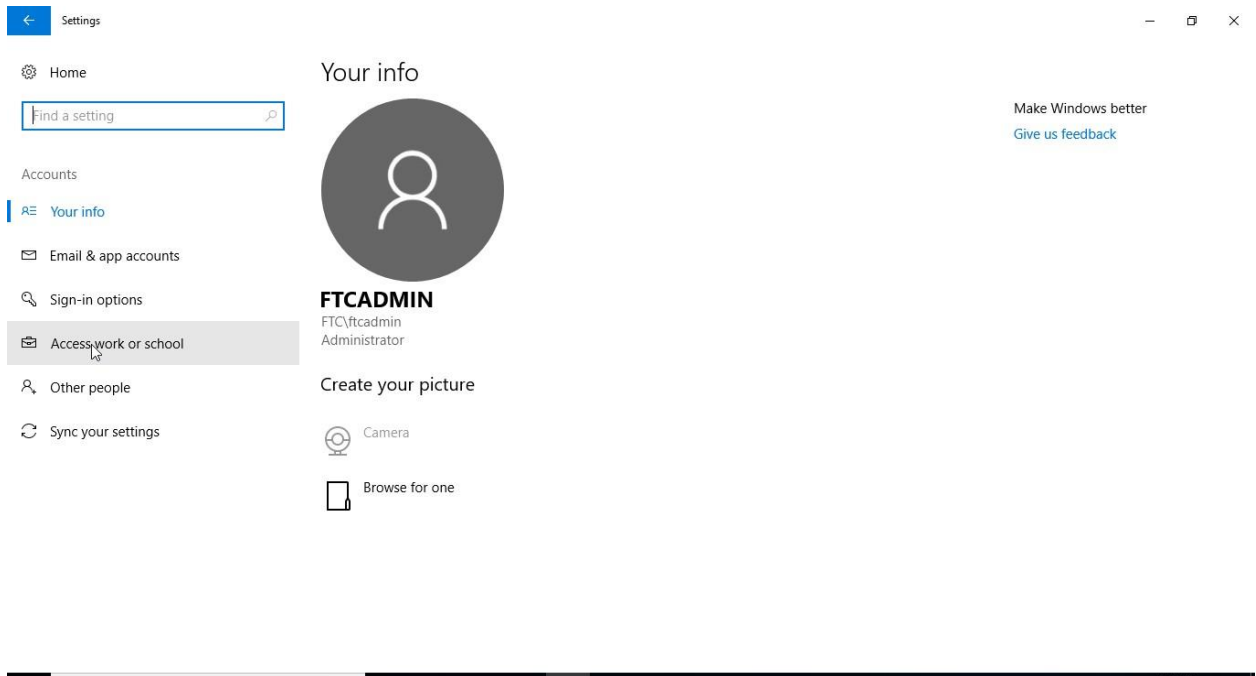


2. Next, navigate to **Accounts**.

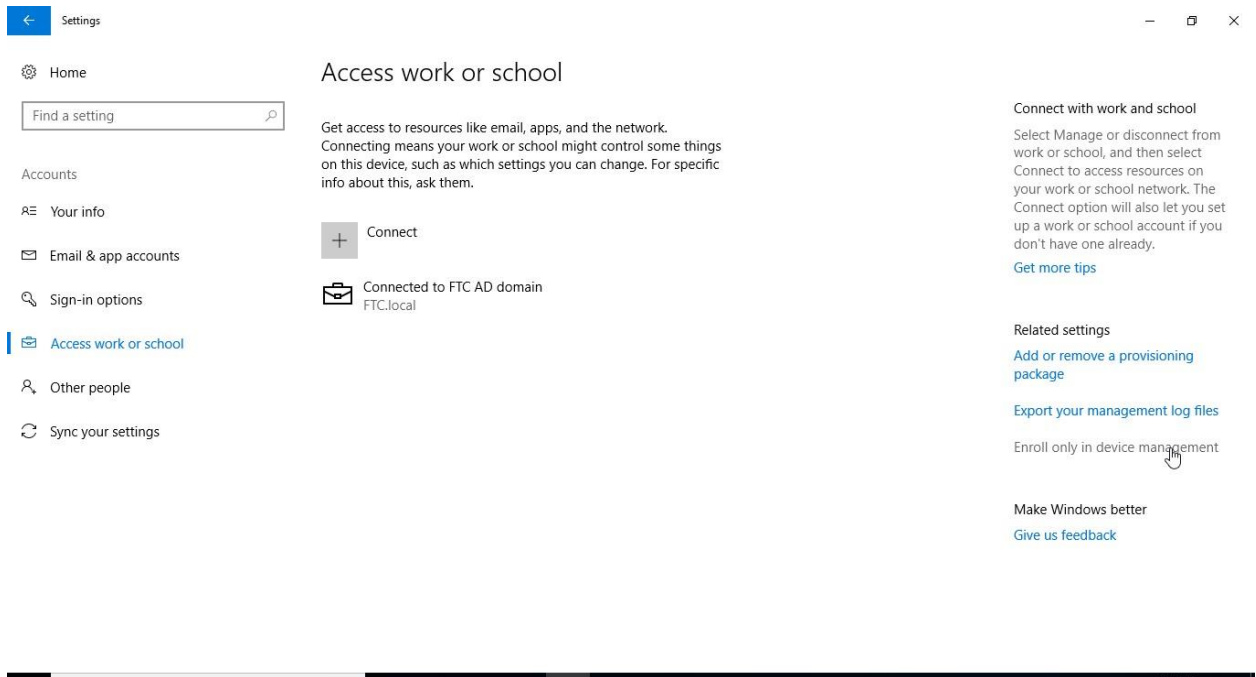


3. Navigate to **Access work or school**.

Microsoft Intune step by step on Azure portal

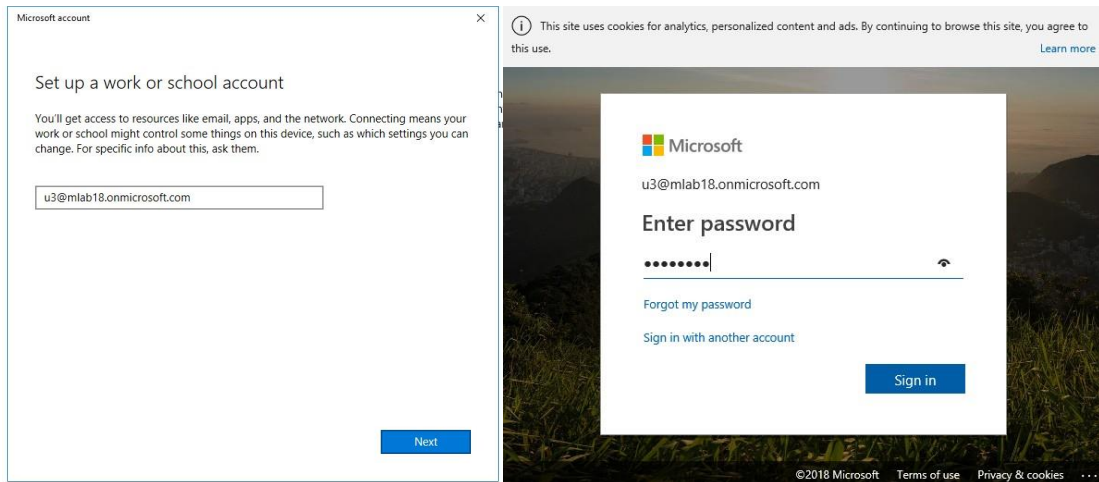


4. Click the **Enroll only in device management** link (available in servicing build 14393.82, KB3176934).

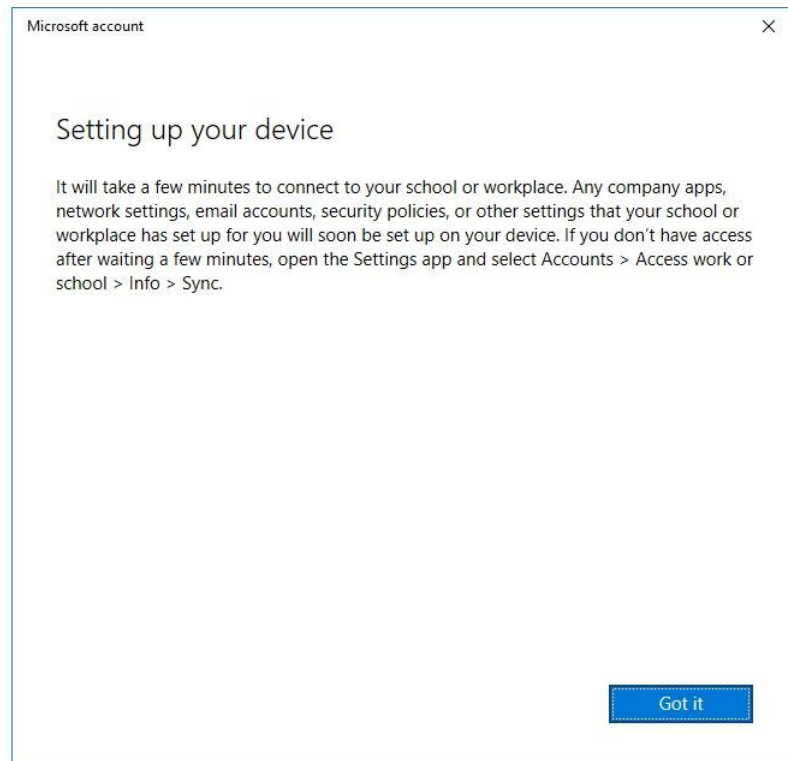


5. Type in your work email address.

Microsoft Intune step by step on Azure portal

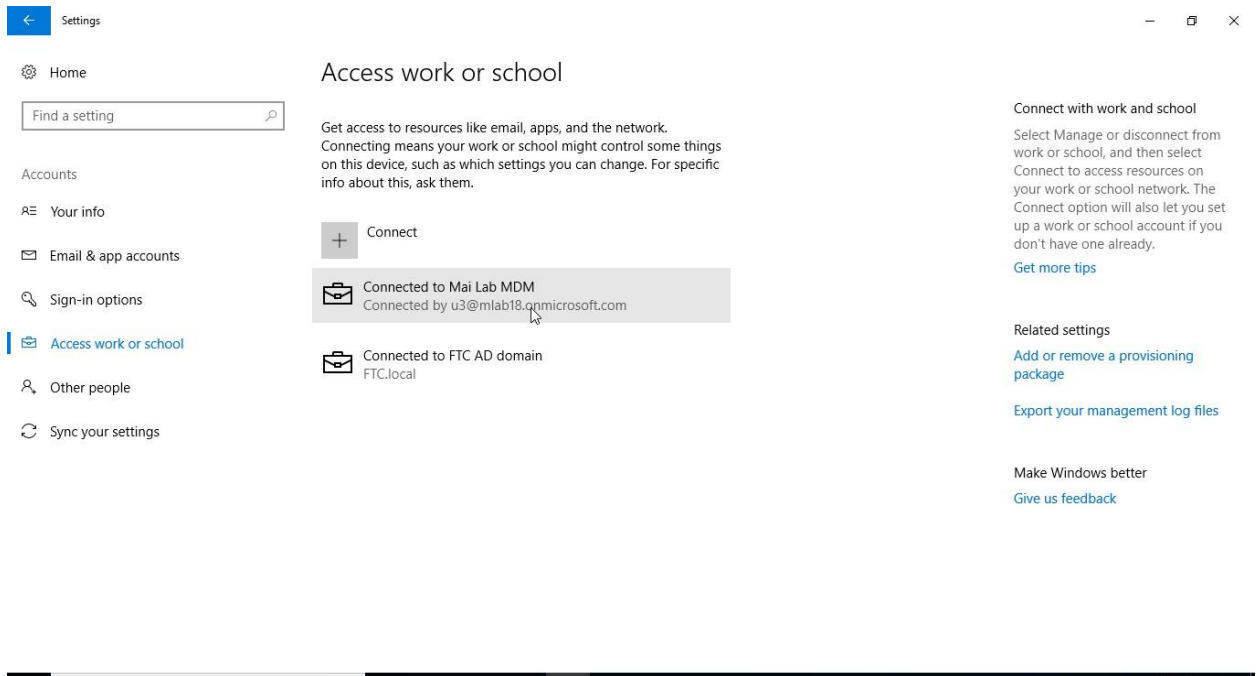


6. Click **Got it**.



7. After you complete the flow, your device will be connected to your organization's MDM.

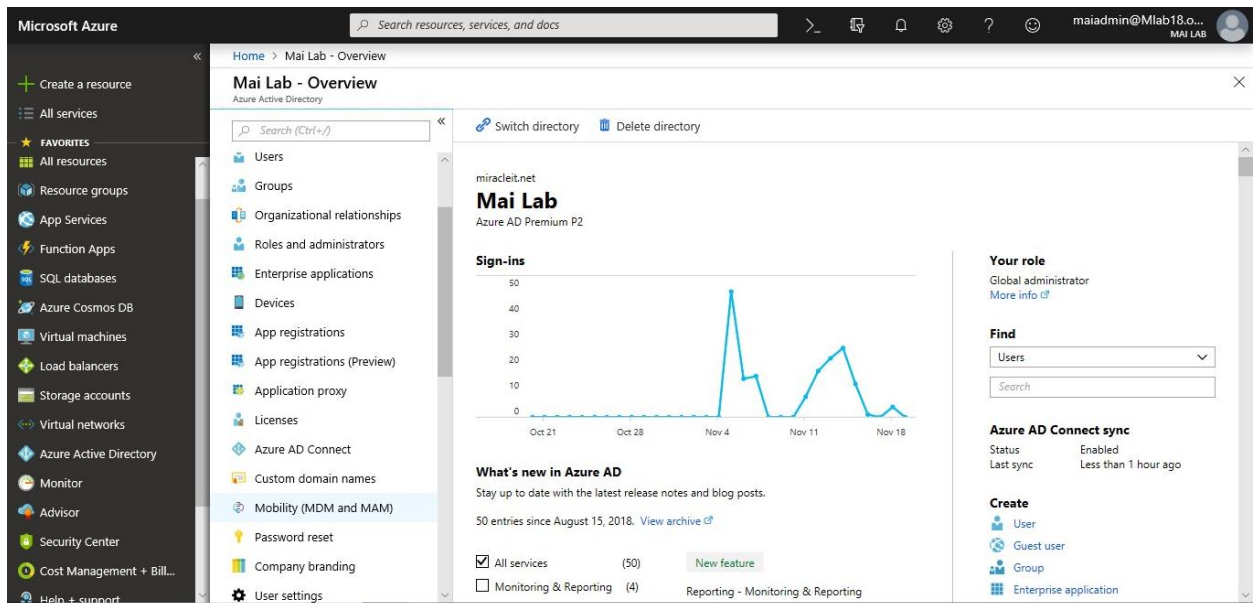
Microsoft Intune step by step on Azure portal



Automatically Enroll Windows 10 Using Azure AD

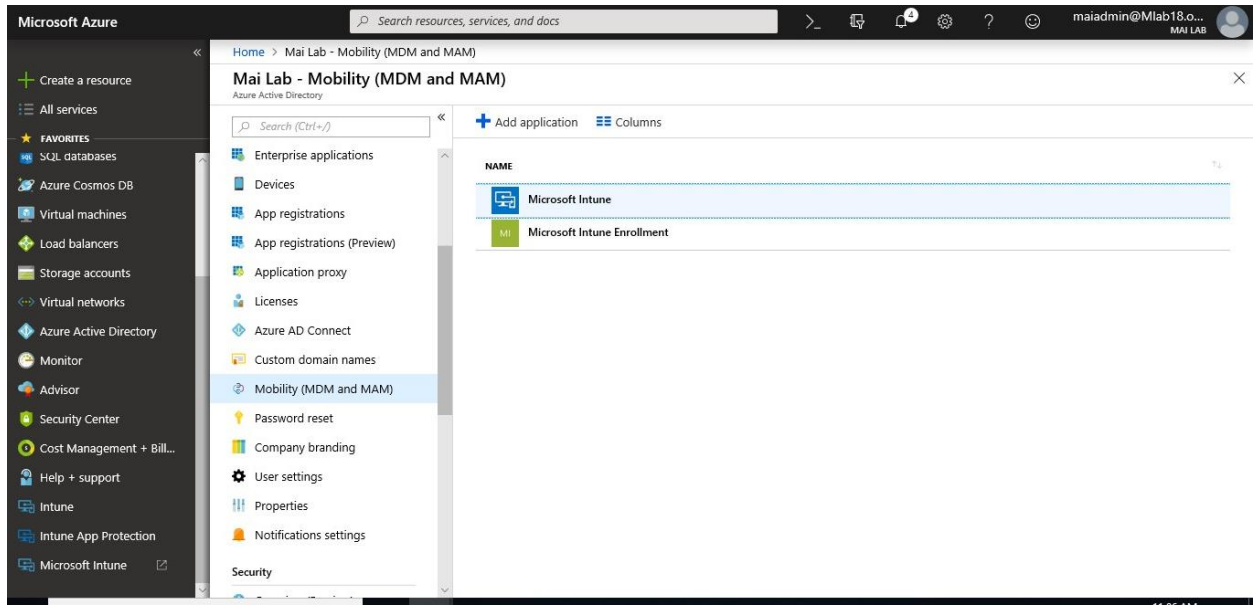
Windows 10 can automatic enroll using Azure AD if your device is register or join Azure AD

1. Sign in to the [Azure portal](#), and select **Azure Active Directory**.
2. Select **Mobility (MDM and MAM)**.

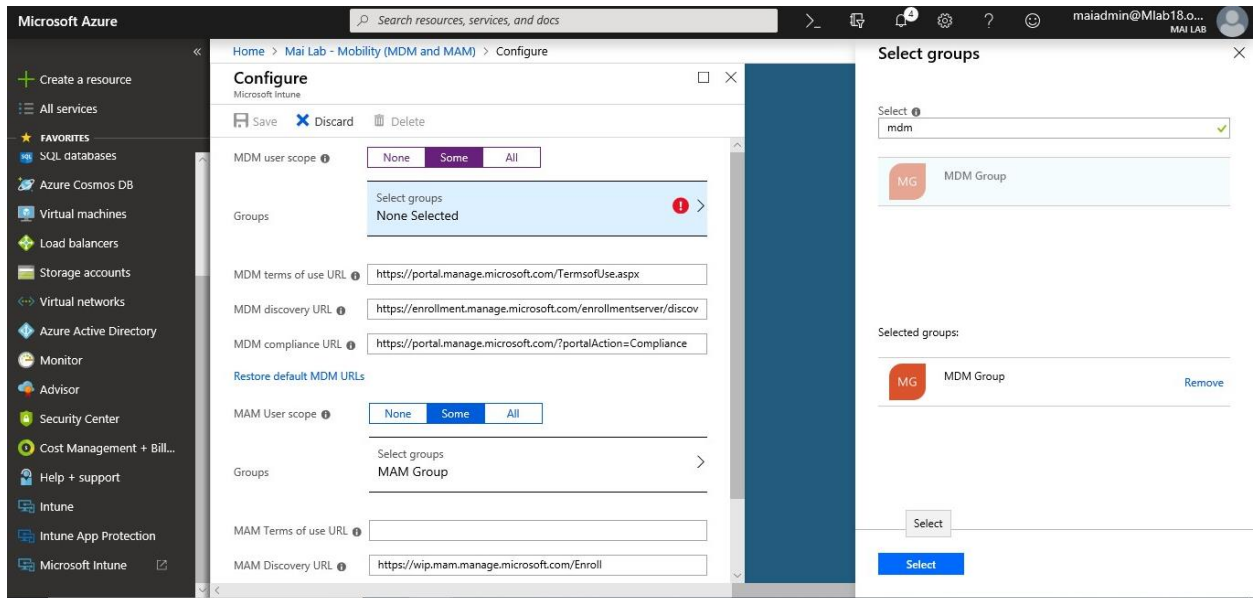


3. Select **Microsoft Intune**.

Microsoft Intune step by step on Azure portal

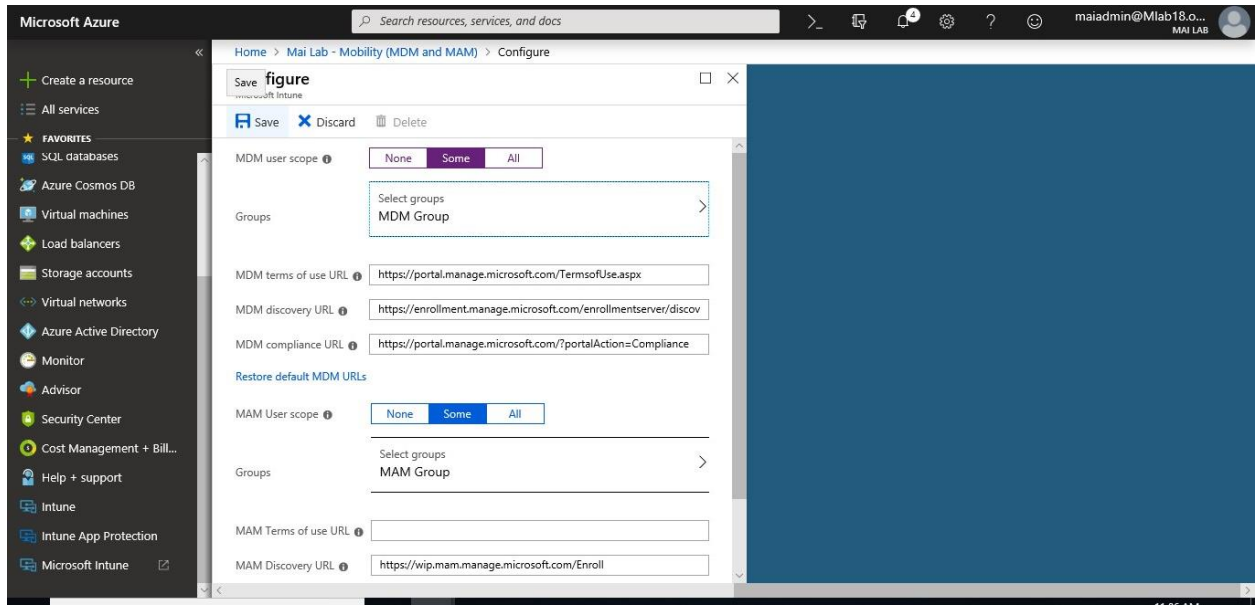


4. Configure **MDM User scope**. Specify which users' devices should be managed by Microsoft Intune. These Windows 10 devices can automatically enroll for management with Microsoft Intune.

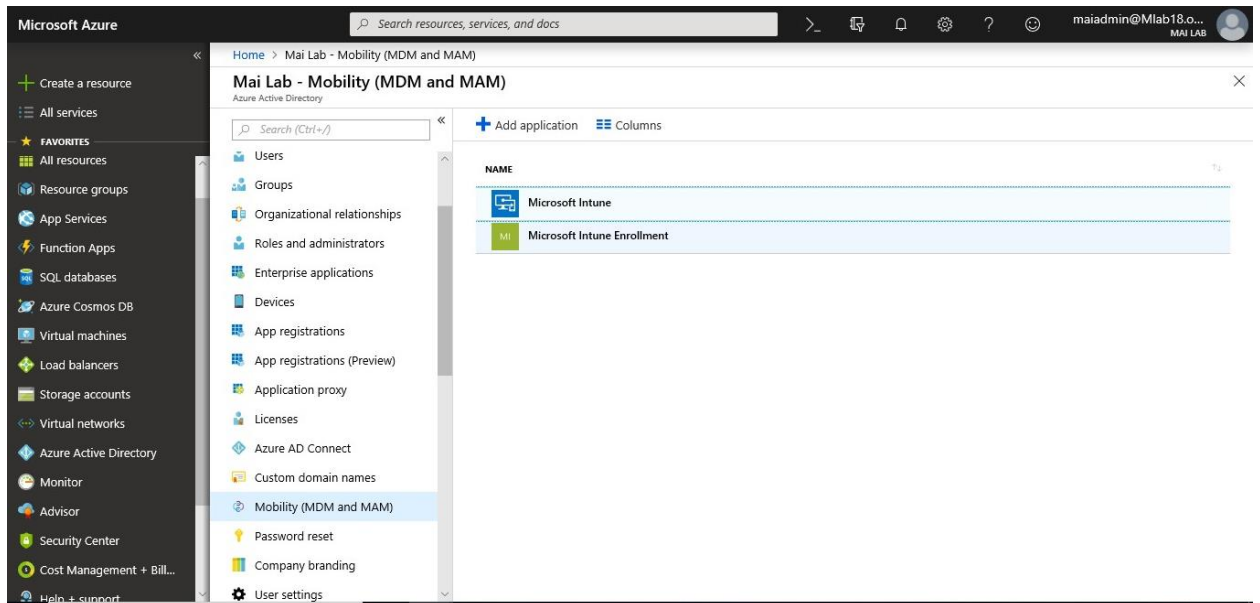


5. Use the default values for the following URLs:
 - **MDM Terms of use URL**
 - **MDM Discovery URL**
 - **MDM Compliance URL**
6. Select **Save**.

Microsoft Intune step by step on Azure portal

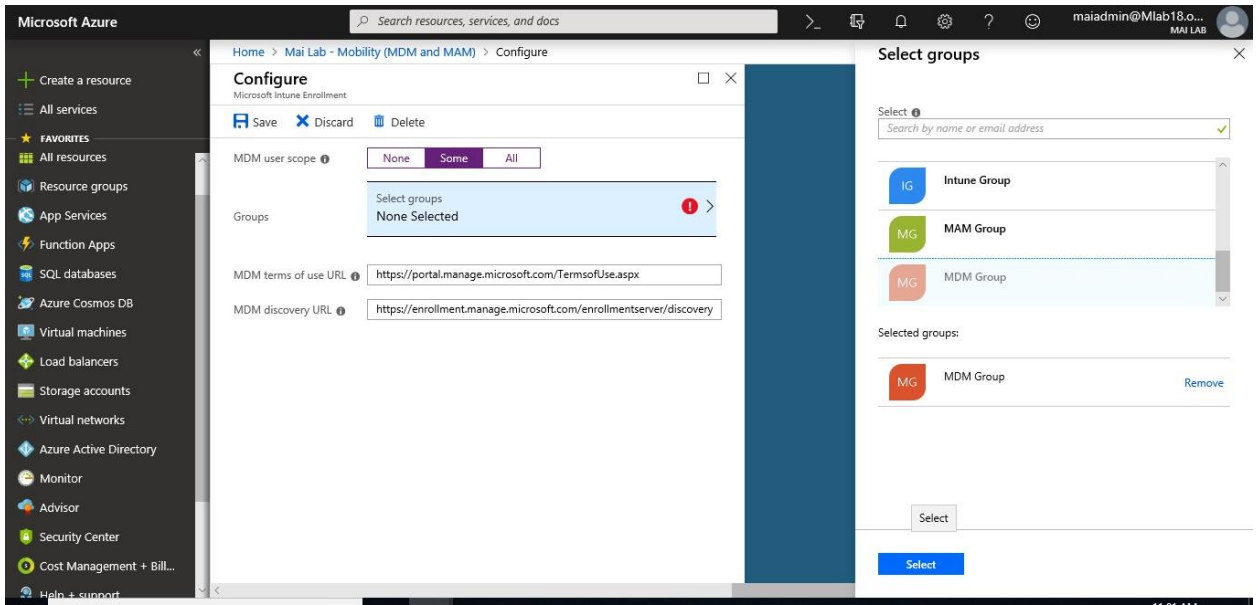


7. Select **Microsoft Intune Enrollment** (in case, you find it on your tenant)

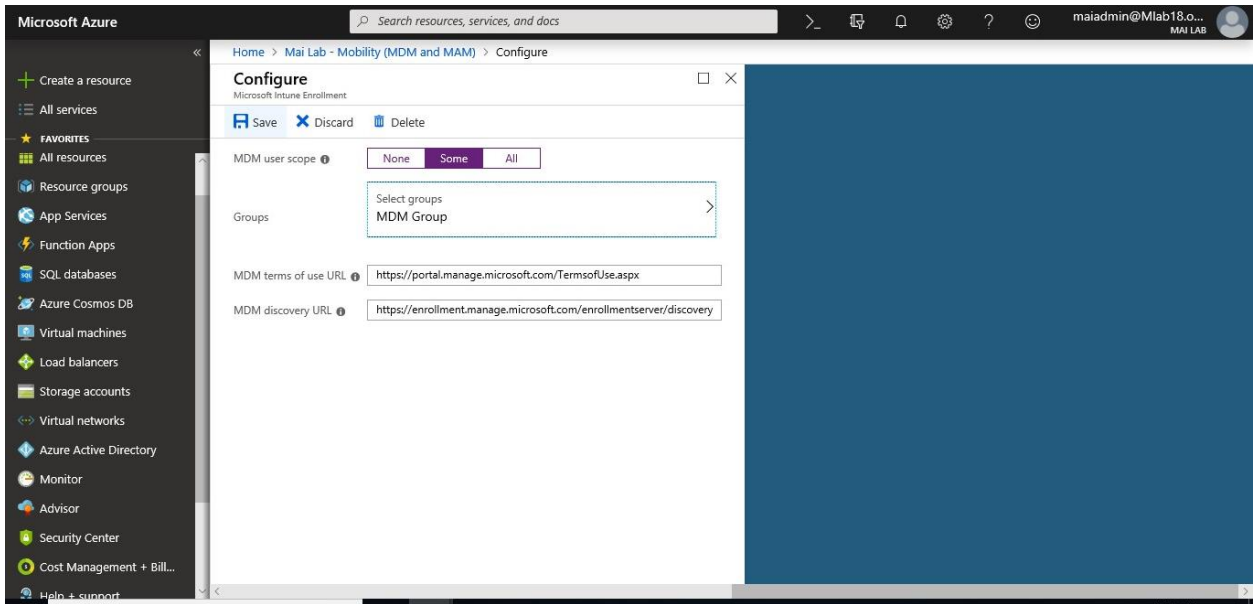


8. Configure **MDM User scope**. Specify which users' devices should be managed by Microsoft Intune. These Windows 10 devices can automatically enroll for management with Microsoft Intune.

Microsoft Intune step by step on Azure portal

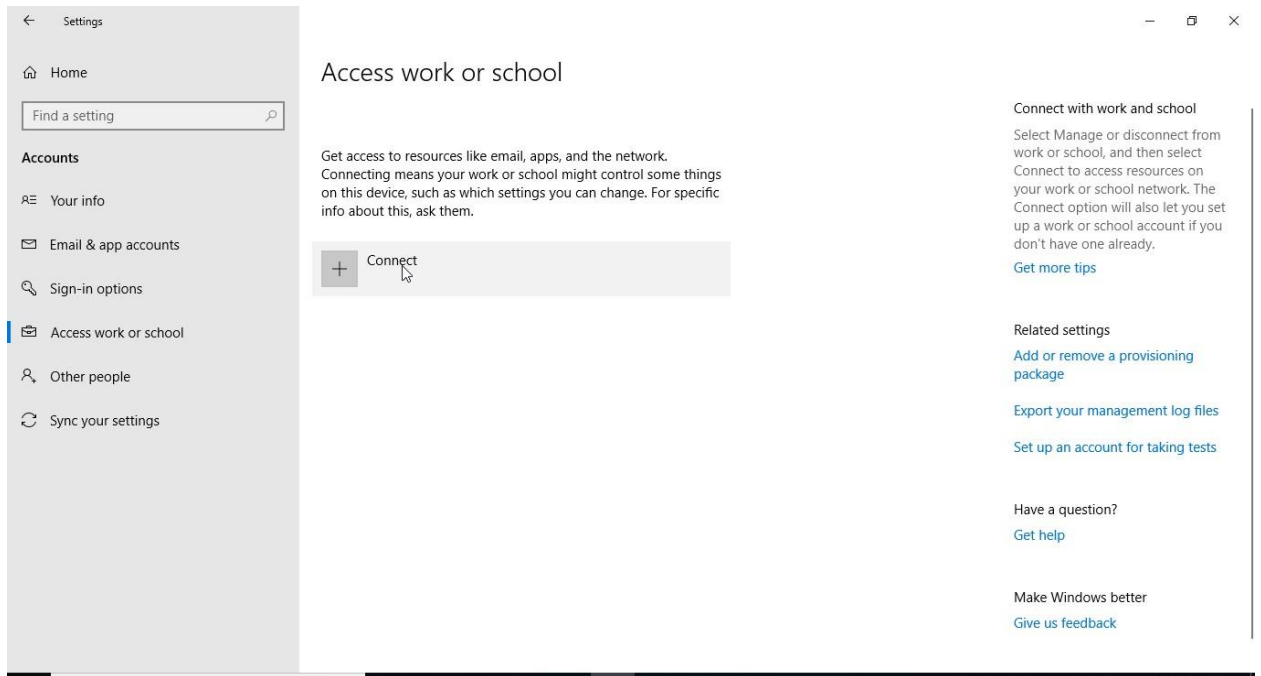


9. Use the default values for the following URLs:
 - **MDM Terms of use URL**
 - **MDM Discovery URL**
10. Select **Save**.

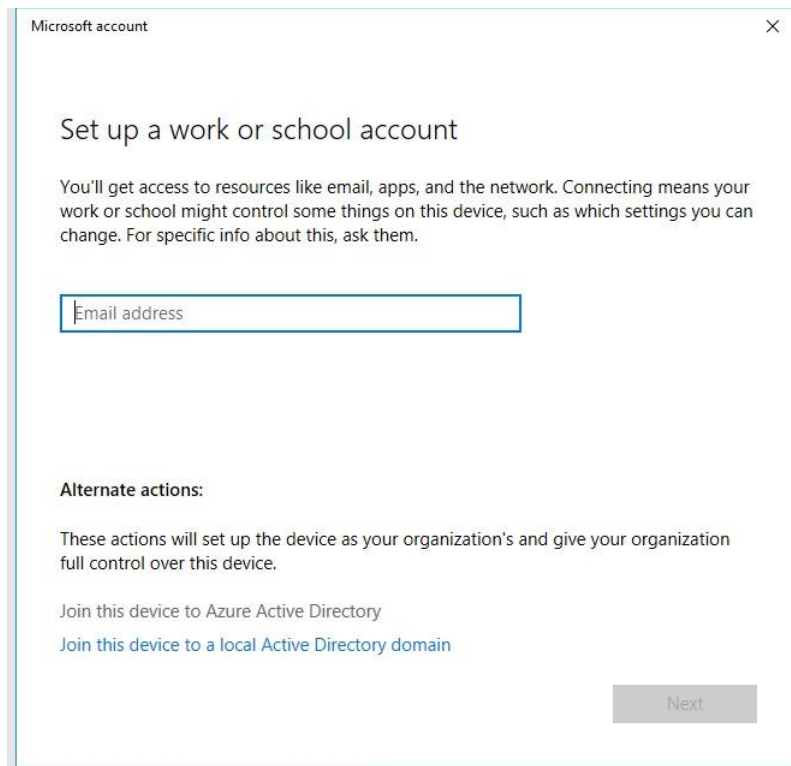


Join Windows 10 to Azure AD

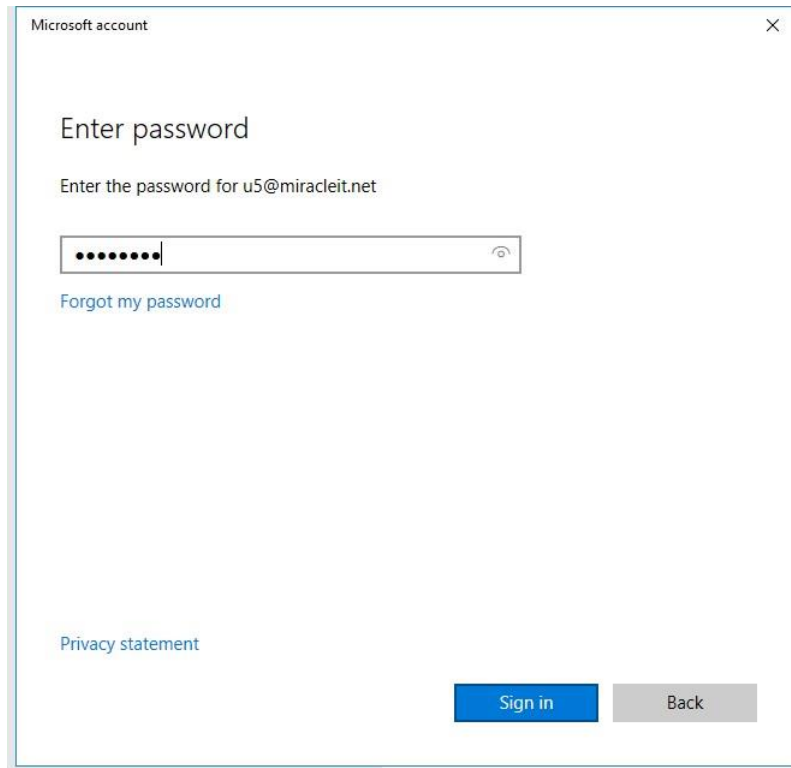
1. Open **Settings > Accounts > Access work or school** and click **Connect**.



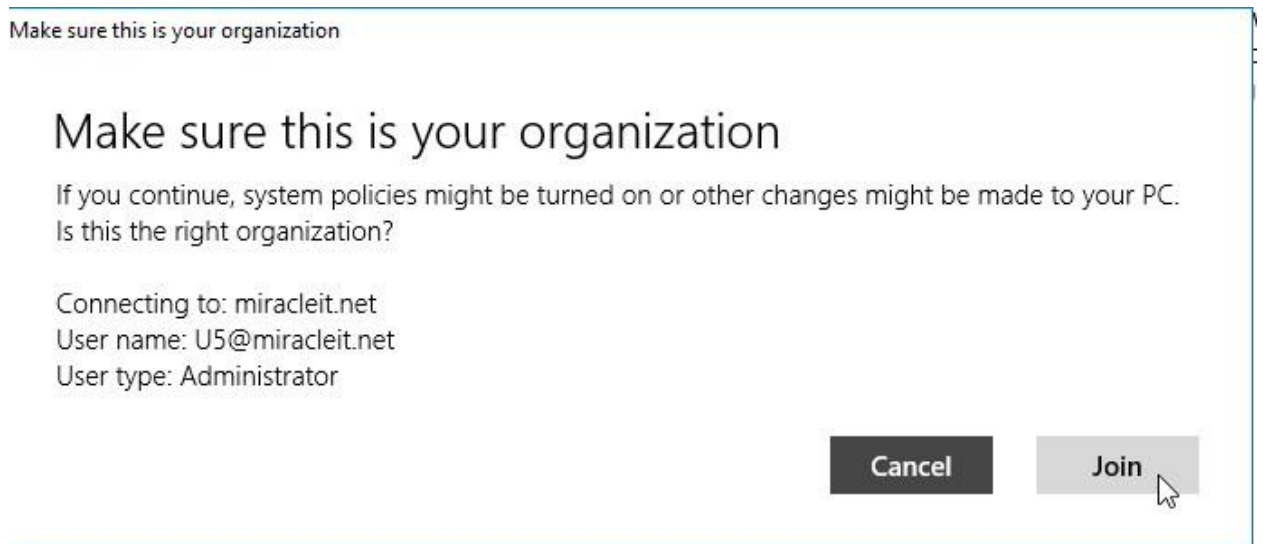
2. Select **Join this device to Azure Active Directory**.



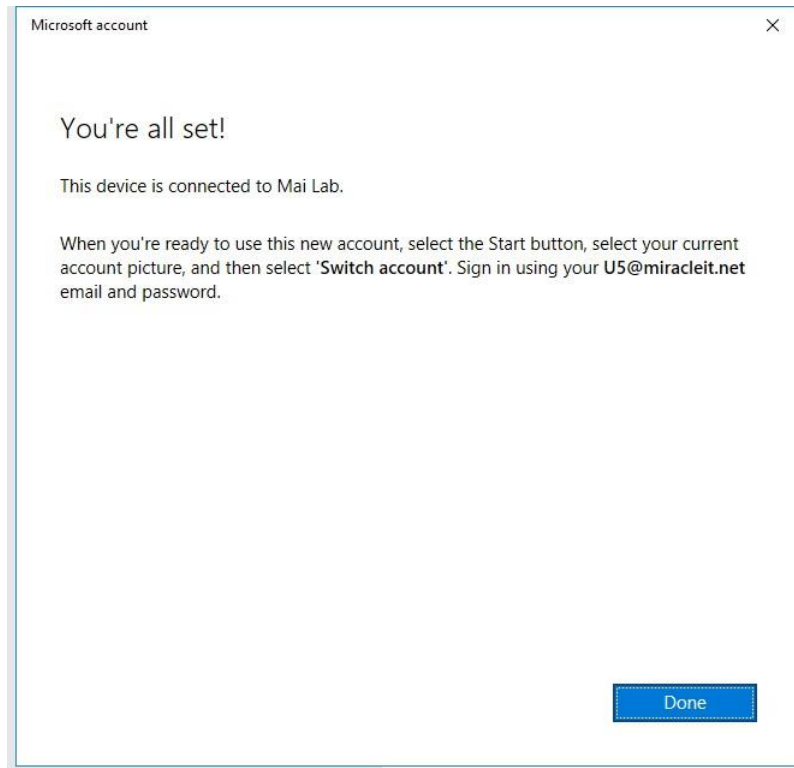
3. Sign in with your Azure AD credentials.



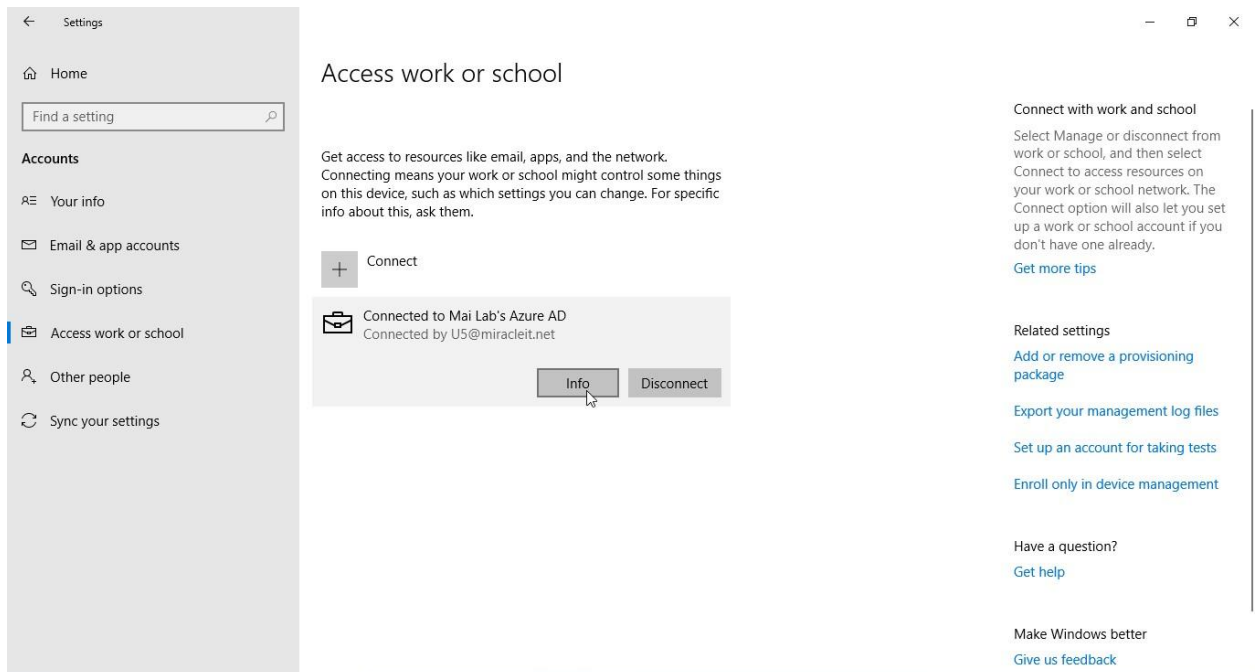
4. Click **Join** after checking that information is correct.



5. Click Done to close window.



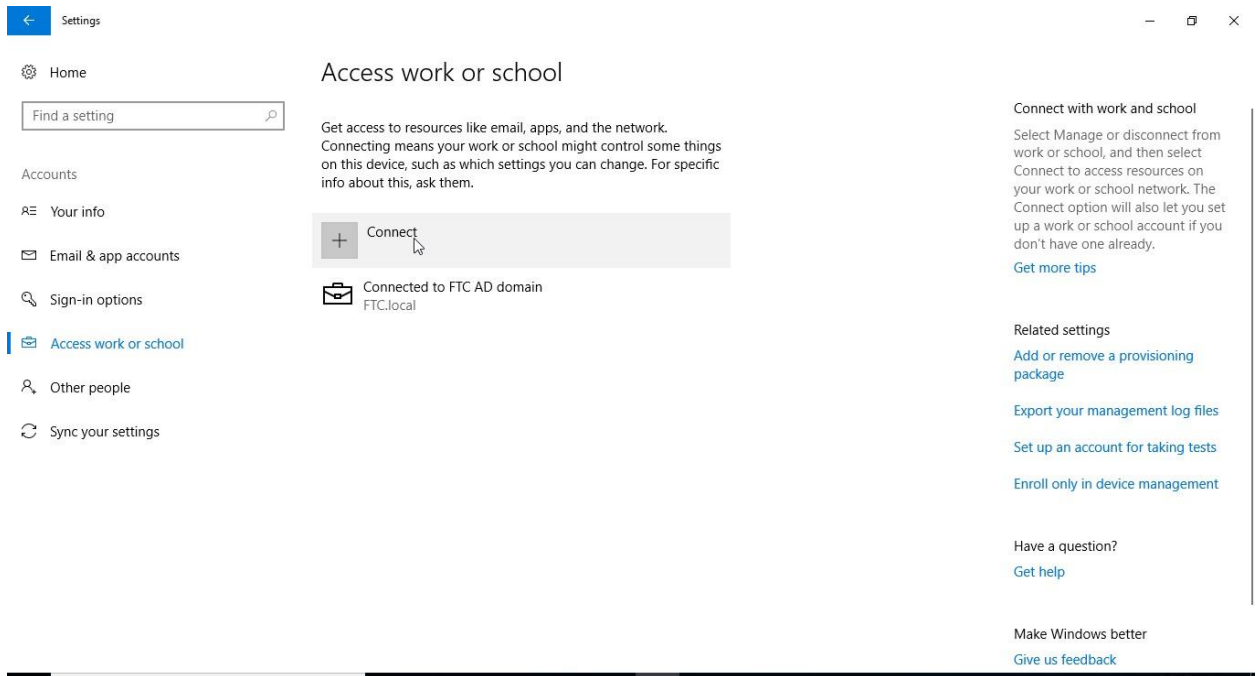
6. All done, your device is joined to Azure AD.



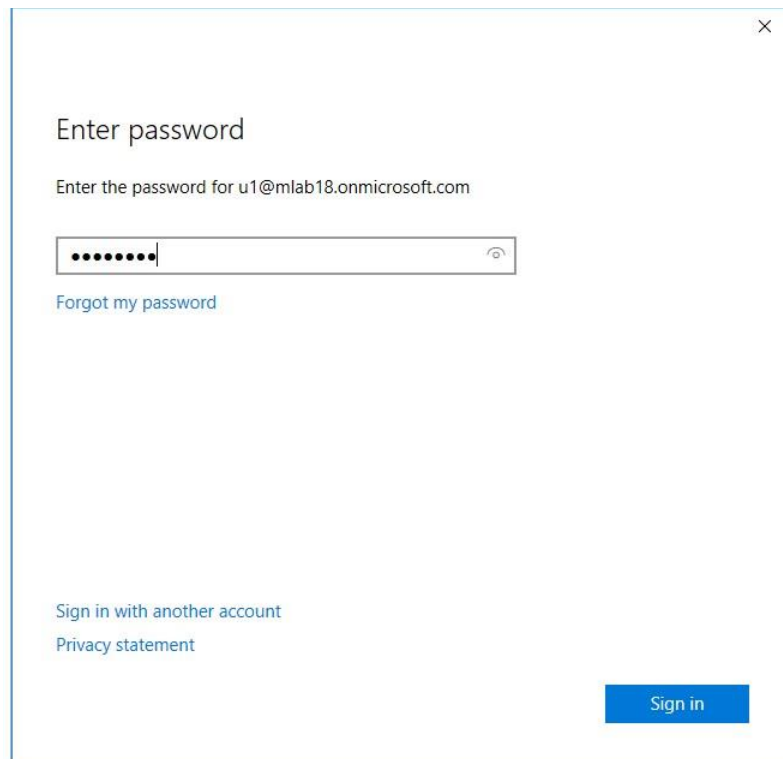
Register Windows 10 to Azure AD

1. Open **Settings > Accounts > Access work or school** and click **Connect**.

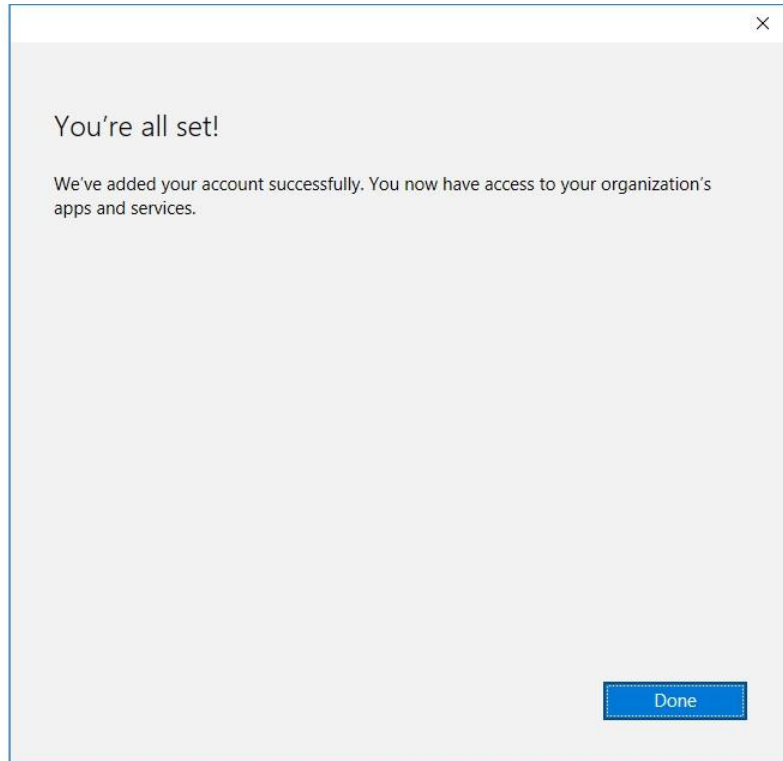
Microsoft Intune step by step on Azure portal



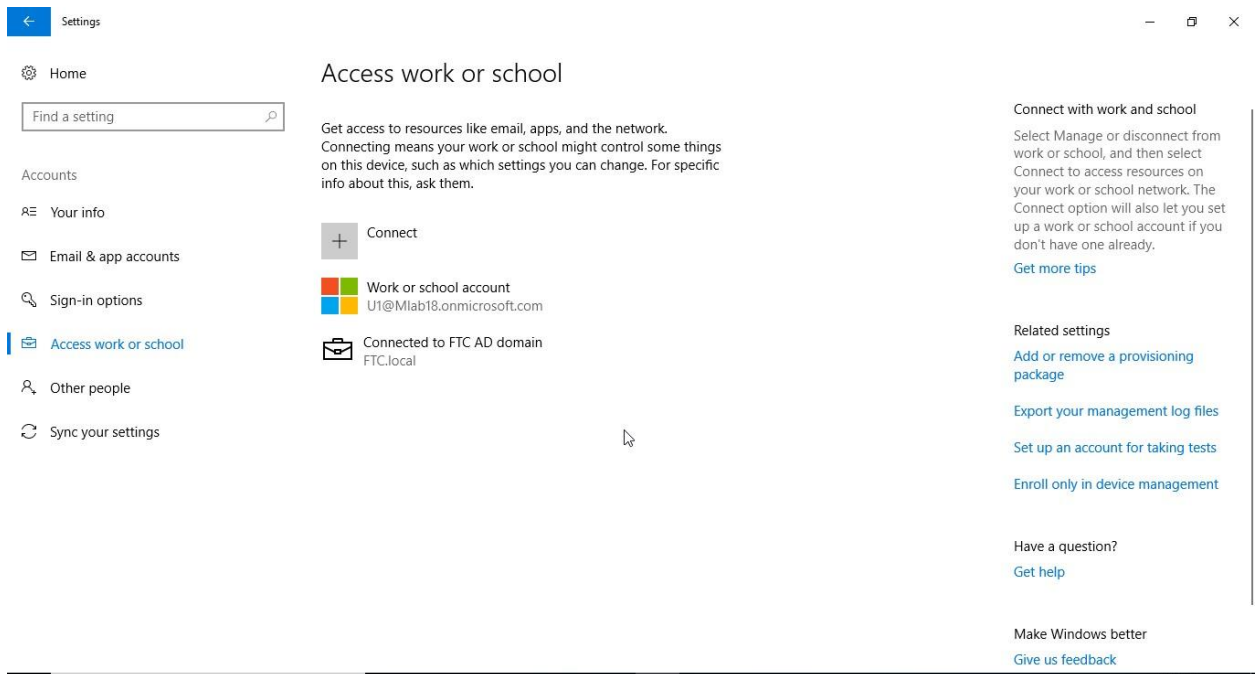
2. Enter your Azure AD email address & password and click **Sign in**.



3. Once you finish the registration process, Click **Done**.



4. The device is now joined as workplace to Azure AD.



Automatically Enroll Windows 10 Using Group Policy

Starting in Windows 10, version 1709 you can use a Group Policy to trigger auto-enrollment to MDM for Active Directory (AD) domain joined devices.

Prerequisites:

- AD-joined PC running Windows 10, version 1709
- Enterprise has MDM service already configured
- Enterprise AD must be registered with Azure AD
- Device should not already be enrolled in Intune using the classic agents
- [Enable Automatic Enrollment](#).

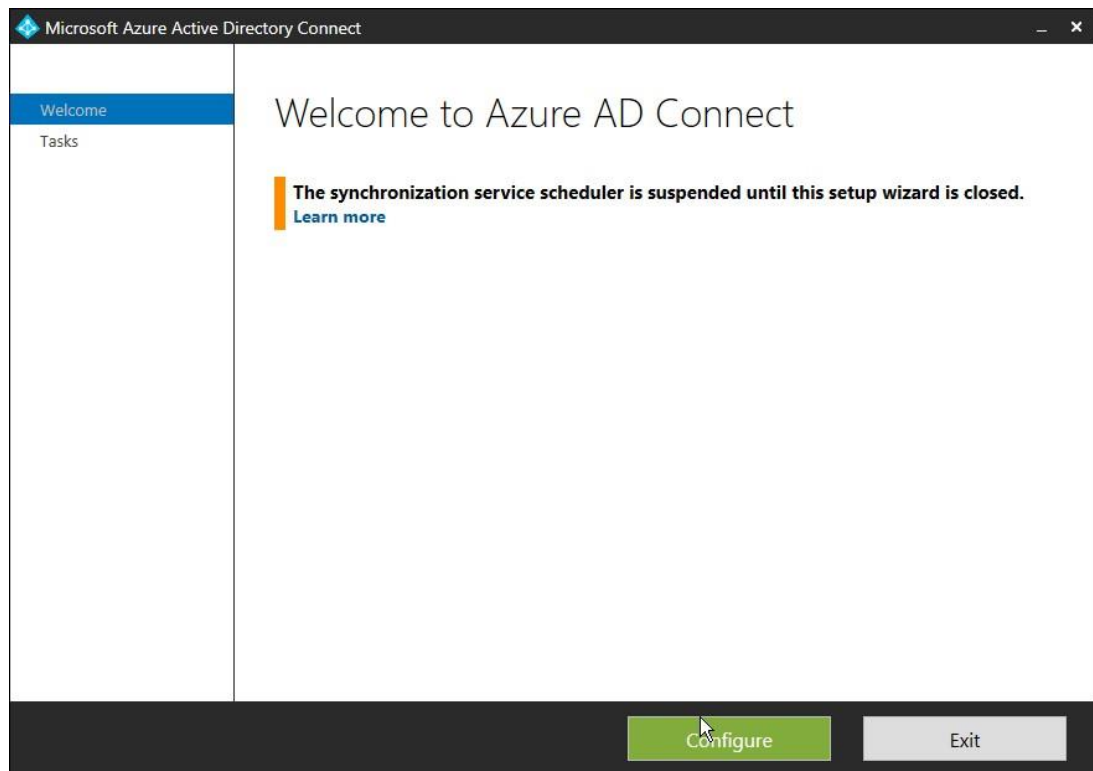
Step 1: Configure hybrid Azure AD join

To configure a hybrid Azure AD join using Azure AD Connect, you need:

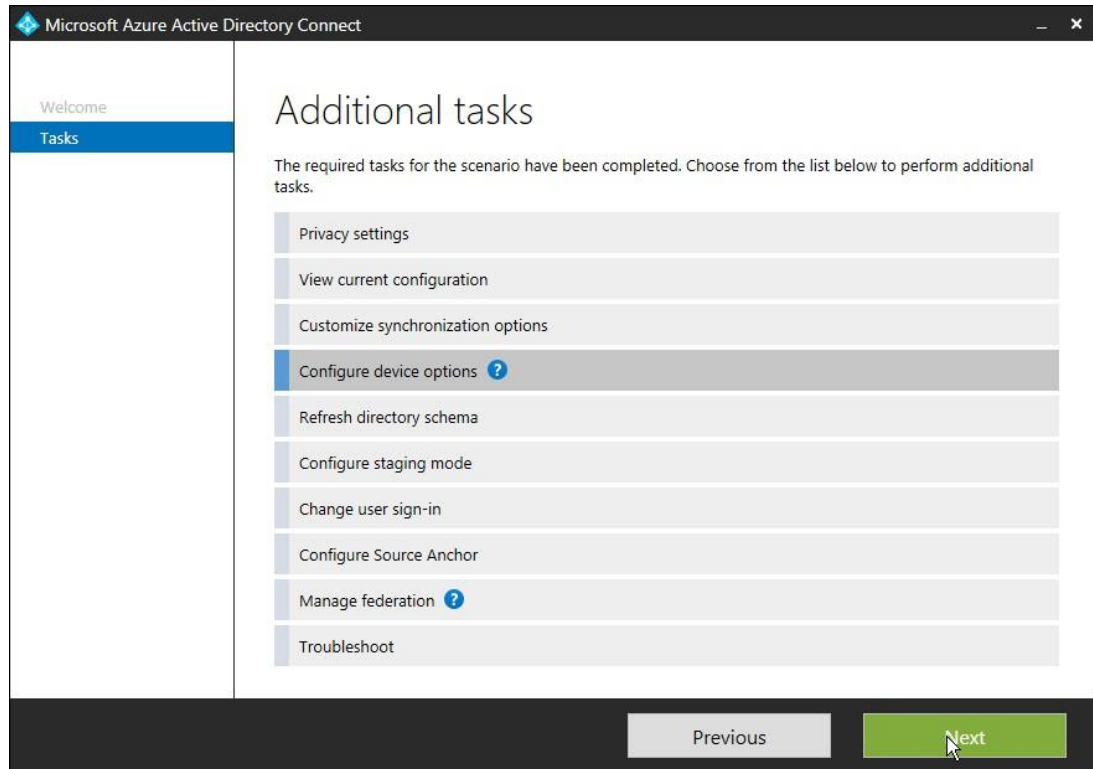
- The credentials of a global administrator for your Azure AD tenant.
- The enterprise administrator credentials for each of the forests.

To configure a hybrid Azure AD join using Azure AD Connect:

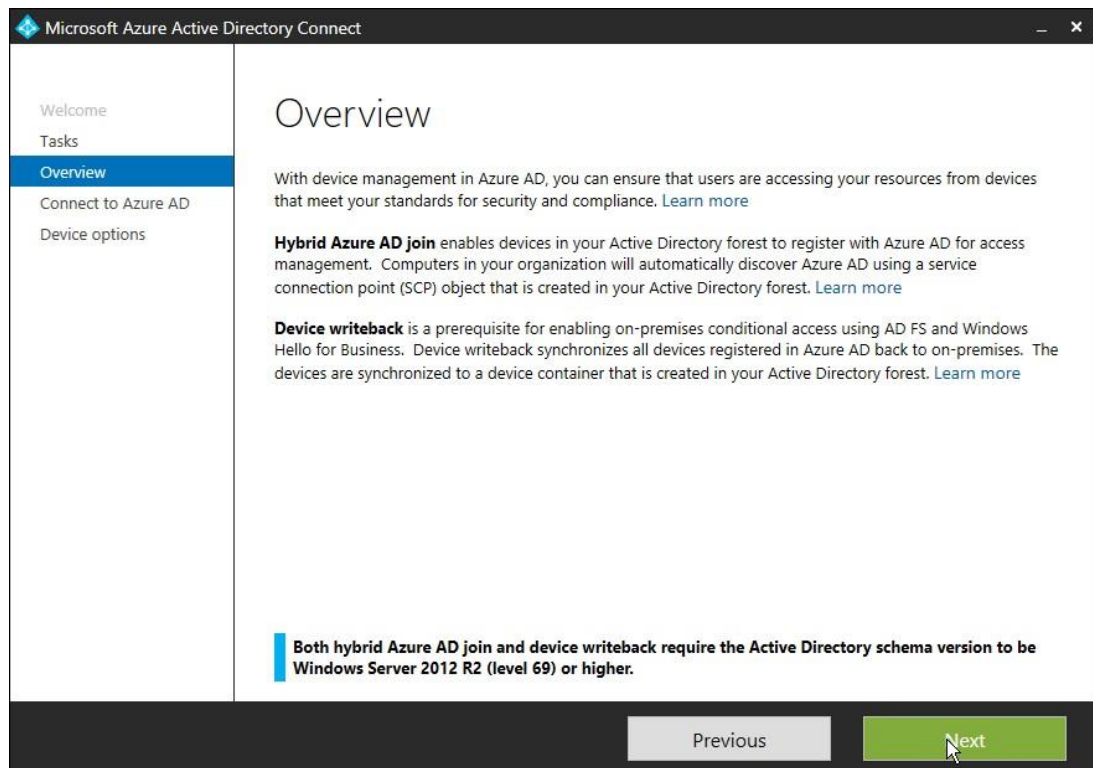
1. Launch Azure AD Connect, and then click **Configure**.



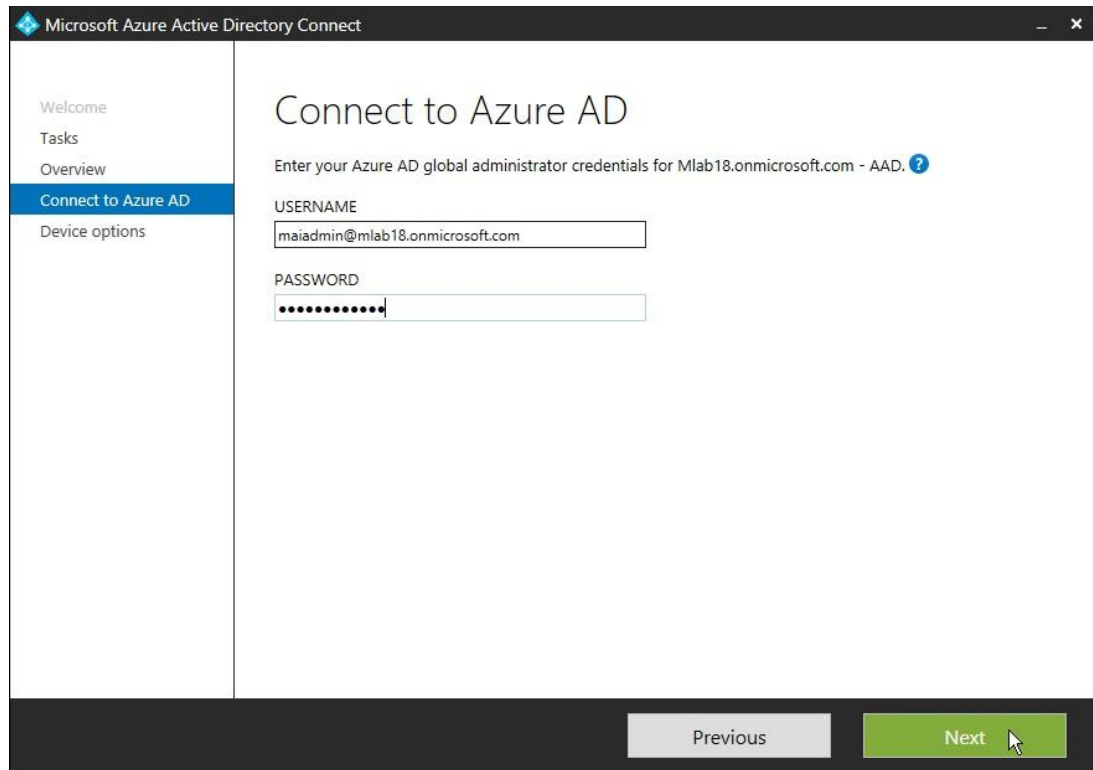
2. On the **Additional tasks** page, select **Configure device options**, and then click **Next**.



3. On the **Overview** page, click **Next**.

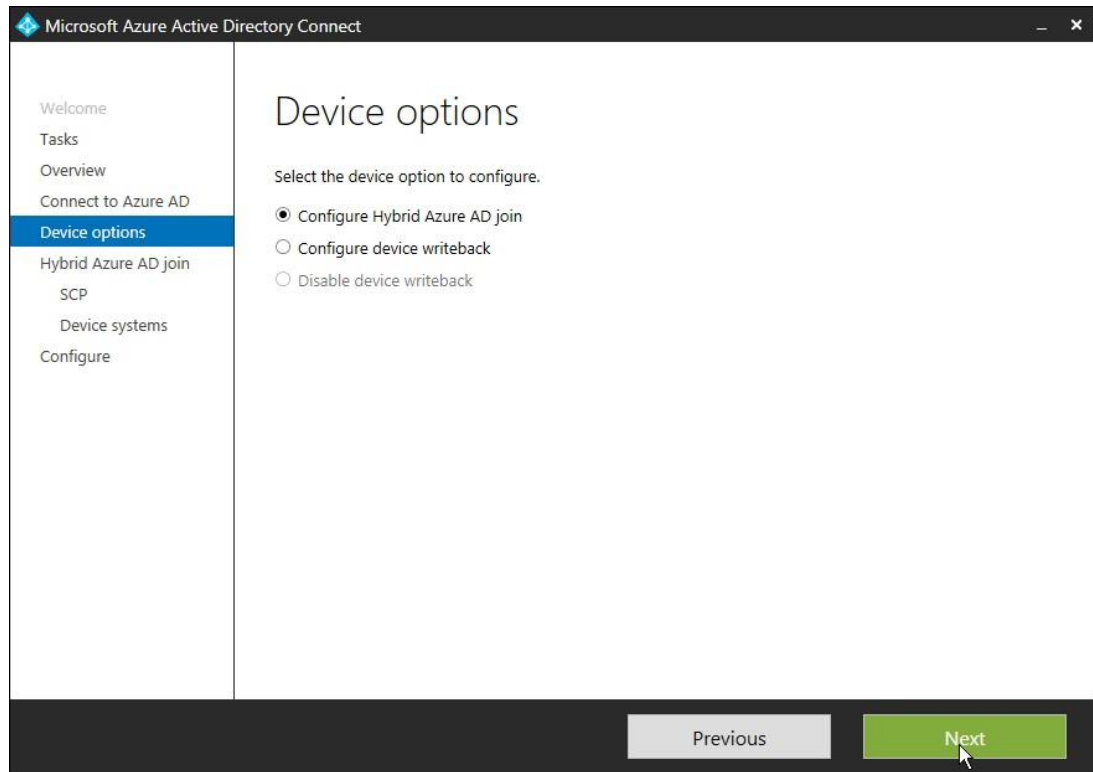


4. On the **Connect to Azure AD** page, enter the credentials of a global administrator for your Azure AD tenant.

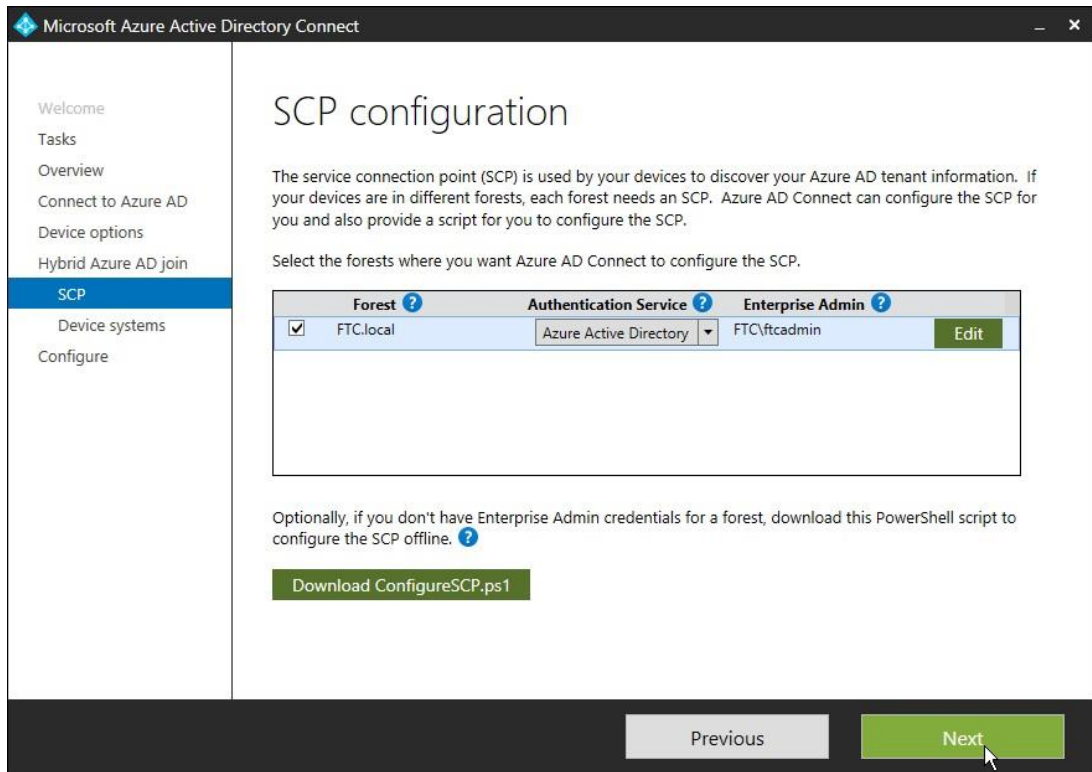


The screenshot shows the 'Microsoft Azure Active Directory Connect' application window. The title bar reads 'Microsoft Azure Active Directory Connect'. On the left, a navigation pane lists 'Welcome', 'Tasks', 'Overview', 'Connect to Azure AD' (highlighted in blue), and 'Device options'. The main content area is titled 'Connect to Azure AD' and prompts the user to 'Enter your Azure AD global administrator credentials for Mlab18.onmicrosoft.com - AAD.' Below this, there are two input fields: 'USERNAME' containing 'maiaadmin@mlab18.onmicrosoft.com' and 'PASSWORD' containing a series of dots. At the bottom right, there are two buttons: 'Previous' (disabled) and 'Next' (active, highlighted in green).

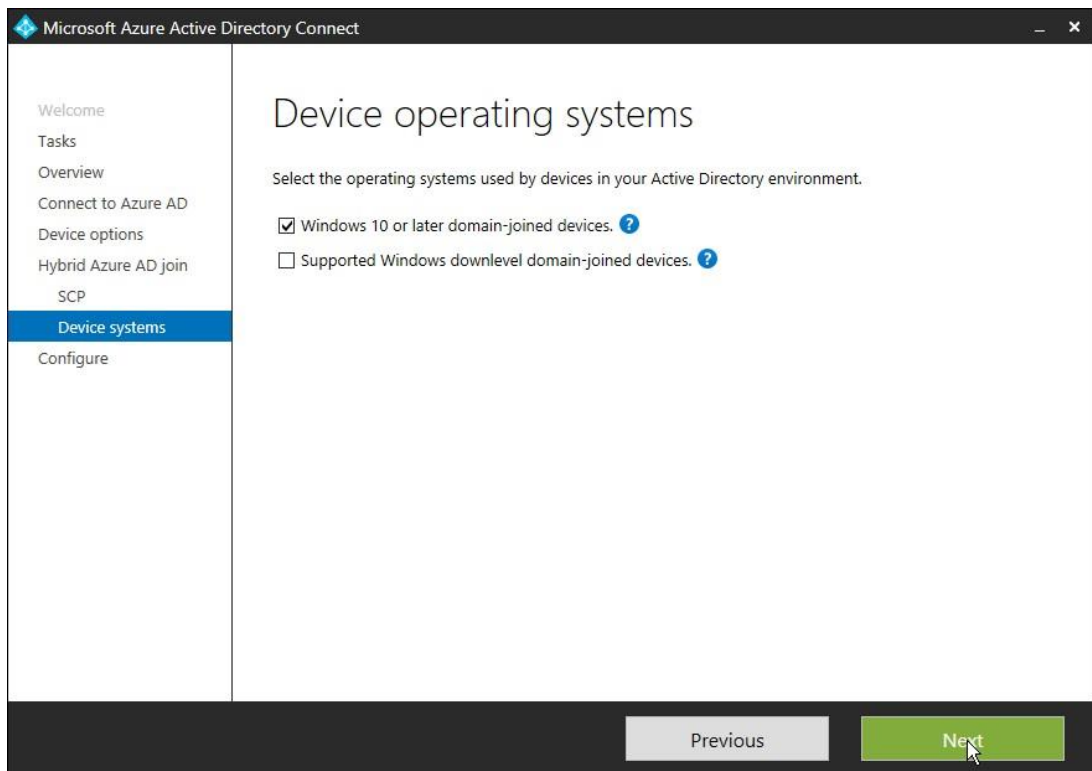
5. On the **Device options** page, select **Configure Hybrid Azure AD join**, and then click **Next**.



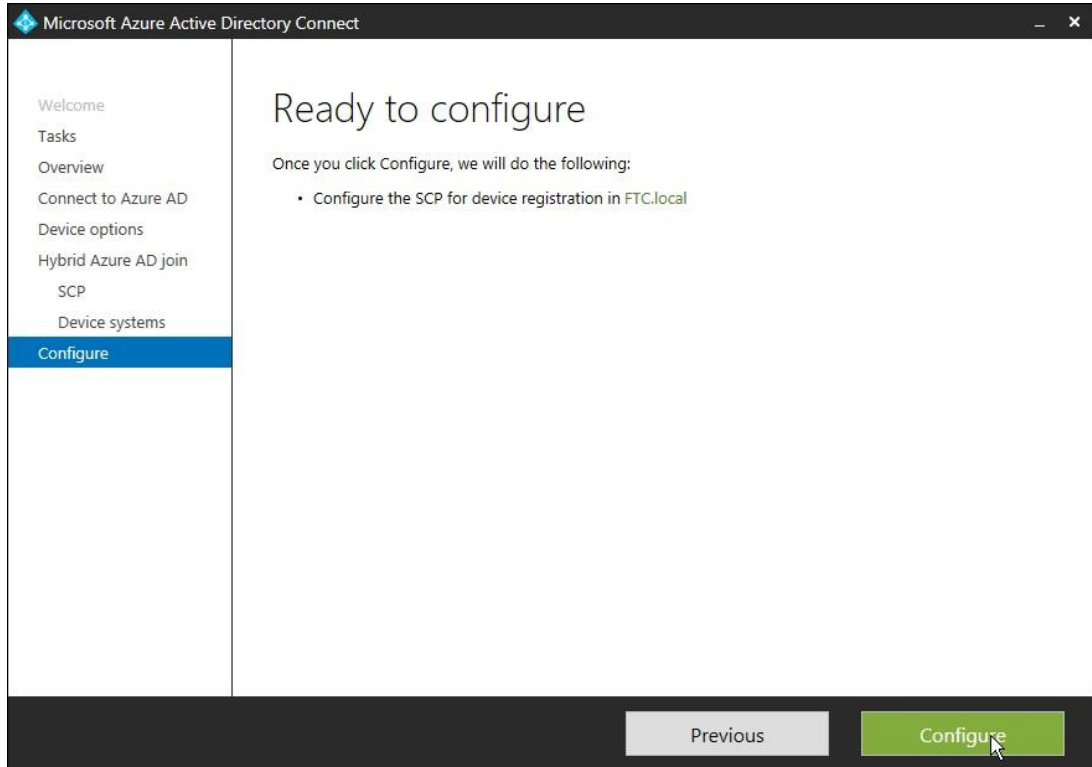
6. On the **SCP** page, for each forest you want Azure AD Connect to configure the SCP, perform the following steps, and then click **Next**:
 - Select the forest.
 - Select the authentication service.
 - Click **Add** to enter the enterprise administrator credentials.



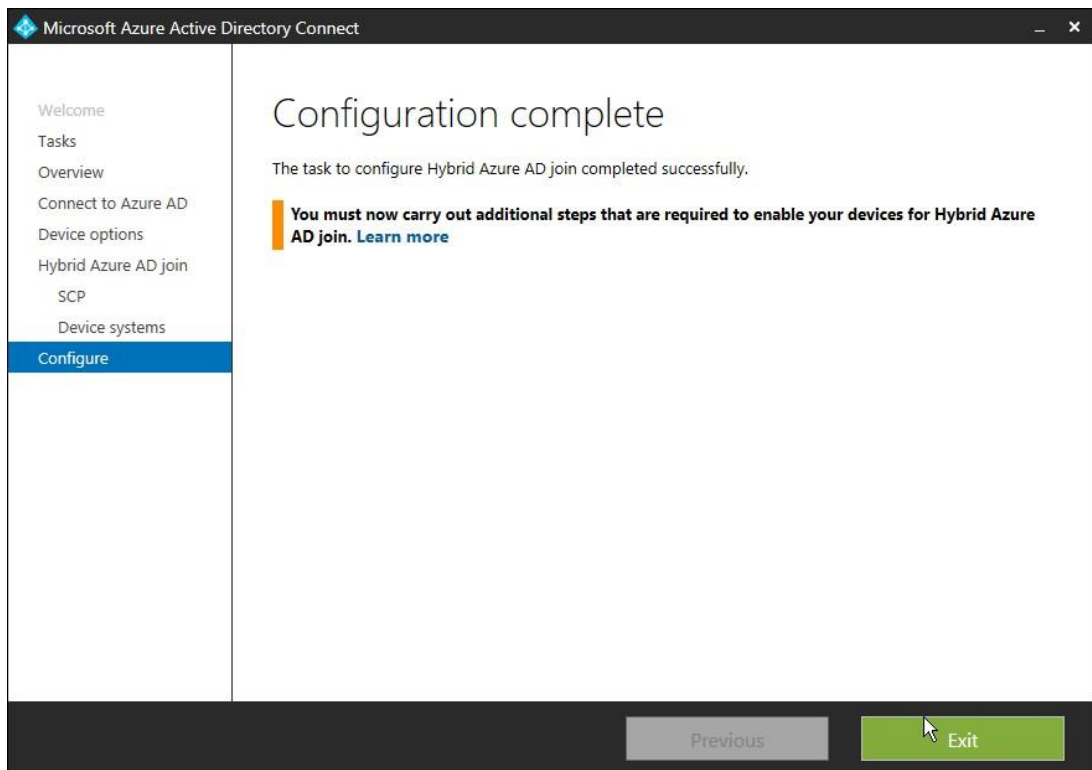
7. On the **Device operating systems** page, select the operating systems used by devices in your Active Directory environment, and then click **Next**.



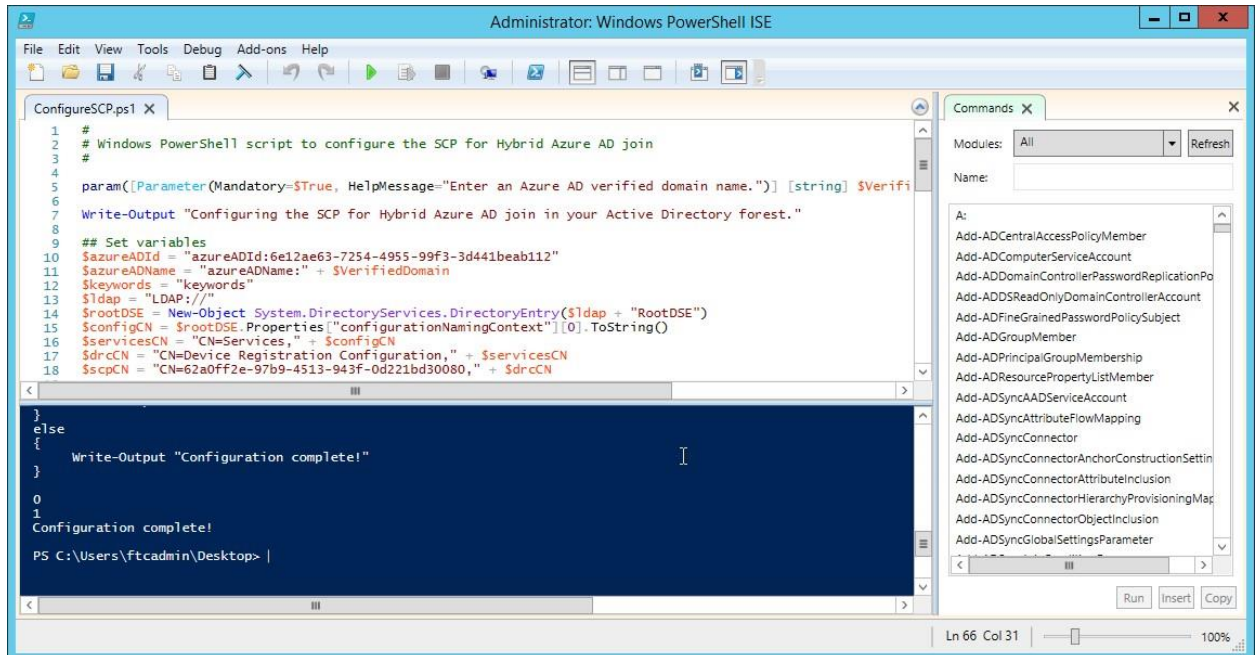
8. On the **Ready to configure** page, click **Configure**.



9. On the **Configuration complete** page, click **Exit**.



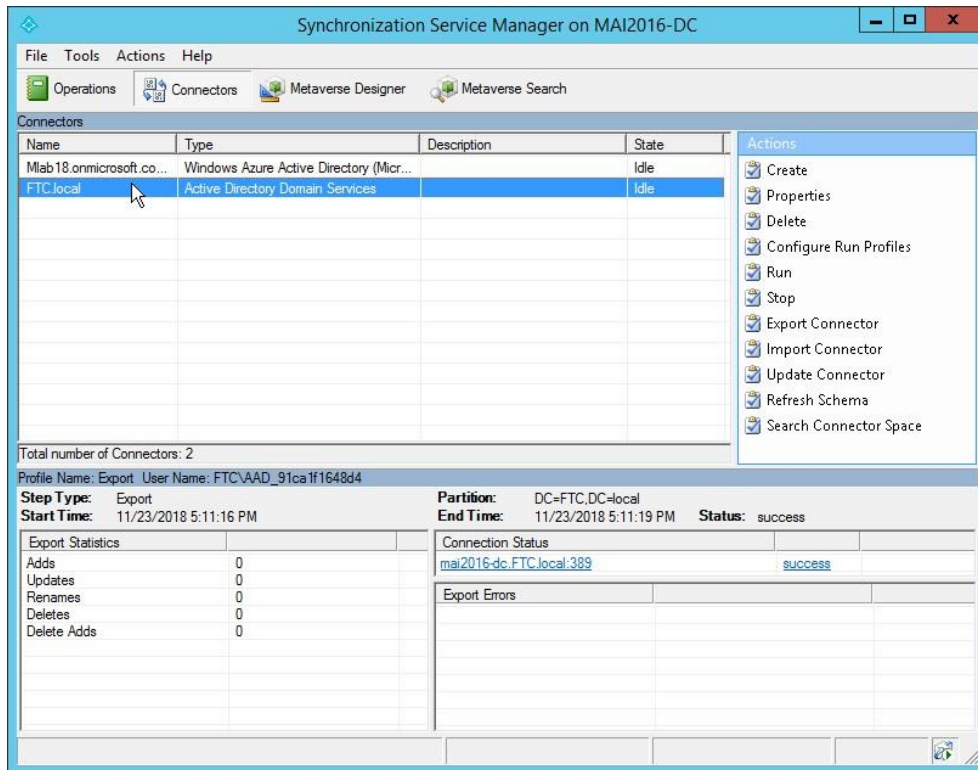
Note: In Case, SCP don't apply automatic from AD connect, you can download Configure SCP script from step 6 and run it on your AD, it will ask you to enter your verified domain. The result of the script should be configuration complete as below screenshot.



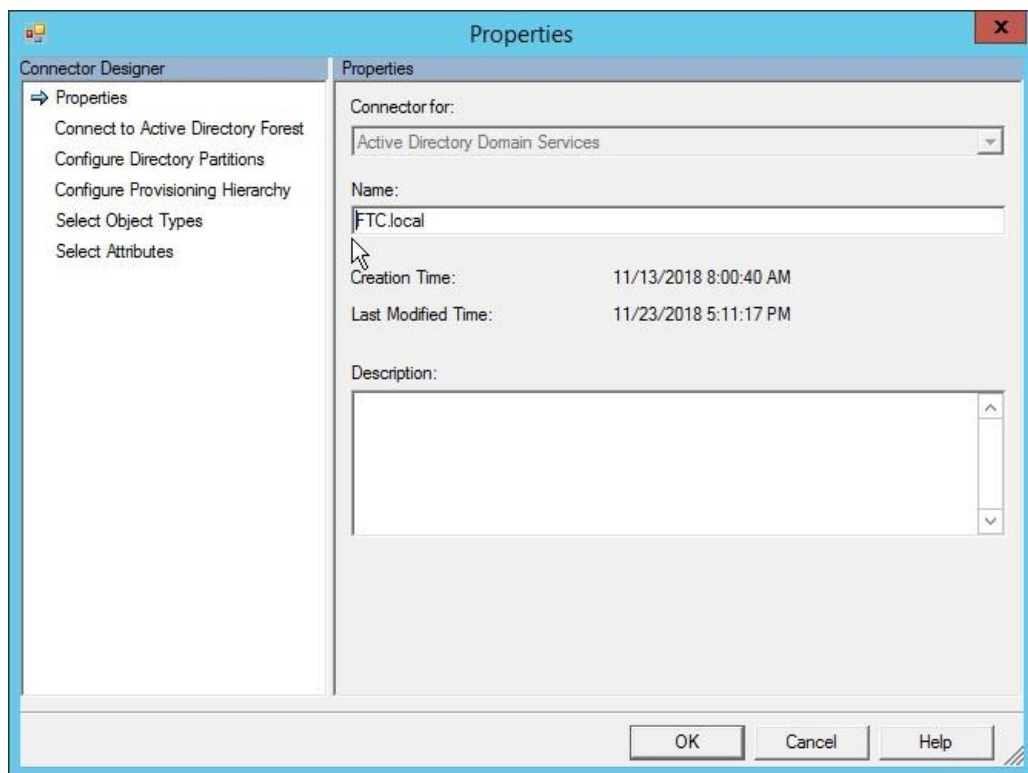
```
1 #
2 # Windows PowerShell script to configure the SCP for Hybrid Azure AD join
3 #
4
5 param([Parameter(Mandatory=$True, HelpMessage="Enter an Azure AD verified domain name.")] [string] $VerifiedDomain)
6
7 Write-Output "Configuring the SCP for Hybrid Azure AD join in your Active Directory forest."
8
9 ## Set variables
10 $azureADId = "azureADId:6e12ae63-7254-4955-99f3-3d441beab112"
11 $azureADName = "azureADName:" + $VerifiedDomain
12 $keywords = "keywords"
13 $ldap = "LDAP://"
14 $rootDSE = New-Object System.DirectoryServices.DirectoryEntry($ldap + "RootDSE")
15 $configCN = $rootDSE.Properties["configurationNamingContext"][0].ToString()
16 $servicesCN = "CN=Services," + $configCN
17 $drcCN = "CN=Device Registration Configuration," + $servicesCN
18 $scpCN = "CN=62a0ff2e-97b9-4513-943f-0d221bd30080," + $drcCN
19
20 }
21 else
22 {
23     Write-Output "Configuration complete!"
24 }
25 }
26 0
27 1
28 Configuration complete!
29
30 PS C:\Users\ftcadmin\Desktop>
```

10. Azure AD connect has synchronized all the computer objects of the devices you want to be hybrid Azure AD joined. If the computer objects belong to specific organizational units (OU), then make sure these OUs are set for synchronization in Azure AD connect as well.

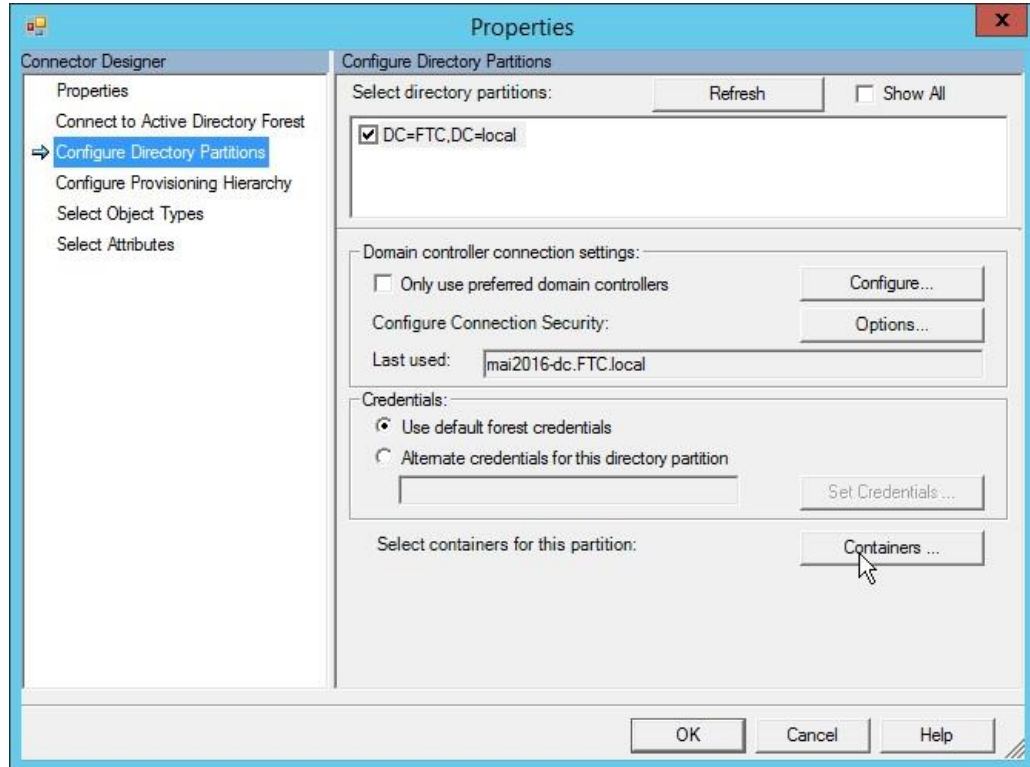
- a) Open **Synchronization Service**, Select **Active Directory Domain services** management agent.



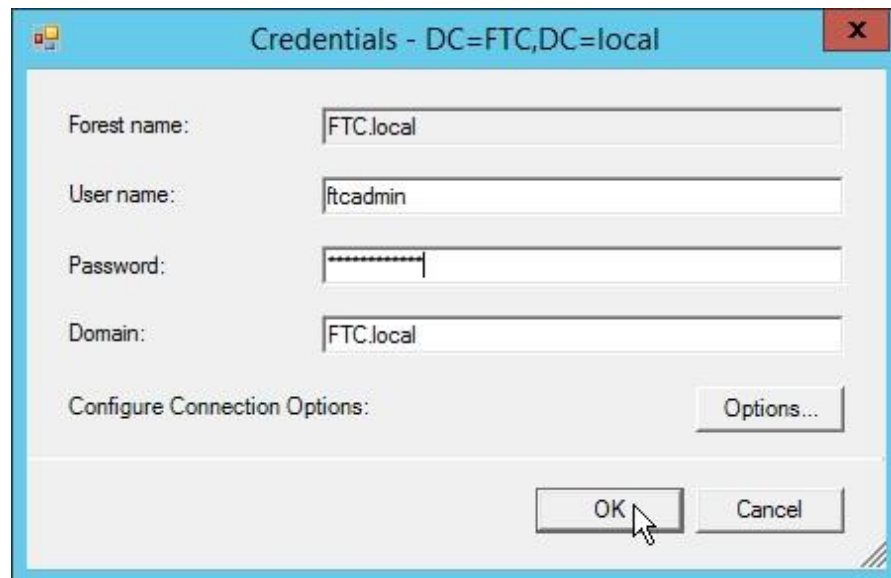
- b) Right Click on Active Directory management agent, Click **properties**.
- c) On **Properties** tab, Select **Configure Directory partitions**.



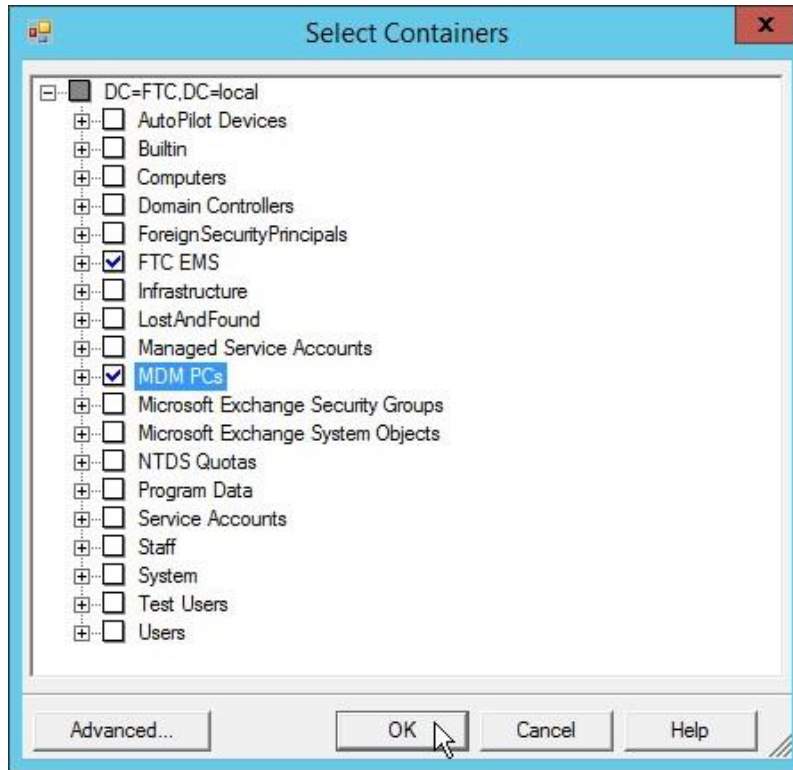
d) On **Configure Directory Partitions** blade, Click **Containers**.



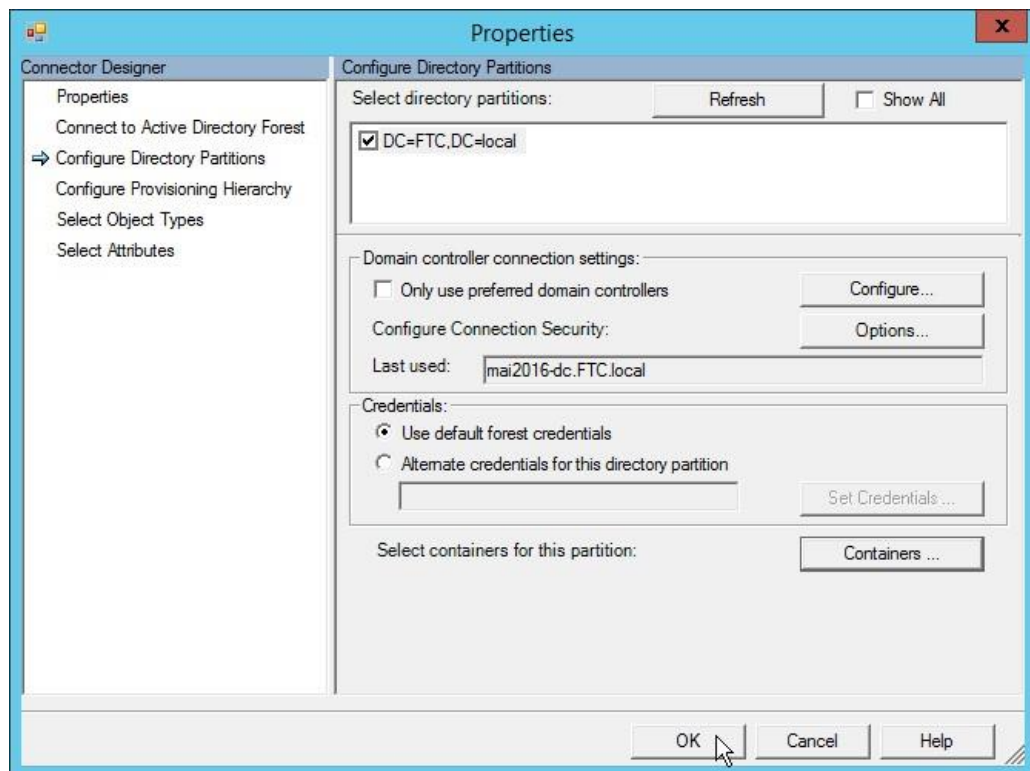
e) Enter credentials of Active Directory.



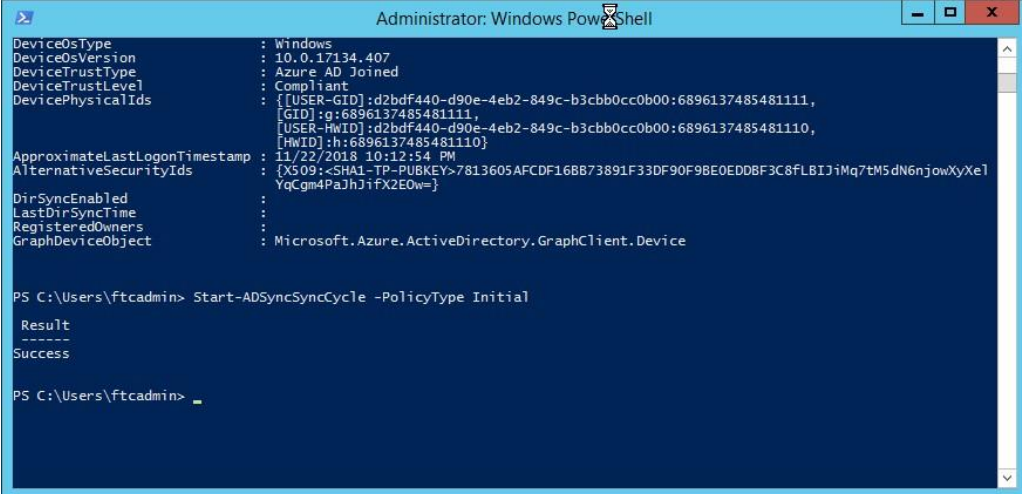
f) Select **Computers OU**.



g) Click **OK**.



h) Open Windows PowerShell, run command *Start-ADSyncCycle -PolicyType Initial*



```
Administrator: Windows PowerShell
DeviceOsType : Windows
DeviceOsVersion : 10.0.17134.407
DeviceTrustType : Azure AD Joined
DeviceTrustLevel : Compliant
DevicePhysicalIds : {[USER-GID]:d2bdf440-d90e-4eb2-849c-b3cbb0cc0b00:6896137485481111,
                    [GID]:g:6896137485481111,
                    [USER-HWID]:d2bdf440-d90e-4eb2-849c-b3cbb0cc0b00:6896137485481110,
                    [HWID]:h:6896137485481110}
ApproximateLastLogonTimestamp : 11/22/2018 10:12:54 PM
AlternativeSecurityIds : {XS09;<SHA1-TP-PUBKEY>7813605AFCDF16BB73891F33DF90F9BE0EDD8F3C8F8LBIjIMq7EM5dN6njowXyXe1
                        YqCgm4PaJhJiFX2E0w=}
DirSyncEnabled :
LastDirSyncTime :
RegisteredOwners :
GraphDeviceObject : Microsoft.Azure.ActiveDirectory.GraphClient.Device

PS C:\Users\ftcadmin> Start-ADSyncSyncCycle -PolicyType Initial

Result
-----
Success

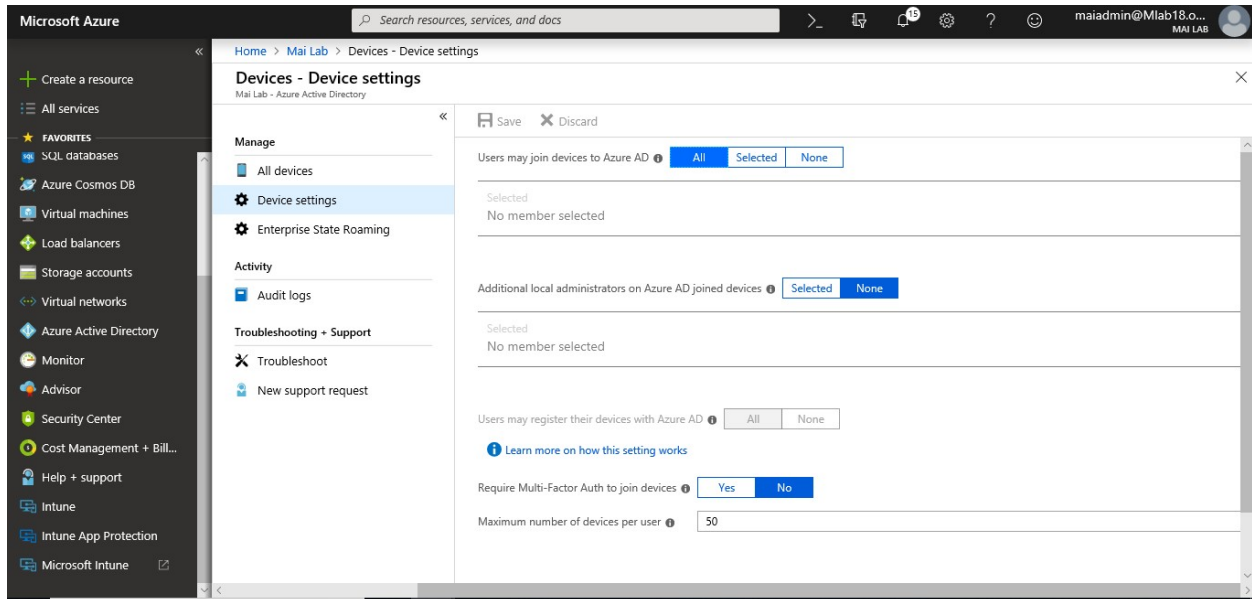
PS C:\Users\ftcadmin> _
```

Note: you can add specific OU by running AD connect and select customize synchronization option and run wizard. You should run AD Connect at least version 1.1.819.0 to find configure hybrid Azure AD join option.

Step 2: Update device settings

To register Windows down-level devices, you need to make sure that the device settings to allow users to register devices in Azure AD are set. In the [Azure portal](#) > Azure Active Directory > Devices, you can find this setting under:

The following policy must be set to **All: Users may register their devices with Azure AD**



Step 3: Create GPO for MDM Enrollment.

If you have Active Directory 2012 R2 & your group policy don't contain following group policy. To import administrative template for windows 10. You need to follow below steps:

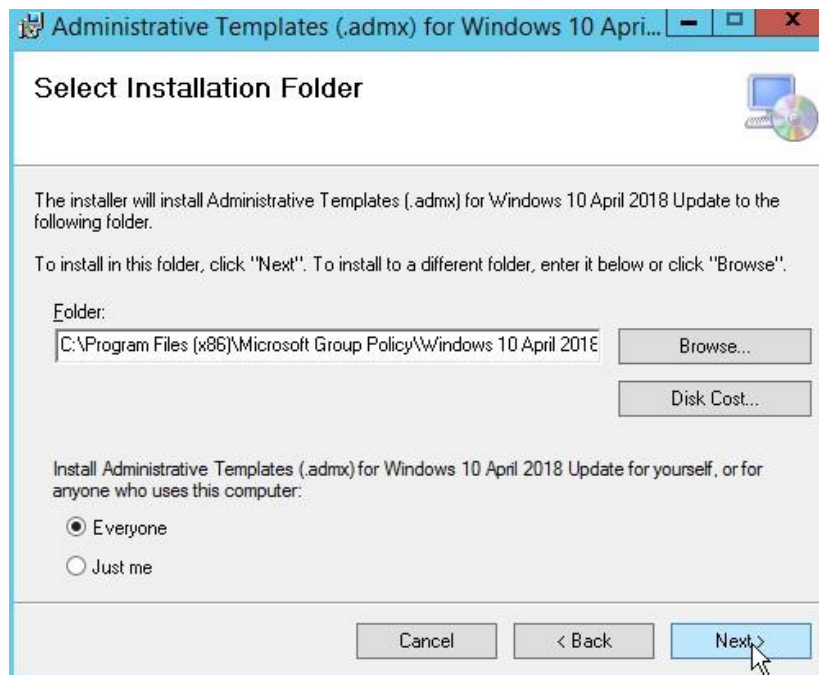
1. Download [administrative template](#) for windows 10 and Run wizard to install this window 10 template.



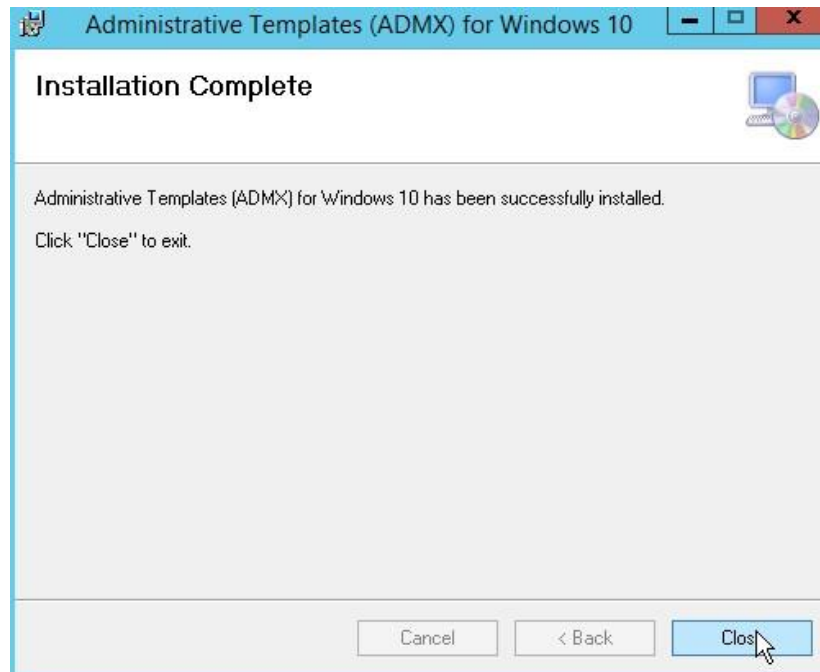
2. On **License Agreement** page, Select **I agree** and click **Next**.



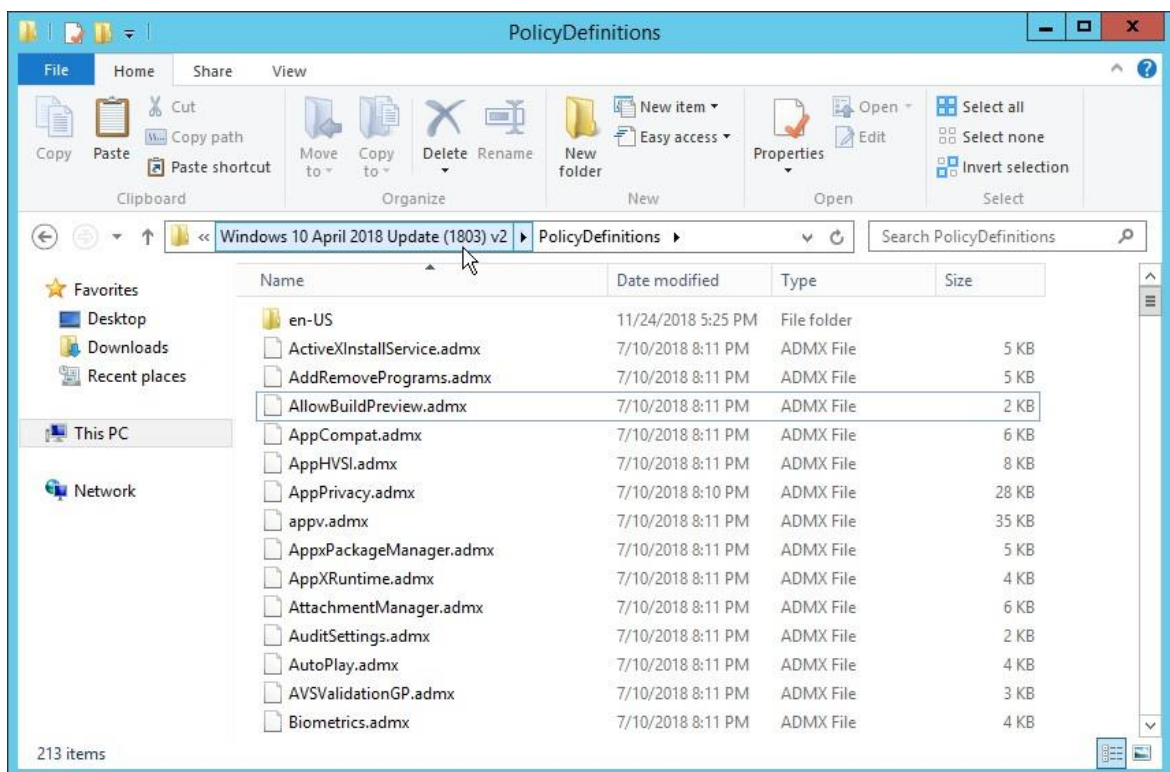
3. On **Select Installation folder**, click **Next**.



4. Click **Next** on confirm installation. Then click **Close**.

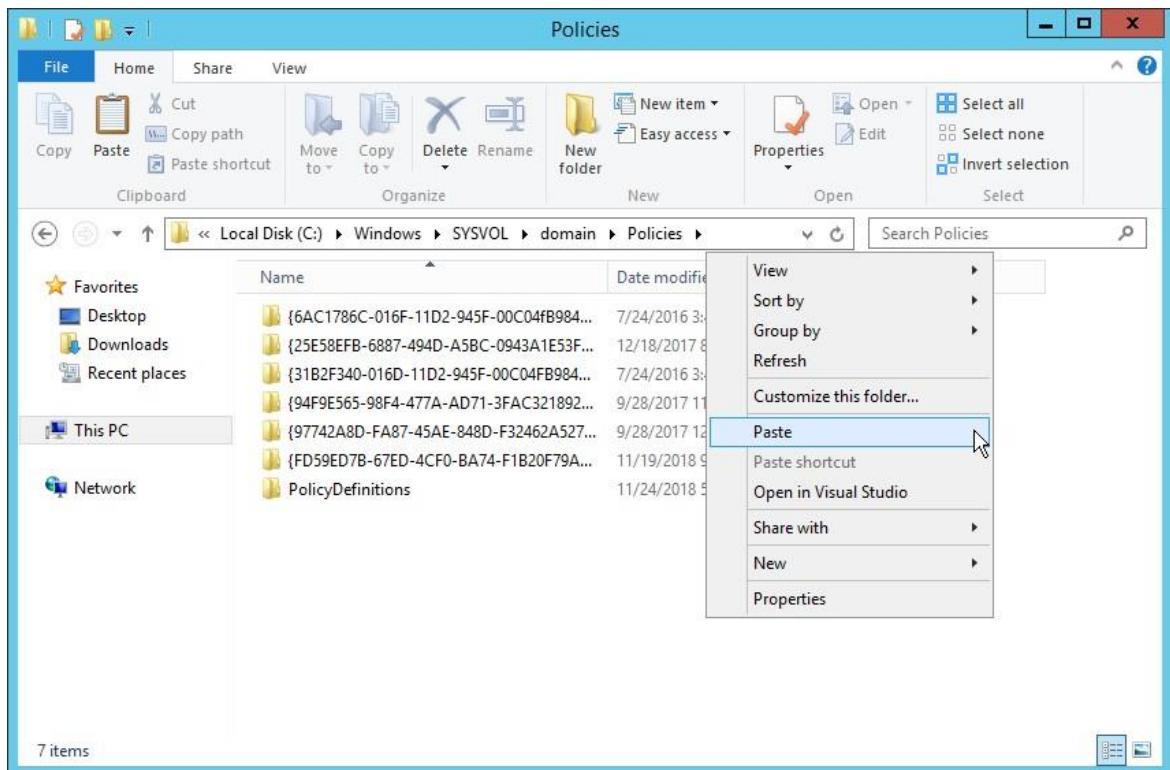
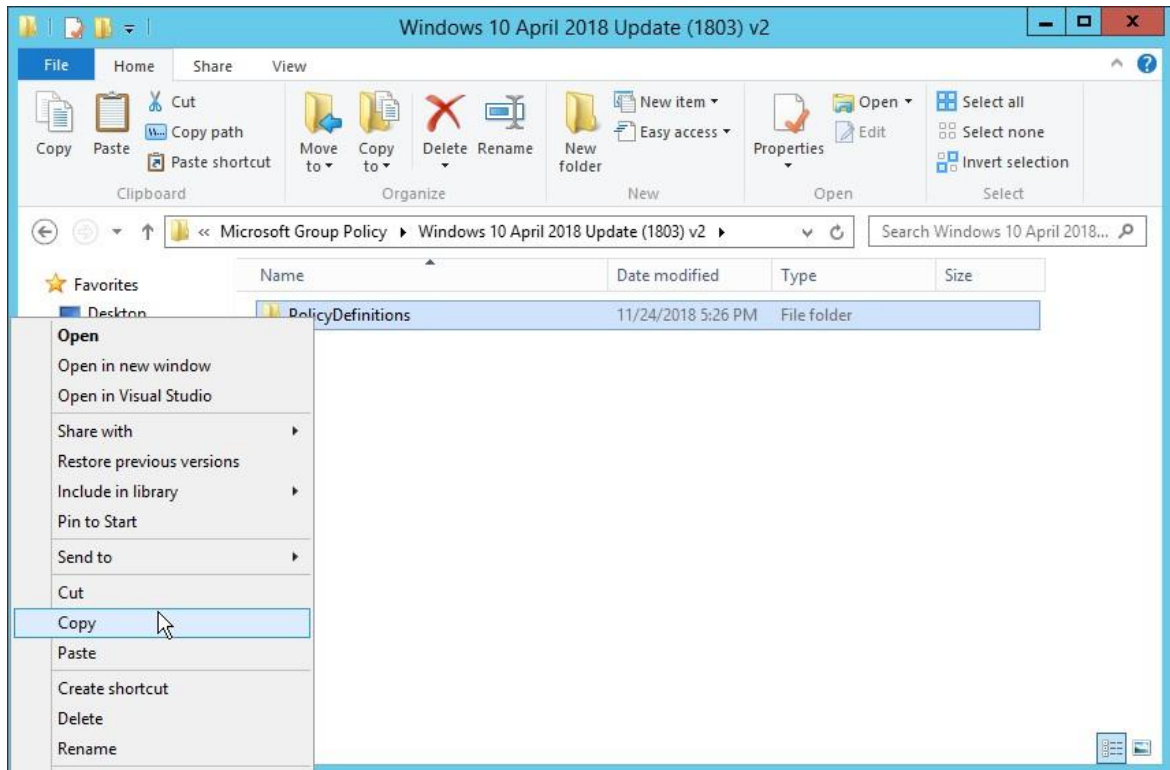


5. Delete all other languages & leave English and all ADMX files.

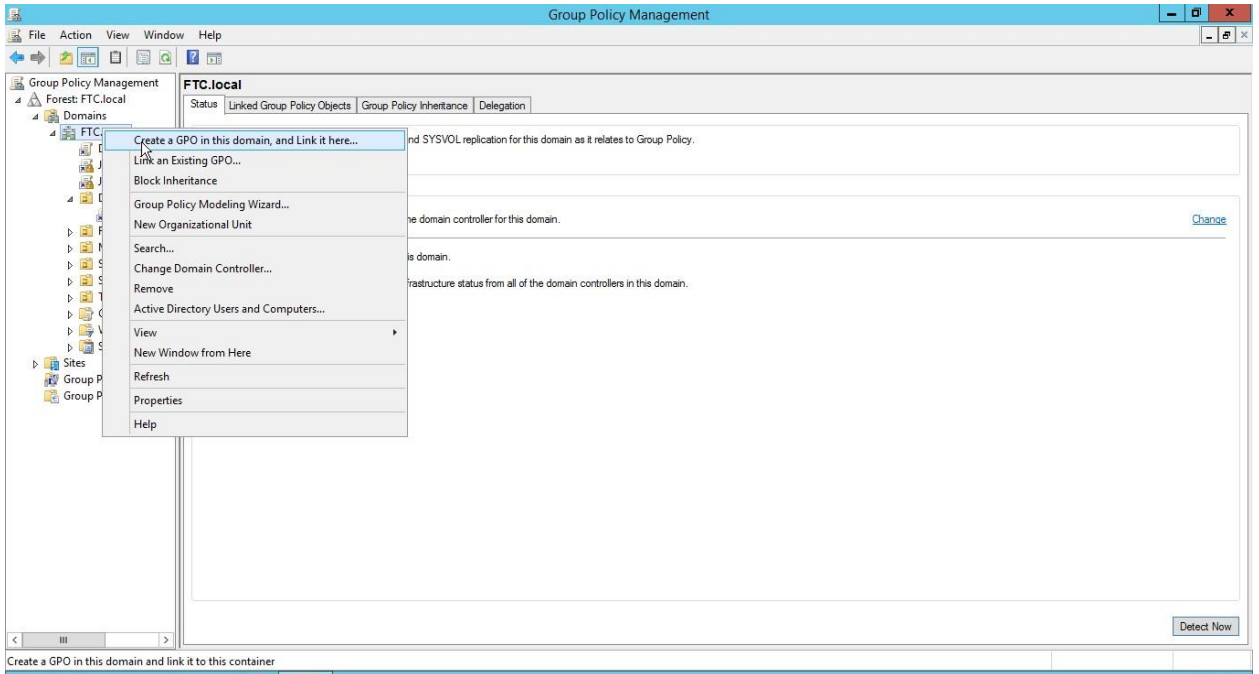


6. Copy all ADMX files from *C:\Program Files (x86)\Microsoft Group Policy\Windows 10\PolicyDefinitions* to *C:\windows\sysvol\domain\policies*

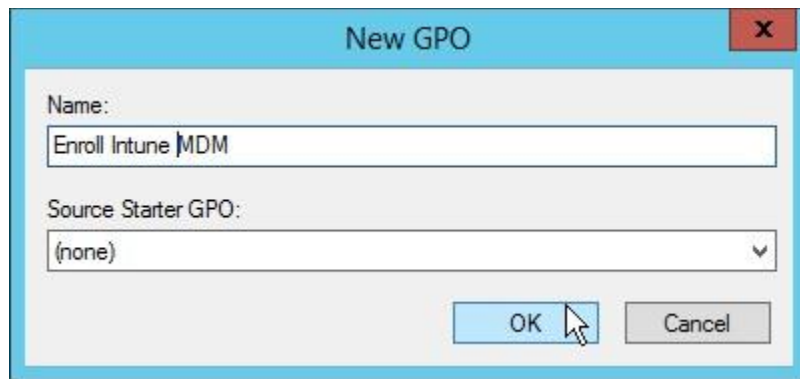
Microsoft Intune step by step on Azure portal



7. Open start menu, Type **gpedit.msc**.
8. On Group Policy Management, right click on domain, Select **Create a GPO in this domain and link it here**.

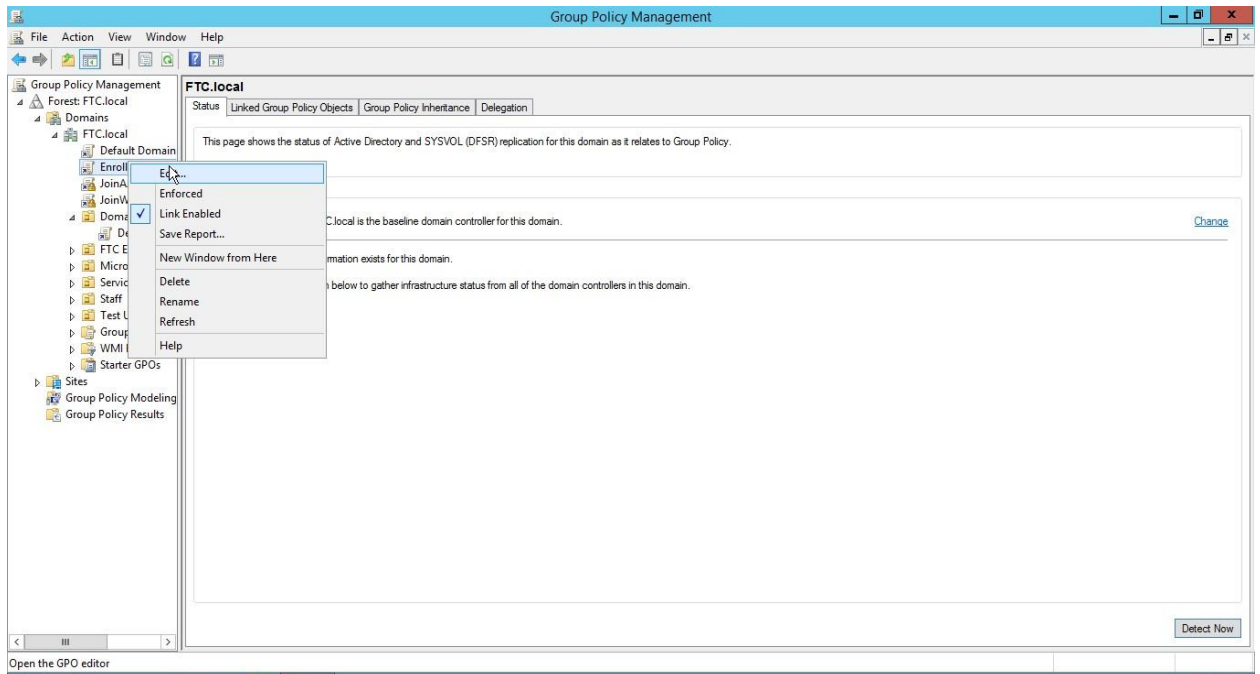


9. Enter Name for your GPO.

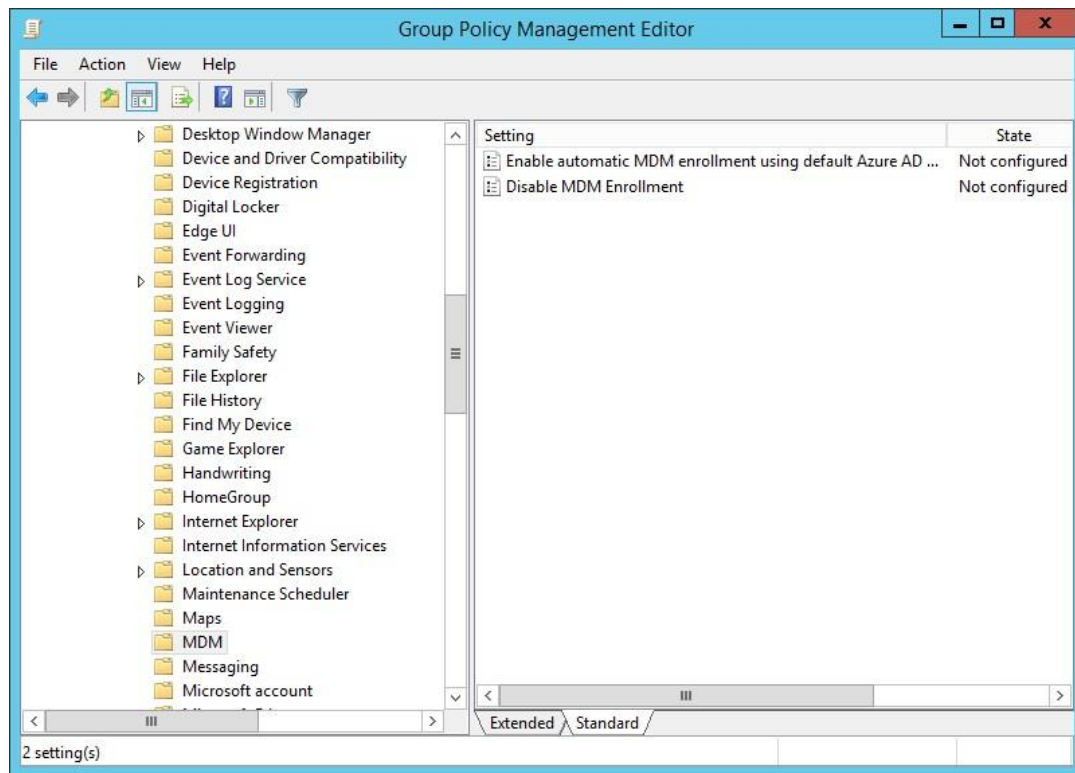


10. On Group Policy Management, select your GPO and right click **Edit**.

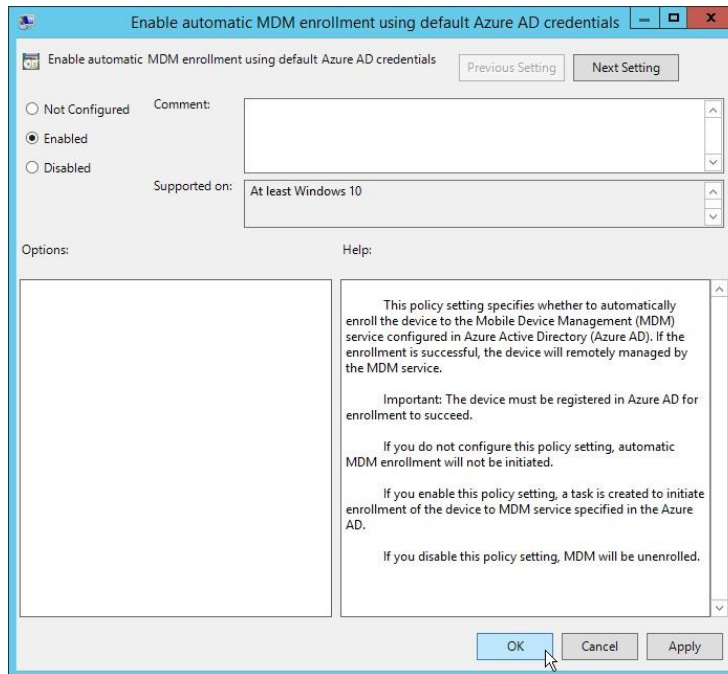
Microsoft Intune step by step on Azure portal



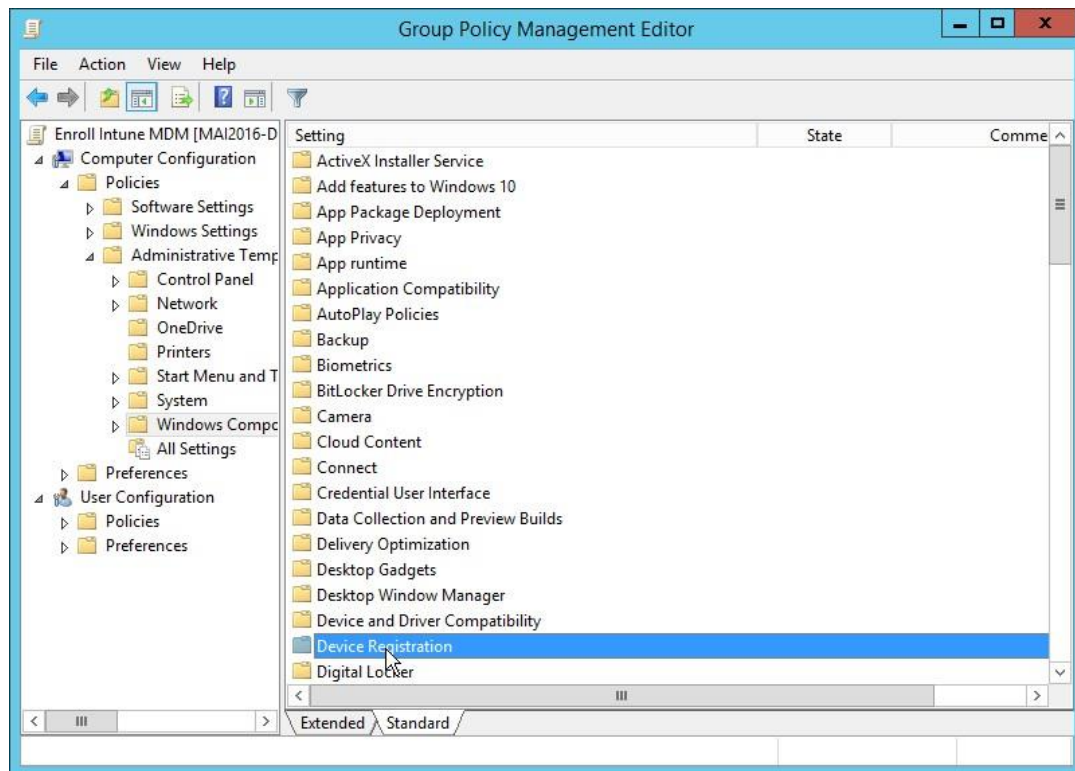
11. Go to **Computer Configuration > Policies > Administrative Templates > Windows Components > MDM**



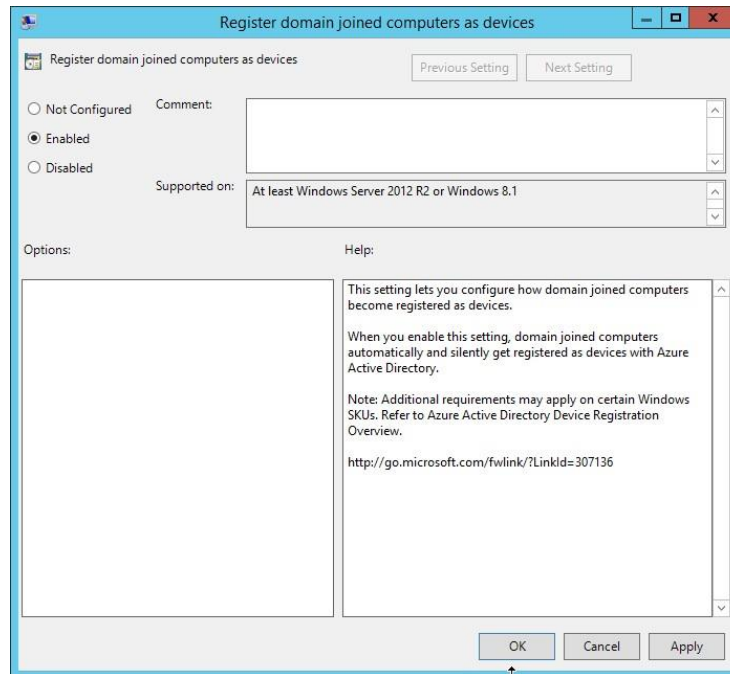
12. Open **Auto MDM Enrollment with AAD Token setting**, choose Enabled, then click OK.



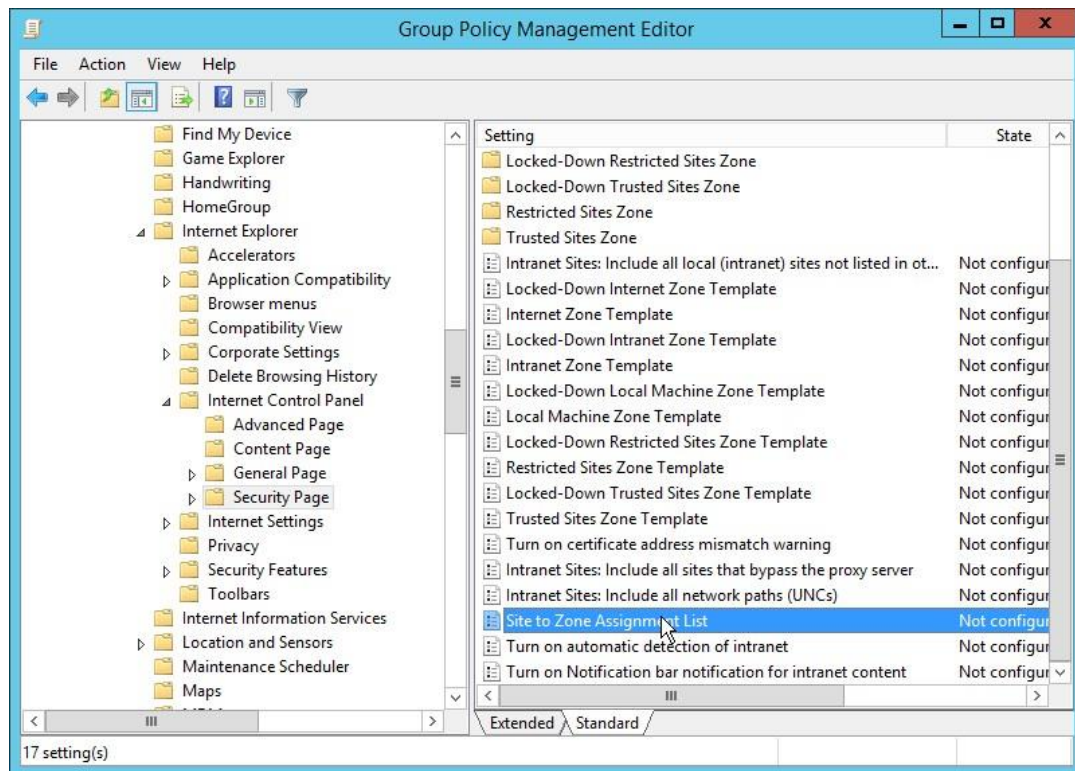
13. Go then to **Computer Configuration > Policies > Administrative Templates > Windows Components > Device Registration.**



14. Open **Register domain joined computers as devices**, choose Enabled, then click OK.

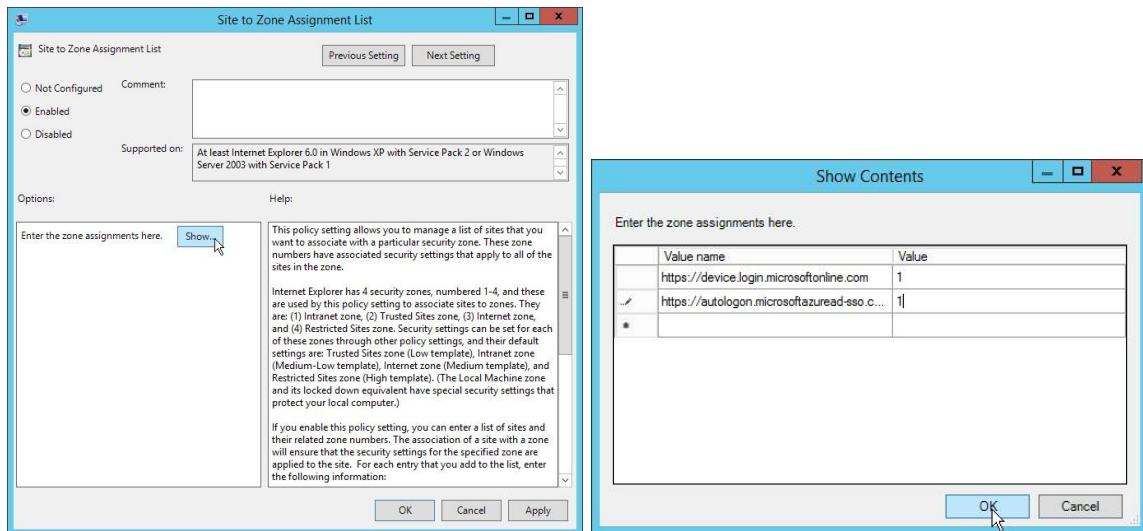


15. Go to **Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page.**

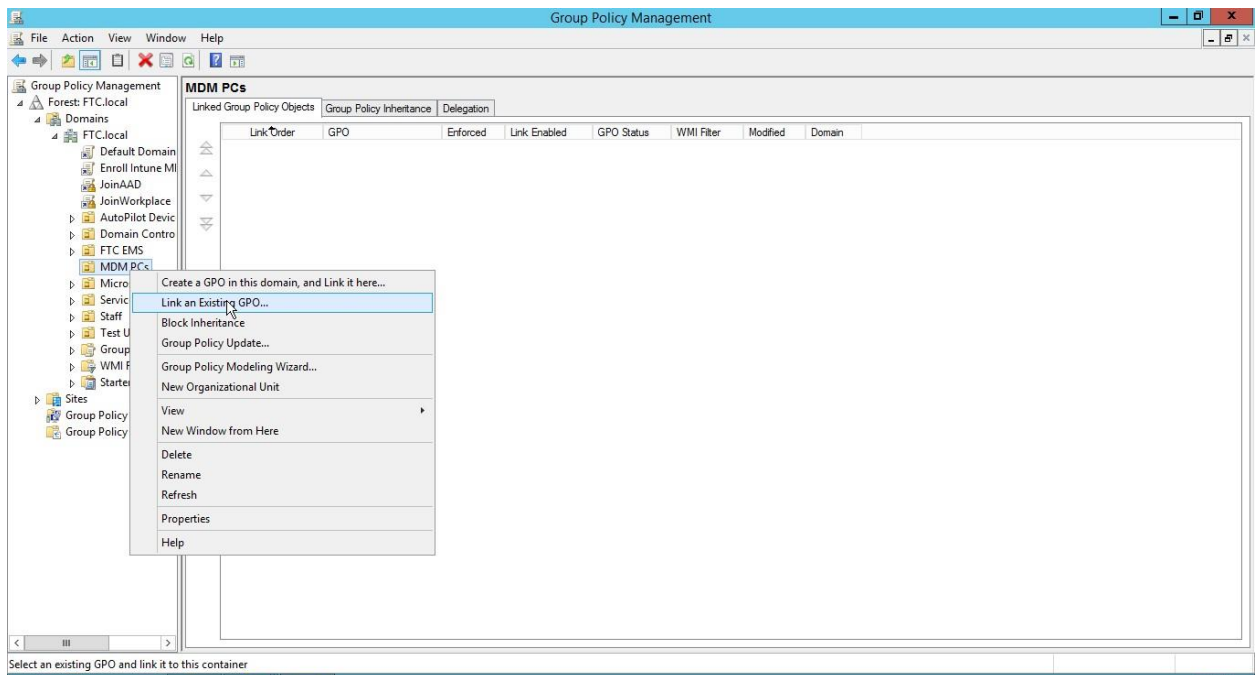


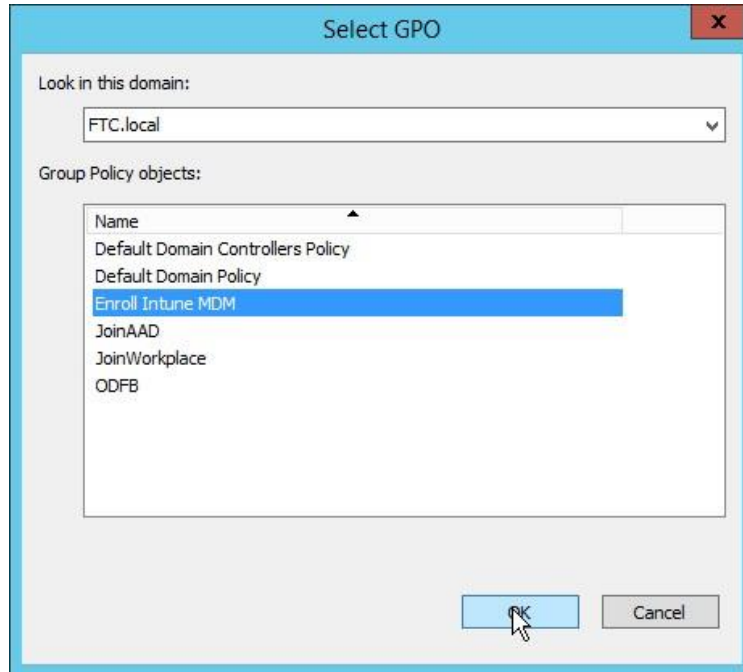
16. Open **Site to Zone Assignment List**, choose Enabled, click then on Show under Options and add:

https://device.login.microsoftonline.com with the value 1 for it,
https://autologon.microsoftazuread-ssocombi.com with the value 1 for it to end up under Local Intranet Zone.

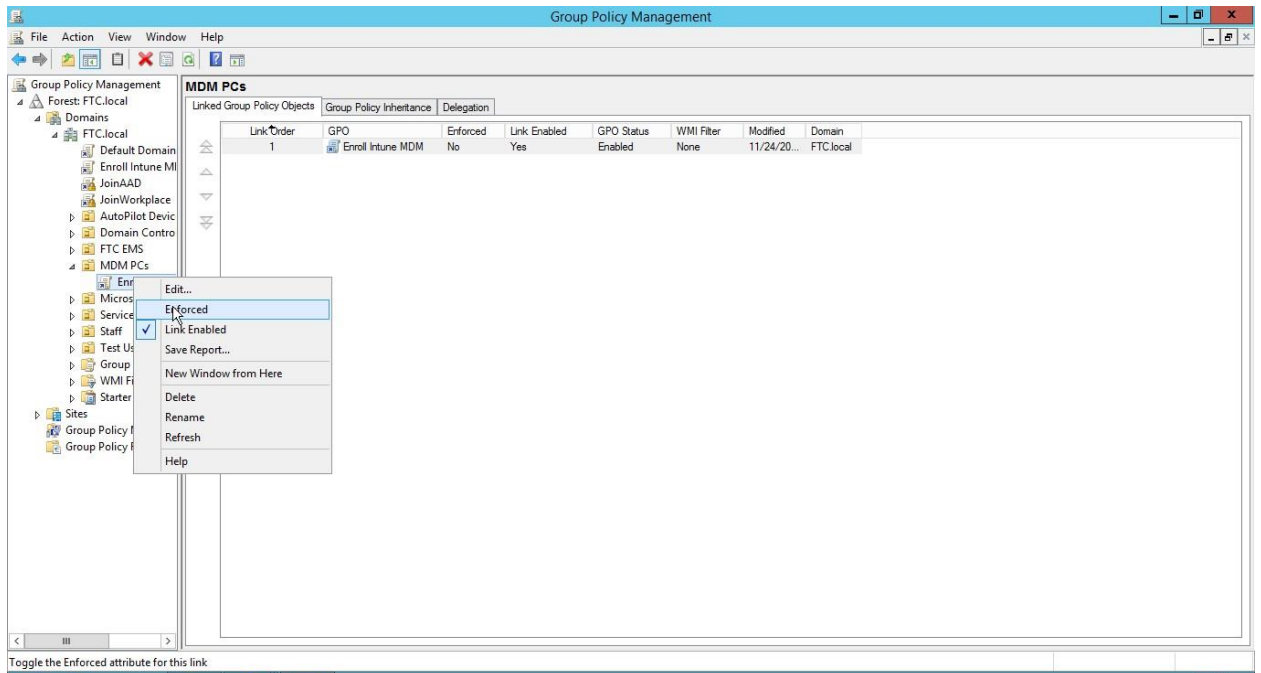


17. On **Group Policy Management** console, Select Computer OU that you want to apply policy on it, right click **link an existing GPO**.





18. You can enforce policy to applied in this OU if you have many policies. On link GPO, select **Enforced**.



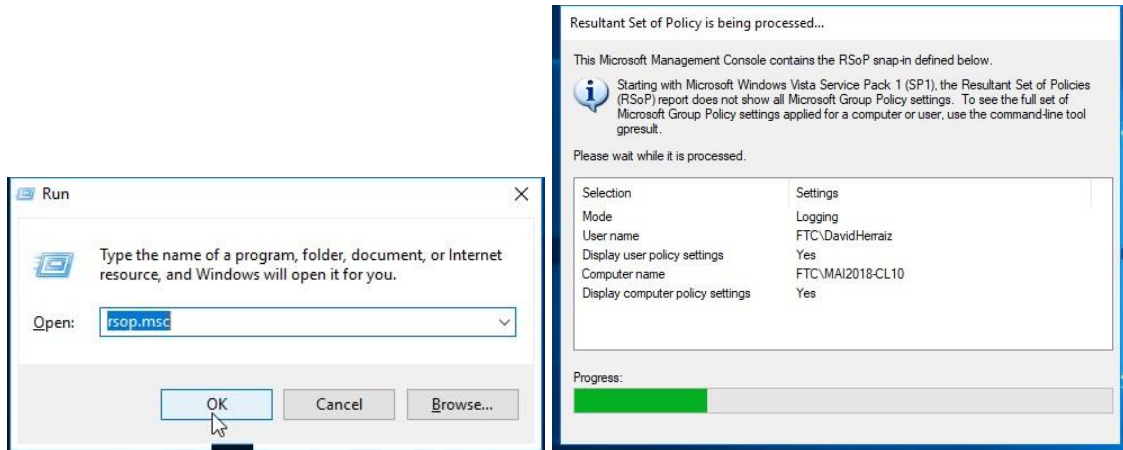
19. Open Command prompt, Run *gpedit /force*.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.16299.611]
(c) 2017 Microsoft Corporation. All rights reserved.

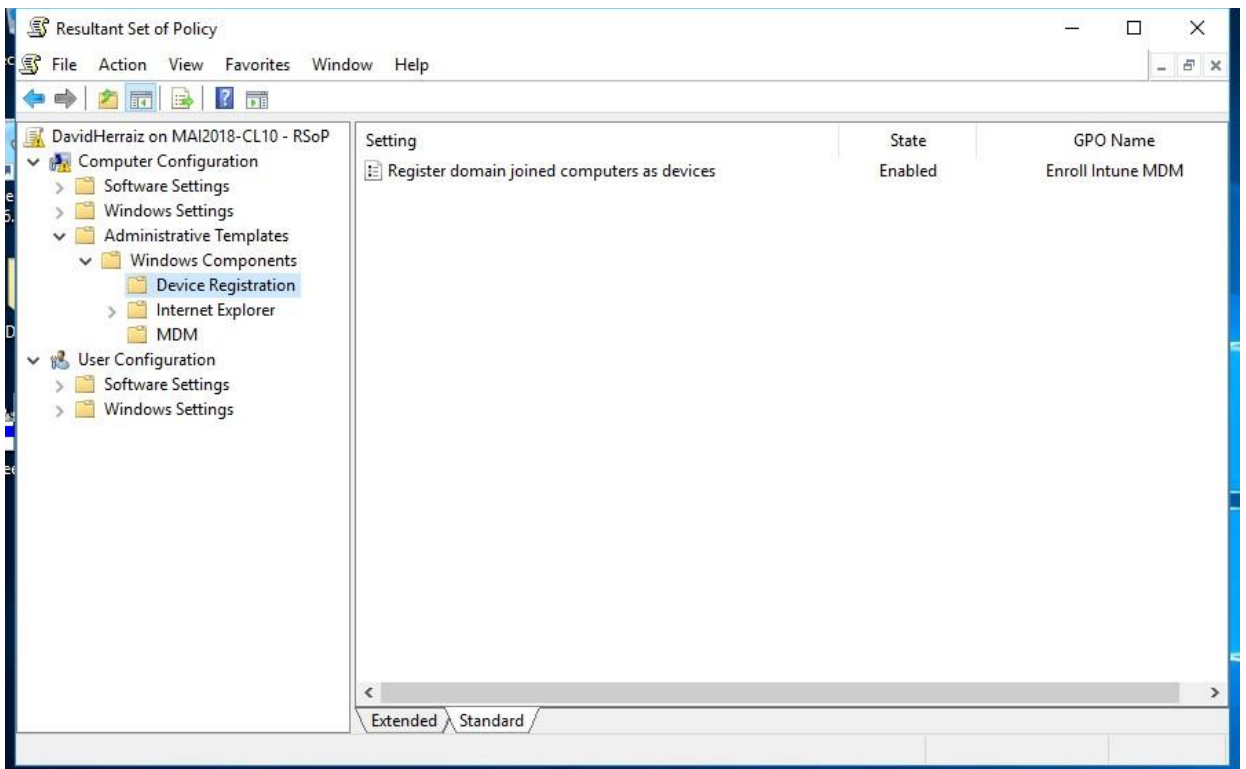
C:\Users\davidherriz>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

20. On Client PC, Type **rsop.msc**. to check that GPO is applied.



21. On **Resultant set of Policy**, you should find all policy that you apply from DC.



Microsoft Intune step by step on Azure portal

Note: The above policy can be applying on windows 10 machine direct.

Step 4: Verify the registration.

1. Open [Azure admin portal](#) > **Azure Active Directory**> **Devices**. You should find PC appear that it's managed by Microsoft Intune

NAME	ENABLED	OS	VERSION	JOIN TYPE	OWNER	MDM	COMPLI...	REGISTERED	ACTIVITY
MAI2018-CL10	Yes	Windows	10.0.162...	Hybrid Azure...	N/A	Microsoft Intune	Yes	11/24/2018 11...	11/24/2...
Mai2018-cl1803	Yes	Windows	10.0.177...	Azure AD join...	User 2	Microsoft Intune	Yes	11/19/2018 11...	11/19/20...
Mai2018-Pro1...	Yes	Window...	10.0 (171...	Hybrid Azure...	N/A	None	N/A	N/A	N/A
DESKTOP-RU...	Yes	Windows	10.0.171...	Azure AD join...	User 4	None	No	11/22/2018 3...	11/22/2...
MAI2016-CL2	Yes	Windows	10.0.162...	Azure AD regi...	User 1	None	Yes	11/19/2018 11...	11/19/20...
U2_Android_1...	Yes	Android	8.0.0	Azure AD regi...	User 2	Microsoft Intune	Yes	11/14/2018 3:3...	11/14/20...
MAI2016-DC	Yes	Window...	6.3 (9600)	Hybrid Azure...	N/A	None	N/A	N/A	N/A
Mai2018-CI1809	Yes	Windows	10.0.171...	Azure AD join...	User 5	Microsoft Intune	Yes	11/23/2018 1:1...	11/23/2...

2. Open [Azure admin portal](#) > **Intune** > **Device Compliance** > **Device Compliance**. You should find PC appear

DEVICE NAME	USER PRINCIPAL NAME	MANAGED BY	COMPLIANCE	OS	OS VERSION
MAI2016-CL2	UI@Mlab18.onmicrosof...	MDM/ConfigMgr Agent	See ConfigMgr	Windows	10.0.16299.4
MAI2018-CL10	DavidHerraiz@miracleit...	MDM	Compliant	Windows	10.0.16299.7
Mai2018-cl1803	U2@Mlab18.onmicroso...	MDM	Compliant	Windows	10.0.17763.1
Mai2018-CI1809	U5@miracleit.net	MDM	Compliant	Windows	10.0.17134.4
MAI2018-CL3	u3@m1ab18.onmicrosof...	MDM/ConfigMgr Agent	See ConfigMgr	Windows	10.0.16299.4
U2_Android_11/14/2018...	U2@Mlab18.onmicroso...	MDM	Compliant	Android	8.0.0

- From admin PowerShell, run below command:

Install-Module MSOnline
Install-Module AzureADPreview
Connect-MsolService



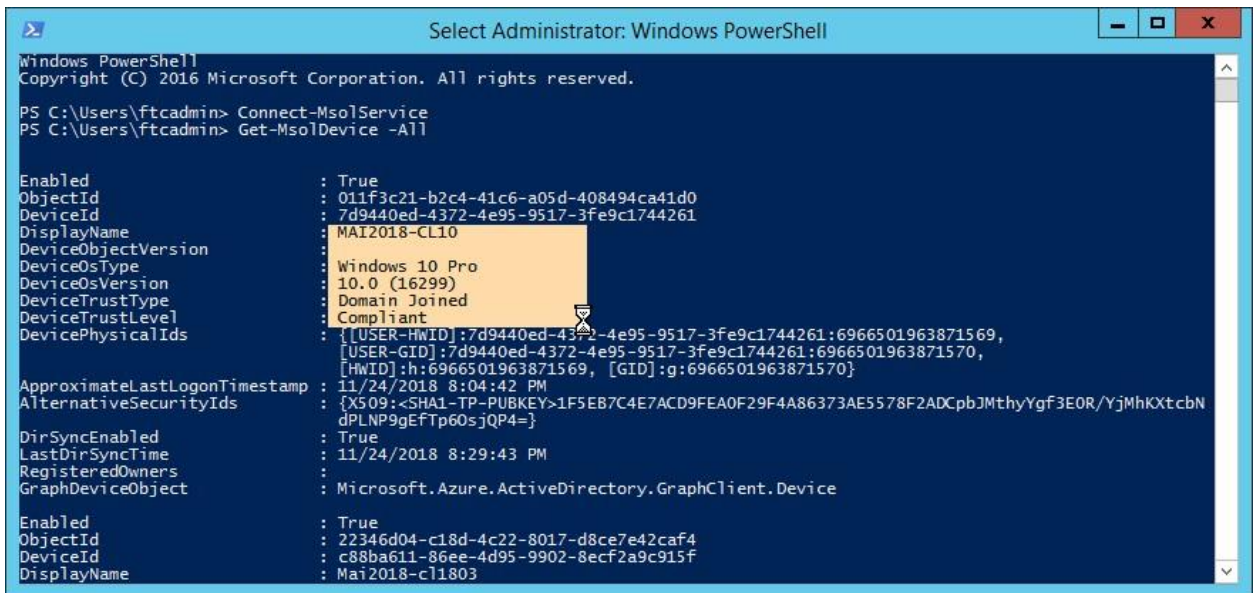
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\ftcadmin> Install-Module MSOnline

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
PS C:\Users\ftcadmin> Install-Module AzureADPreview

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
PS C:\Users\ftcadmin> Connect-MsolService_
```

Get-msoldevice -All



```
Select Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\ftcadmin> Connect-MsolService
PS C:\Users\ftcadmin> Get-MsolDevice -All

Enabled : True
ObjectId : 011f3c21-b2c4-41c6-a05d-408494ca41d0
DeviceId : 7d9440ed-4372-4e95-9517-3fe9c1744261
DisplayName : MAI2018-CL10
DeviceObjectVersion :
DeviceOsType : Windows 10 Pro
DeviceOsVersion : 10.0 (16299)
DeviceTrustType : Domain Joined
DeviceTrustLevel : Compliant
DevicePhysicalIds : {[USER-HWID]:7d9440ed-4372-4e95-9517-3fe9c1744261:6966501963871569,
[USER-GID]:7d9440ed-4372-4e95-9517-3fe9c1744261:6966501963871570,
[HWID]:h:6966501963871569, [GID]:g:6966501963871570}
ApproximateLastLogonTimestamp : 11/24/2018 8:04:42 PM
AlternativeSecurityIds : {X509:<SHA1-TP-PUBKEY>1F5EB7C4E7ACD9FEA0F29F4A86373AE5578F2ADCpbJMthyYgf3E0R/YjMhKXtcbn
dPLNP9gEFTp60sjQP4=}
DirSyncEnabled : True
LastDirSyncTime : 11/24/2018 8:29:43 PM
RegisteredOwners :
GraphDeviceObject : Microsoft.Azure.ActiveDirectory.GraphClient.Device

Enabled : True
ObjectId : 22346d04-c18d-4c22-8017-d8ce7e42caf4
DeviceId : c88ba611-86ee-4d95-9902-8ecf2a9c915f
DisplayName : Mai2018-cl1803
```

- From Client PC, open command prompt, run below command ***dsregcmd /status***, Check Device state should be ***AzureAdJoined*** is ***Yes***

Microsoft Intune step by step on Azure portal

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.16299.785]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\windows\system32>dsregcmd /status

-----+
| Device State |
+-----+

AzureAdJoined : YES
EnterpriseJoined : NO
DeviceId : 7d9440ed-4372-4e95-9517-3fe9c1744261
Thumbprint : 1F5EB7C4E7ACD9FEA0F29F4A86373AE5578F2ADC
KeyContainerId : b902cef0-a2a2-4108-8977-48cf96510e22
KeyProvider : Microsoft Software Key Storage Provider
TpmProtected : NO
KeySignTest : PASSED
Idp : login.windows.net
TenantId : 6e12ae63-7254-4955-99f3-3d441beab112
TenantName : Mai Lab
AuthCodeUrl : https://login.microsoftonline.com/6e12ae63-7254-4955-99f3-3d441beab112/oauth2/authorize
AccessTokenUrl : https://login.microsoftonline.com/6e12ae63-7254-4955-99f3-3d441beab112/oauth2/token
MdmUrl : https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc
MdmTouUrl : https://portal.manage.microsoft.com/TermsOfUse.aspx
MdmComplianceUrl : https://portal.manage.microsoft.com/?portalAction=Compliance
SettingsUrl :
JoinSrvVersion : 1.0
JoinSrvUrl : https://enterpriseregistration.windows.net/EnrollmentServer/device/
JoinSrvId : urn:ms-drs:enterpriseregistration.windows.net
KeySrvVersion : 1.0
KeySrvUrl : https://enterpriseregistration.windows.net/EnrollmentServer/key/
KeySrvId : urn:ms-drs:enterpriseregistration.windows.net
WebAuthNSrvVersion : 1.0
WebAuthNSrvUrl : https://enterpriseregistration.windows.net/webauthn/6e12ae63-7254-4955-99f3-3d441beab112/
```

5. Result from same command, Check **User state** should be **WamDefaultset** is **Yes**.

```
Administrator: Command Prompt

-----+
| User State |
+-----+

NgcSet : NO
WorkplaceJoined : NO
WamDefaultSet : YES
WamDefaultAuthority : organizations
WamDefaultId : https://login.microsoft.com
WamDefaultGUID : {B16898C6-A148-4967-9171-64D755DA8520} (AzureAd)
AzureAdPrt : YES
AzureAdPrtAuthority : https://login.microsoftonline.com/6e12ae63-7254-4955-99f3-3d441beab112
EnterprisePrt : NO
EnterprisePrtAuthority :

-----+
| Ngc Prerequisite Check |
+-----+

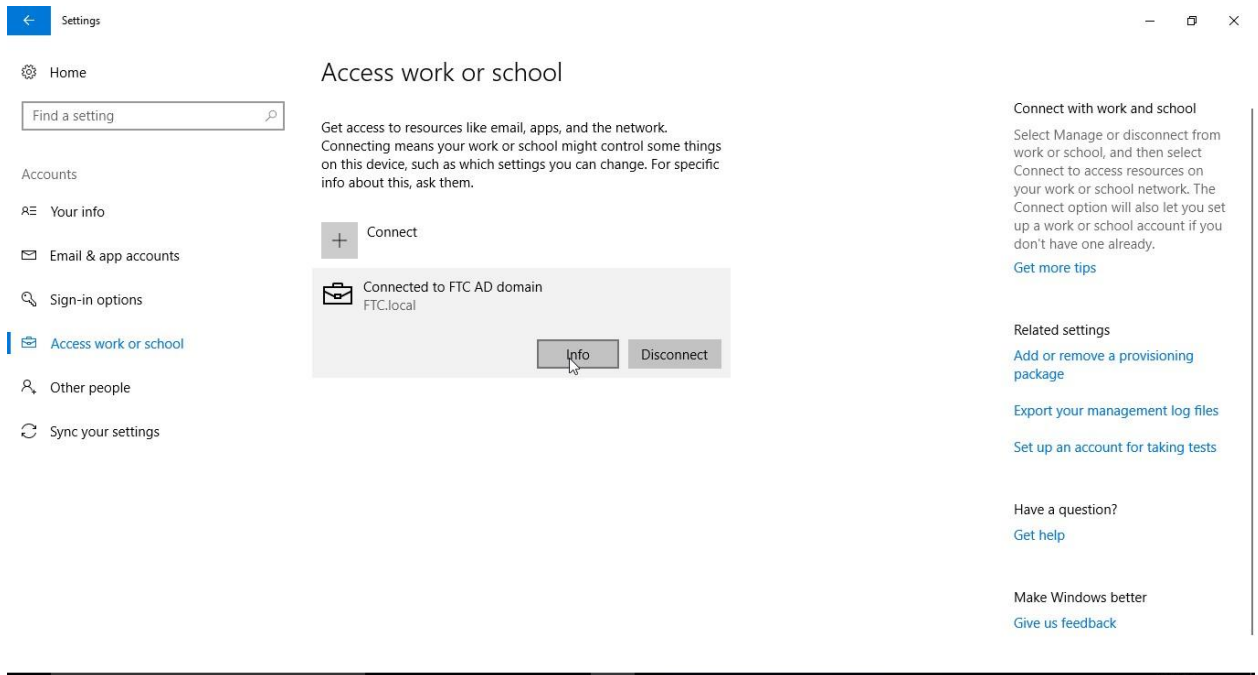
IsUserAzureAD : YES
PolicyEnabled : YES
DeviceEligible : YES
SessionIsNotRemote : NO
CertEnrollment : none
AadRecoveryNeeded : NO
PreReqResult : WillNotProvision

C:\windows\system32>
```

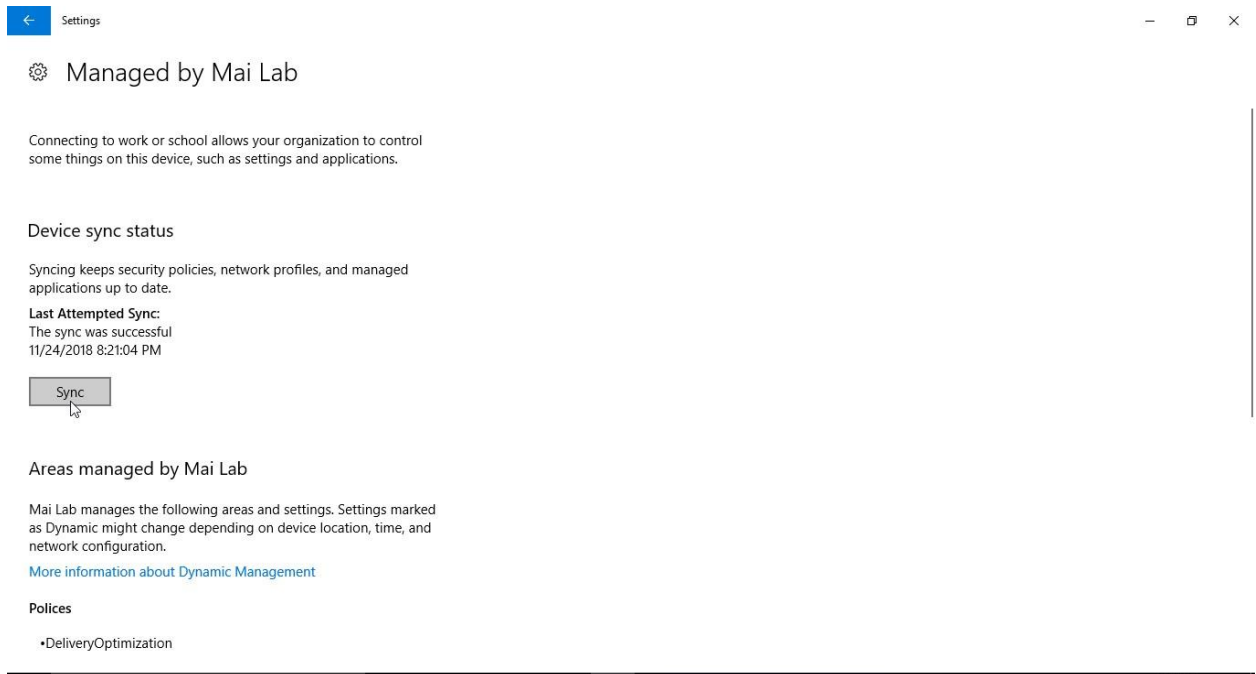
6. From Client PC, Open **Task Scheduler**. In **Task Scheduler Library**, open **Microsoft > Windows**, then click **EnterpriseMgmt**. You should find task schedule created by enrollment is disappeared.



7. From Client PC, Select **Settings** > **Accounts** > **Access work or School**. When you click on connect to your domain, you should find **Info** tab.



8. On **Info** tab you should find it show that it's managed by your tenant name, click **sync** to sync MDM policy from tenant



Enroll Windows 10 Devices by Using the Windows Autopilot

The Windows Autopilot simplifies enrolling devices. Building and maintaining customized operating system images is a time-consuming process. You might also spend time applying these custom operating system images to new devices to prepare them for use before giving them to your end users. With Microsoft Intune and Autopilot, you can give new devices to your end users without the need to build, maintain, and apply custom operating system images to the devices. When you use Intune to manage Autopilot devices, you can manage policies, profiles, apps, and more after they're enrolled.

You have two types for Enroll using Windows Autopilot:

- Windows Autopilot - Azure AD.
- Windows Autopilot - Hybrid Azure AD join.

Network Connectivity Requirements

The Windows Autopilot Deployment Program uses a number of cloud services to get your devices to a productive state. This means those services need to be accessible from devices registered as Windows Autopilot devices.

To manage devices behind firewalls and proxy servers, the following URLs need to be accessible:

- <https://go.microsoft.com>
- <https://login.microsoftonline.com>
- <https://login.live.com>
- <https://account.live.com>

- <https://signup.live.com>
- <https://licensing.mp.microsoft.com>
- <https://licensing.md.mp.microsoft.com>
- ctldl.windowsupdate.com
- download.windowsupdate.com

Note: Where not explicitly specified, both HTTPS (443) and HTTP (80) need to be accessible.

Windows Autopilot – Azure AD

In this mode, you can use Windows Autopilot to join a device to Azure Active Directory using Windows Autopilot user-driven mode. This capability is now available with Windows 10, version 1703 (or later).

Note: You can deploy autopilot using Self-deploying. Windows Autopilot self-deploying mode offers truly zero touch provisioning. With this mode, all you need to do is power on a device, plug it into Ethernet, and watch Windows Autopilot fully configure the device. **Self-deploying mode does not support Active Directory Join or Hybrid Azure AD Join.** All devices will be joined to Azure Active Directory. If you attempt a **self-deploying mode deployment** on a device that **does not have support TPM 2.0 or on a virtual machine**, the process will fail when verifying the device with an 0x800705B4 timeout error.

Prerequisites

- Windows automatic enrollment enabled.
- Azure Active Directory Premium subscription.
- Devices must have access to the internet.

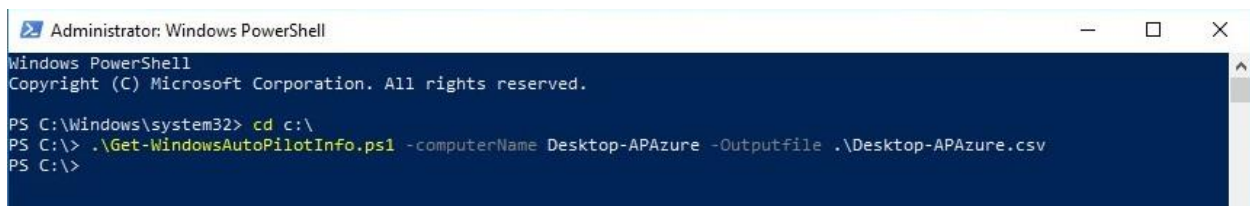
Step 1: How to get the CSV for Import in Intune

See the understanding PowerShell cmdlet for more information how to use it.

[Get-WindowsAutoPilotInfo](#)

If you don't have Serial no. for required PC, you can run above PowerShell script on required PC as following to export CSV file.

On Windows PowerShell, run following command “*.\Get-WindowsAutoPilotInfo -ComputerName <Type your computer name> -OutPutFile .\filename.csv*”



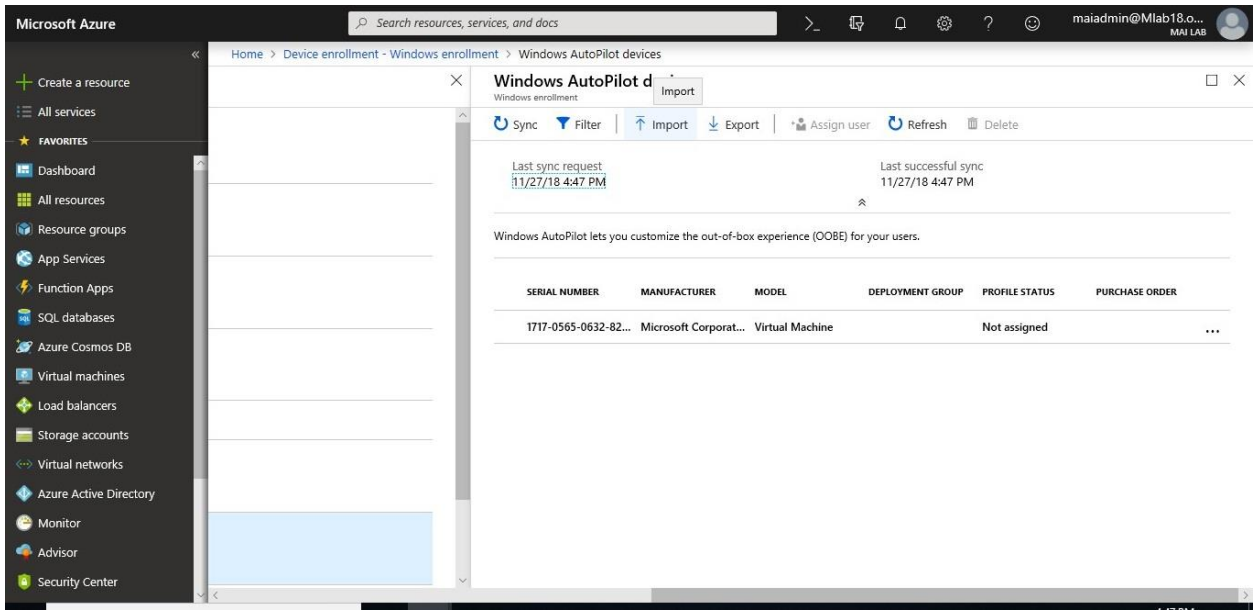
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd c:\
PS C:\> .\Get-WindowsAutoPilotInfo.ps1 -computerName Desktop-APAzure -Outputfile .\Desktop-APAzure.csv
PS C:\>
```

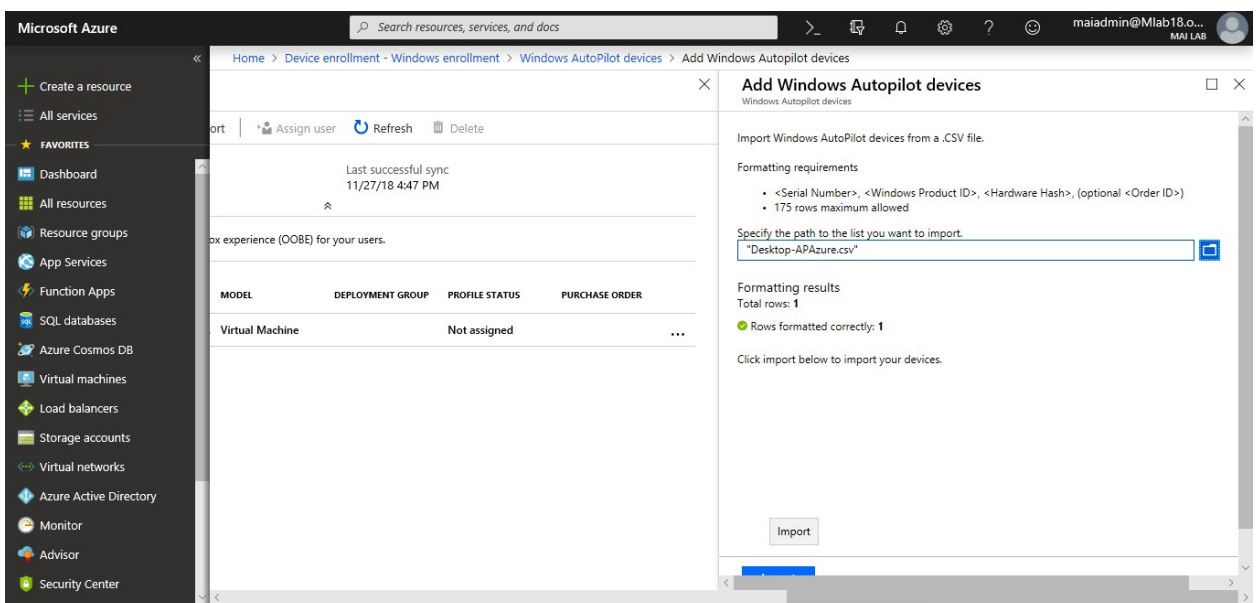
Step 2: Add devices

You can add Windows Autopilot devices by importing a CSV file with their information.

1. In [Intune in the Azure portal](#), choose **Device enrollment** > **Windows enrollment** > **Devices** > **Import**.

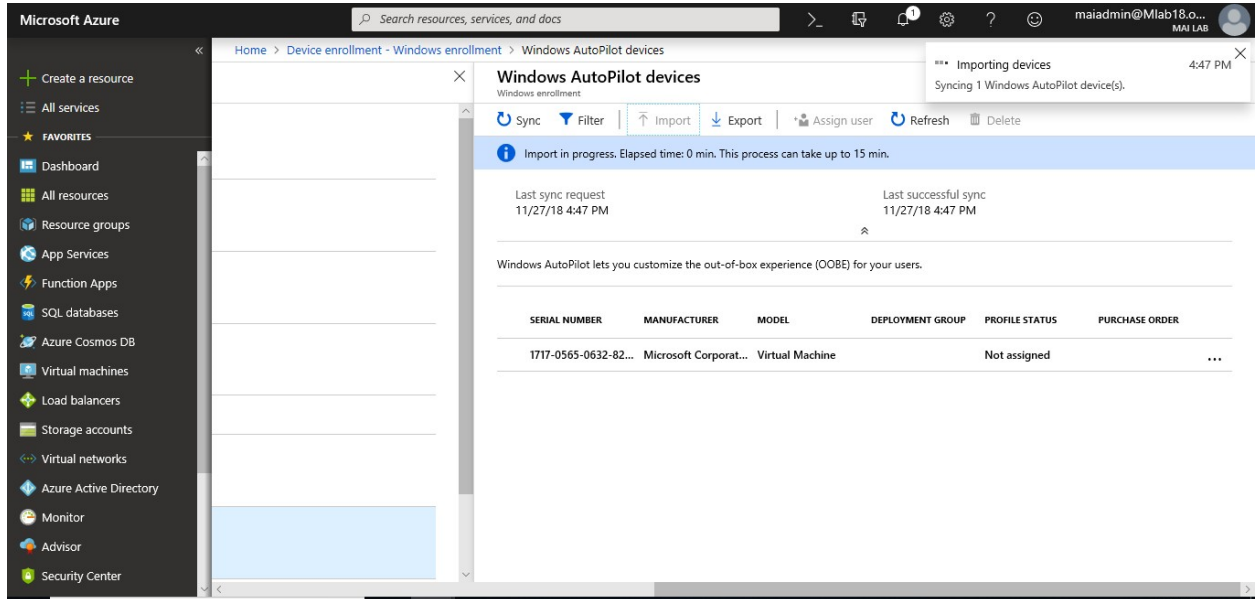


2. Under **Add Windows Autopilot devices**, browse to a CSV file listing the devices that you want to add. The file should list the serial numbers, Windows product IDs, hardware hashes, and optional order IDs of the devices.
3. Choose **Import** to start importing the device information. Importing can take several minutes.



Microsoft Intune step by step on Azure portal

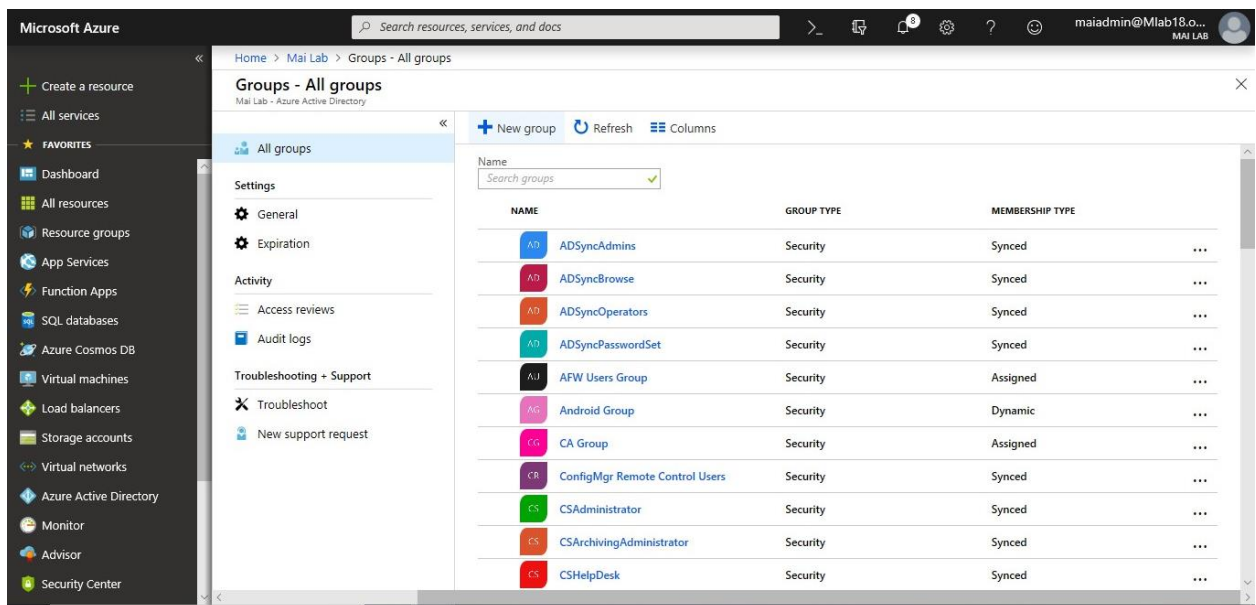
- After import is complete, choose **Device enrollment > Windows enrollment > Windows Autopilot > Devices > Sync**. A message displays that the synchronization is in progress. The process might take a few minutes to complete, depending on how many devices are being synchronized.



- Refresh the view to see the new devices.

Step 3: Create an Autopilot device group

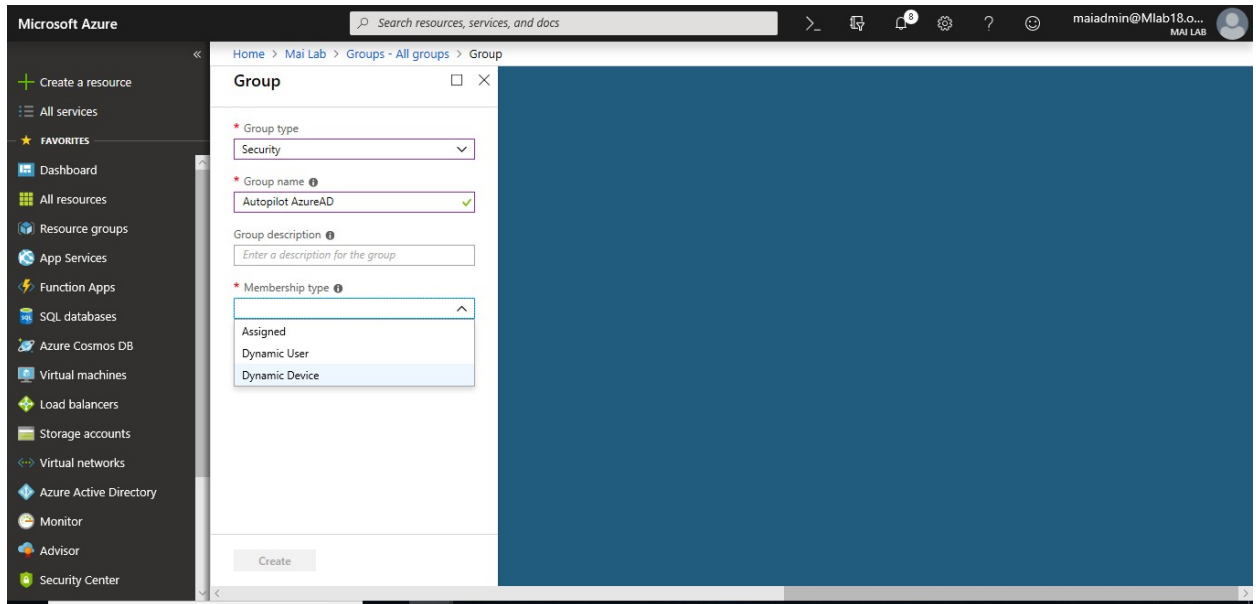
- In [Intune in the Azure portal](#), choose **Groups > New group**.



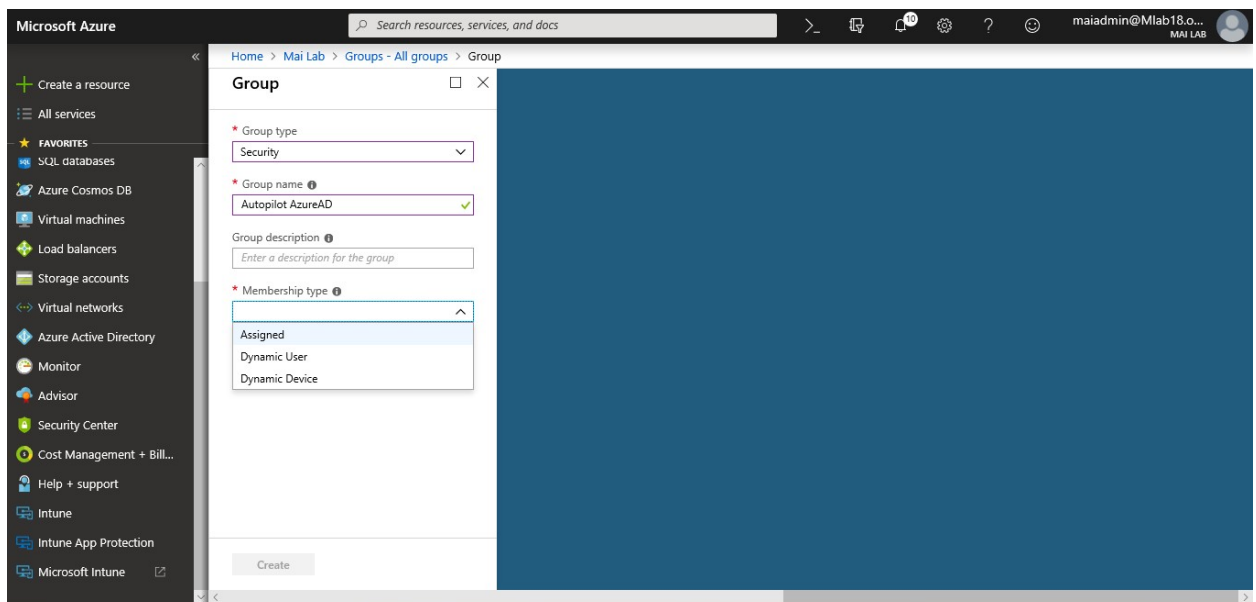
- In the **Group** blade:

Microsoft Intune step by step on Azure portal

- For **Group type**, choose **Security**.
- Type a **Group name** and **Group description**.
- For **Membership type**, choose either **Assigned** or **Dynamic Device**.



3. If you chose **Assigned** for **Membership type** in the previous step, then in the **Group** blade, choose **Members** and add Autopilot devices to the group. Autopilot devices that aren't yet enrolled are devices where the name equals the serial number of the device.

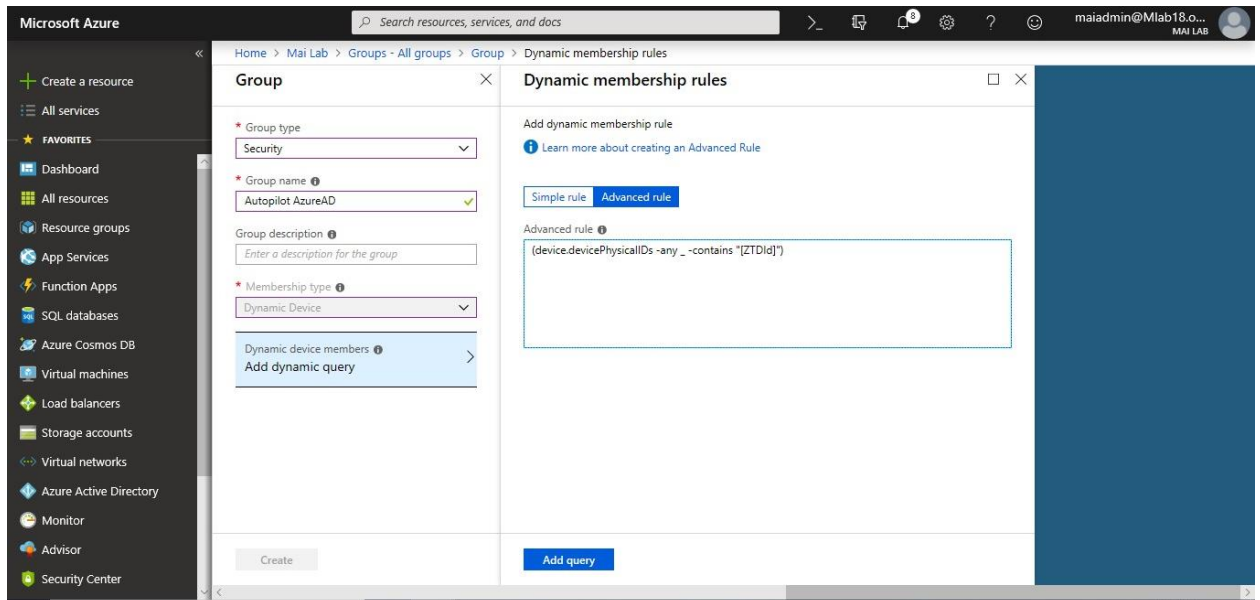


4. If you chose **Dynamic Devices** for **Membership type** above, then in the **Group** blade, choose **Dynamic device members** and type any of the following code in the **Advanced rule** box.

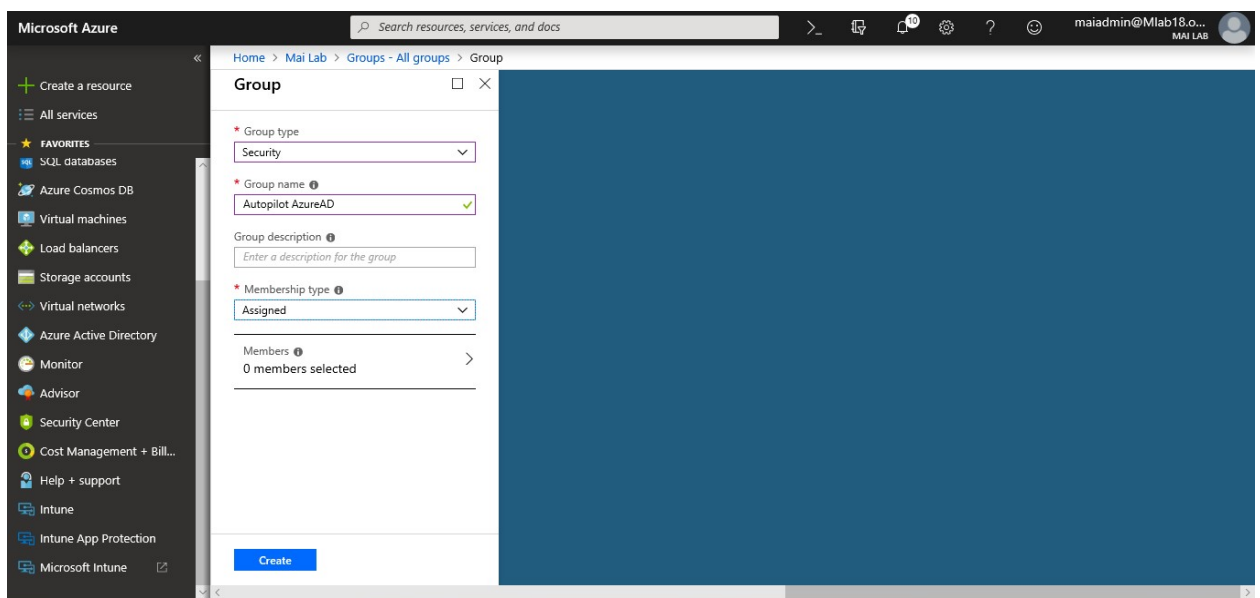
Microsoft Intune step by step on Azure portal

- If you want to create a group that includes all of your Autopilot devices, type (device.devicePhysicalIDs -any _ -contains "[ZTDId]")
- If you want to create a group that includes all of your Autopilot devices with a specific order ID, type: (device.devicePhysicalIDs -any _ -eq "[OrderID]:179887111881")
- If you want to create a group that includes all of your Autopilot devices with a specific Purchase Order ID, type: (device.devicePhysicalIDs -any _ -eq "[PurchaseOrderId]:76222342342")

After adding the **Advanced rule** code, choose **Save**.



5. Choose Create.

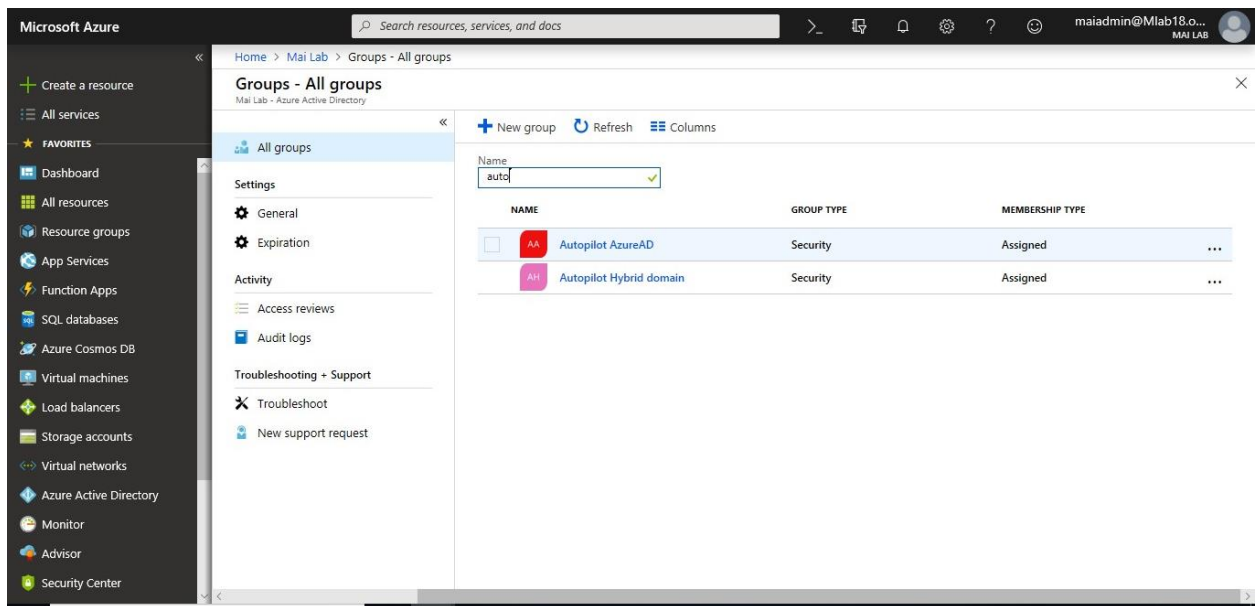


Microsoft Intune step by step on Azure portal

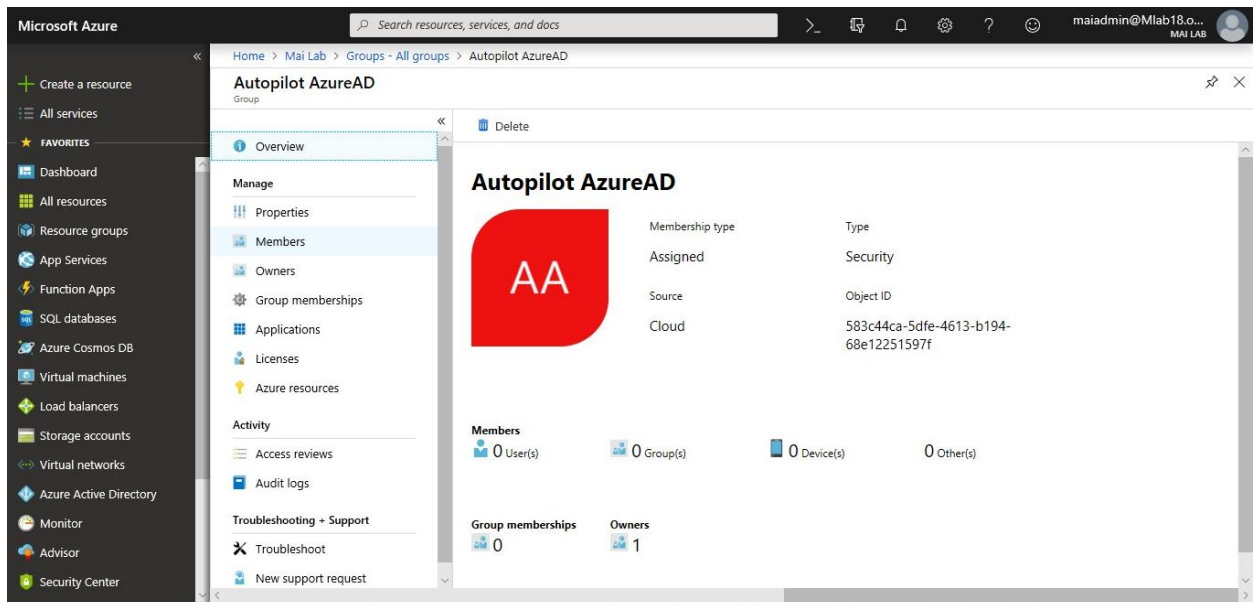
Note: On my lab, I created this group assigned Group and add device manually to don't have any conflict between Group for Hybrid domain join & Group for Azure AD.

To add device to your device group, you need to follow below steps: (Below steps required in case you create assigned group but if you create dynamic group, devices should add automatic)

1. In [Azure Portal](#), Click **Azure Active Directory** > **Groups**, Click on Group that you created.

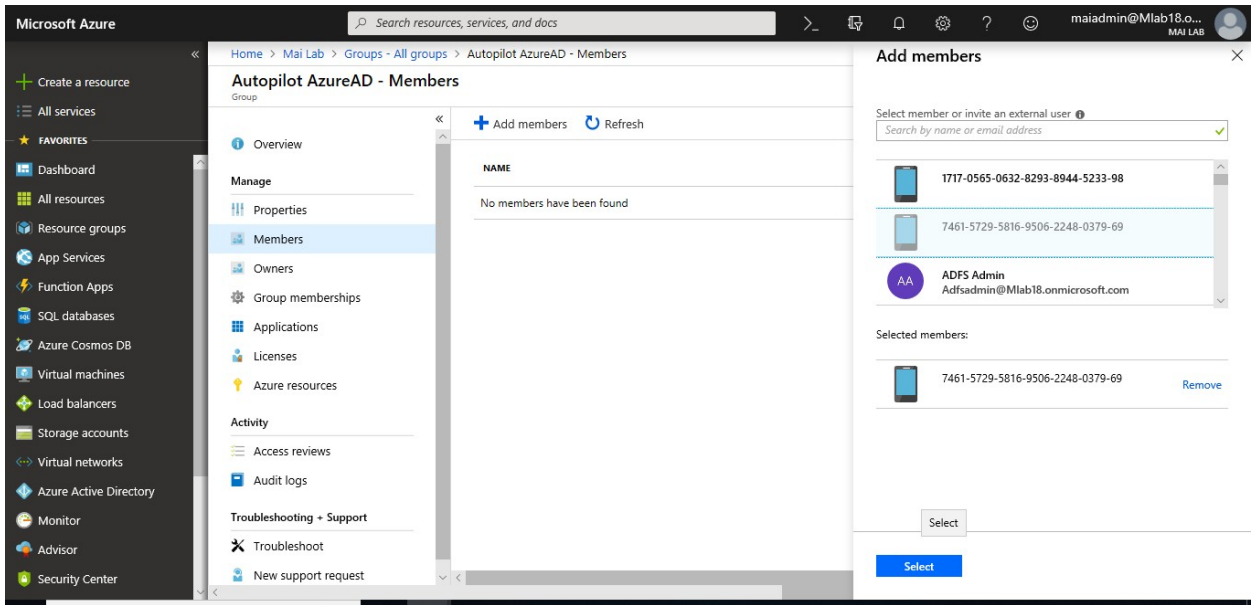


2. Click **Members**.

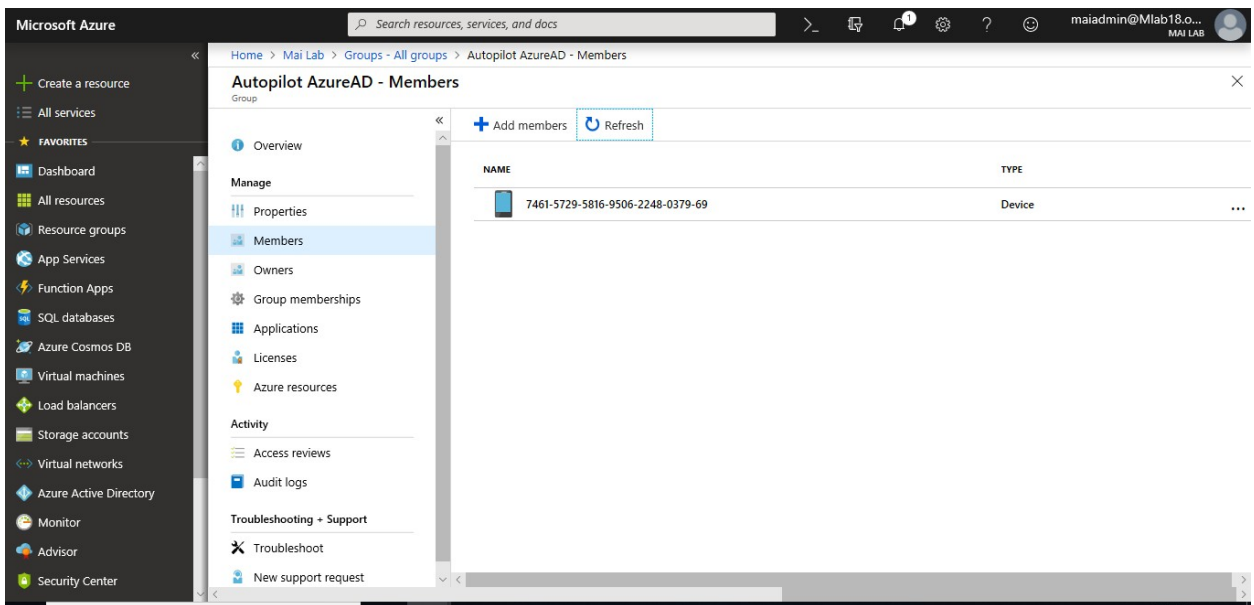


3. Click **Add Members**. Select the device that you want.

Microsoft Intune step by step on Azure portal



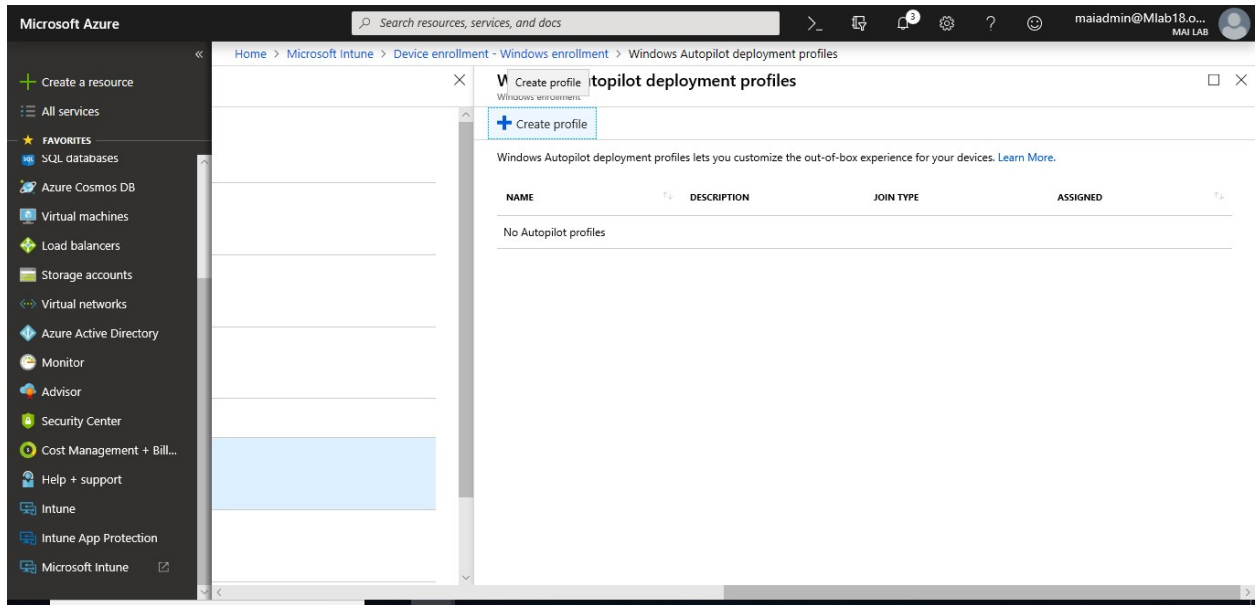
4. Click **Refresh** to see that device add on Group.



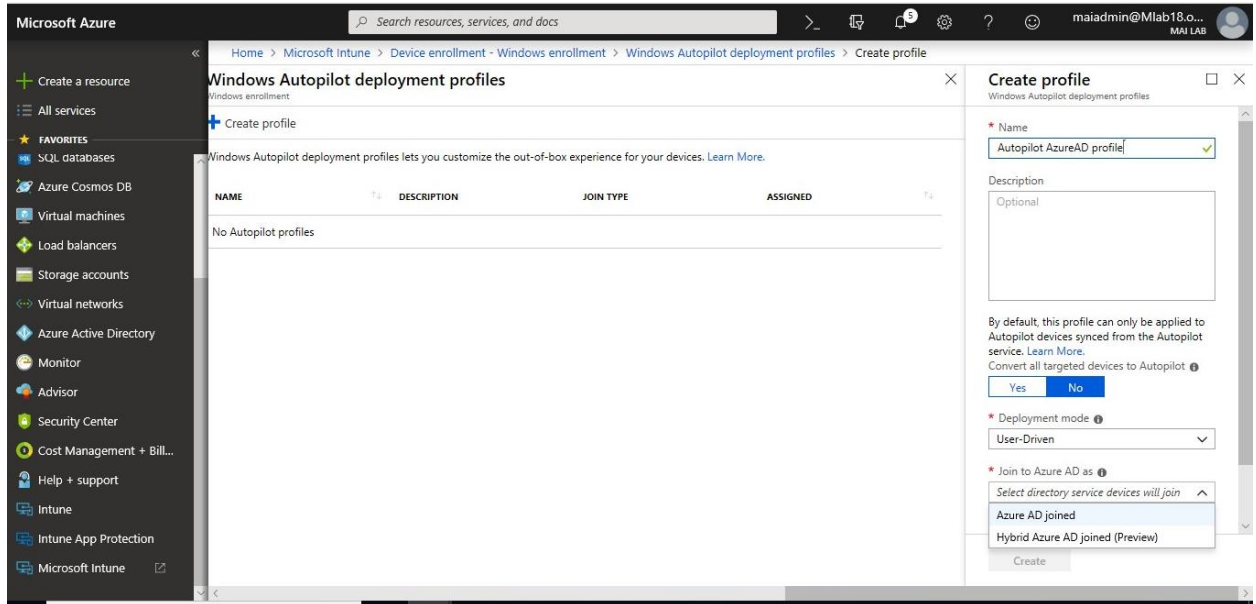
Step 4: Create an Autopilot deployment profile

Autopilot deployment profiles are used to configure the Autopilot devices.

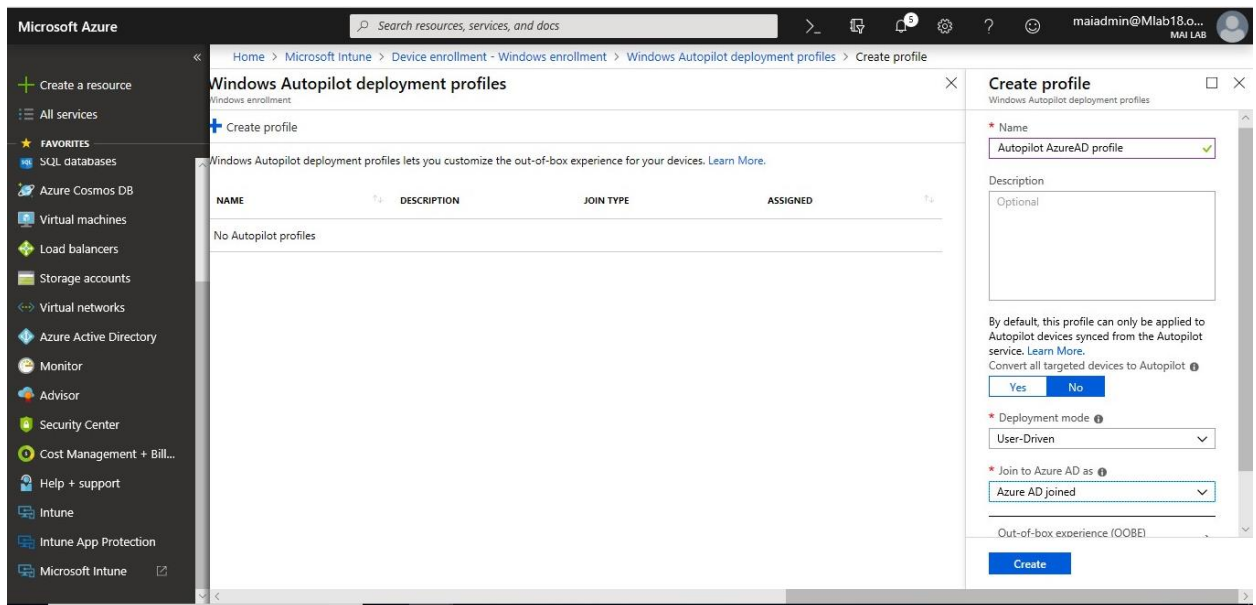
1. In [Intune in the Azure portal](#), choose **Device enrollment > Windows enrollment > Deployment Profiles > Create Profile**.



2. Type a **Name** and optional **Description**.
3. If you want all devices in the assigned groups to automatically convert to Autopilot, set **Convert all targeted devices to Autopilot to Yes**. All non-Autopilot devices in assigned groups will register with the Autopilot deployment service. Allow 48 hours for the registration to be processed. When the device is unenrolled and reset, Autopilot will enroll it. After a device is registered in this way, disabling this option or removing the profile assignment won't remove the device from the Autopilot deployment service. You must remove the device directly from the [Intune in the Azure portal](#), choose **Device enrollment > Windows enrollment > Devices**. Under **Windows Autopilot devices**, choose the devices you want to delete, and then choose **Delete**.
4. For **Deployment mode**, choose one of these two options:
 - **User-driven**: Devices with this profile are associated with the user enrolling the device. User credentials are required to enroll the device.
 - **Self-deploying (preview)**: (requires the most recent Windows 10 Insider Preview Build) Devices with this profile aren't associated with the user enrolling the device. User credentials aren't required to enroll the device.



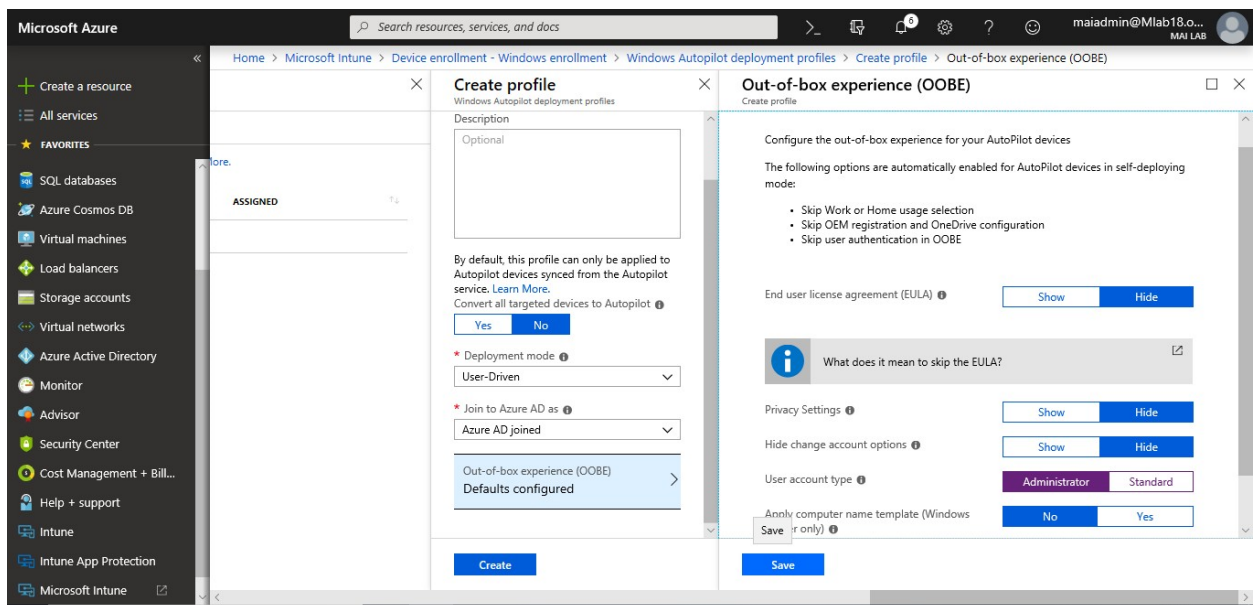
5. In the **Join to Azure AD as** box, choose **Azure AD joined**.



6. Choose **Out-of-box experience (OOBE)**, configure the following options, and then choose **Save**:

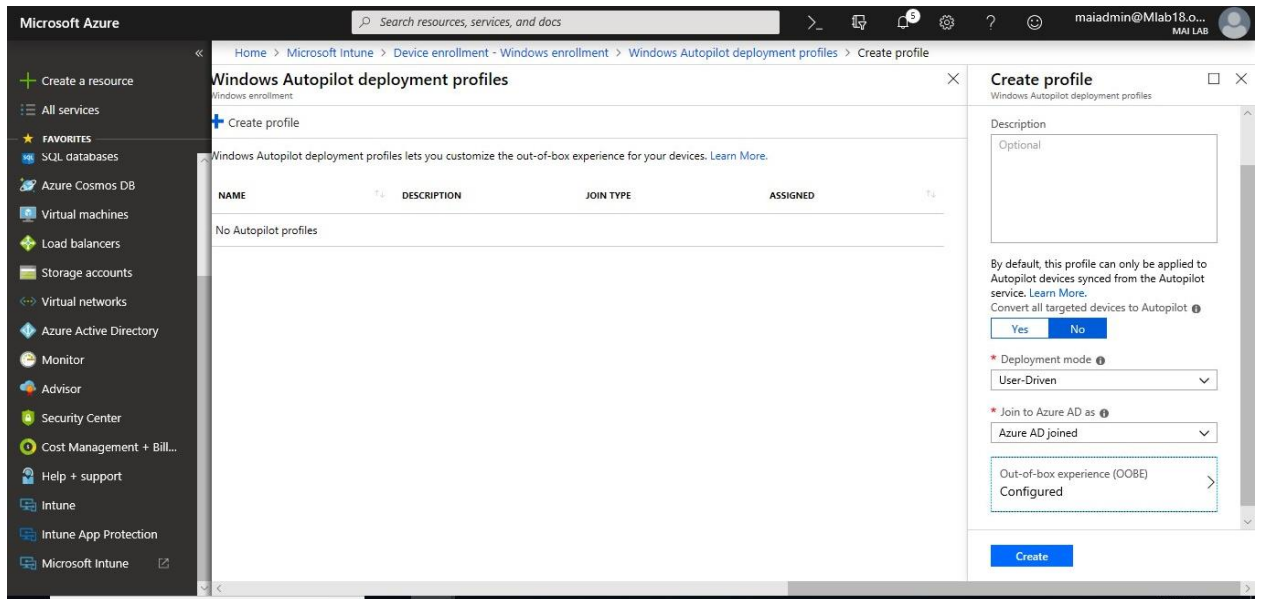
- **Language (Region)***: Choose the language to use for the device. This option is only available if you chose **Self-deploying** for **Deployment mode**.
- **Automatically configure keyboard***: If a **Language (Region)** is selected, choose **Yes** to skip the keyboard selection page. This option is only available if you chose **Self-deploying** for **Deployment mode**.

- **End-user license agreement (EULA):** (Windows 10, version 1709 or later)
Choose if you want to show the EULA to users.
- **Privacy settings:** Choose if you want to show privacy settings to users.
- **Hide change account options (Windows Insider only):** Choose **Hide** to prevent change account options from displaying on the company sign-in and domain error pages. This option requires company branding to be configured in Azure Active Directory.
- **User account type:** Choose the user's account type (**Administrator** or **Standard** user).
- **Apply computer name template (Windows Insider only):** Choose **Yes** to create a template to use when naming a device during enrollment. Names must be 15 characters or less, and can have letters, numbers, and hyphens. Names can't be all numbers. Use the [%SERIAL% macro](#) to add a hardware-specific serial number. Or, use the [%RAND:x% macro](#) to add a random string of numbers, where x equals the number of digits to add.



7. Choose **Create** to create the profile. The Autopilot deployment profile is now available to assign to devices.

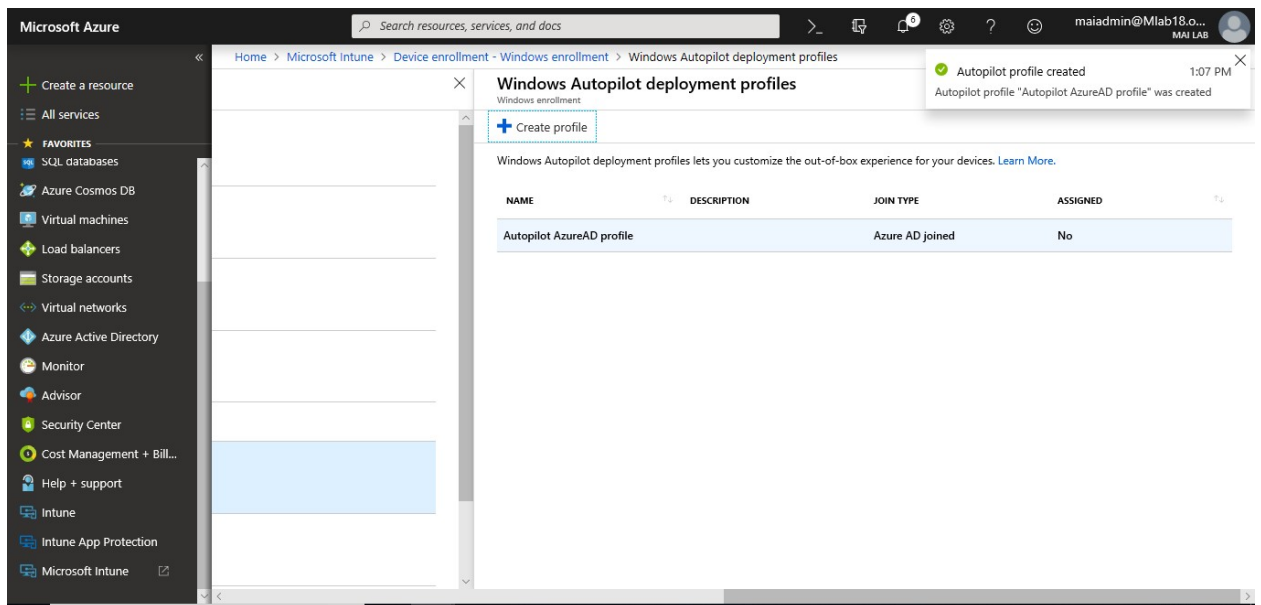
Microsoft Intune step by step on Azure portal



*Both **Language (Region)** and **Automatically configure keyboard** are only available if you chose **Self-deploying (preview)** for **Deployment mode**.

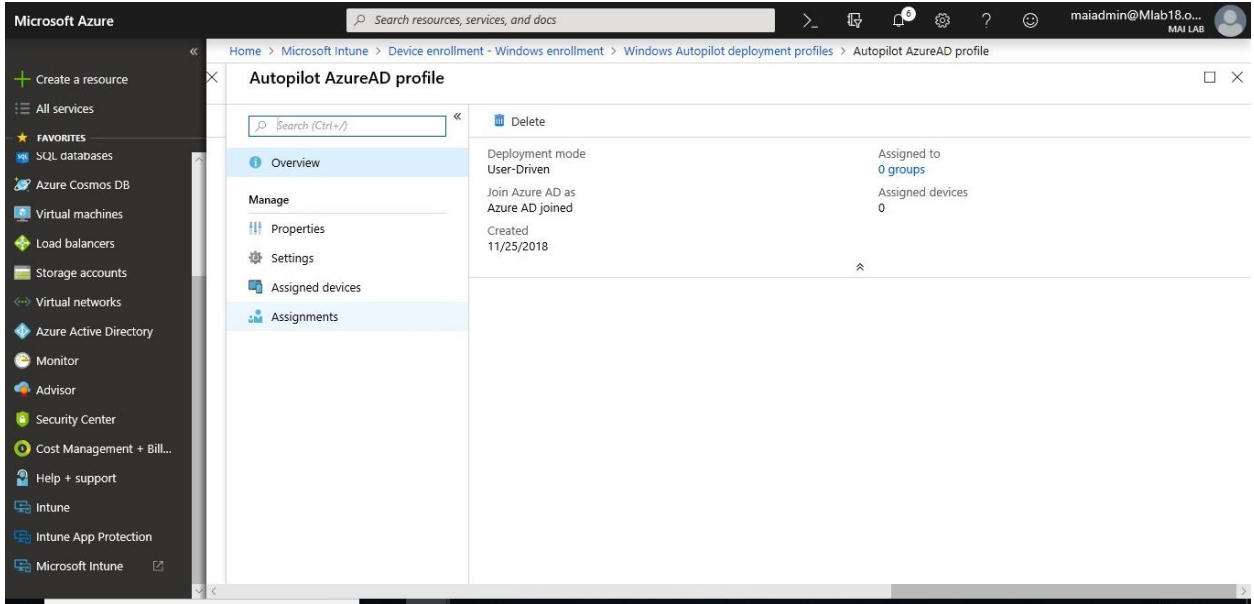
Step 5: Assign an Autopilot deployment profile to a device group

1. In [Intune in the Azure portal](#), choose **Device enrollment > Windows enrollment > Deployment profiles** > choose a profile.

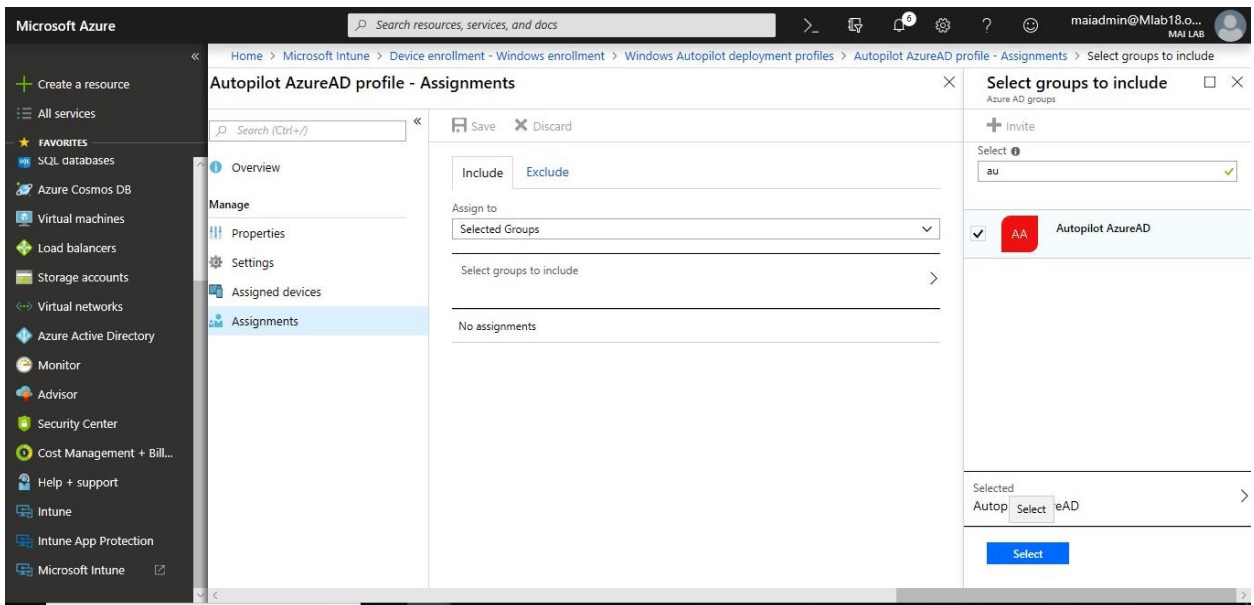


2. In the specific profile blade, choose **Assignments**.

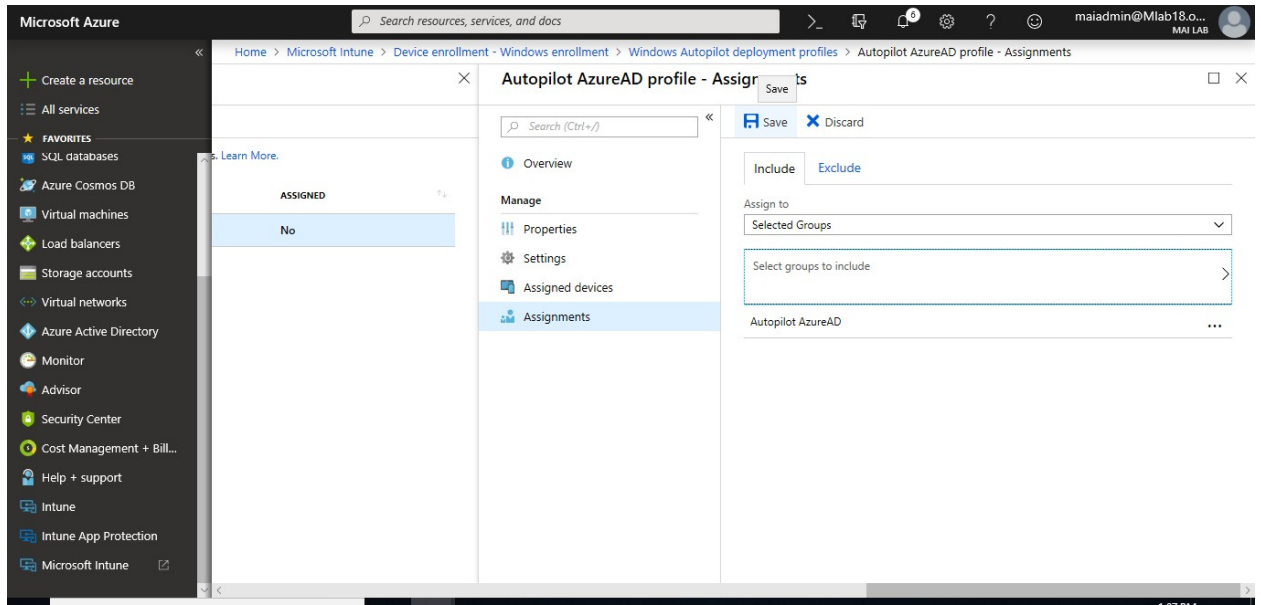
Microsoft Intune step by step on Azure portal



3. Choose **Select groups**, then in the **Select groups** blade, choose the group(s) that you want to assign the profile to, then choose **Select**.



4. Click **Save**.



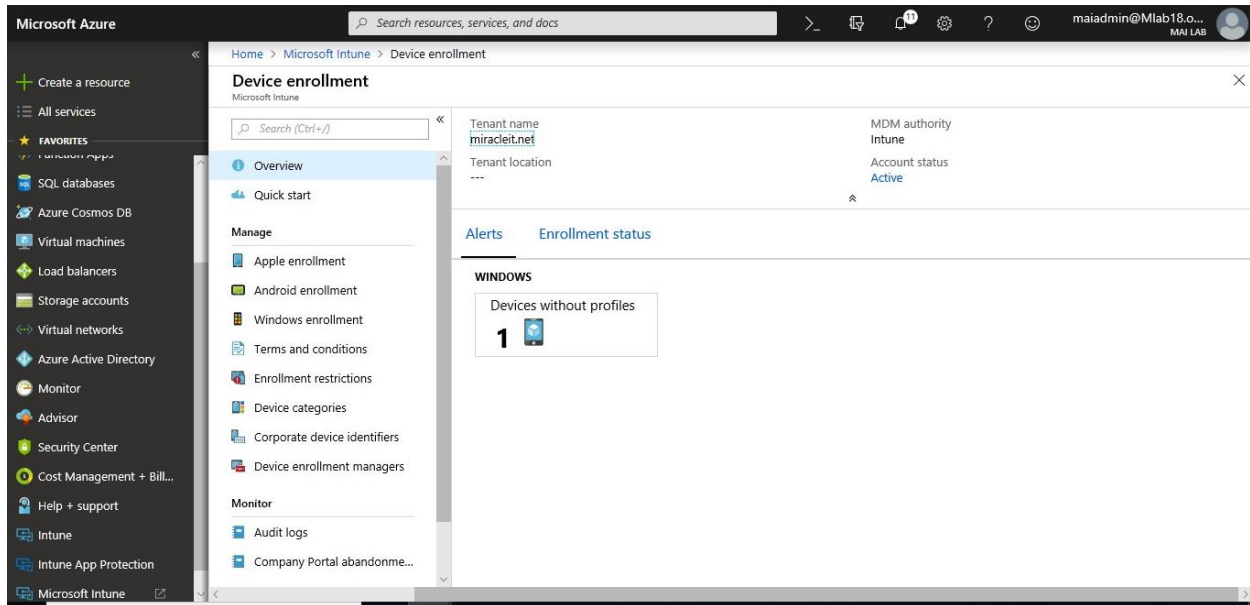
Note: Changes to the profile are applied to devices assigned to that profile. However, the updated profile won't be applied to a device that has already enrolled in Intune until after the device is reset and reenrolled.

Alerts for Windows Autopilot unassigned devices

Alerts will show how many Autopilot program devices don't have Autopilot deployment profiles. Use the information in the alert to create profiles and assign them to the unassigned devices. When you click the alert, you see a full list of Windows Autopilot devices and detailed information about them.

To see alerts for unassigned devices, in [Intune in the Azure portal](#), choose **Device enrollment > Overview > Unassigned devices**.

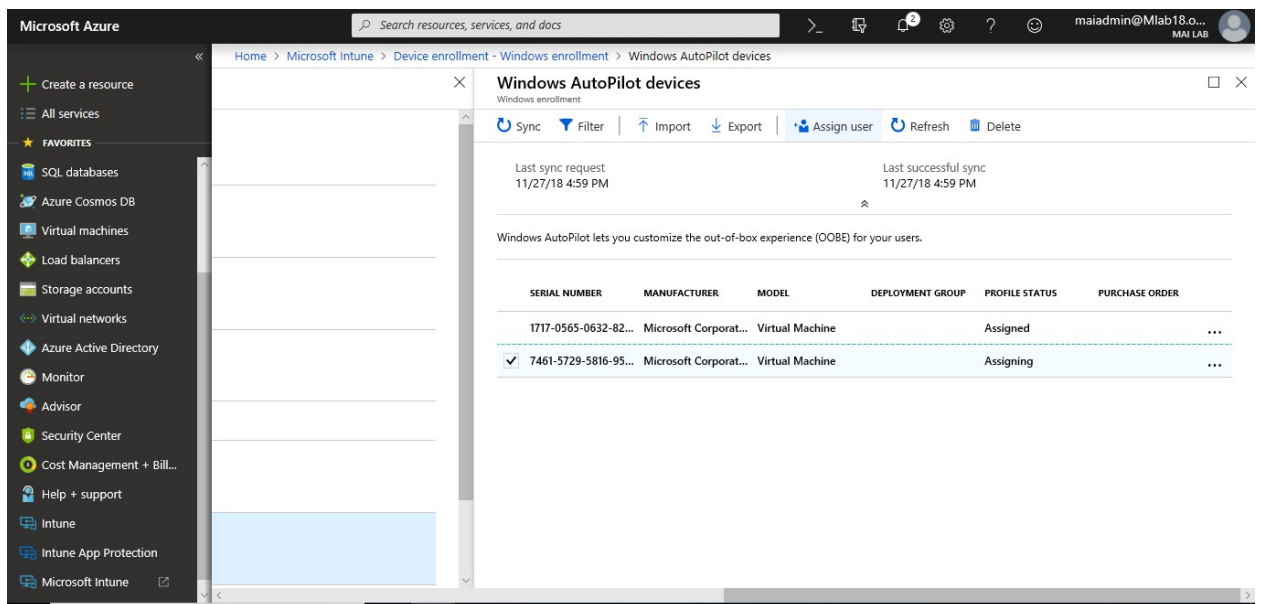
Microsoft Intune step by step on Azure portal



Step 6: Assign a user to a specific Autopilot device

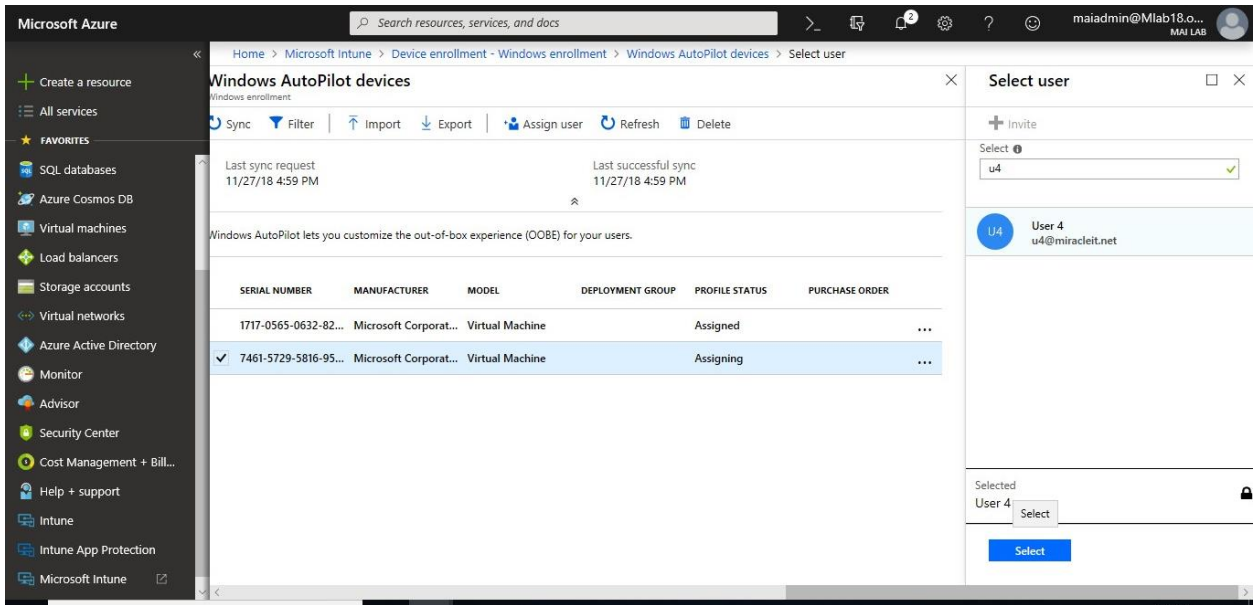
You can assign a user to a specific Autopilot device. This assignment pre-fills a user from Azure Active Directory in the company-branded sign-in page during Windows setup. It also lets you set a custom greeting name. It doesn't pre-fill or modify Windows sign-in. Only licensed Intune users can be assigned in this manner.

1. In the [Intune in the Azure portal](#), choose **Device enrollment > Windows enrollment > Devices > choose the device > Assign user**.

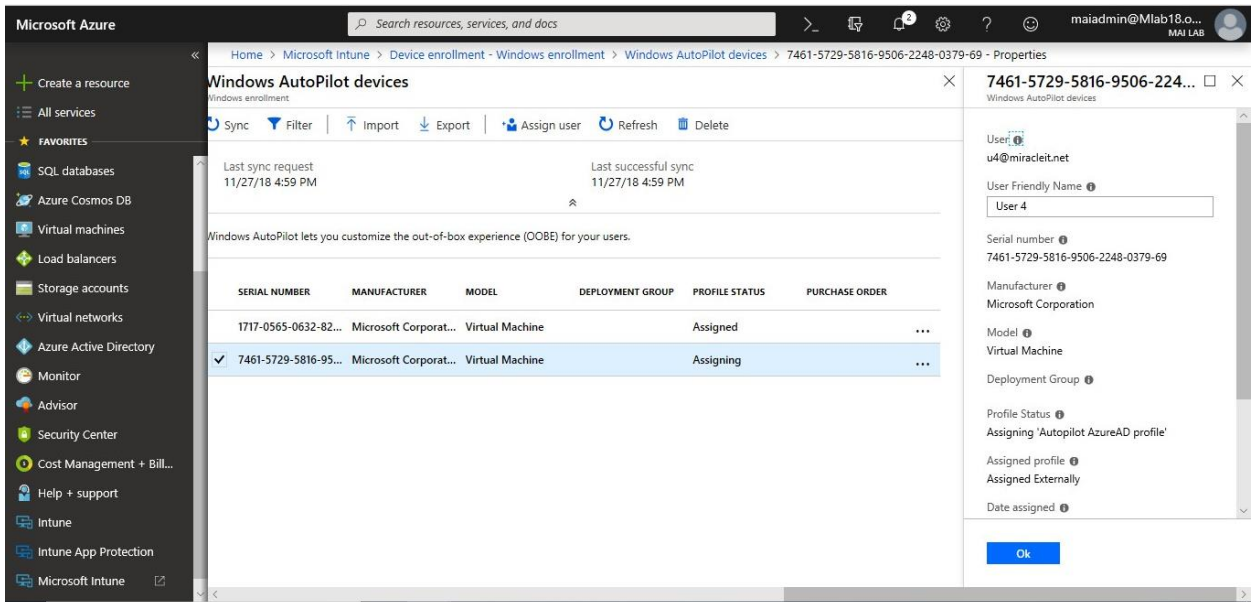


2. Choose an Azure user licensed to use Intune and choose **Select**.

Microsoft Intune step by step on Azure portal

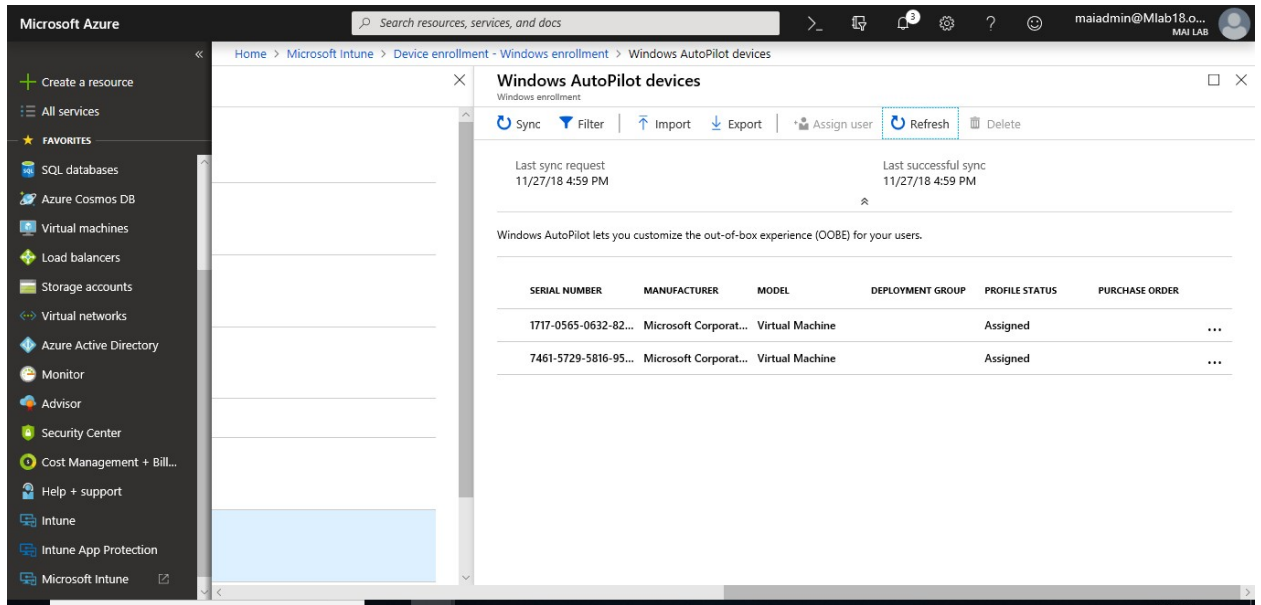


3. In the **User-Friendly Name** box, type a friendly name or just accept the default. This string is the friendly name that displays when the user signs in during Windows setup. Choose **Ok**.



4. Now Device is ready to get Autopilot profile.

Microsoft Intune step by step on Azure portal

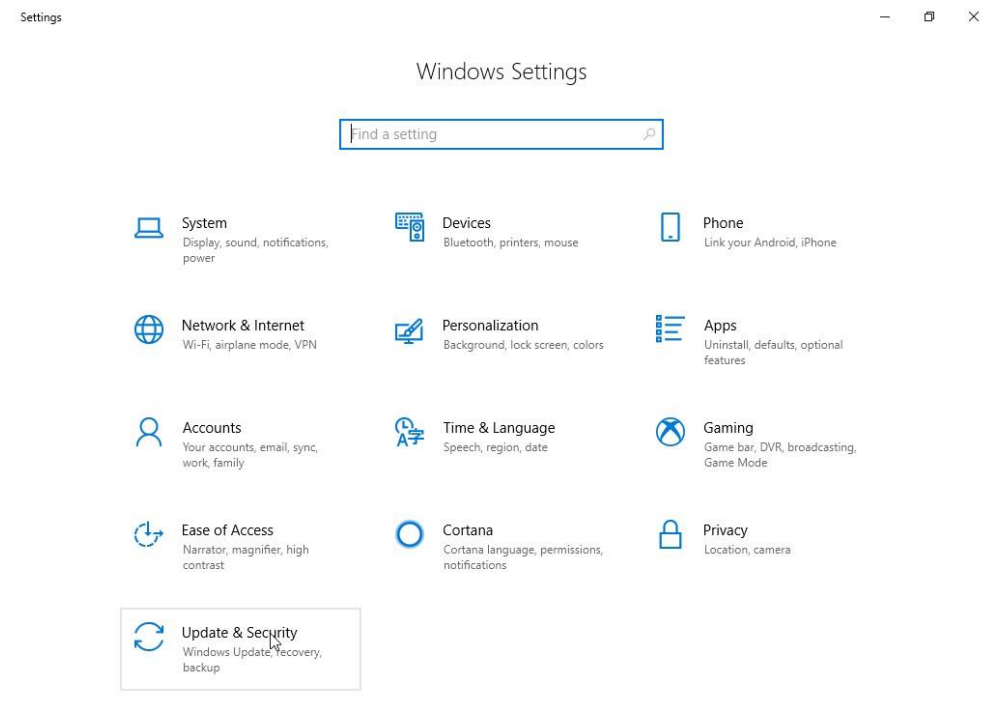


Note: You should verify that user who assign to him Autopilot profile, exist on Group for [Automatic Enrollment](#) if you don't enable automatic enrollment to all users.

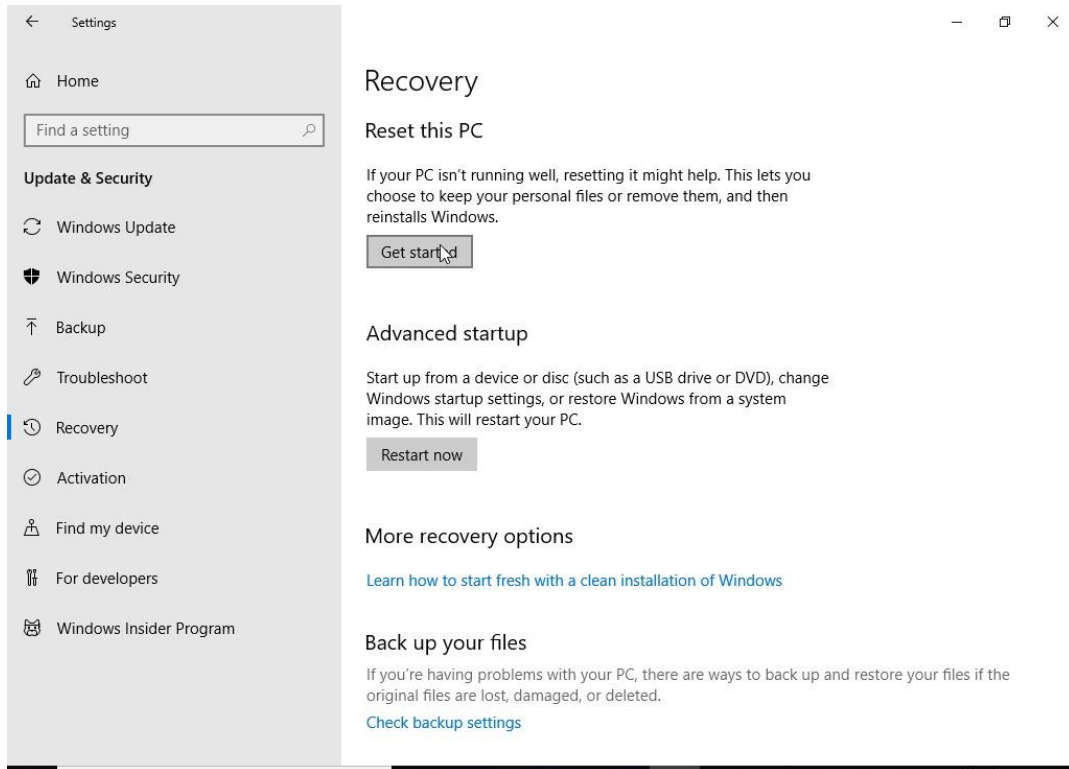
Step 7: Deploy Autopilot Profile & Verify Enrollment.

To Verify Enrollment, you need to follow below steps:

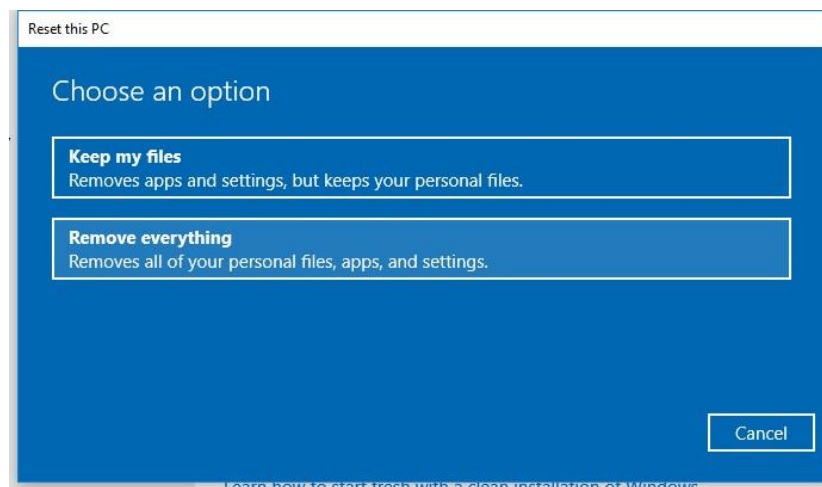
1. On Client PC, if Windows configured, you will need to reset the PC.
2. On **Settings**, Select **Updates & Security**.



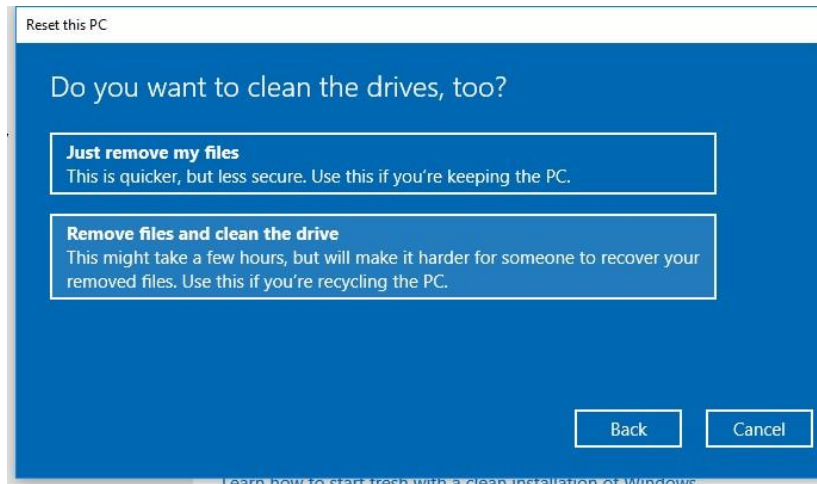
3. On **Updates & Security** Page, Select **Recovery** Then Click **Get Started** on Reset PC.



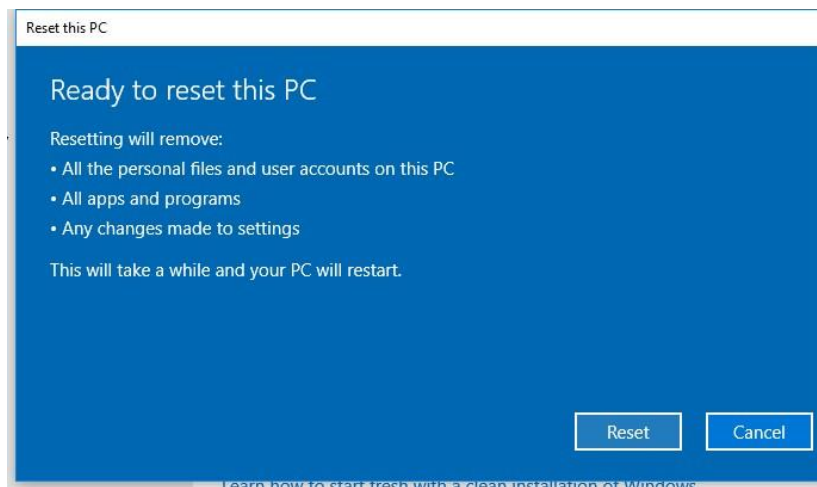
4. Click **Remove everything**.



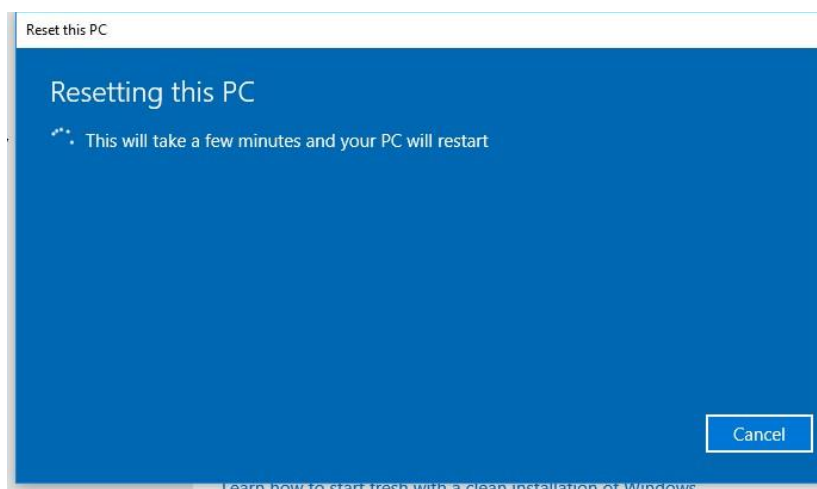
5. Click **Remove files & clean the drive**.



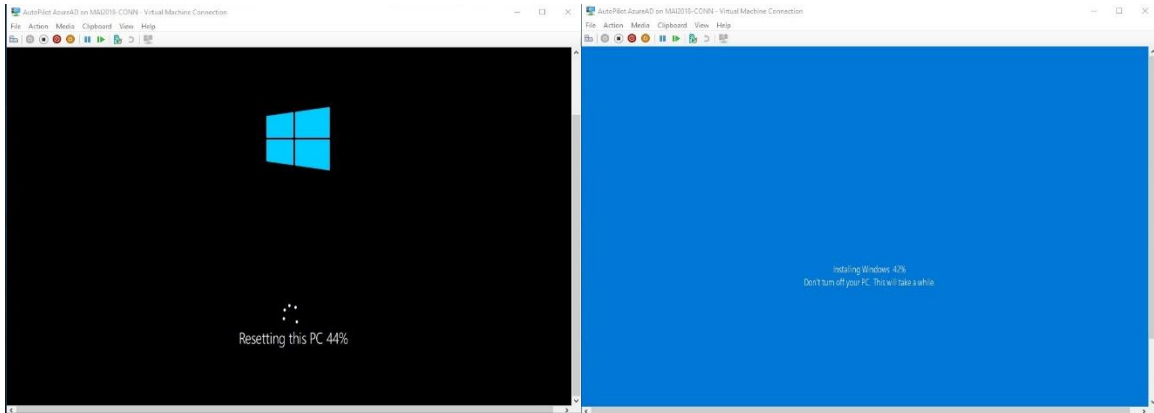
6. Click **Reset**.



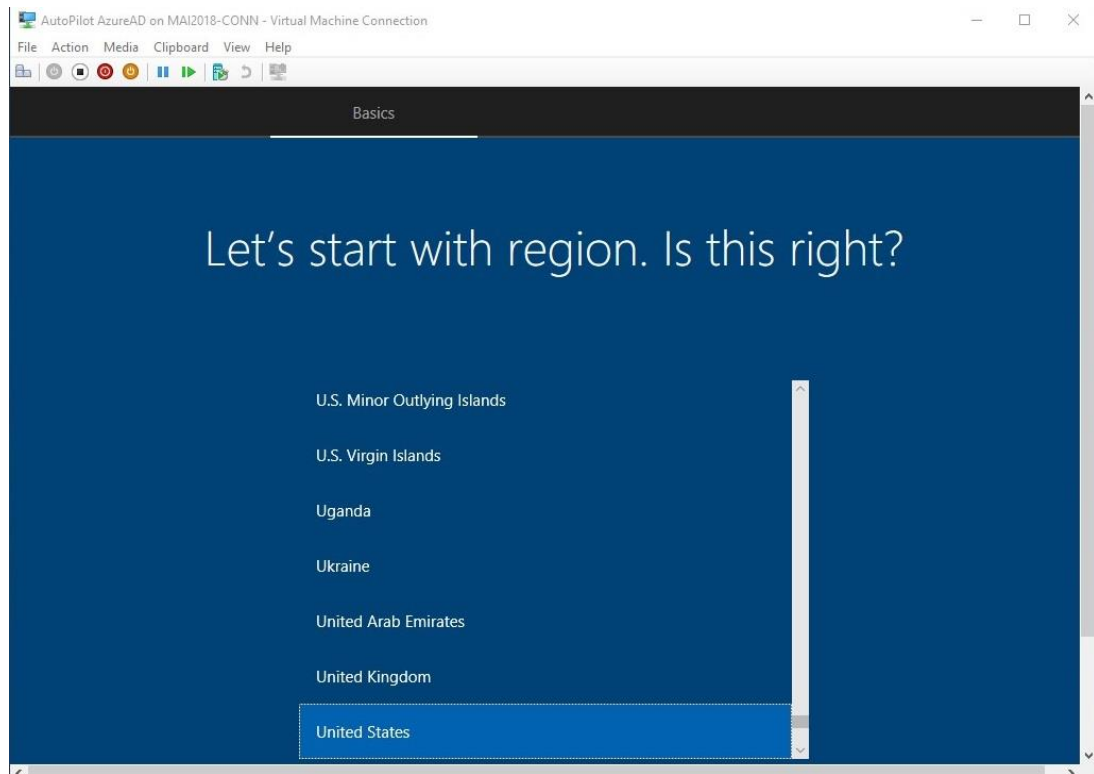
7. PC will start reset.



Microsoft Intune step by step on Azure portal

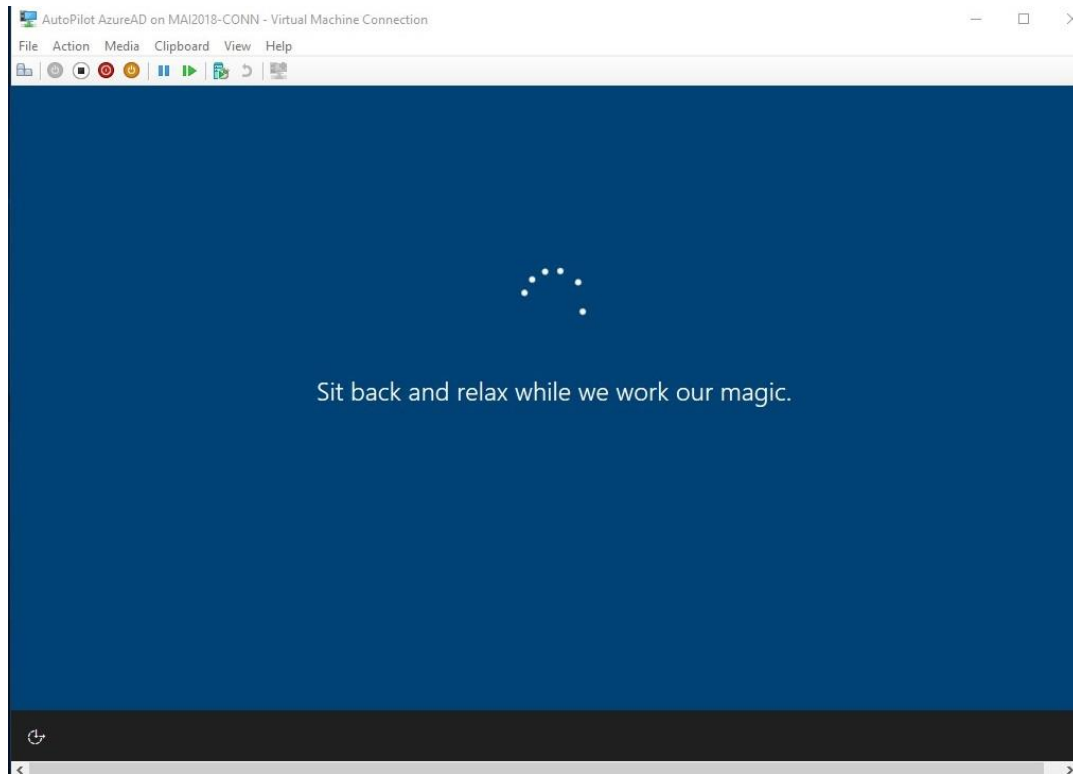


8. PC will start to deploy autopilot Profile.

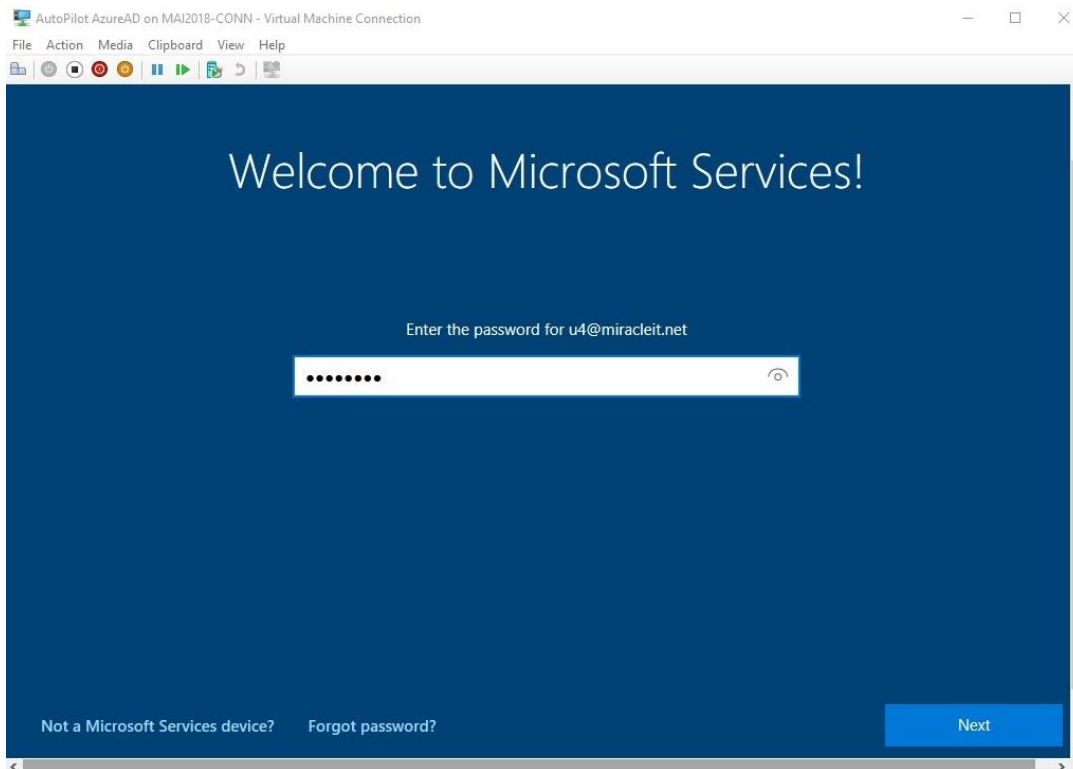


9. Wait until autopilot Profile pushed.

Microsoft Intune step by step on Azure portal

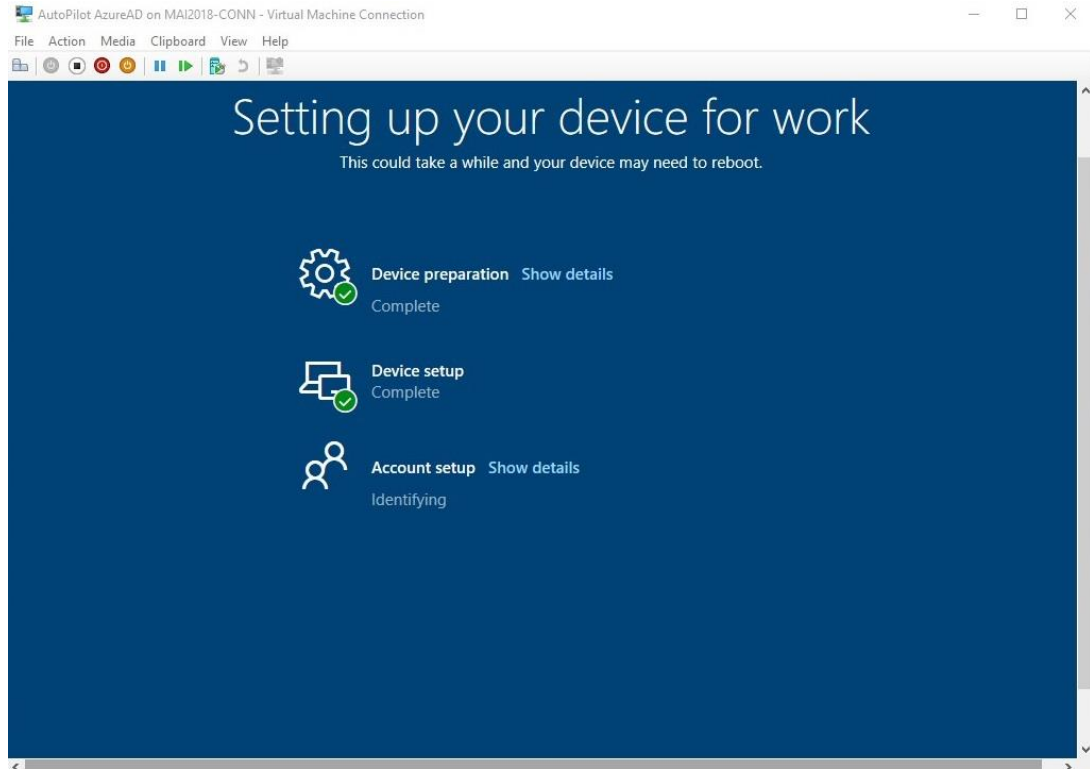


10. Click Yes. Enter your Credentials.

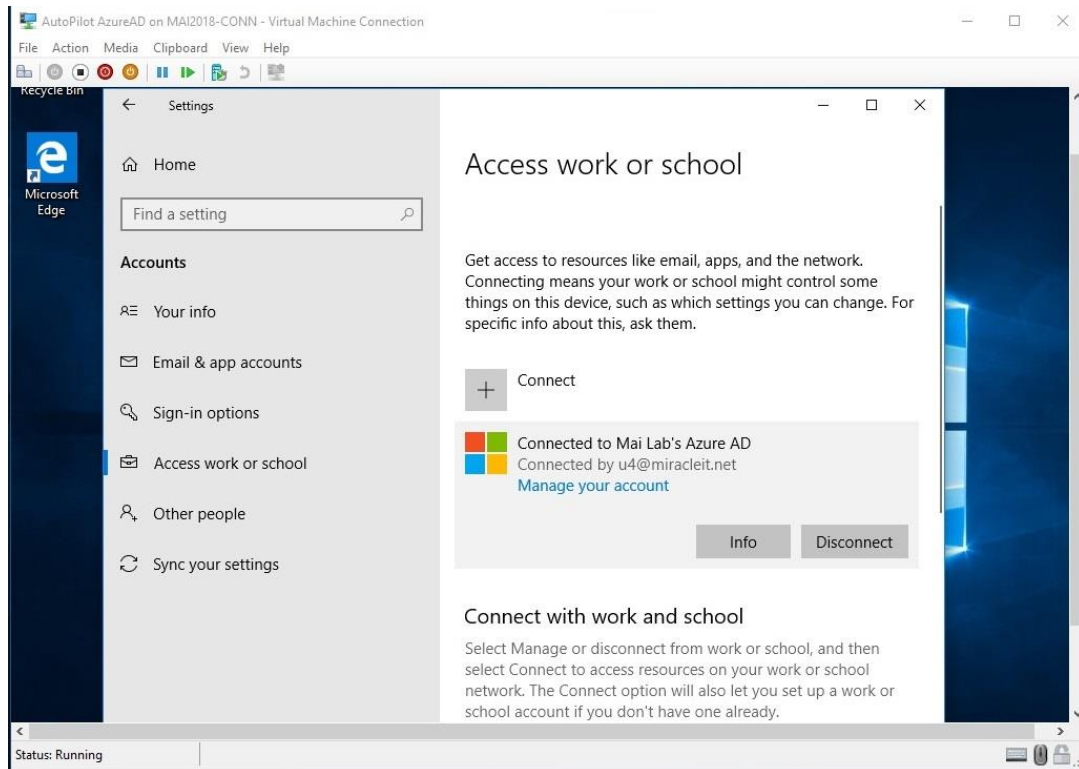


11. Start Setting up your device for work.

Microsoft Intune step by step on Azure portal



12. Sign in to client PC, Open **Settings** > **Accounts** > **Access work or school**. You should find pc join Azure AD.



13. Open [Azure admin portal](#) > **Azure Active Directory**> **Devices**. You should find PC appear that it's managed by Microsoft Intune.

NAME	ENABLE...	OS	VERSION	JOIN TYPE	OWNER	MDM	COMPL...	REGISTERED	ACTIVITY
MAI2018-CL10	Yes	Wind...	10.0 (16...	Hybrid Azure...	N/A	Microsoft Intune	Yes	11/24/2018 11:0...	11/24/2...
MAI2018-CLXNUJV	Yes	Wind...	10.0.177...	Hybrid Azure...	N/A	Microsoft Intune	Yes	11/27/2018 7:1...	11/27/2...
DESKTOP-H5QLO11	Yes	Wind...	10.0.171...	Azure AD join...	User 4	Microsoft Intune	Yes	11/27/2018 4:5...	11/27/2...
Mai2018-cl1803	Yes	Wind...	10.0.177...	Azure AD join...	User 2	Microsoft Intune	Yes	11/19/2018 11:0...	11/19/20...
Mai2018-Pro1803	Yes	Wind...	10.0 (171...	Hybrid Azure...	N/A	None	N/A	N/A	N/A
DESKTOP-RUJLL...	Yes	Wind...	10.0.171...	Azure AD join...	User 4	None	No	11/22/2018 3:5...	11/22/2...
MAI2016-CL2	Yes	Wind...	10.0.162...	Azure AD regi...	User 1	None	Yes	11/19/2018 11:5...	11/19/20...
U2_Android_11/14...	Yes	Andro...	8.0.0	Azure AD regi...	User 2	Microsoft Intune	Yes	11/14/2018 3:3...	11/14/20...

14. On [Intune Portal](#) > Click **Device Compliance** > **Device Compliance**, you should find device appear on portal as Management Devices.

DEVICE NAME	USER PRINCIPAL NAME	MANAGED BY	COMPLIANCE	OS	OS VERSION
DESKTOP-H5QLO11	u4@miracleit.net	MDM	Compliant	Windows	10.0.17134.2
MAI2016-CL2	U1@Mlab18.onmicrosof...	MDM/ConfigMgr Agent	See ConfigMgr	Windows	10.0.16299.4
MAI2018-CL10	DavidHerraiz@miracleit...	MDM	Compliant	Windows	10.0.16299.7
Mai2018-cl1709	Ghady@miracleit.net	MDM	Compliant	Windows	10.0.17134.4
Mai2018-cl1803	U2@Mlab18.onmicrosof...	MDM	Compliant	Windows	10.0.17763.1
Mai2018-Cl1809	U5@miracleit.net	MDM	Compliant	Windows	10.0.17134.4
MAI2018-CL3	u3@m1ab18.onmicrosof...	MDM/ConfigMgr Agent	See ConfigMgr	Windows	10.0.16299.4
MAI2018-CLXNUJV	mfawzy@miracleit.net	MDM	Compliant	Windows	10.0.17763.1
U2_Android_11/14/2018...	U2@Mlab18.onmicrosof...	MDM	Compliant	Android	8.0.0

Windows Autopilot – Hybrid Azure AD join

In this mode, you can use Windows Autopilot to join a device to an on-premises Active Directory domain which support for Hybrid Azure AD join (on-premises AD) using Windows Autopilot user-driven mode. This capability is now available with Windows 10, version 1809 (or later).

Prerequisites

- Successfully configure [hybrid Azure Active Directory join devices](#).

The devices to be enrolled must also:

- Be running Windows 10 with the [October 2018 update](#).
- Have access to the internet.
- Have access to your Active Directory (VPN connection not supported).
- Go through the Out-of-Box Experience (OOBE).

Step 1: Increase the computer account limit in the Organizational Unit

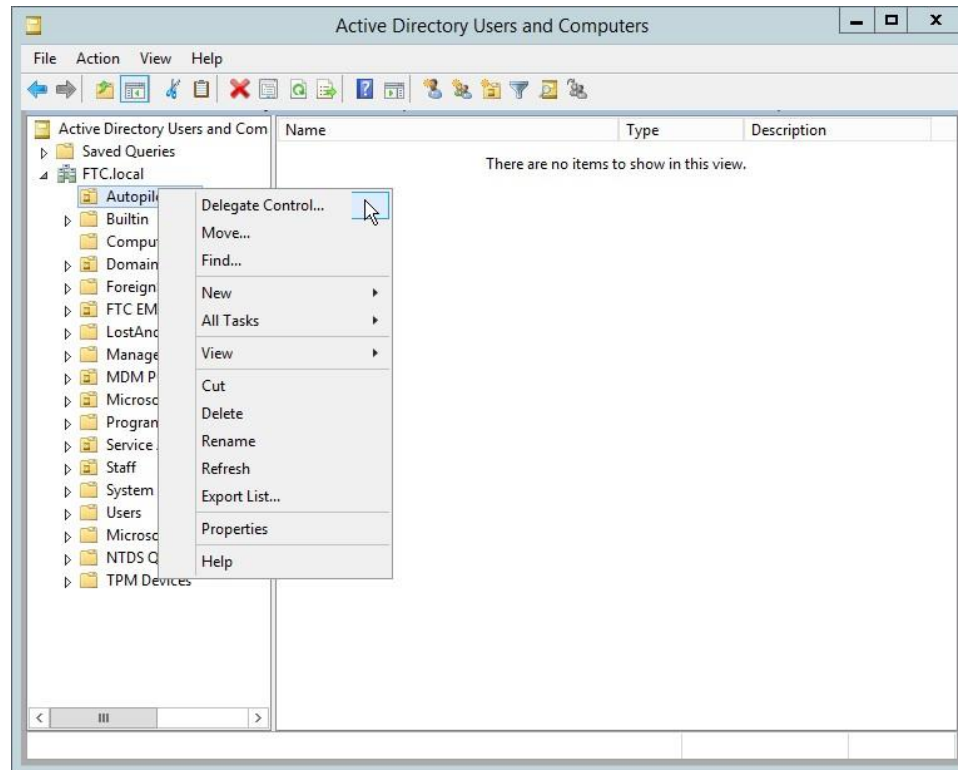
The Intune Connector for Active Directory creates Autopilot enrolled computers in the On-Premises Active directory domain. The computer hosting the Intune Connector must have the rights to create the computer objects within the domain.

On some domains, computers are not granted the rights to create computers. Or maybe Admins do not want to increase the Domain-wide computer account limit. In these situations, the rights can be delegated to the organizational unit where Hybrid Azure AD joined devices are created.

The organizational unit granted the right to create computers must match:

- the organizational unit entered in the Domain Join profile
- or, if no profile is selected, the computer's domain name for your domain.

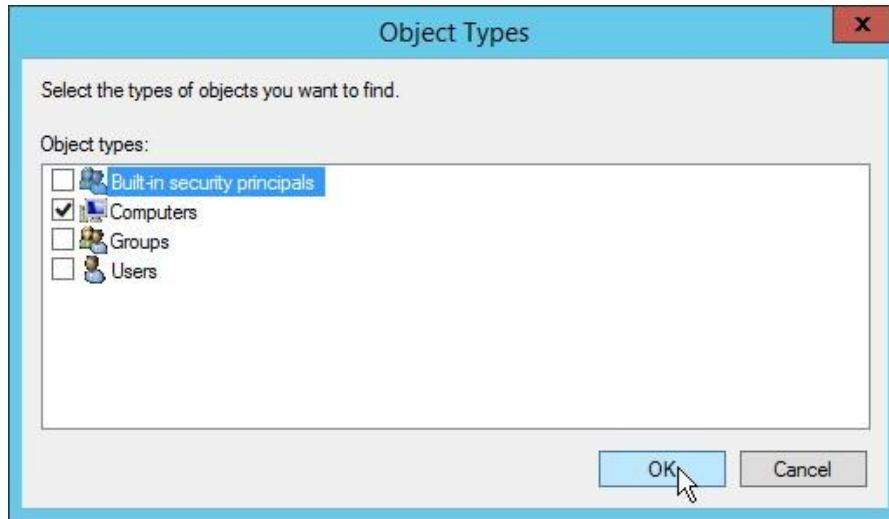
1. Open **Active Directory Users and Computers**.
2. Right-click the organizational unit you'll use to create Hybrid Azure AD joined computers > **Delegate Control**.



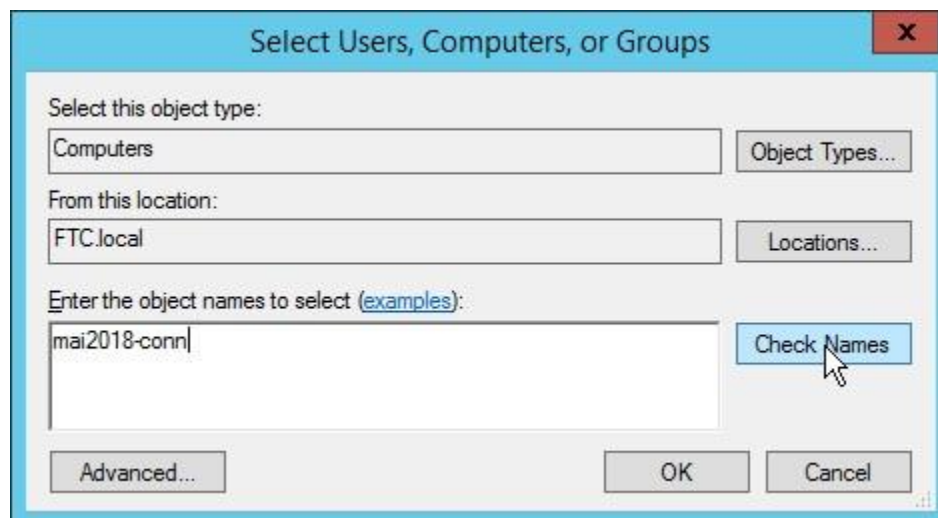
3. In the **Delegation of Control** wizard, choose **Next > Add... > Object Types**.



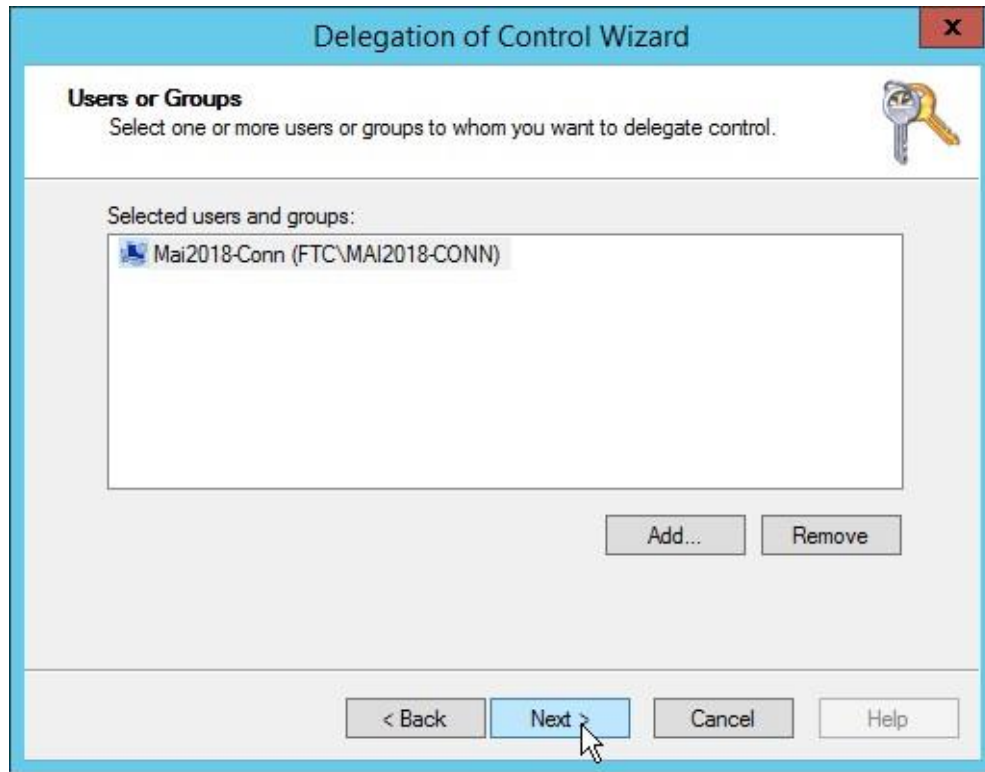
4. In the **Object Types** dialog box, check **Computers**, and then choose **OK**.



5. In the **Select Users, Computers, or Groups** dialog box, in the **Enter the object names to select** box, enter the name of the computer where the Connector is installed.



6. Choose **Check Names** to validate your entry, then choose **OK > Next**.



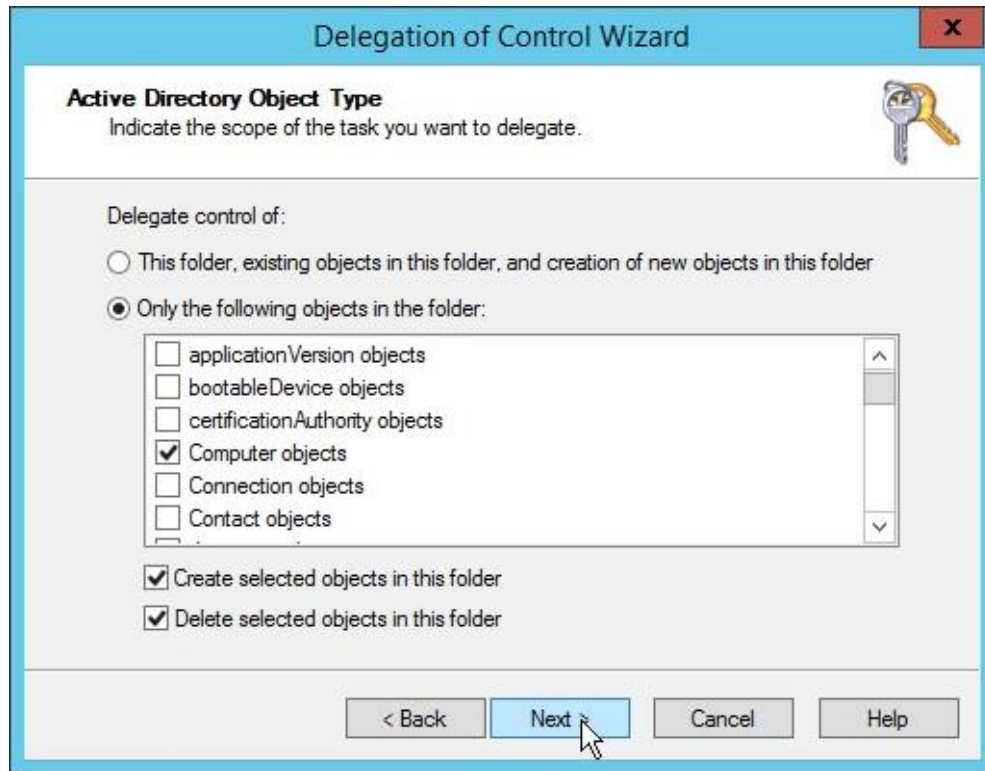
7. Choose **Create a custom task to delegate** > **Next**.



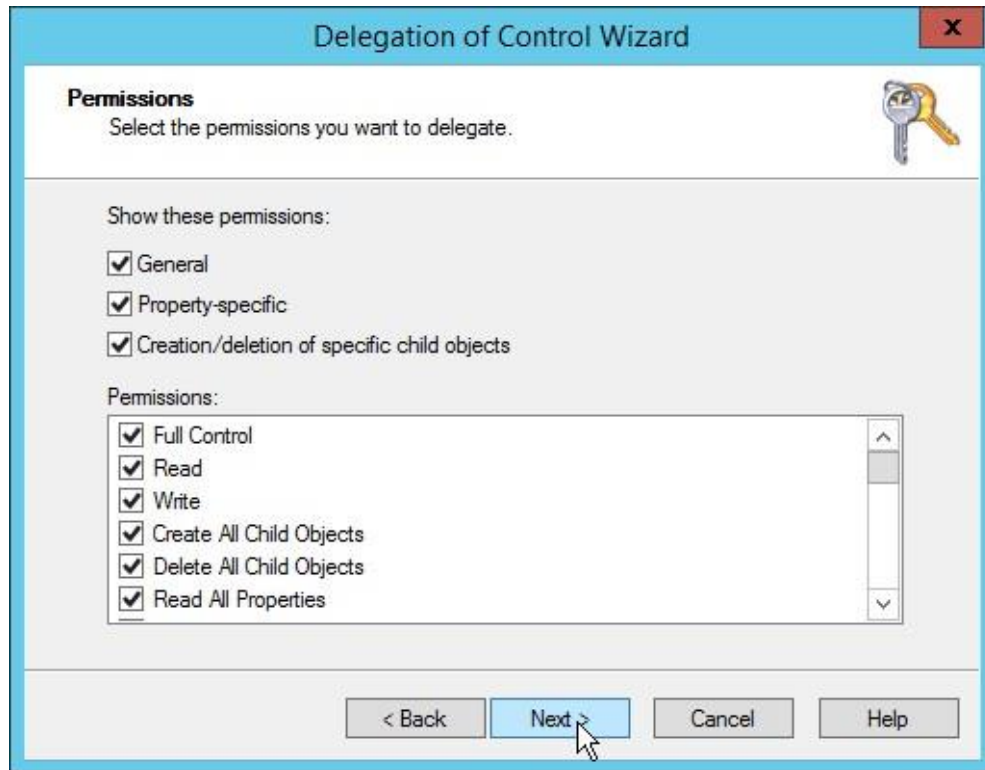
8. Choose **Only the following objects in the folder** and then check the following options:

- **Computer objects**
- **Create selected objects in this folder**
- **Delete selected objects in this folder**

9. Choose **Next**.



10. Under **Permissions**, check **Full Control** (this will check all other options) > **Next**.

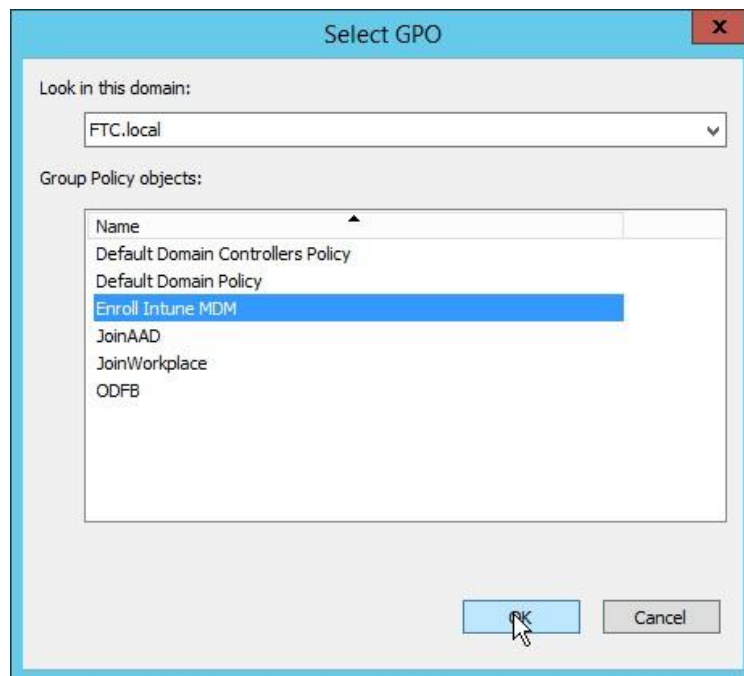
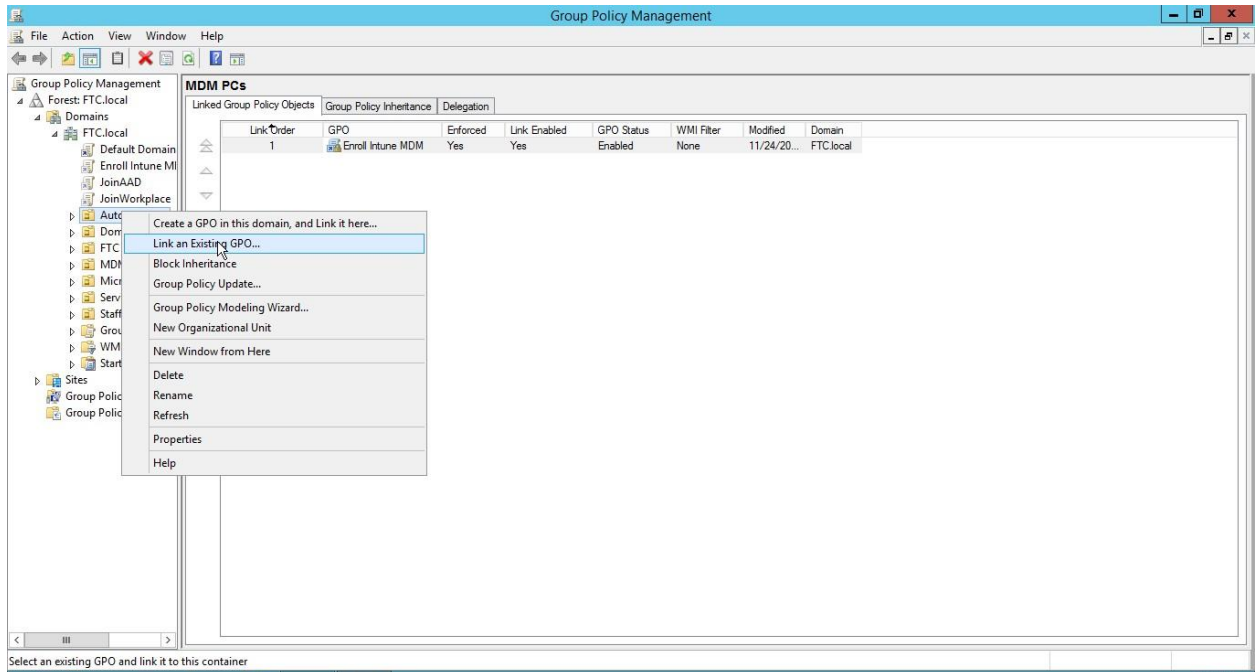


11. Click **Finish**.

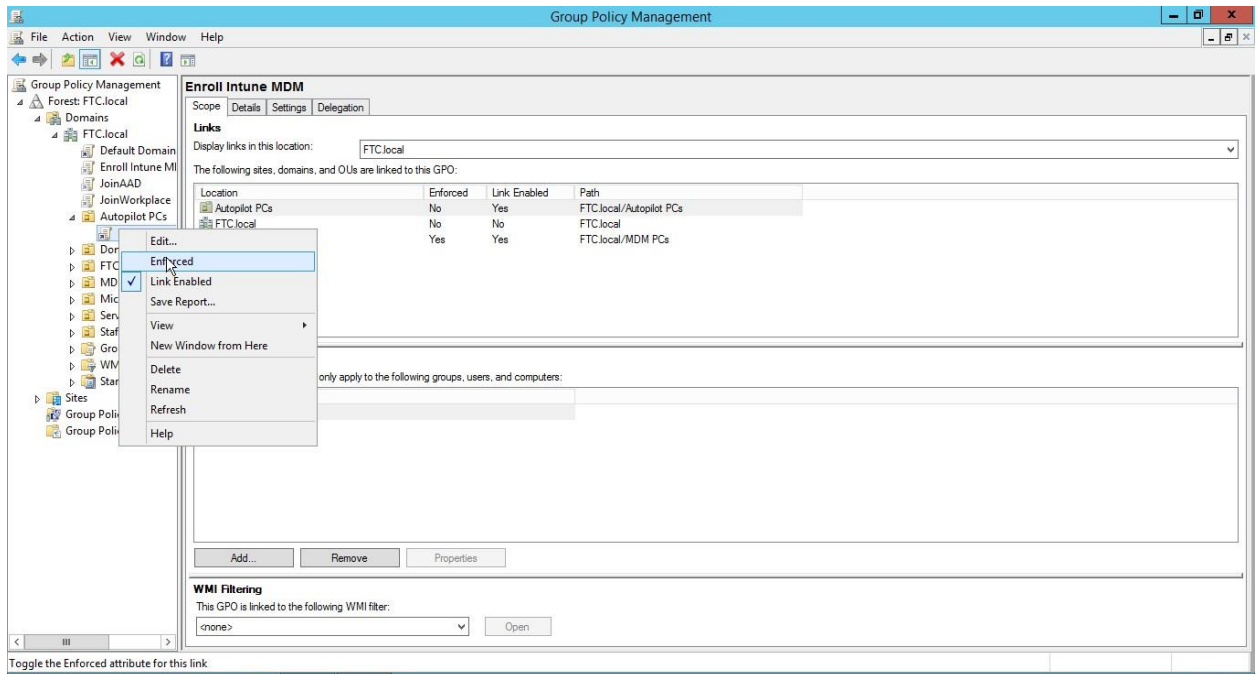


12. You will need to verify that you assign GPO as exist on [step 3 for Automatic Enroll Windows 10 by Using GPO](#)

- On **Group Policy Management console**, Select Computer OU that you want to apply policy on it, right click **link an existing GPO**.



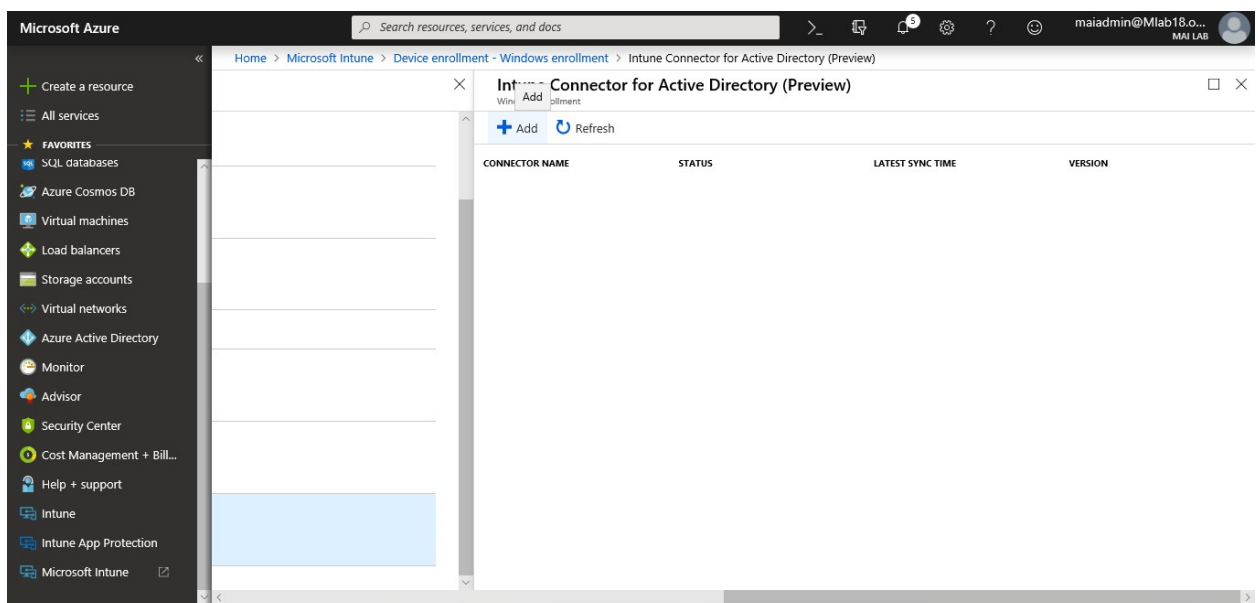
- You can enforce policy to applied in this OU if you have many policies. On link GPO, select **Enforced**.



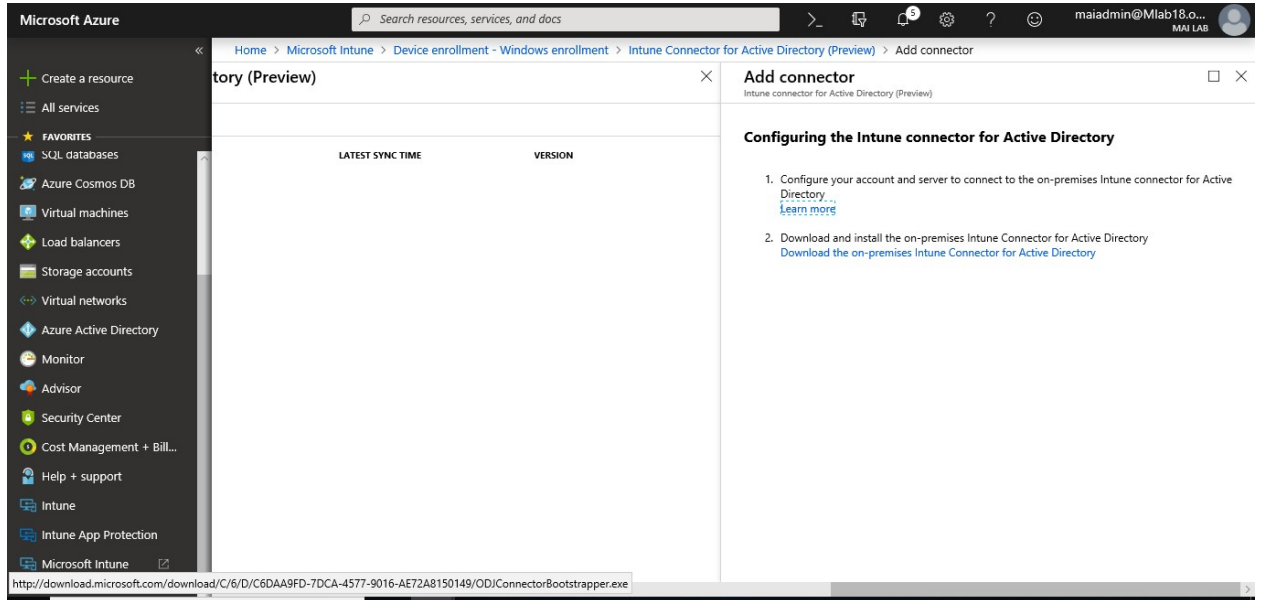
Step 2: Install the Intune Connector

The Intune Connector for Active Directory needs to be installed on a computer running Windows Server 2016 that has access to the Internet and your Active Directory. To increase scale and availability or to support multiple Active Directory domains, you can install multiple connectors in your environment. We recommend installing the connector on a server that is not running any other Intune connectors.

1. In [Intune](#), choose **Device enrollment** > **Windows enrollment** > **Intune Connector for Active Directory (Preview)** > **Add connector**.



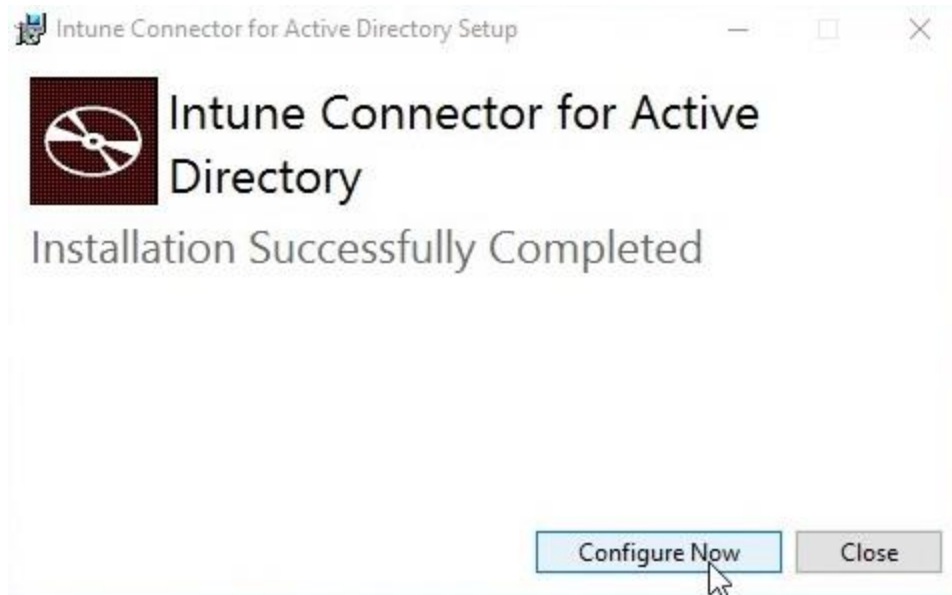
2. Follow the instructions to download the connector.



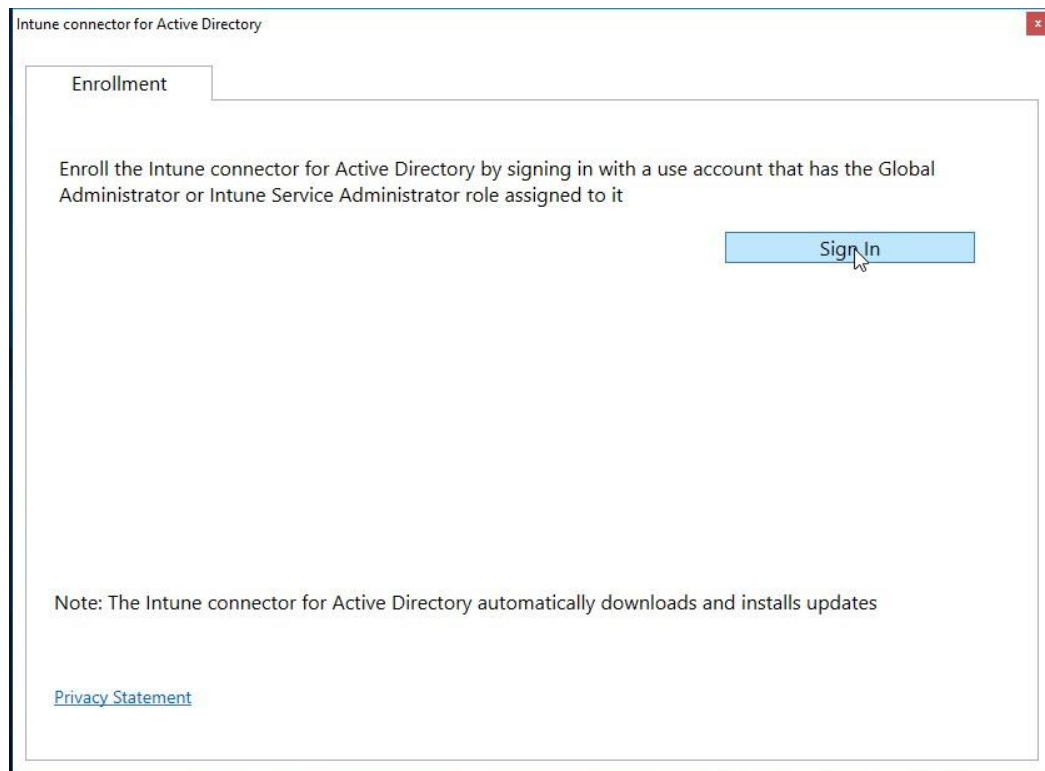
3. Open the downloaded connector setup file to install the connector (ODJConnectorBootstrapper.exe). Check **I agree** & Click **Install**.



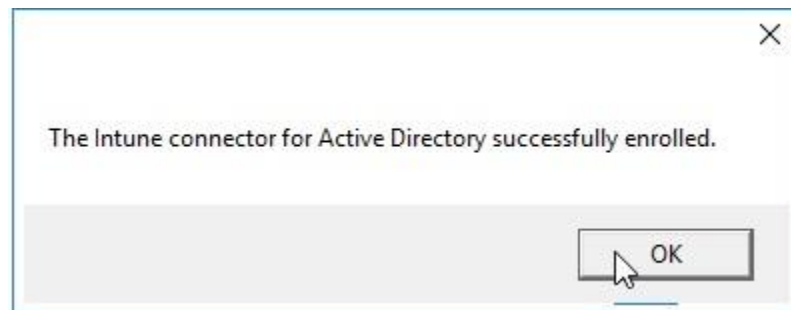
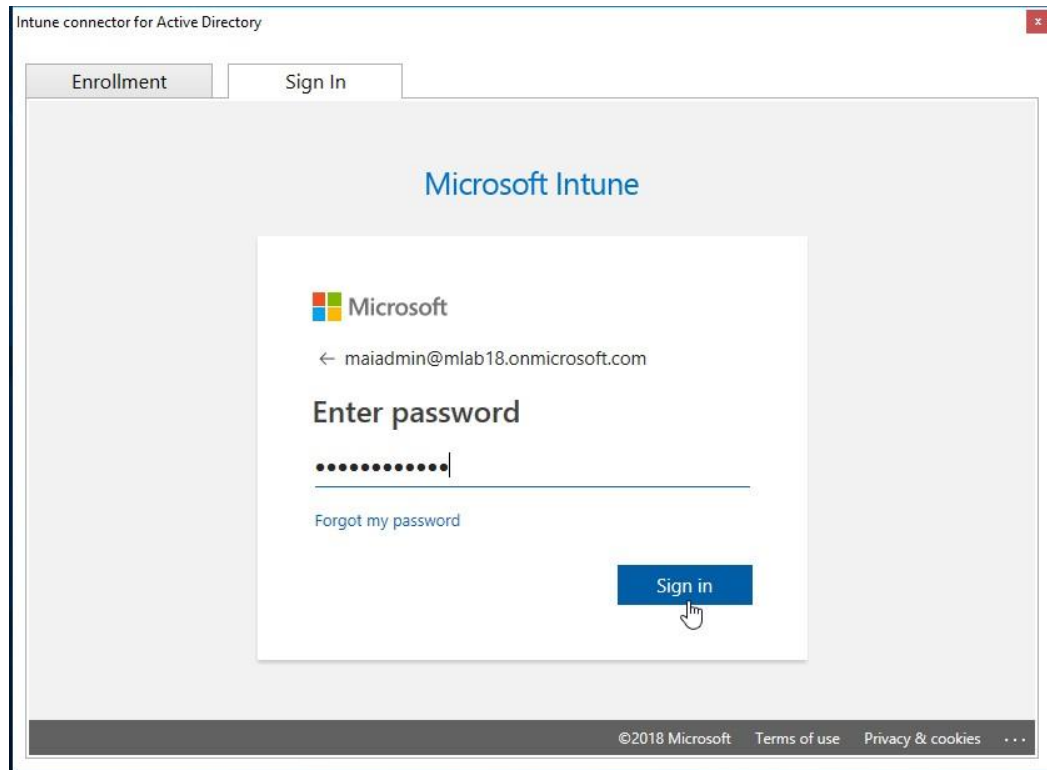
4. At the end of setup, choose **Configure**.



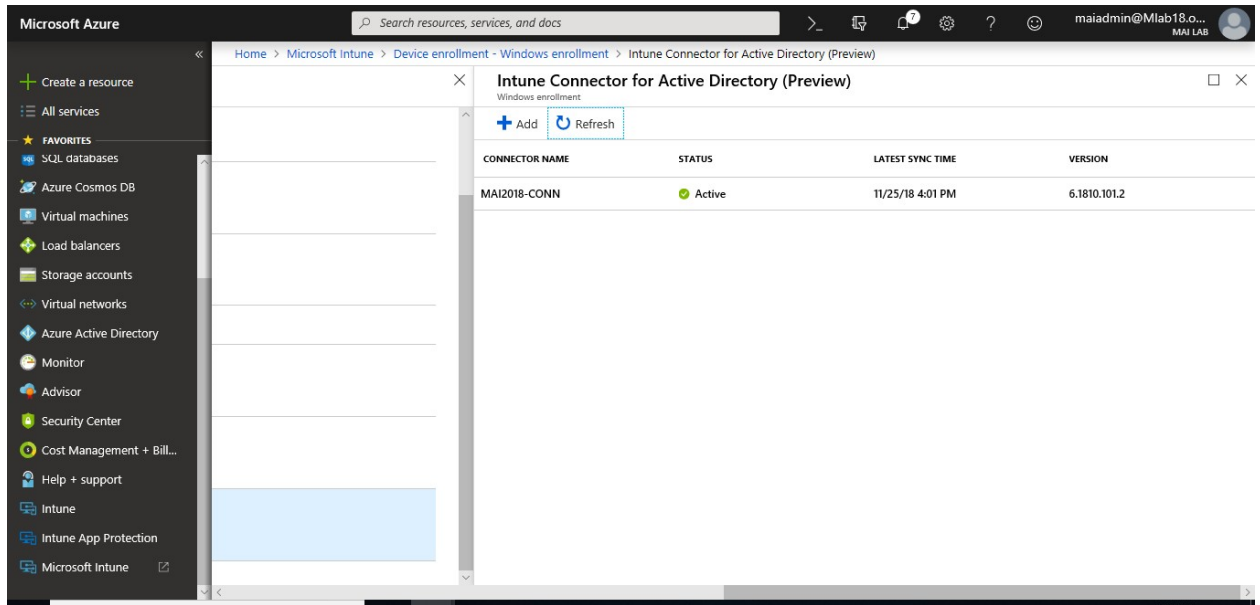
5. Choose **Sign In**.



6. Enter user Global Administrator or Intune Administrator role credentials.



7. Go to **Device enrollment > Windows enrollment > Intune Connector for Active Directory (Preview)** and confirm the connection status is **Active**.



Step 3: Register your Autopilot devices

Choose one of the following ways to enroll your Autopilot devices:

Register Autopilot devices that are already enrolled

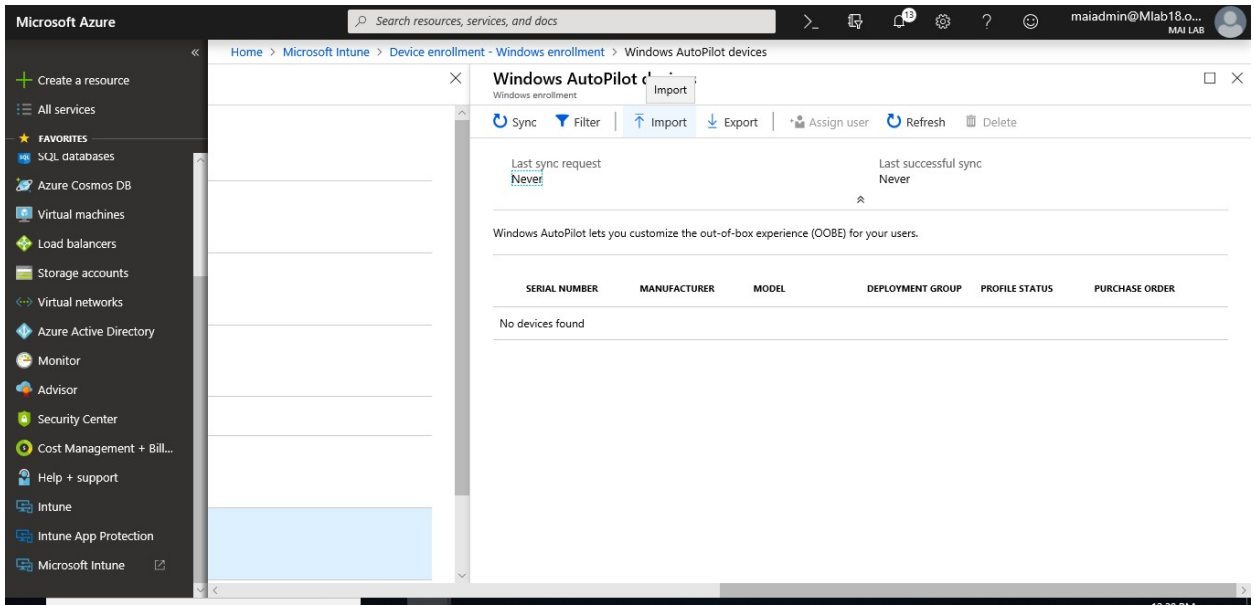
1. Create an Autopilot deployment profile with **Convert all targeted devices to Autopilot** set to **Yes**.
2. Assign the profile to a group containing the members that you want to automatically register with Autopilot.

Register Autopilot devices that aren't enrolled

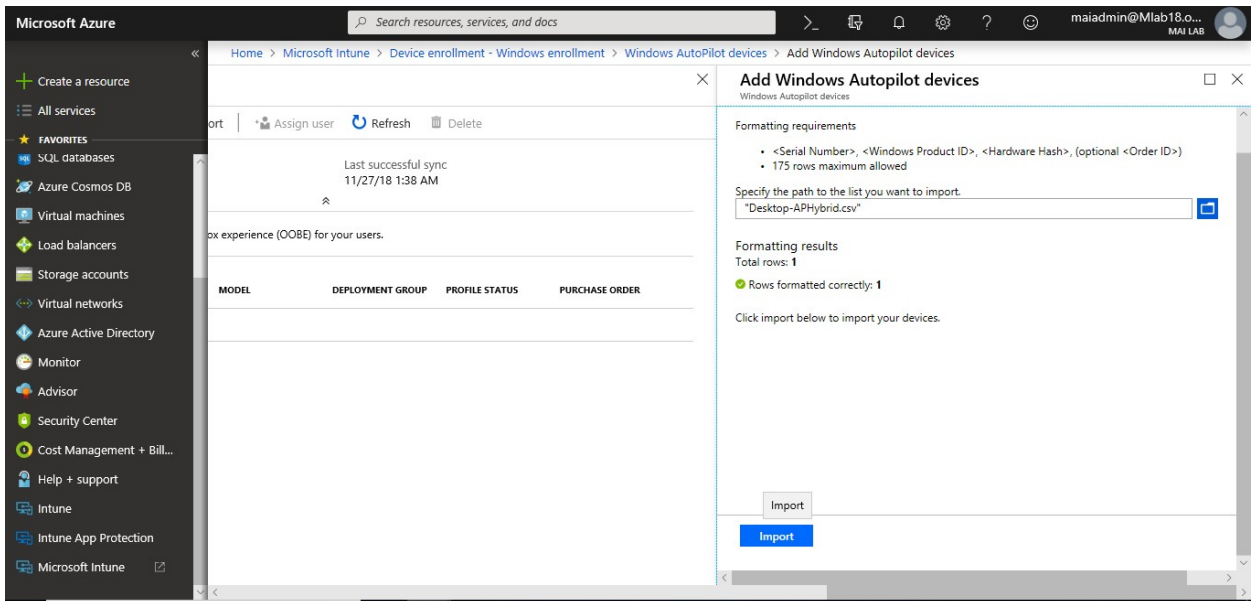
If your devices aren't yet enrolled, you can register them yourself. You can add Windows Autopilot devices by importing a CSV file with their information. You can get device info as shown previously on [step 1 for Autopilot – Azure AD](#).

1. In [Intune in the Azure portal](#), choose **Device enrollment > Windows enrollment > Devices > Import**.

Microsoft Intune step by step on Azure portal

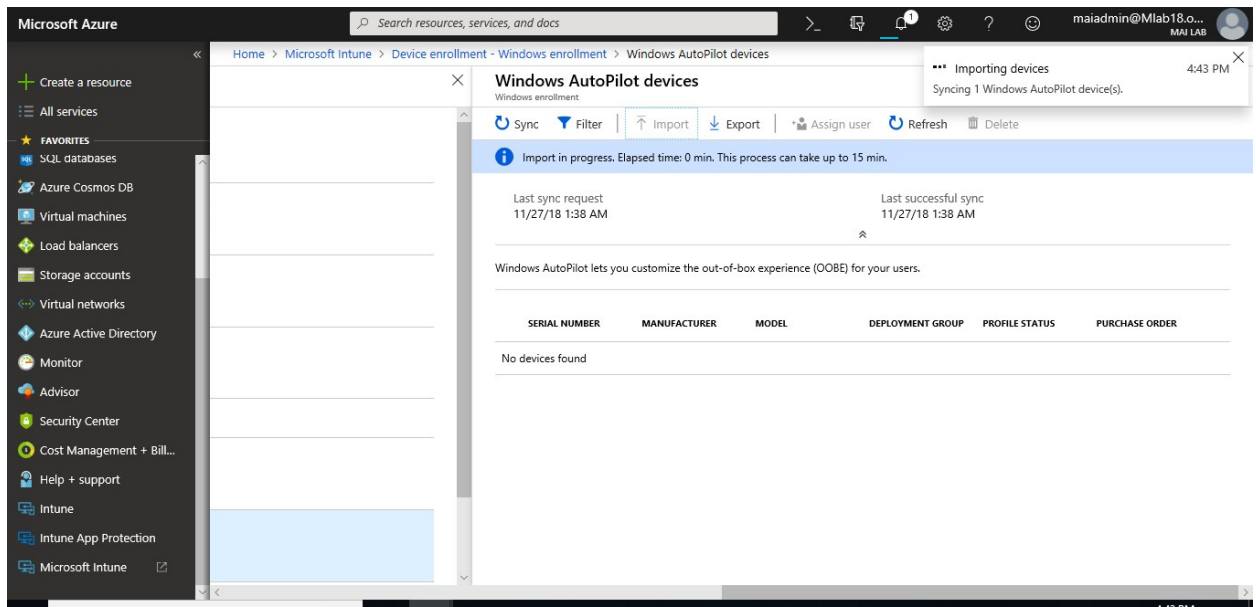


2. Under **Add Windows Autopilot devices**, browse to a CSV file listing the devices that you want to add. The file should list the serial numbers, Windows product IDs, hardware hashes, and optional order IDs of the devices.
3. Choose **Import** to start importing the device information. Importing can take several minutes.

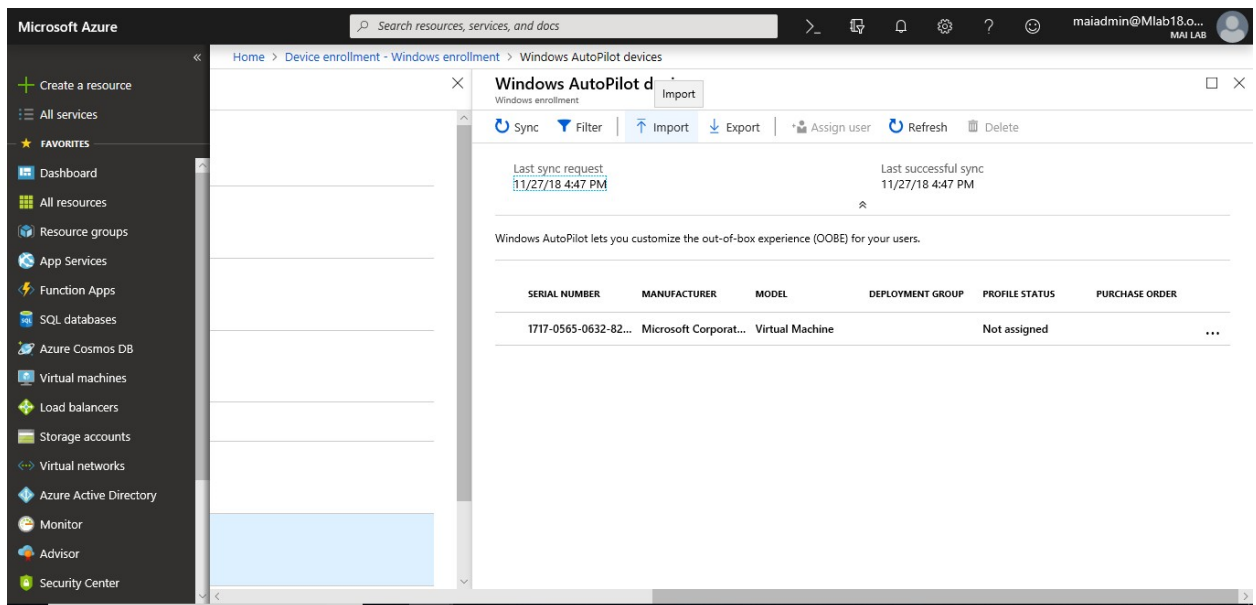


4. After import is complete, choose **Device enrollment > Windows enrollment > Windows Autopilot > Devices > Sync**. A message displays that the synchronization is in progress. The process might take a few minutes to complete, depending on how many devices are being synchronized.

Microsoft Intune step by step on Azure portal



5. Refresh the view to see the new devices.



Register devices from an OEM

If you're buying new devices, some OEMs can register the devices for you.

When Autopilot devices are registered (and before they are enrolled into Intune), you'll see them in three places (with names set to their serial numbers):

- Autopilot Devices blade in the Intune in the Azure portal (**Device enrollment > Windows enrollment > Devices**).

Microsoft Intune step by step on Azure portal

- Azure AD devices blade in the Intune in the Azure portal (**Devices > Azure AD Devices**).
- AAD All Devices blade in Azure Active Directory in the Azure portal (**Devices > All Devices**).

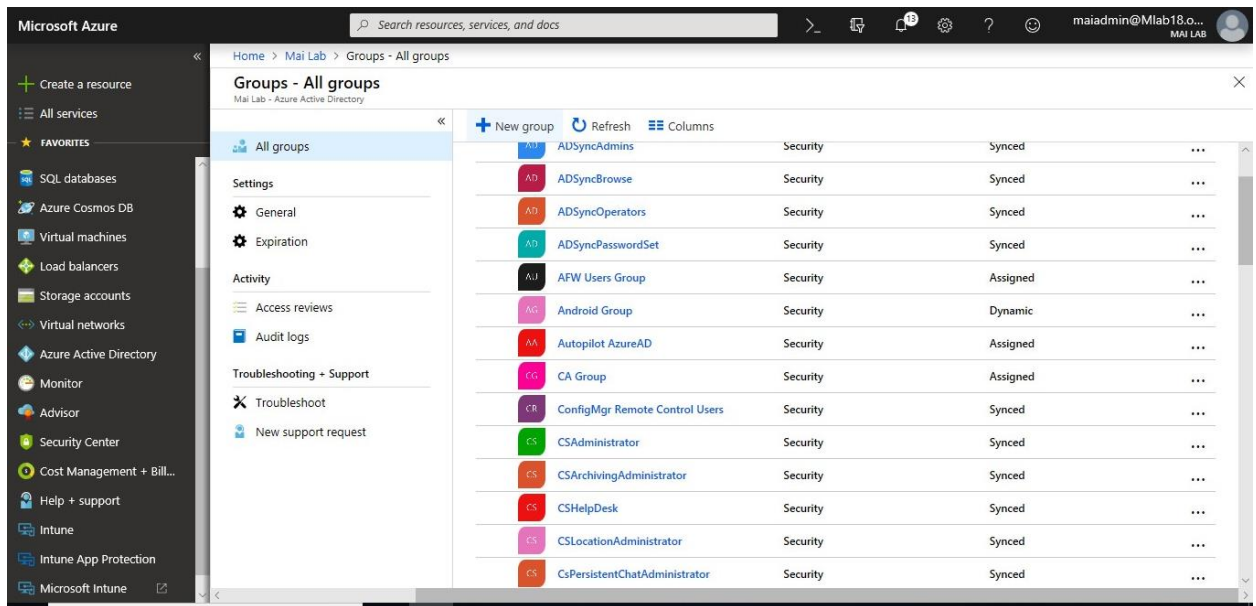
After Autopilot devices are enrolled, you'll see them in four places:

- Autopilot Devices Blade in the Intune in the Azure portal (**Device enrollment > Windows enrollment > Devices**).
- Azure AD devices blade in the Intune in the Azure portal (**Devices > Azure AD Devices**).
- AAD All Devices blade in Azure Active Directory in the Azure portal (**Devices > All Devices**).
- All Devices blade in the Intune in the Azure portal (**Devices > All Devices**).

After Autopilot devices are enrolled, their device names change to the hostname of the device. By default, it begins with "DESKTOP-".

Step 4: Create a device group

1. In [Intune portal](#), choose **Groups > New group**.

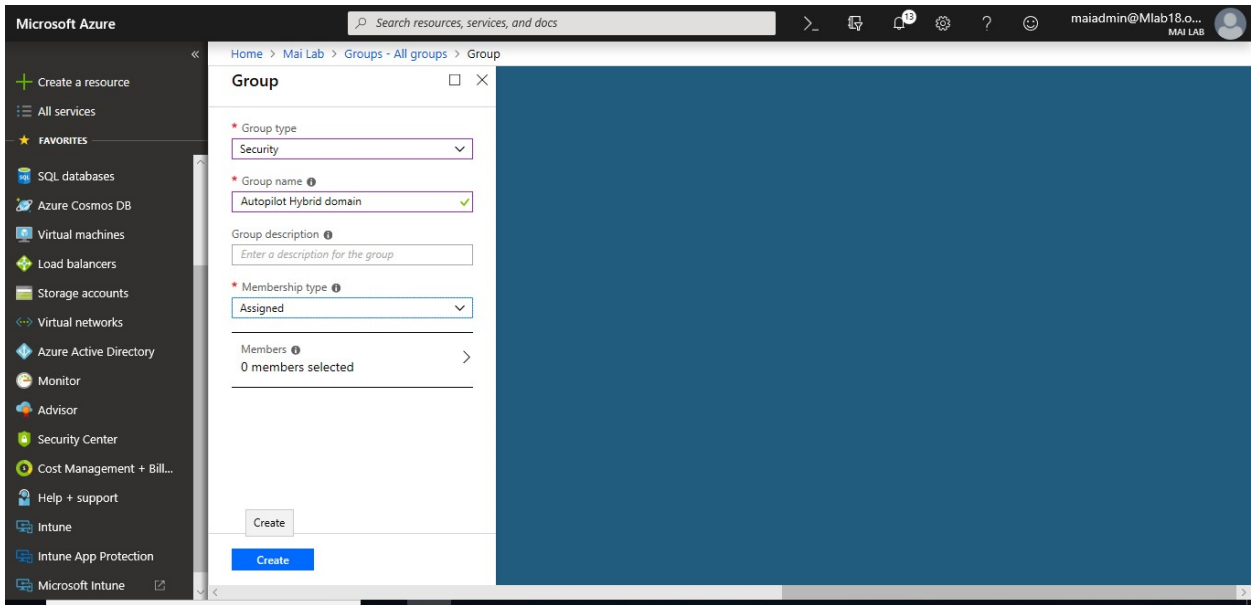


2. In the **Group** blade:

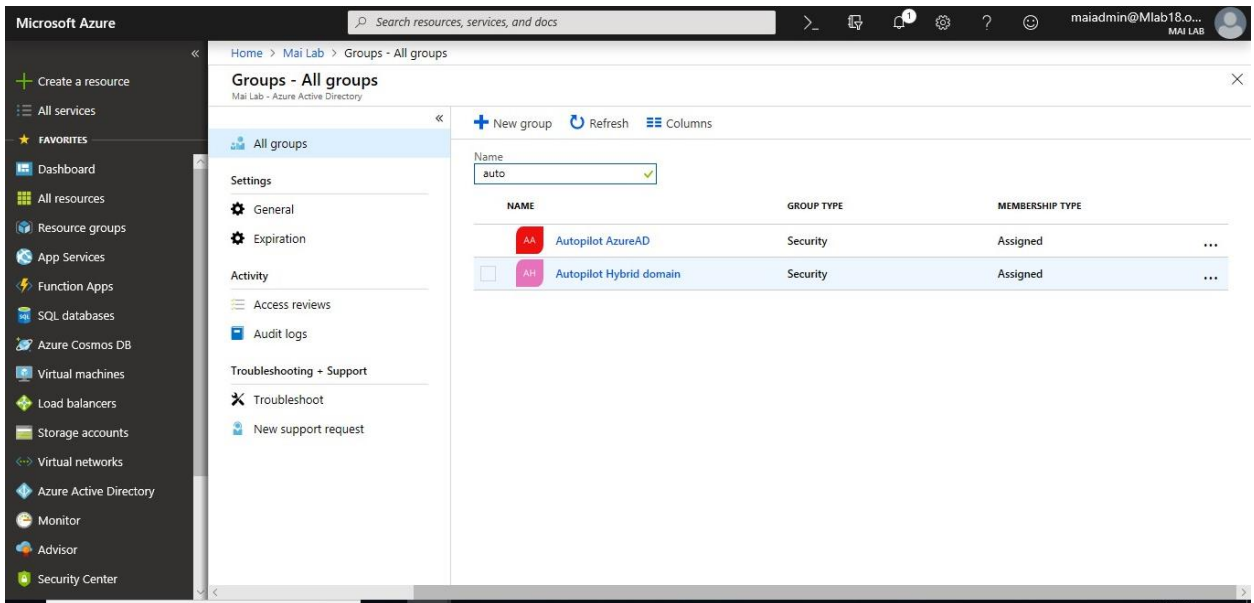
- For **Group type**, choose **Security**.
- Type a **Group name** and **Group description**.
- Choose a **Membership type**.

5. Choose **Create**.

Microsoft Intune step by step on Azure portal

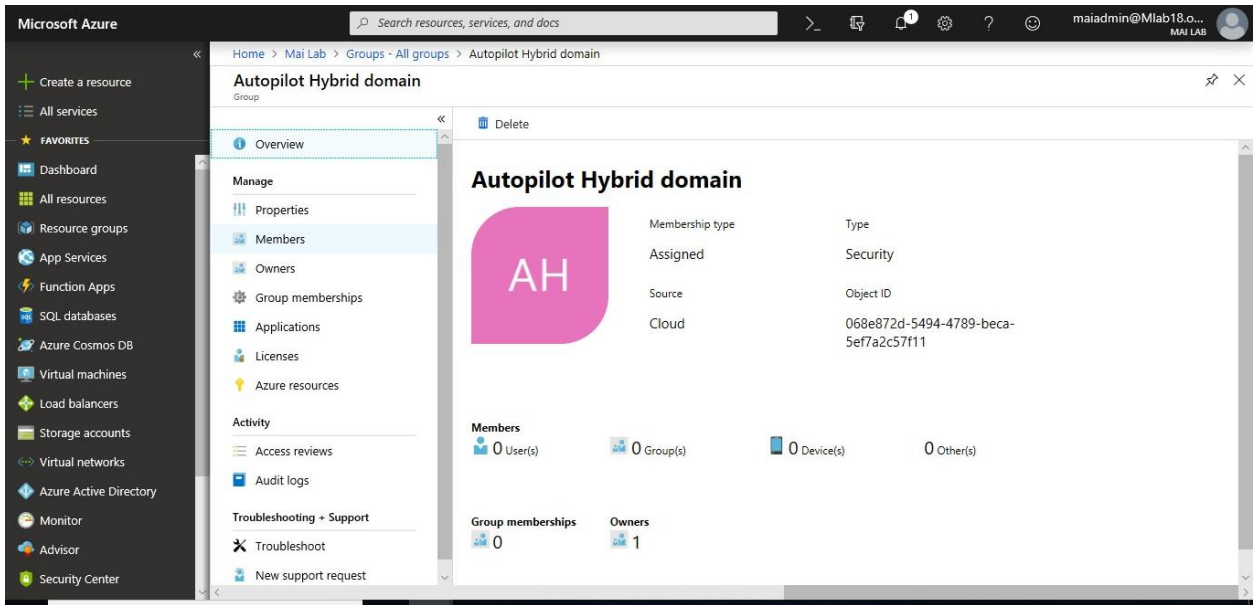


6. Add Devices to this assigned Group, Click on Group that you created.

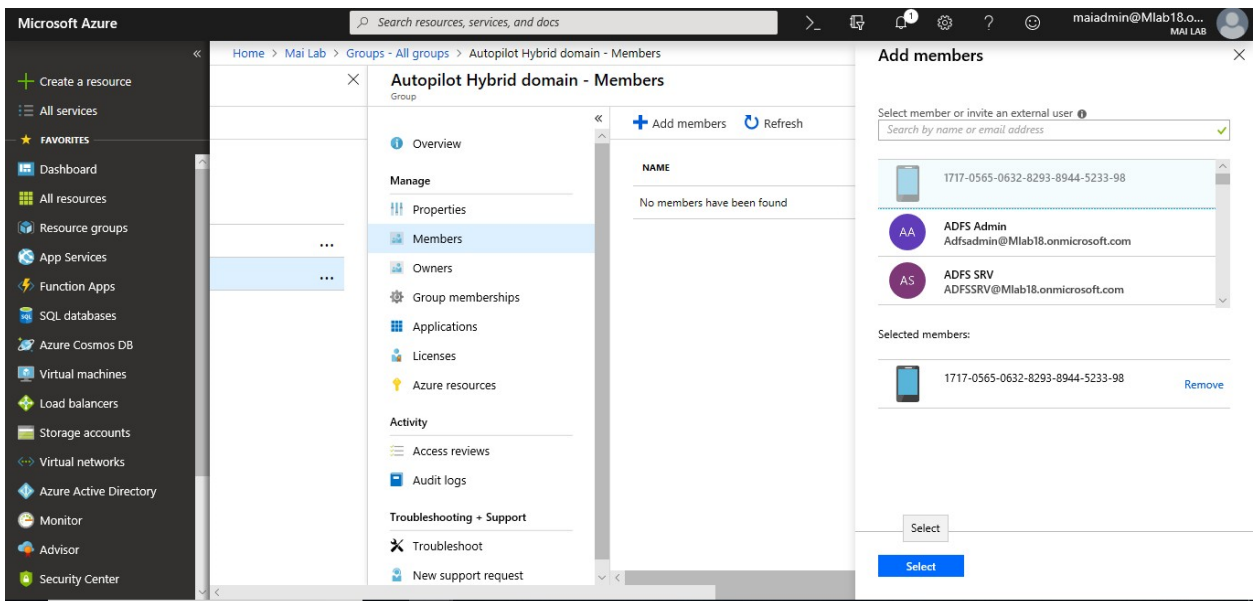


7. Click **Members**.

Microsoft Intune step by step on Azure portal

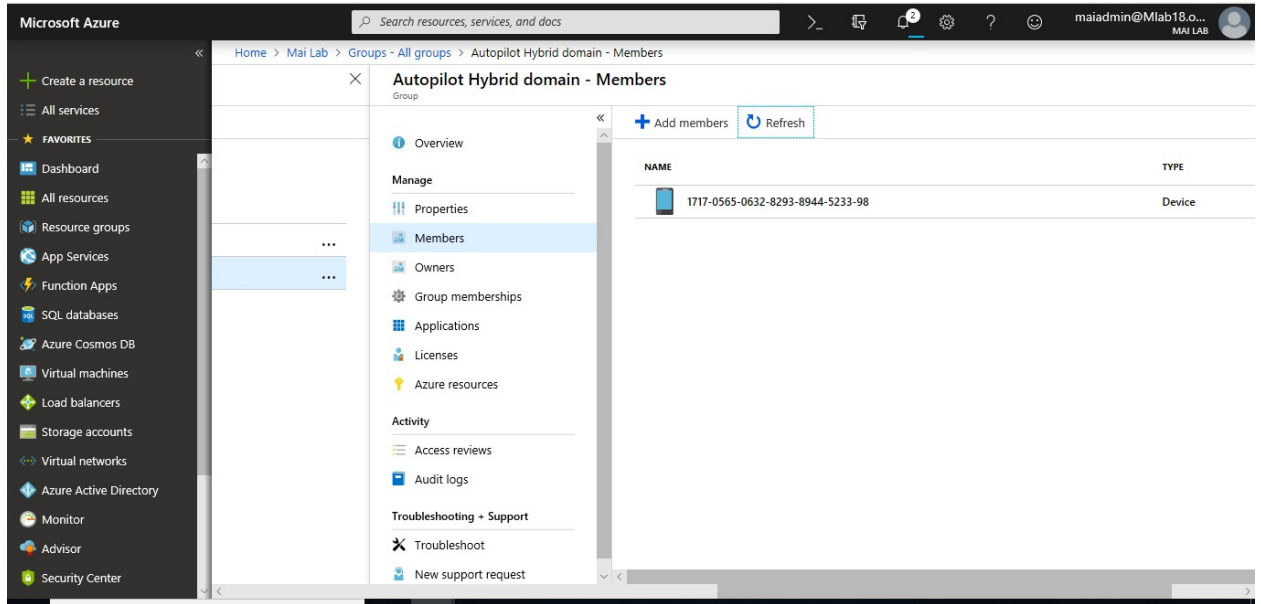


8. Click **Add Members**. Select the device that you want.



9. Click **Refresh** to see that device add on Group.

Microsoft Intune step by step on Azure portal

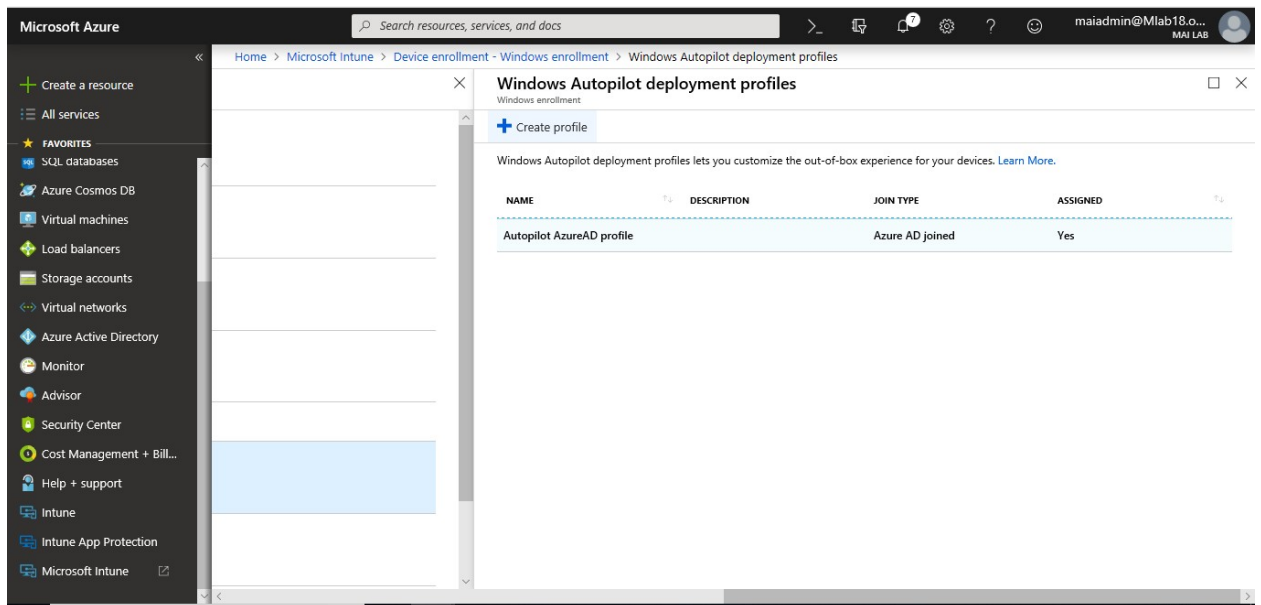


Note: On my lab, I created this group assigned Group and add device manually to don't have any conflict between Group for Hybrid domain join & Group for Azure AD but you can add dynamic group as show previously on [step 3 for Autopilot – Azure AD](#).

Step 5: Create and assign an Autopilot deployment profile

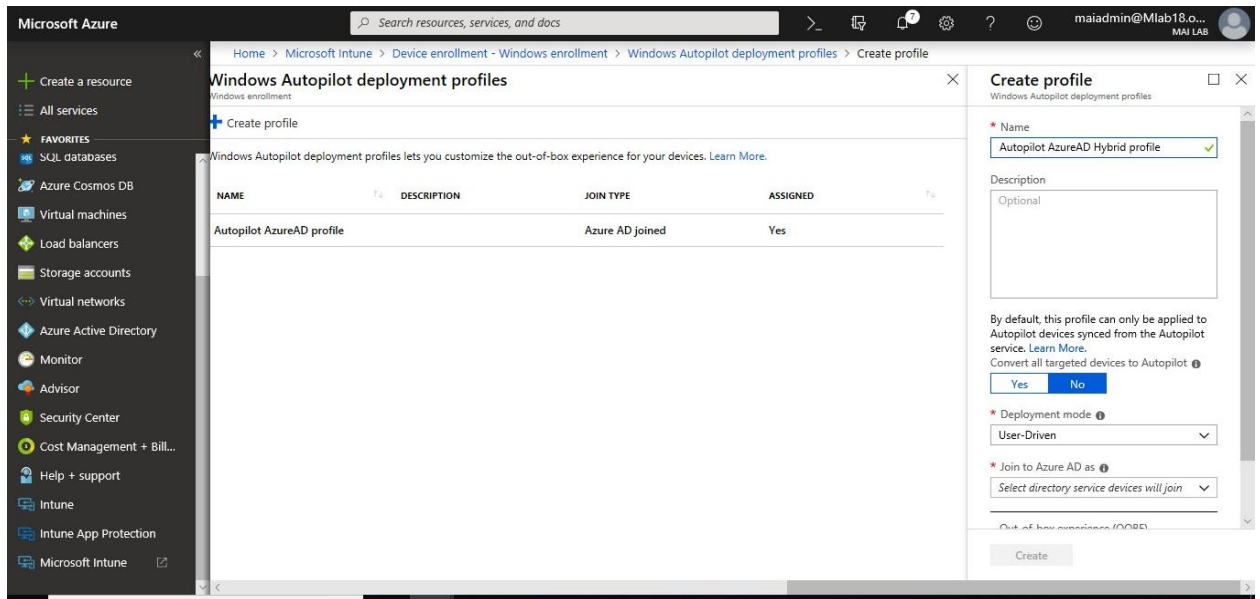
Autopilot deployment profiles are used to configure the Autopilot devices.

1. In [Intune portal](#), choose **Device enrollment > Windows enrollment > Deployment Profiles > Create Profile**.

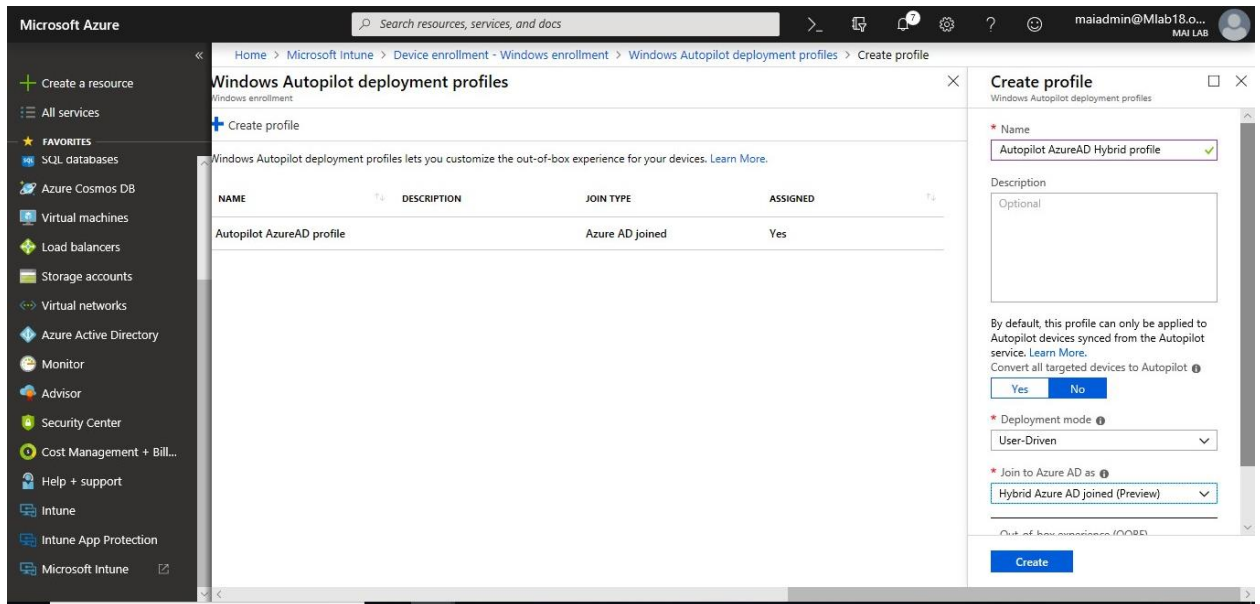


Microsoft Intune step by step on Azure portal

2. Type a **Name** and optional **Description**.
3. For **Deployment mode**, choose **User-driven**.

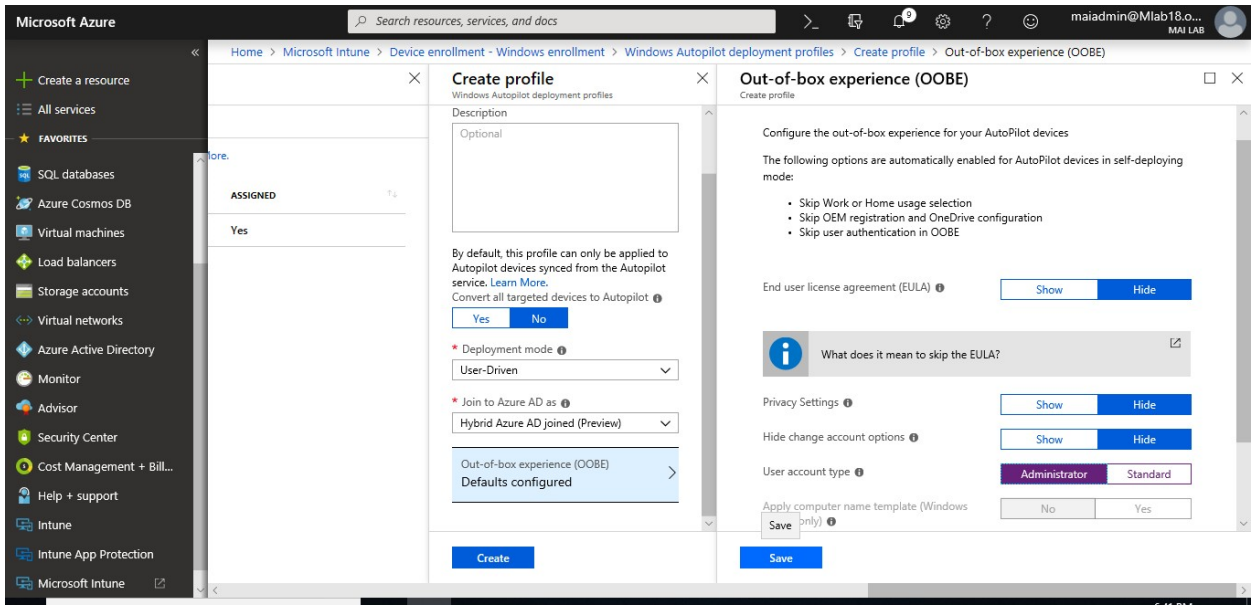


4. In the **Join to Azure AD as** box, choose **Hybrid Azure AD joined (Preview)**.

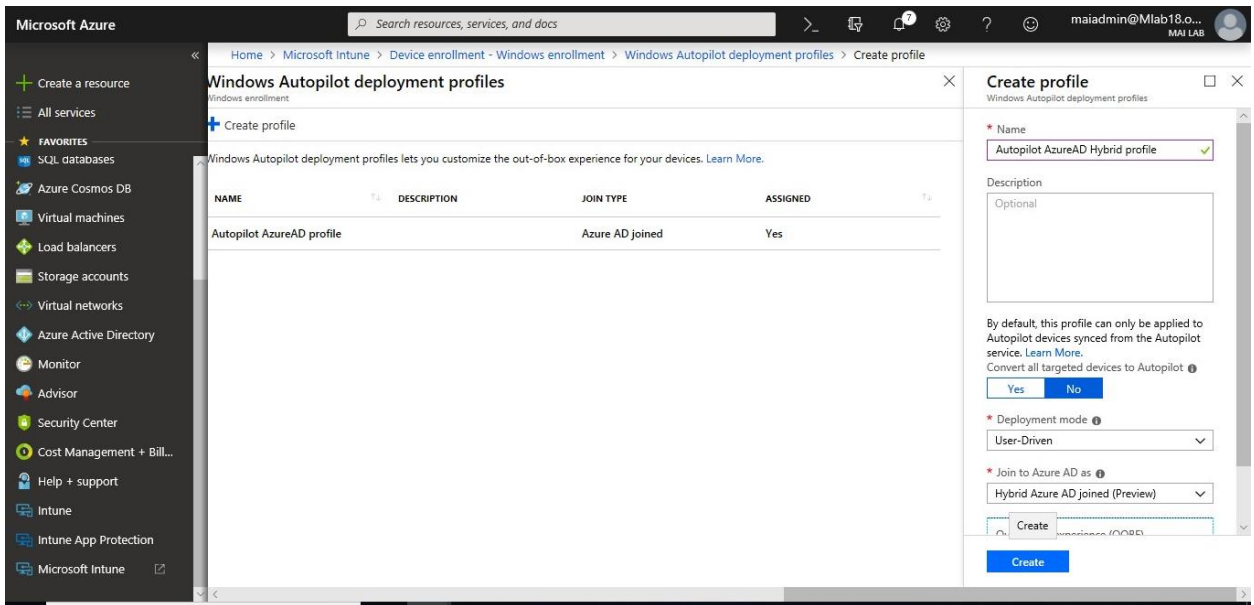


5. Choose **Out-of-box experience (OOBE)**, configure the options as needed, and then choose **Save**.

Microsoft Intune step by step on Azure portal

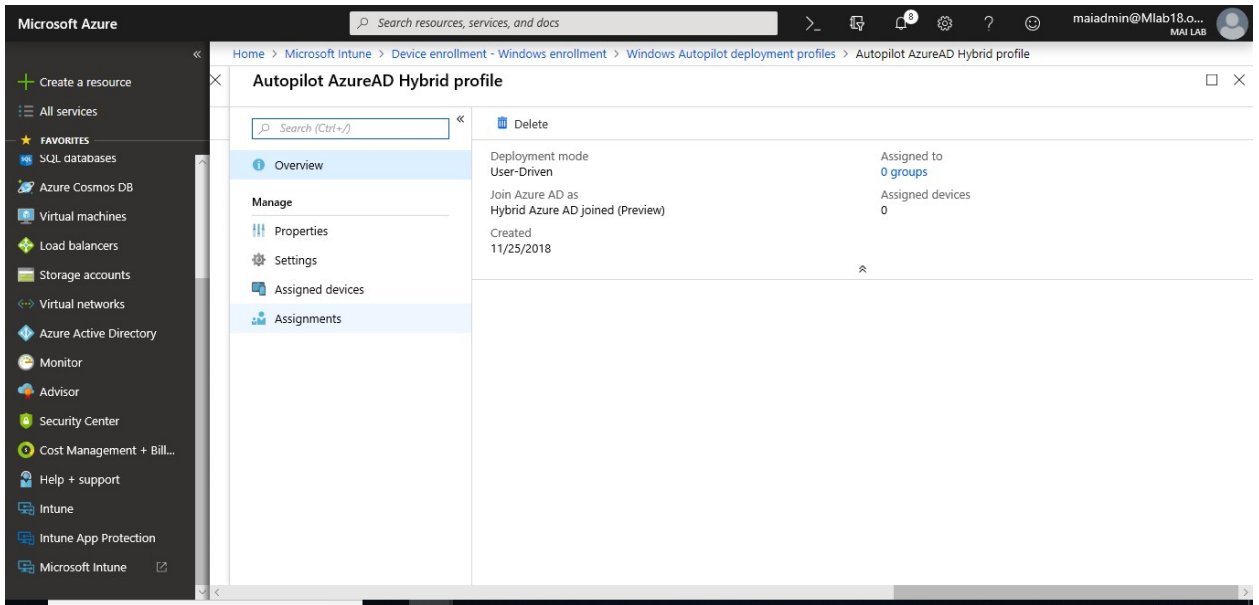


6. Choose **Create** to create the profile.

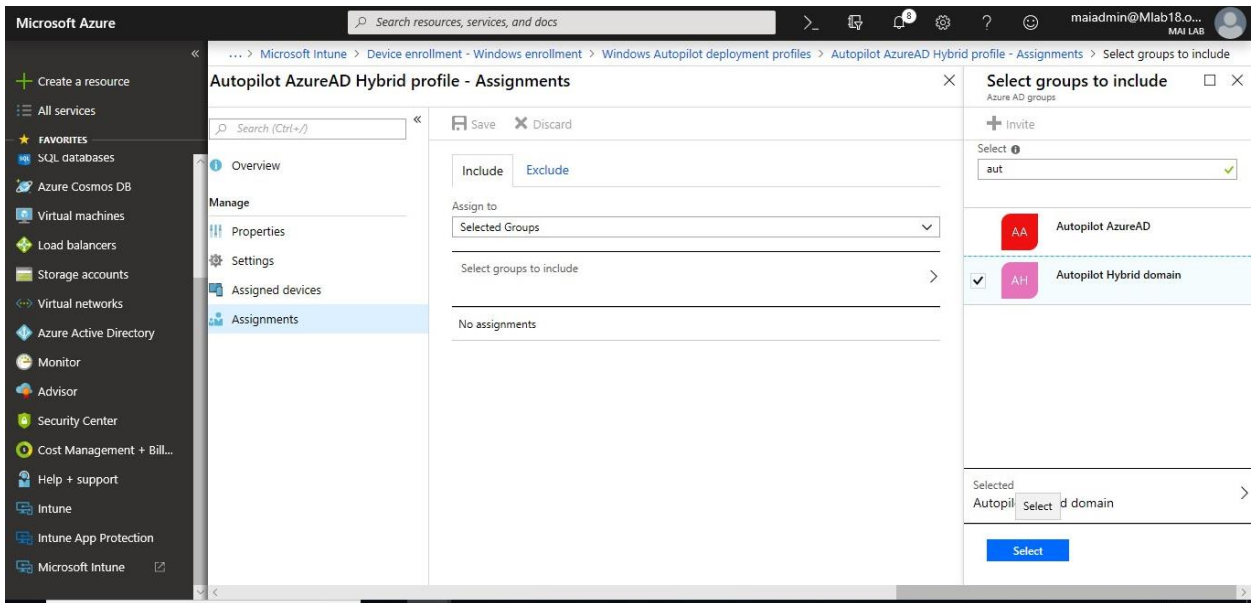


7. In the profile blade, choose **Assignments**.

Microsoft Intune step by step on Azure portal

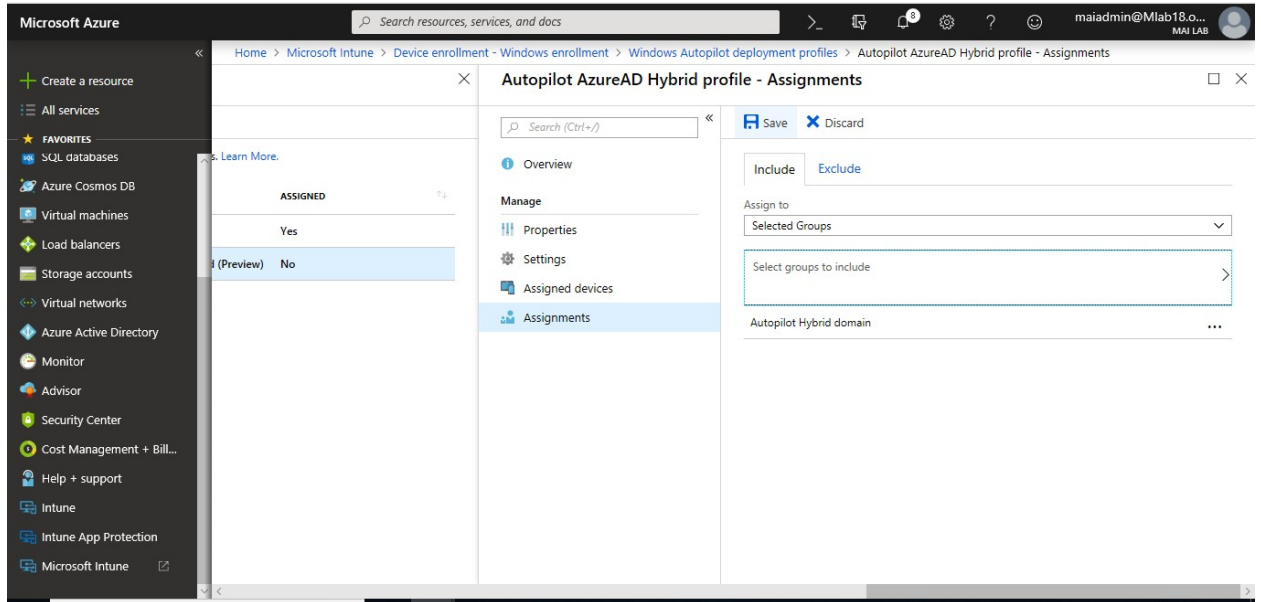


8. Choose **Select groups** > in the **Select groups** blade, choose the device group > **Select**.



9. Click **Save**.

Microsoft Intune step by step on Azure portal



It will take around 15 minutes for the device profile status to change from **Not assigned** to **Assigning** and finally to **Assigned**.

Step 6: Turn on the enrollment status page (optional)

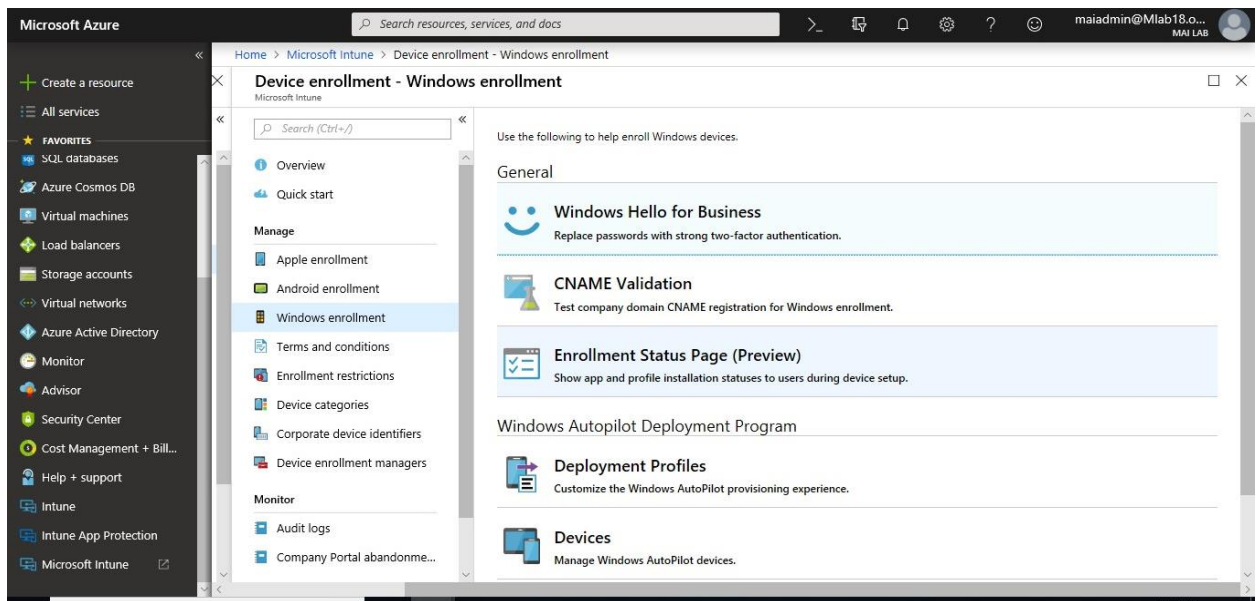
The following settings can be configured to customize behavior of the enrollment status page:

Setting	Yes	No
Show app and profile installation progress	The enrollment status page is displayed.	The enrollment status page is not displayed.
Block device use until all apps and profiles are installed	The settings in this table are made available to customize behavior of the enrollment status page, so that the user can address potential installation issues.	The enrollment status page is displayed with no additional options to address installation failures.
Allow users to reset device if installation error occurs	A Reset device button is displayed if there is an installation failure.	The Reset device button is not displayed if there is an installation failure.
Allow users to use device if installation error occurs	A Continue anyway button is displayed if there is an installation failure.	The Continue anyway button is not displayed if there is an installation failure.
Show error when installation takes longer than specified number of minutes	Specify the number of minutes to wait for installation to complete. A default value of 60 minutes is entered.	
Show custom message when an error occurs	A text box is provided where you can specify a custom message to display in case of an installation error.	The default message is displayed: Oh no! Something didn't do what it was supposed to. Please contact your IT department.

Setting	Yes	No
Allow users to collect logs about installation errors	If there is an installation error, a Collect logs button is displayed. If the user clicks this button they are asked to choose a location to save the log file MDMDiagReport.cab	The Collect logs button is not displayed if there is an installation error.

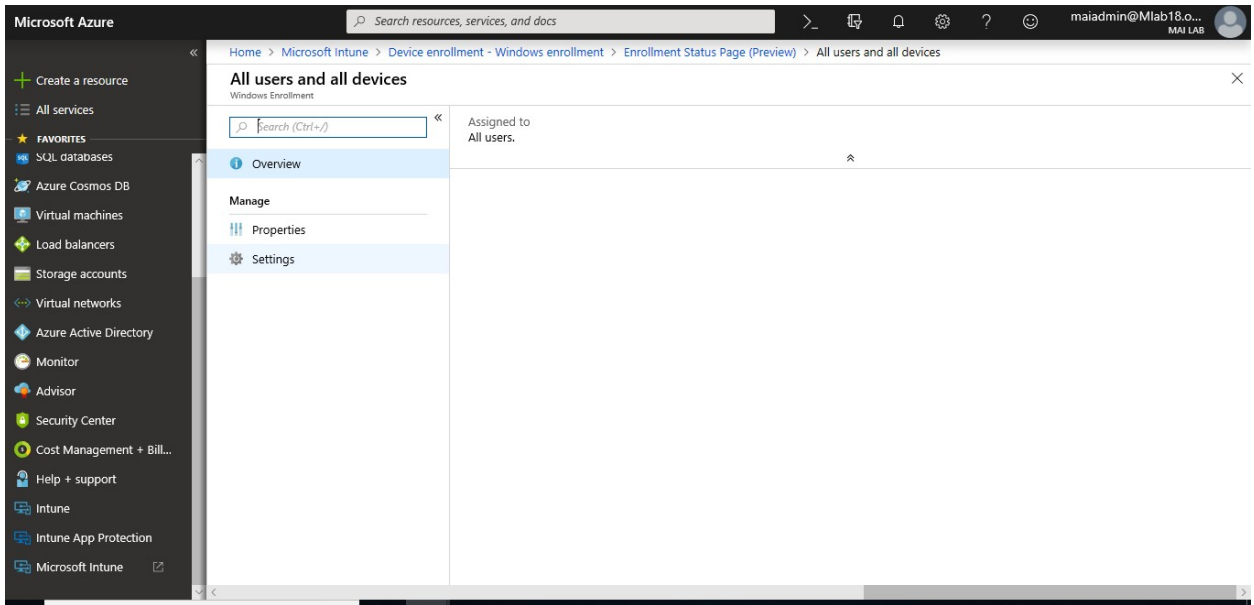
To Configure Enrollment settings, you can follow below steps

1. In [Intune portal](#), choose **Device enrollment** > **Windows enrollment** > **Enrollment Status Page (Preview)**.

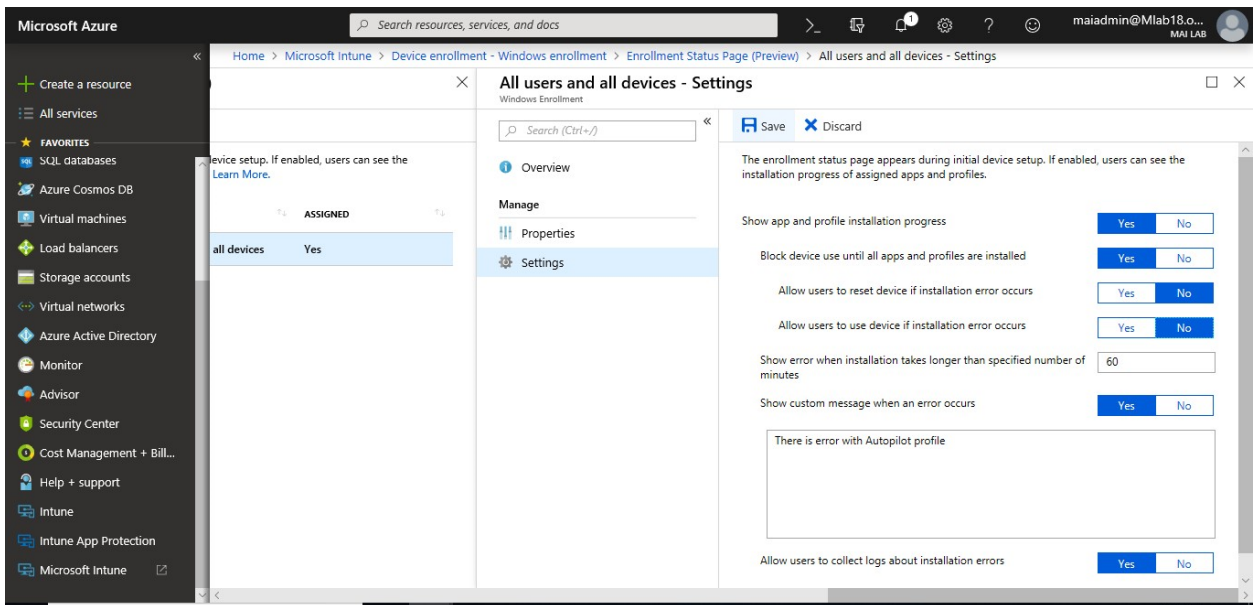


2. In the **Enrollment Status Page** blade, choose **Default** > **Settings**.

Microsoft Intune step by step on Azure portal



3. For **Show app and profile installation progress**, choose **Yes**. Configure the other options as needed.

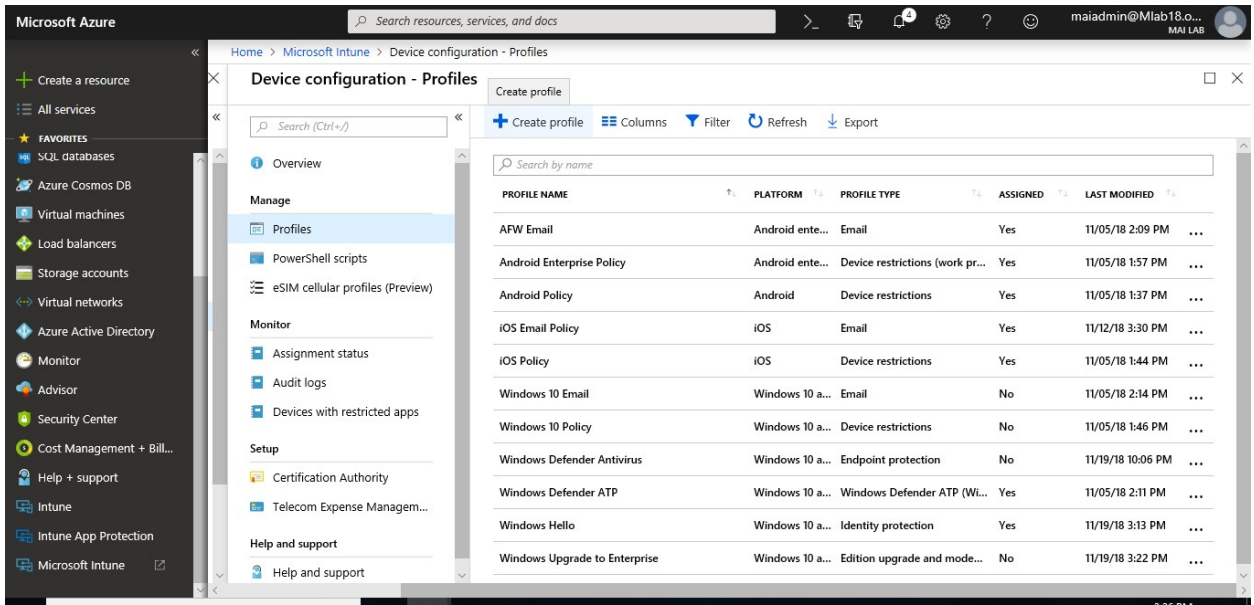


4. Choose **Save**.

Step 7: Create and assign a Domain Join profile

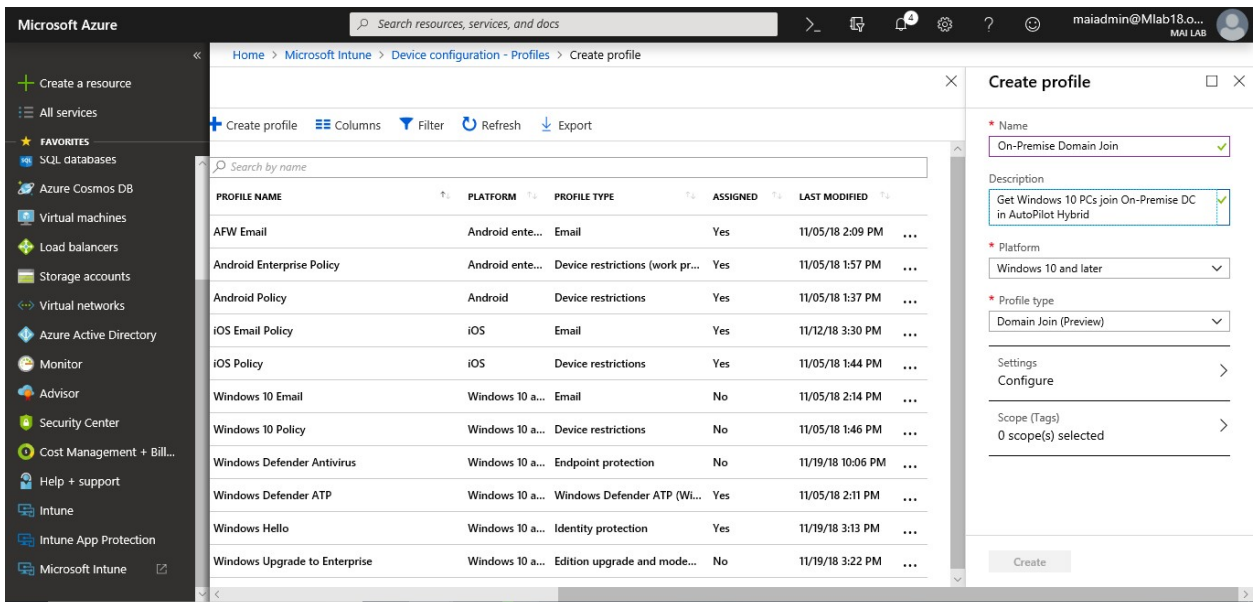
1. In [Intune portal](#), choose **Device configuration** > **Profiles** > **Create Profile**.

Microsoft Intune step by step on Azure portal



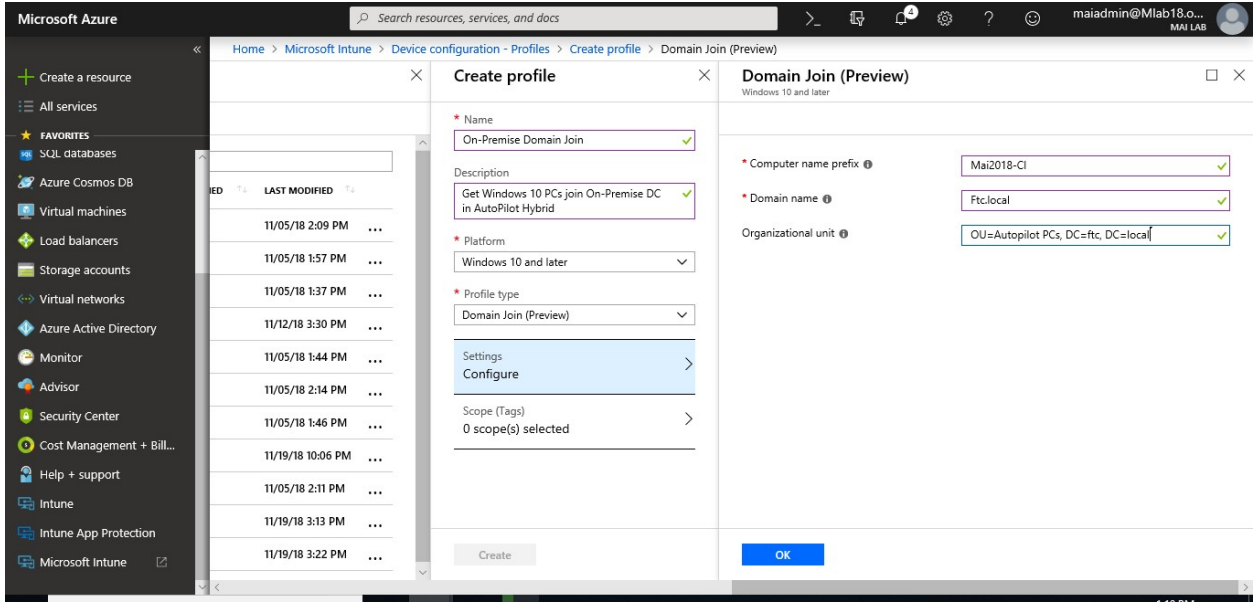
2. Enter the following properties:

- **Name:** Enter a descriptive name for the new profile.
- **Description:** Enter a description for the profile.
- **Platform:** Choose **Windows 10 and later**.
- **Profile type:** Choose **Domain Join (Preview)**.

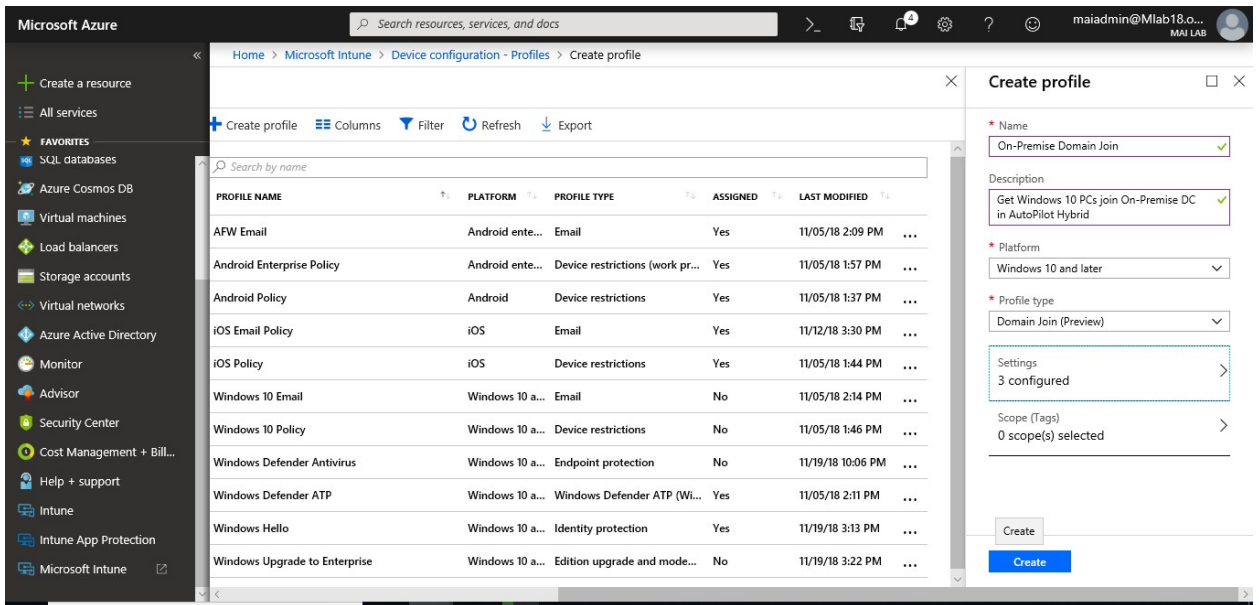


3. Choose **Settings** and provide a **Computer name prefix**, **Domain name**, and **Organizational unit**.

Microsoft Intune step by step on Azure portal

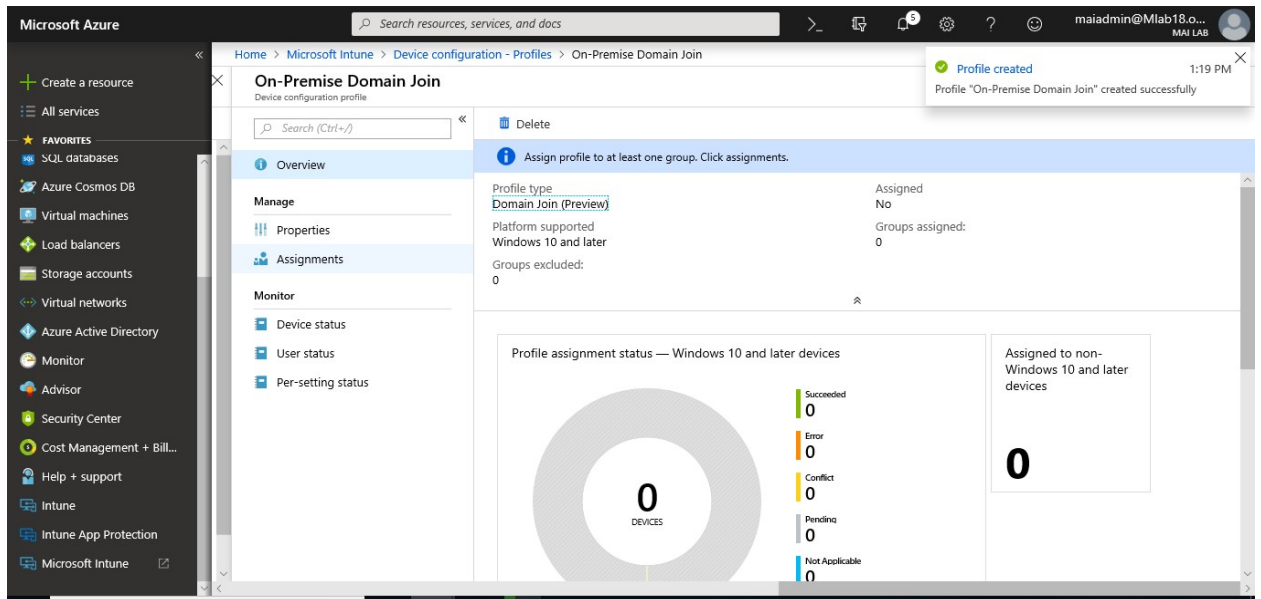


4. Choose **OK** > **Create**. The profile is created and appears in the list.

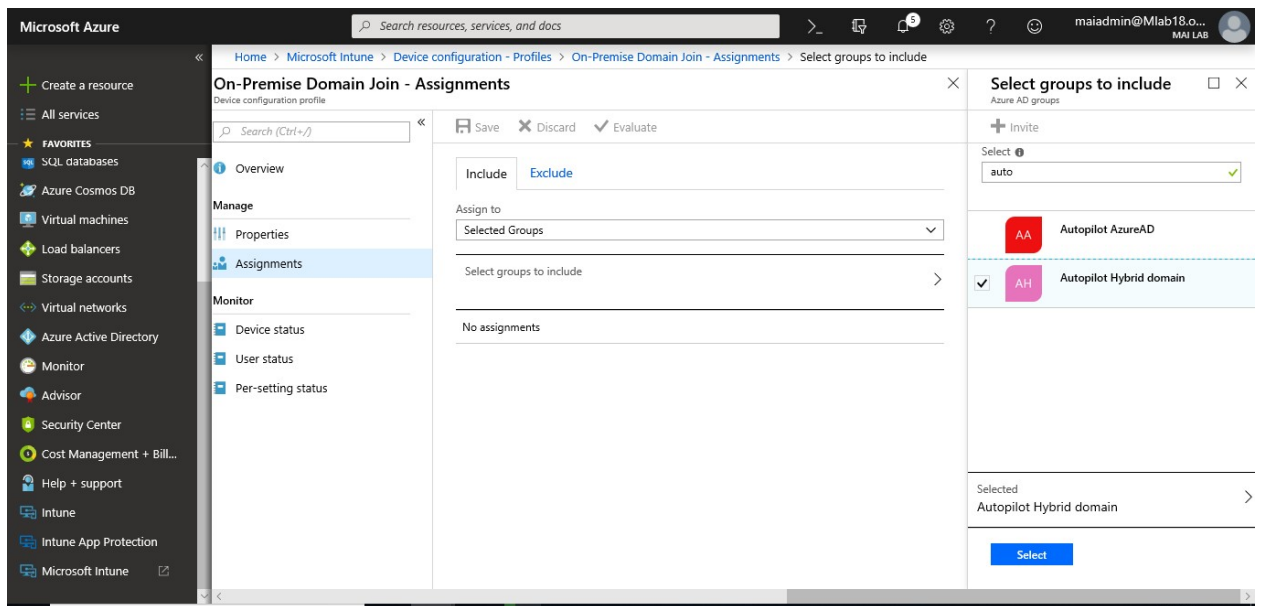


5. To assign the profile, In the list of profiles, select the profile you want to assign, and then select **Assignments**.

Microsoft Intune step by step on Azure portal

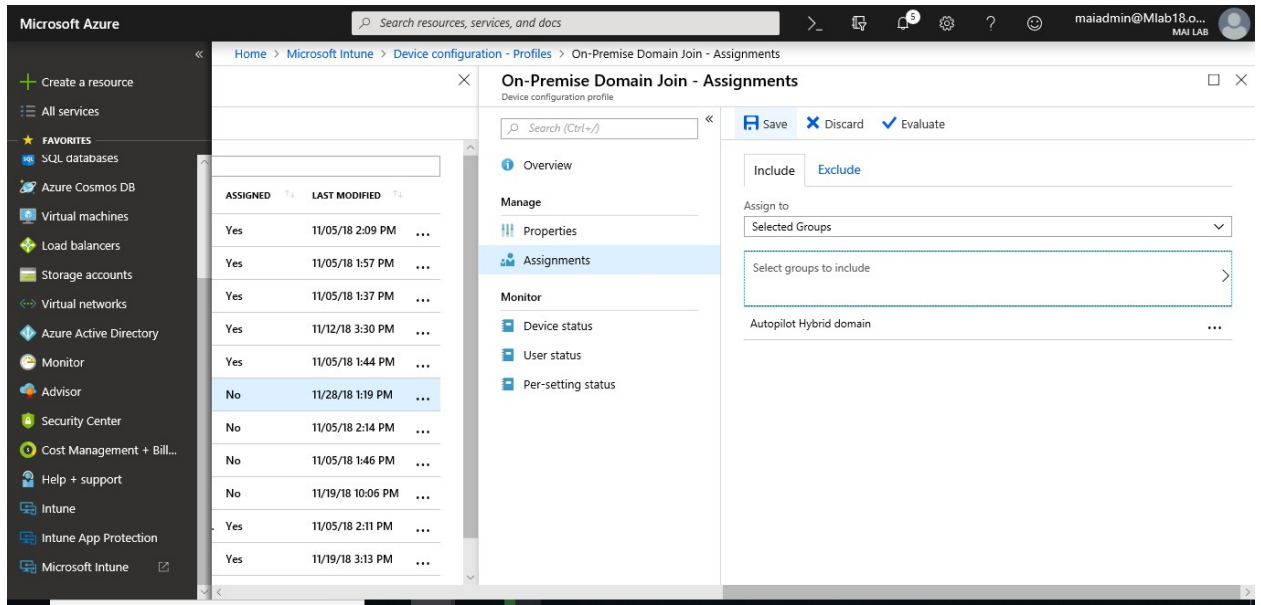


6. Choose to **Include** groups or **Exclude** groups, and then select groups.



7. When you are done, select **Save**.

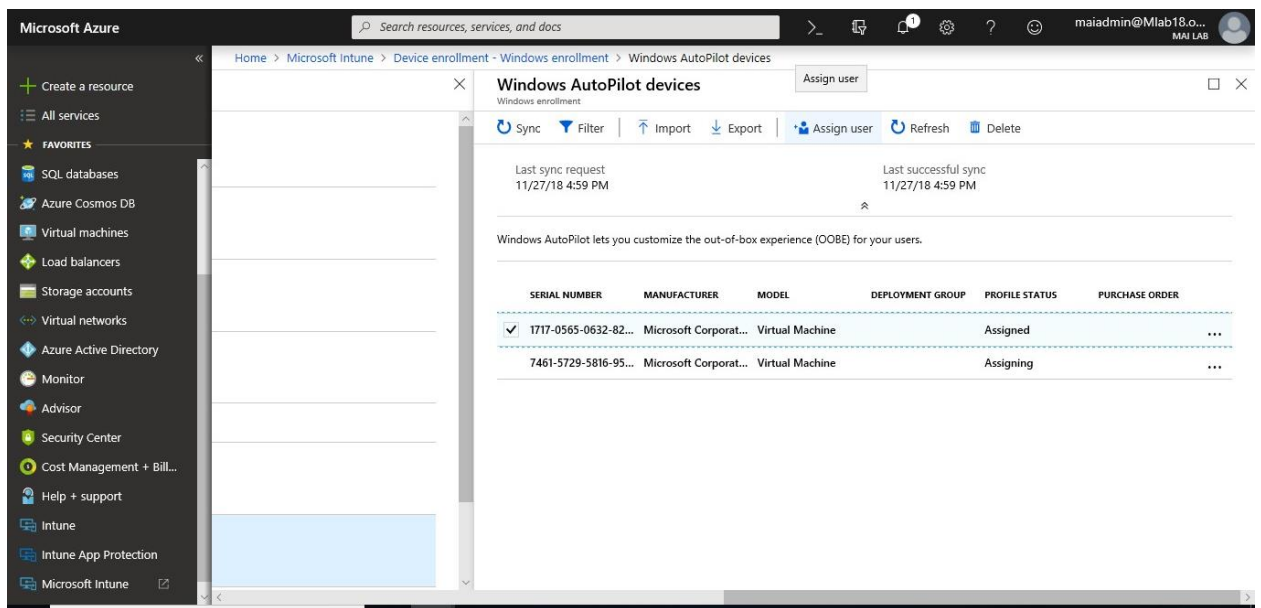
Microsoft Intune step by step on Azure portal



Step 8: Assign a user to a specific Autopilot device

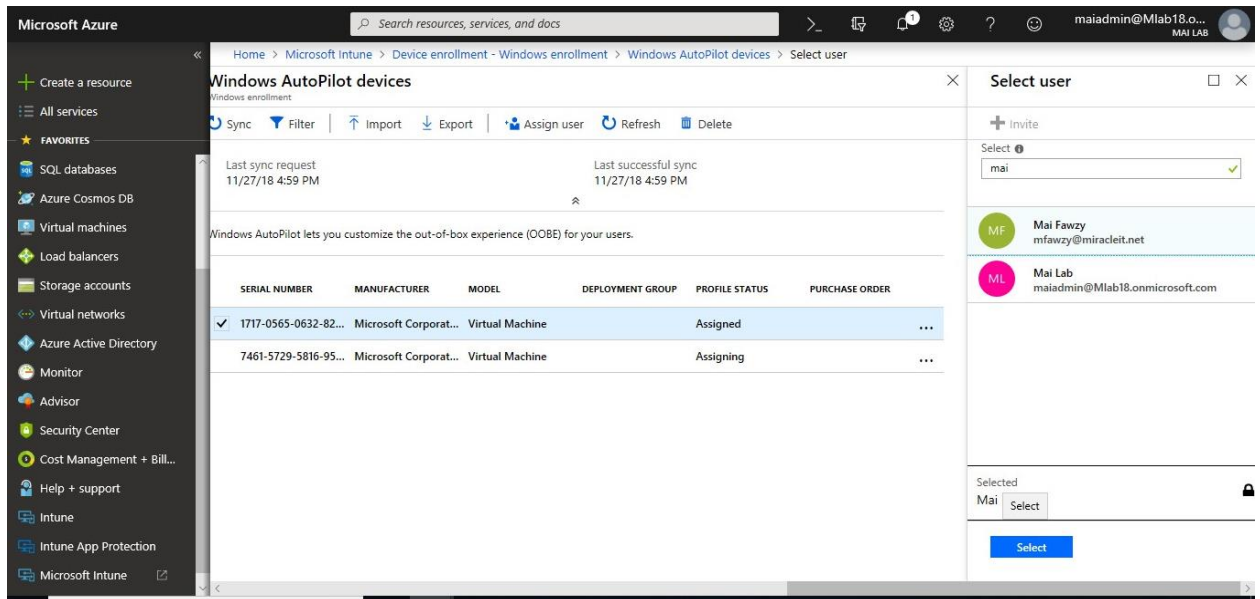
You can assign a user to a specific Autopilot device. This assignment pre-fills a user from Azure Active Directory in the company-branded sign-in page during Windows setup. It also lets you set a custom greeting name. It doesn't pre-fill or modify Windows sign-in. Only licensed Intune users can be assigned in this manner.

1. In the [Intune in the Azure portal](#), choose **Device enrollment > Windows enrollment > Devices > choose the device > Assign user**.

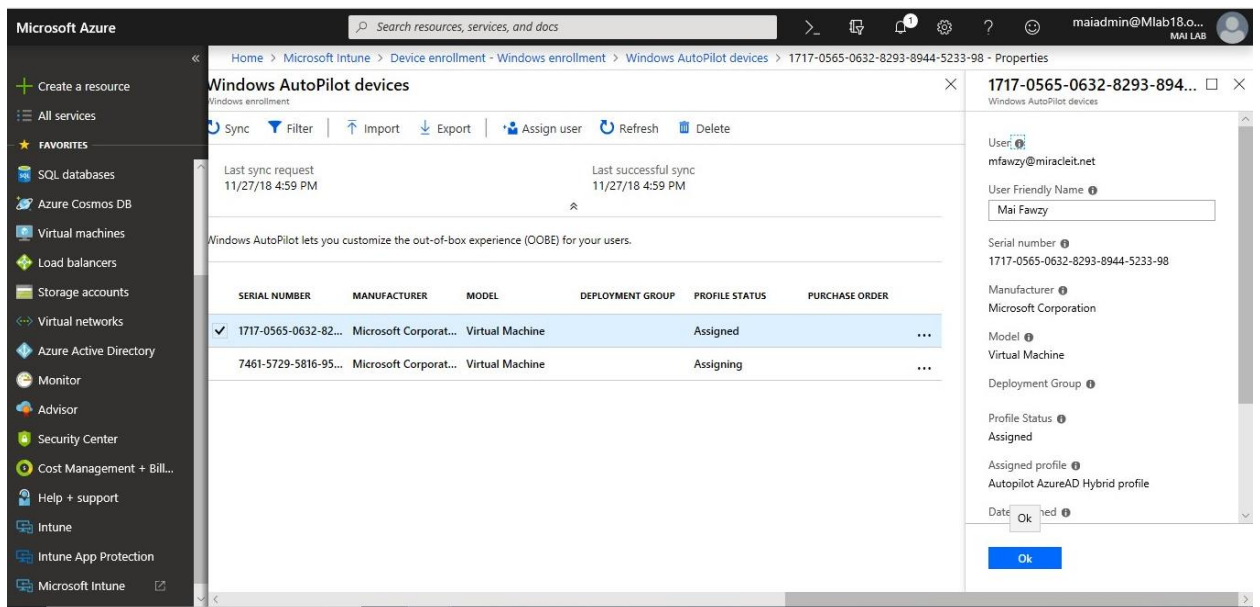


2. Choose an Azure user licensed to use Intune and choose **Select**.

Microsoft Intune step by step on Azure portal



3. In the **User-Friendly Name** box, type a friendly name or just accept the default. This string is the friendly name that displays when the user signs in during Windows setup. Choose **Ok**.



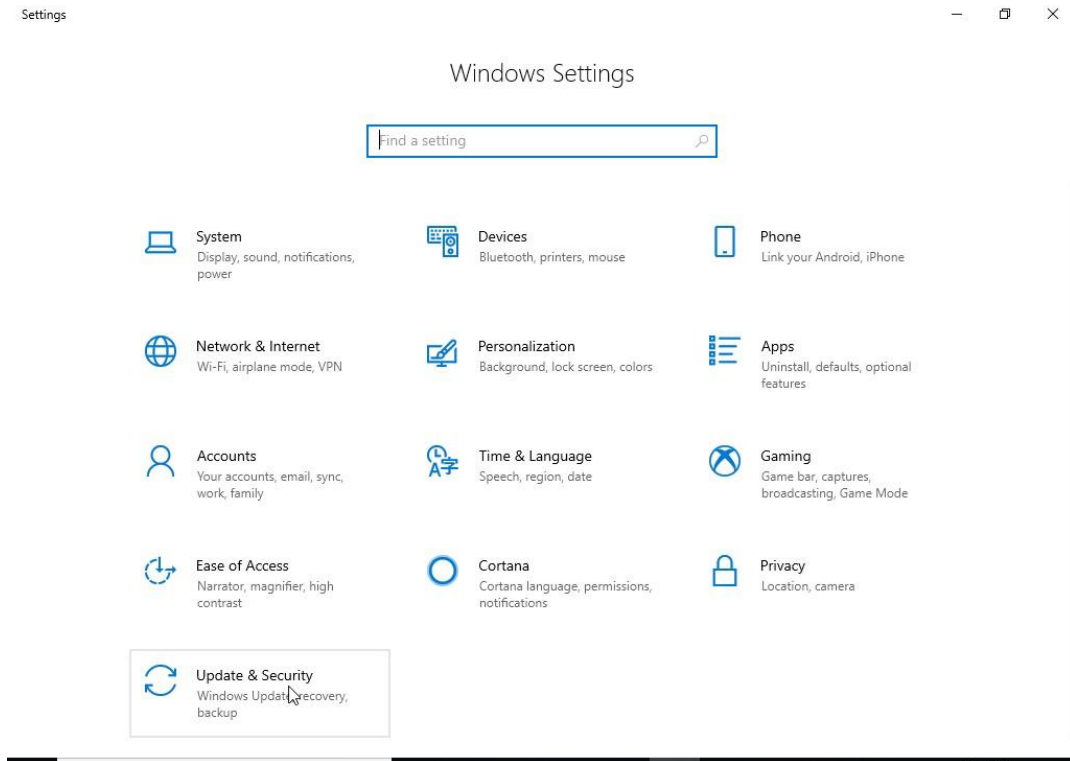
Note: You should verify that user who assign to him Autopilot profile, exist on Group for [Automatic Enrollment](#) if you don't enable automatic enrollment to all users.

Step 9: Deploy Autopilot Profile & Verify Enrollment.

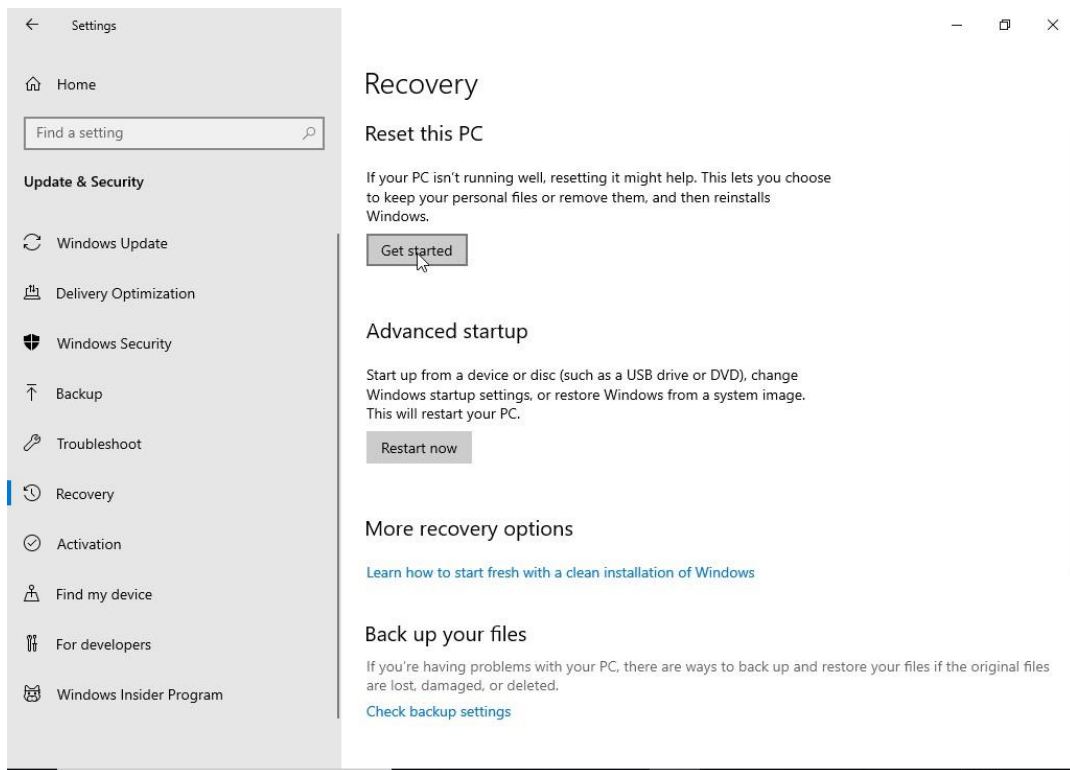
To Verify Enrollment, you need to follow below steps:

1. On Client PC, if Windows configured, you will need to reset the PC.

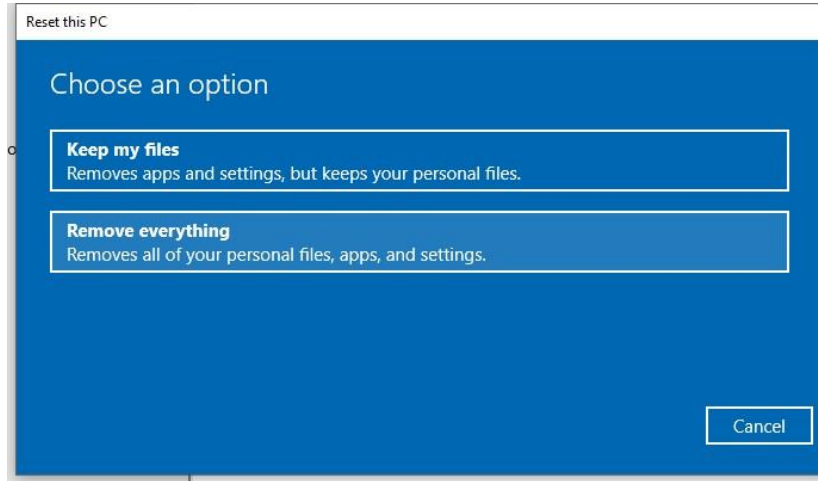
2. On **Settings**, Select **Updates & Security**.



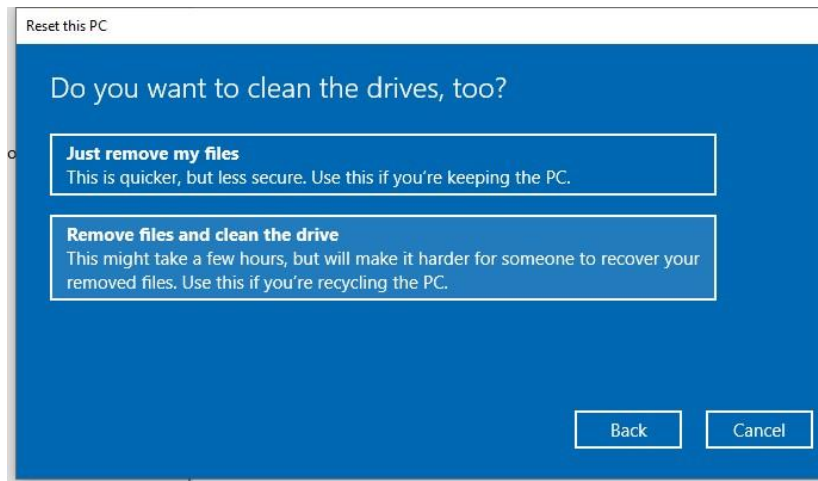
3. On **Updates & Security** Page, Select **Recovery** Then Click **Get Started** on **Reset PC**.



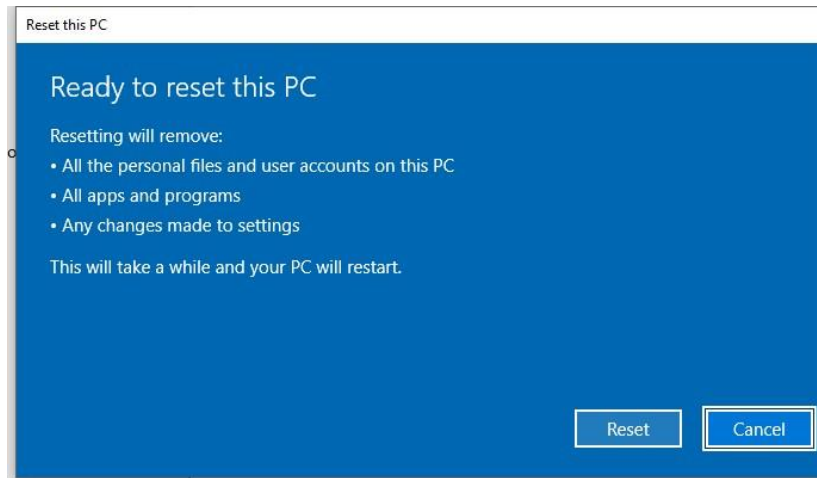
4. Click **Remove everything**.



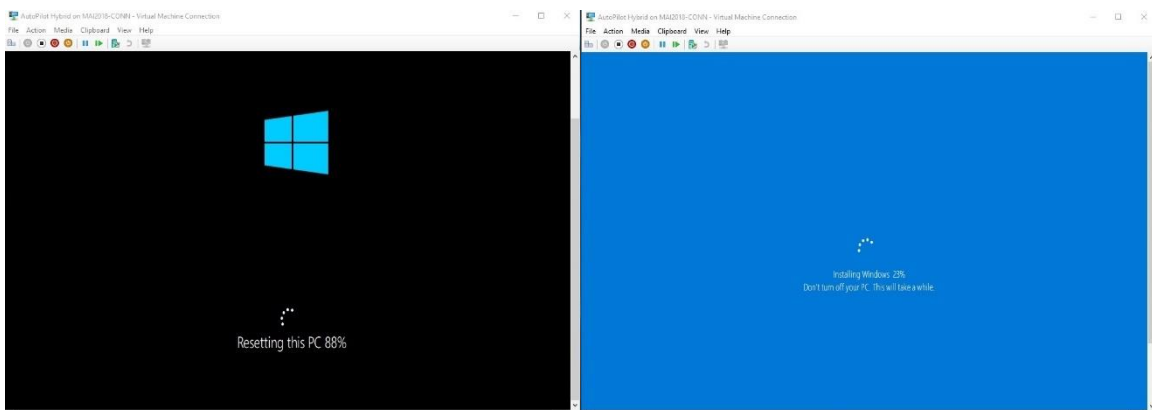
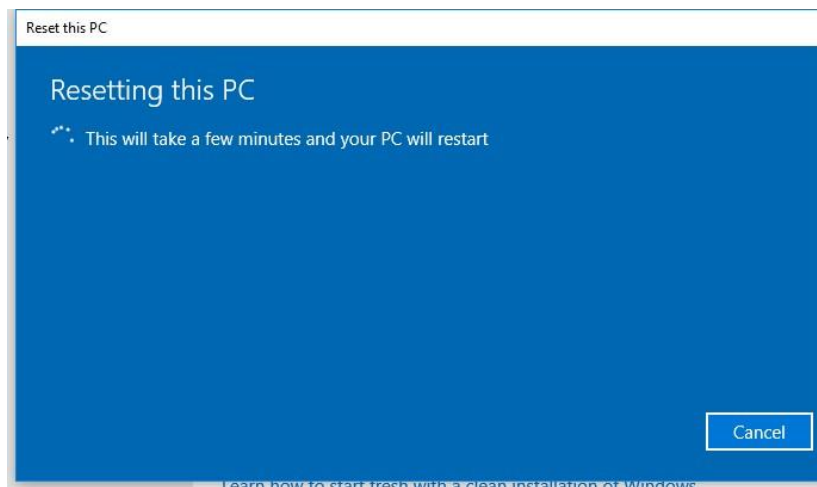
5. Click **Remove files & clean the drive**.



6. Click **Reset**.

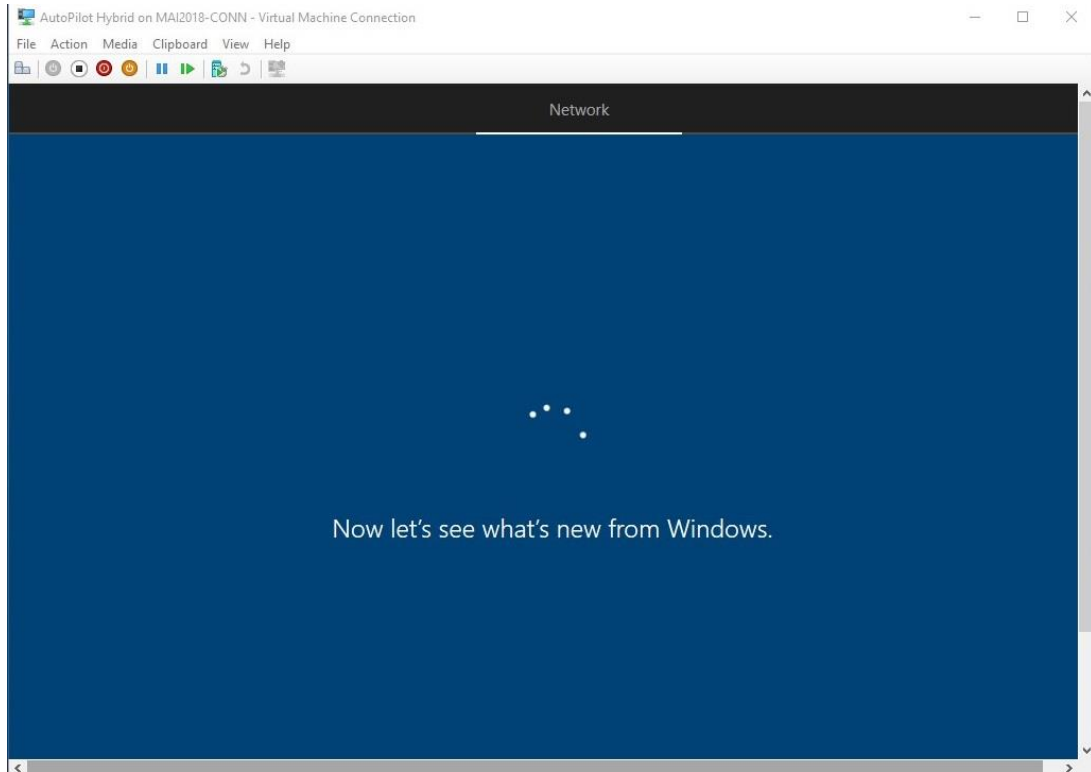


7. PC will start reset.

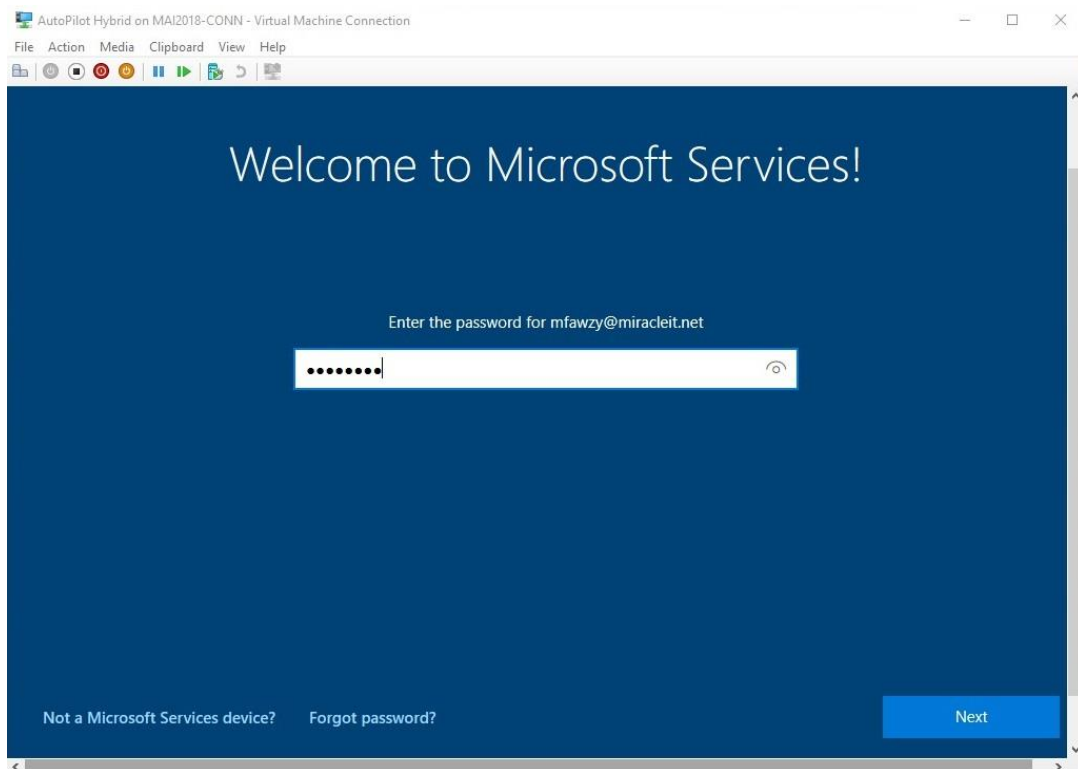


8. PC will start to deploy autopilot Profile.

Microsoft Intune step by step on Azure portal

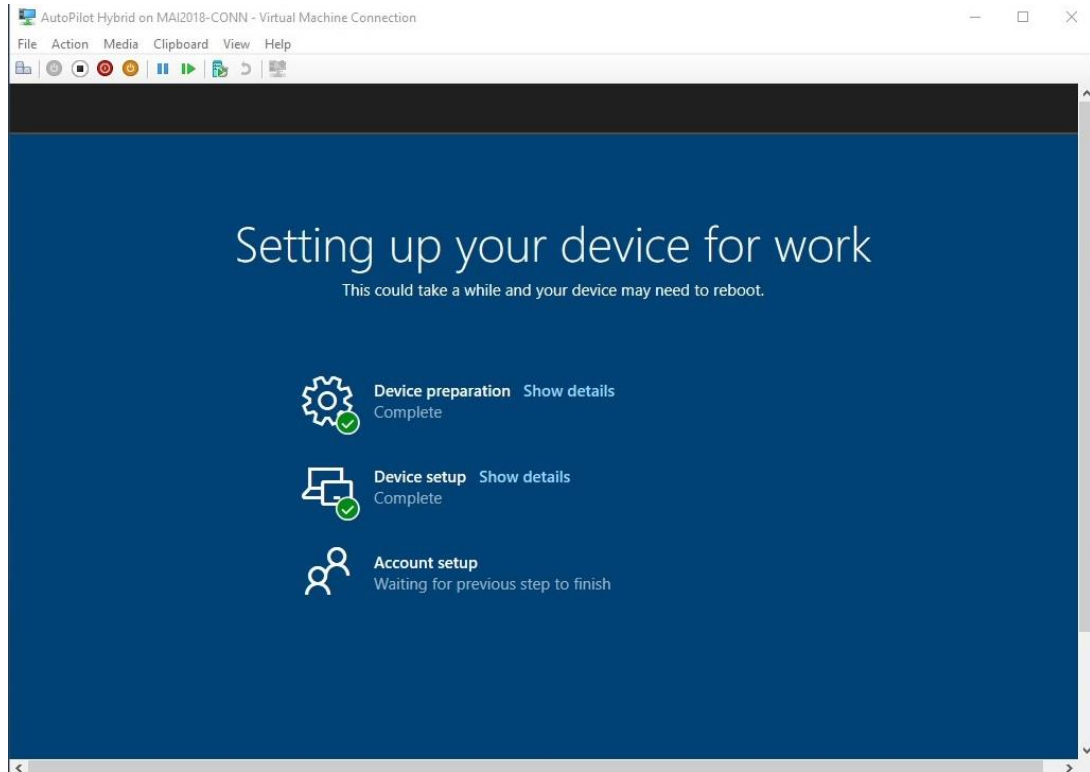


9. Click Yes. Enter your Credentials.

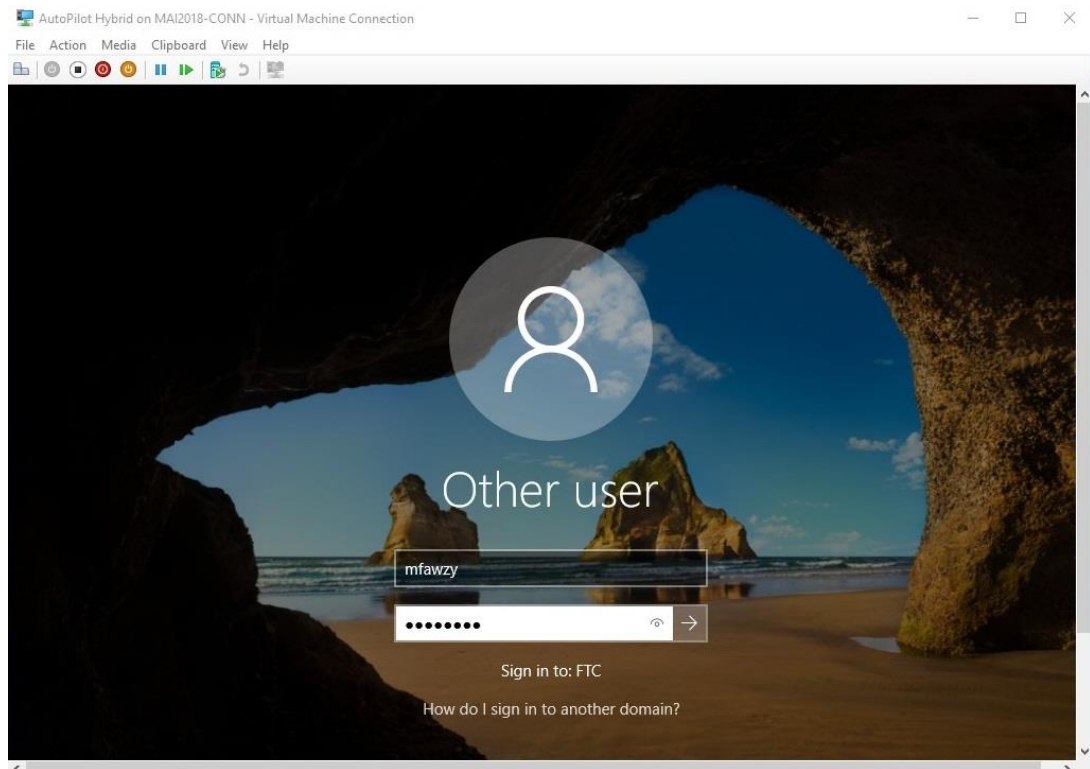


10. Start Setting up your device for work.

Microsoft Intune step by step on Azure portal

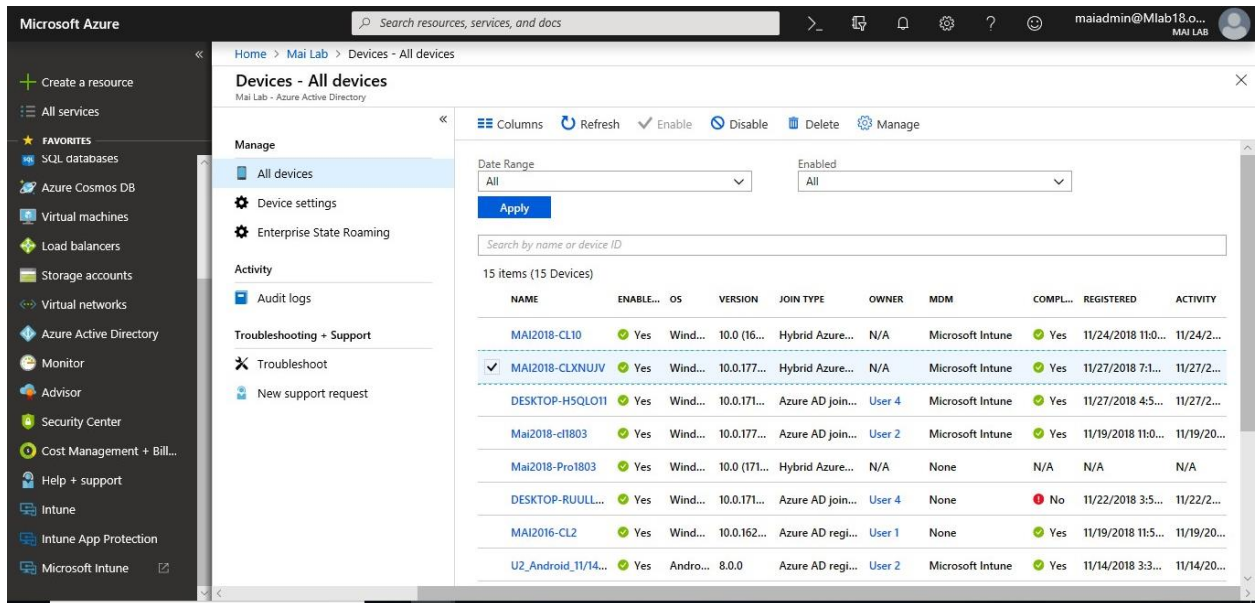


11. Sign in with your domain Credentials.



Microsoft Intune step by step on Azure portal

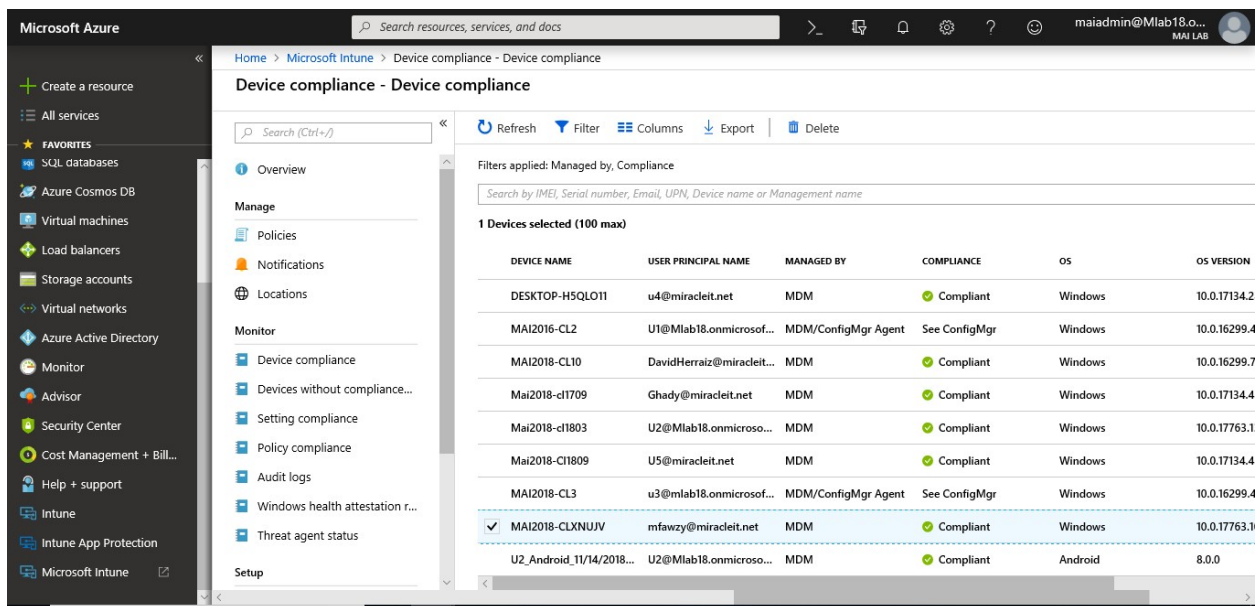
12. Open [Azure admin portal](#) > **Azure Active Directory**> **Devices**. You should find PC appear that it's managed by Microsoft Intune.



The screenshot shows the 'Devices - All devices' page in the Microsoft Azure portal. The page displays a list of 15 devices, including MAI2018-CL10, MAI2018-CLXNUJV, DESKTOP-H5QLO11, and others. The MAI2018-CLXNUJV device is highlighted, indicating it is managed by Microsoft Intune.

NAME	ENABLE...	OS	VERSION	JOIN TYPE	OWNER	MDM	COMPL...	REGISTERED	ACTIVITY
MAI2018-CL10	Yes	Wind...	10.0 (16...	Hybrid Azure...	N/A	Microsoft Intune	Yes	11/24/2018 11:0...	11/24/2...
MAI2018-CLXNUJV	Yes	Wind...	10.0.177...	Hybrid Azure...	N/A	Microsoft Intune	Yes	11/27/2018 7:1...	11/27/2...
DESKTOP-H5QLO11	Yes	Wind...	10.0.171...	Azure AD join...	User 4	Microsoft Intune	Yes	11/27/2018 4:5...	11/27/2...
Mai2018-cl1803	Yes	Wind...	10.0.177...	Azure AD join...	User 2	Microsoft Intune	Yes	11/19/2018 11:0...	11/19/20...
Mai2018-Pro1803	Yes	Wind...	10.0 (171...	Hybrid Azure...	N/A	None	N/A	N/A	N/A
DESKTOP-RUJLL...	Yes	Wind...	10.0.171...	Azure AD join...	User 4	None	No	11/22/2018 3:5...	11/22/2...
MAI2016-CL2	Yes	Wind...	10.0.162...	Azure AD regi...	User 1	None	Yes	11/19/2018 11:5...	11/19/20...
U2_Android_11/14...	Yes	Andro...	8.0.0	Azure AD regi...	User 2	Microsoft Intune	Yes	11/14/2018 3:3...	11/14/20...

13. On [Intune Portal](#) > Click **Device Compliance** > **Device Compliance**, you should find device appear on portal as Management Devices.



The screenshot shows the 'Device compliance - Device compliance' page in the Microsoft Intune portal. The page displays a list of 1 device selected (100 max), including DESKTOP-H5QLO11, MAI2016-CL2, MAI2018-CL10, and others. The MAI2018-CLXNUJV device is highlighted, indicating it is managed by Microsoft Intune.

DEVICE NAME	USER PRINCIPAL NAME	MANAGED BY	COMPLIANCE	OS	OS VERSION
DESKTOP-H5QLO11	u4@miracleit.net	MDM	Compliant	Windows	10.0.17134.2
MAI2016-CL2	U1@Mlab18.onmicrosof...	MDM/ConfigMgr Agent	See ConfigMgr	Windows	10.0.16299.4
MAI2018-CL10	DavidHerraiz@miracleit...	MDM	Compliant	Windows	10.0.16299.7
Mai2018-cl1709	Ghady@miracleit.net	MDM	Compliant	Windows	10.0.17134.4
Mai2018-cl1803	U2@Mlab18.onmicroso...	MDM	Compliant	Windows	10.0.17763.1
Mai2018-Cl1809	U5@miracleit.net	MDM	Compliant	Windows	10.0.17134.4
MAI2018-CL3	u3@mlab18.onmicrosof...	MDM/ConfigMgr Agent	See ConfigMgr	Windows	10.0.16299.4
MAI2018-CLXNUJV	mfawzy@miracleit.net	MDM	Compliant	Windows	10.0.17763.1
U2_Android_11/14/2018...	U2@Mlab18.onmicroso...	MDM	Compliant	Android	8.0.0

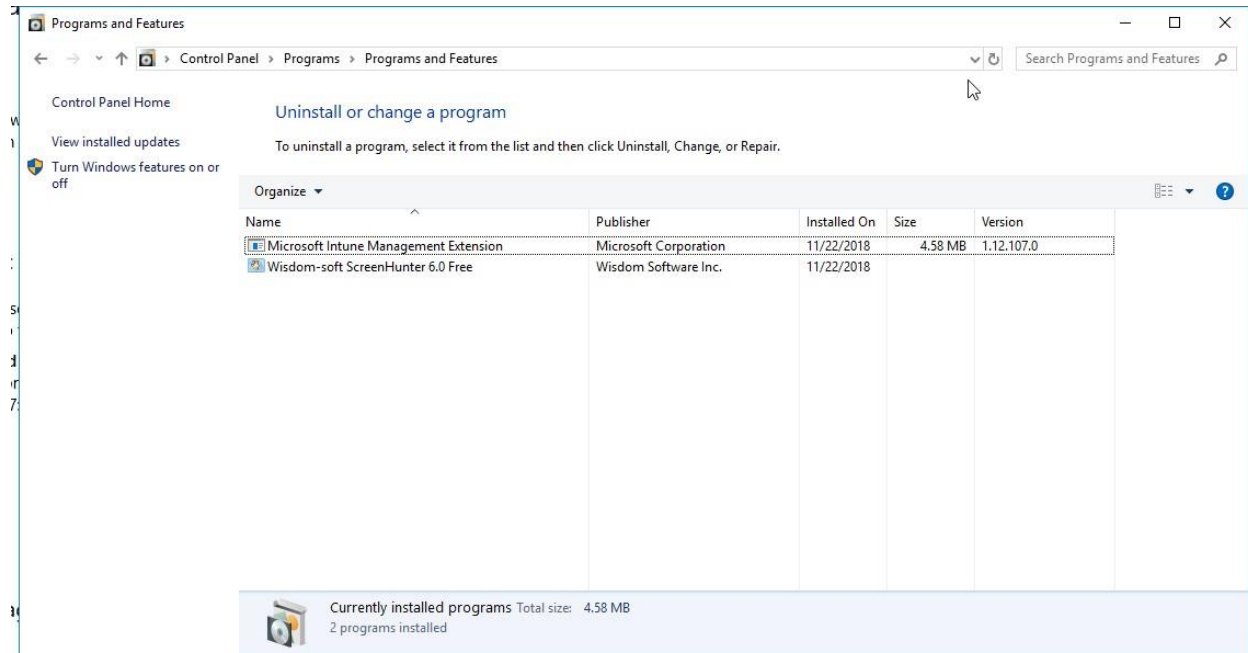
Manage PowerShell Scripts Using Microsoft Intune

The Intune management extension lets you upload PowerShell scripts in Intune to run on Windows 10 devices. The Intune management extension has the following prerequisites:

Microsoft Intune step by step on Azure portal

- Devices must be joined to Azure AD. The Intune management extension supports Azure Active Directory joined, Hybrid Domain joined and Co-Managed enrolled Windows devices.
- Devices must run Windows 10, version 1607 or later.
- Automatic MDM enrollment must be enabled in Azure AD, and devices must be auto-enrolled to Intune.

Note: The above prerequisites are mandatory to deploy PowerShell script or win32 app. You should find Intune extension management on control panel once you enroll your device.

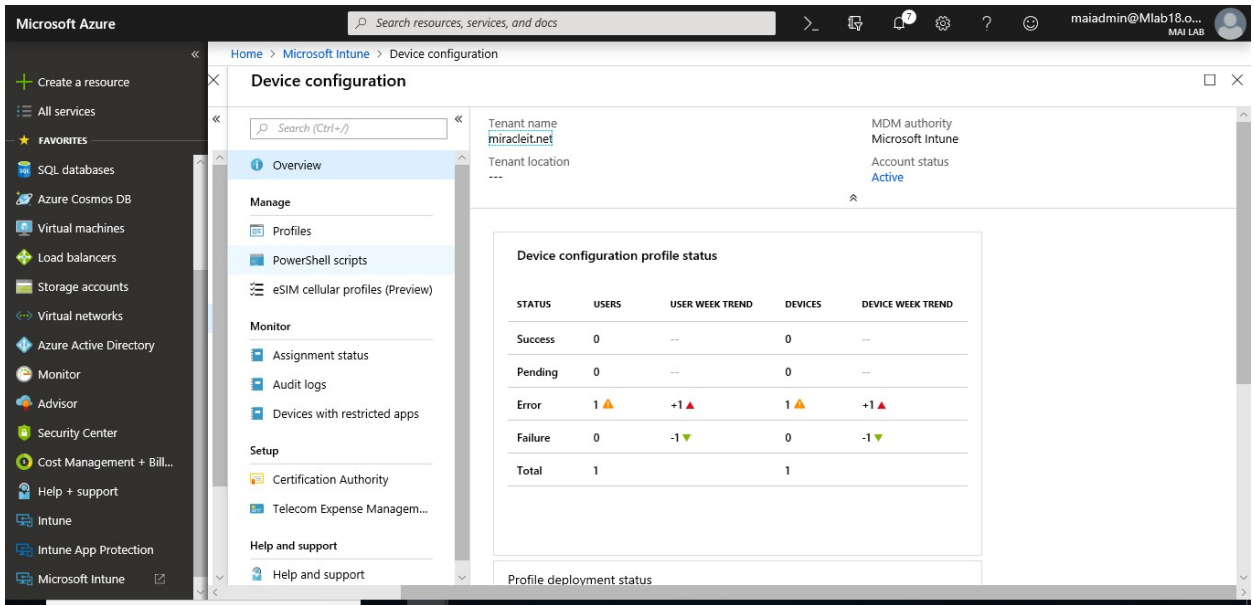


To deploy Microsoft Teams using PowerShell Script through Intune, you can follow below steps:

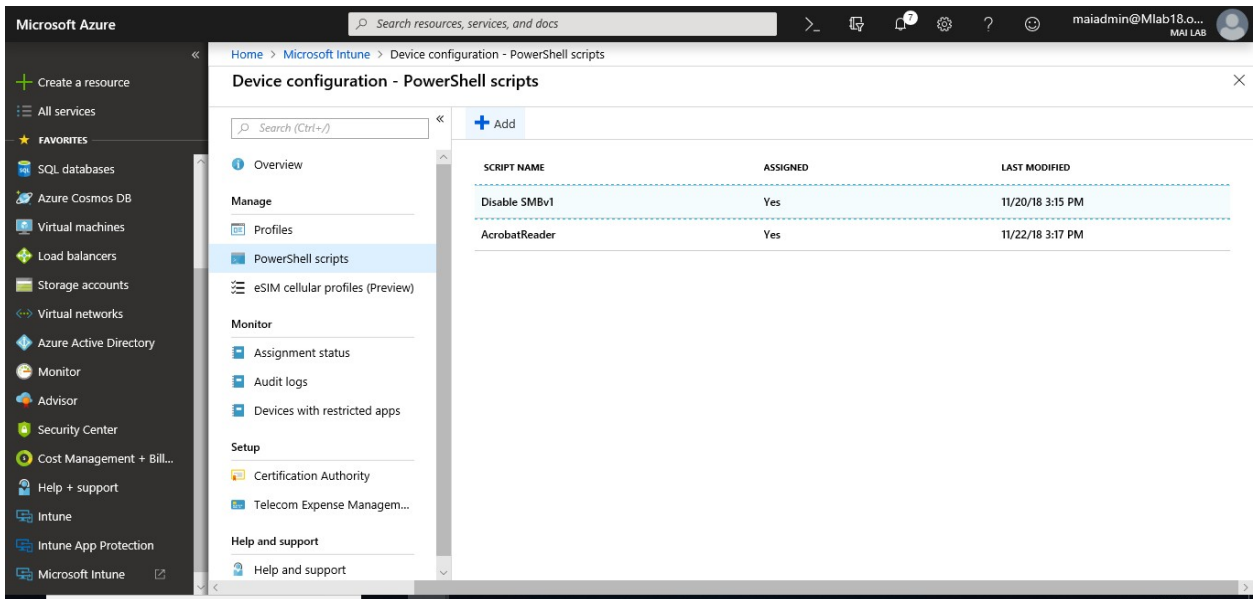
Create a PowerShell script policy

1. Sign in to the [Azure portal](#). Select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device configuration** > **PowerShell scripts**.

Microsoft Intune step by step on Azure portal

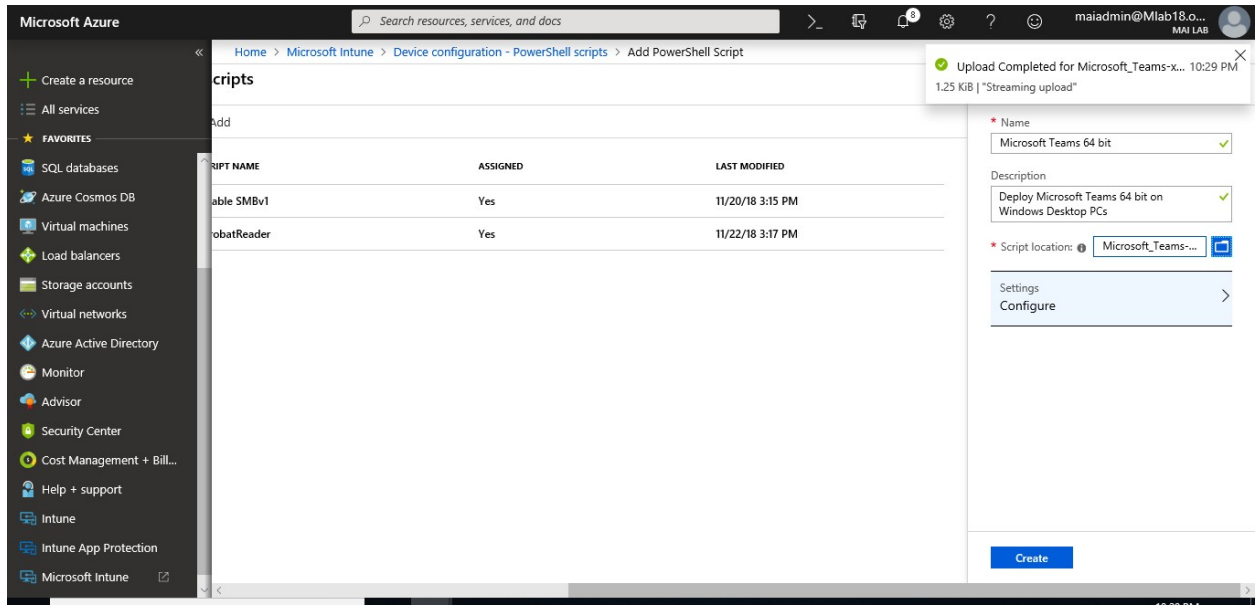


3. In the PowerShell scripts > Select Add.

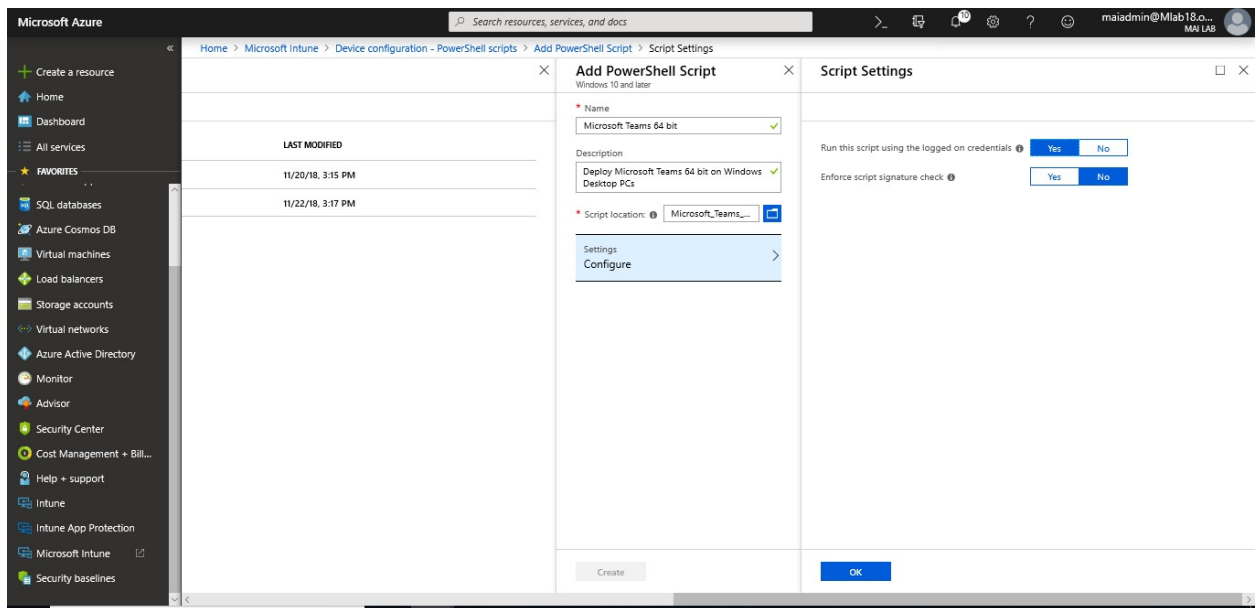


4. Enter a **Name** and **Description** for the PowerShell script.
5. For **Script location**, browse to the PowerShell script. The script must be less than 200KB (ASCII) or 100KB (Unicode) in size. In our example, I deploy [Microsoft Teams using PowerShell script](#).

Microsoft Intune step by step on Azure portal

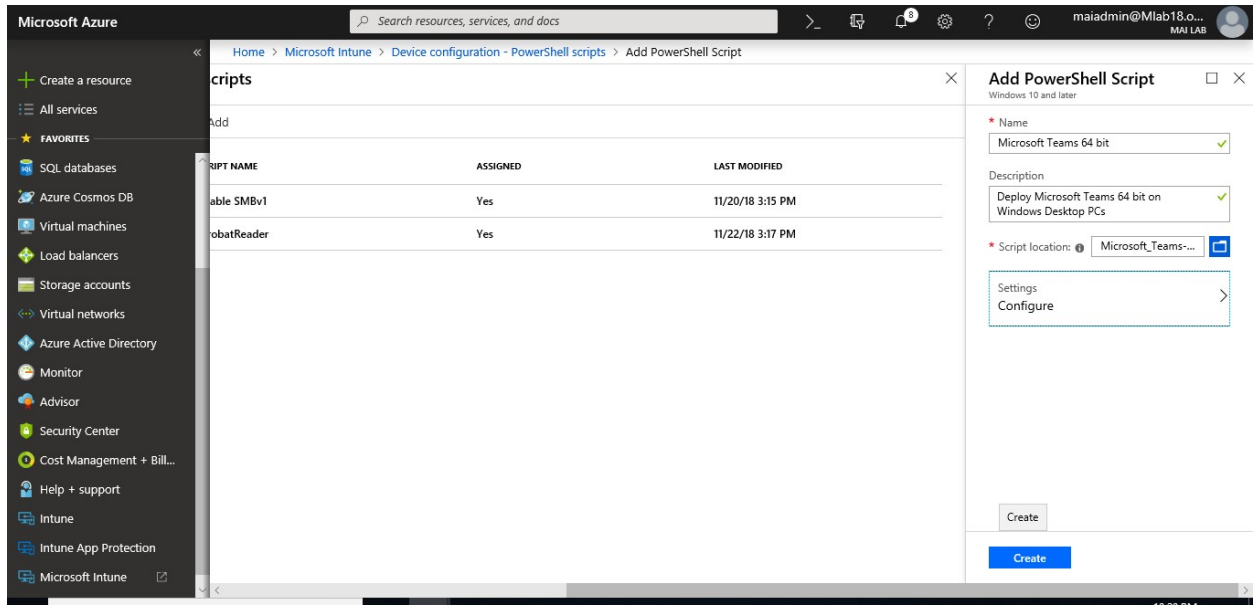


6. Choose **Configure**. Then choose to run the script with the user's credentials on the device (**Yes**), or system context (**No**). By default, the script runs in the system context. Select **Yes** unless the script is required to run in the system context.
7. Choose if the script must be signed by a trusted publisher (**Yes**). By default, there is no requirement for the script to be signed.



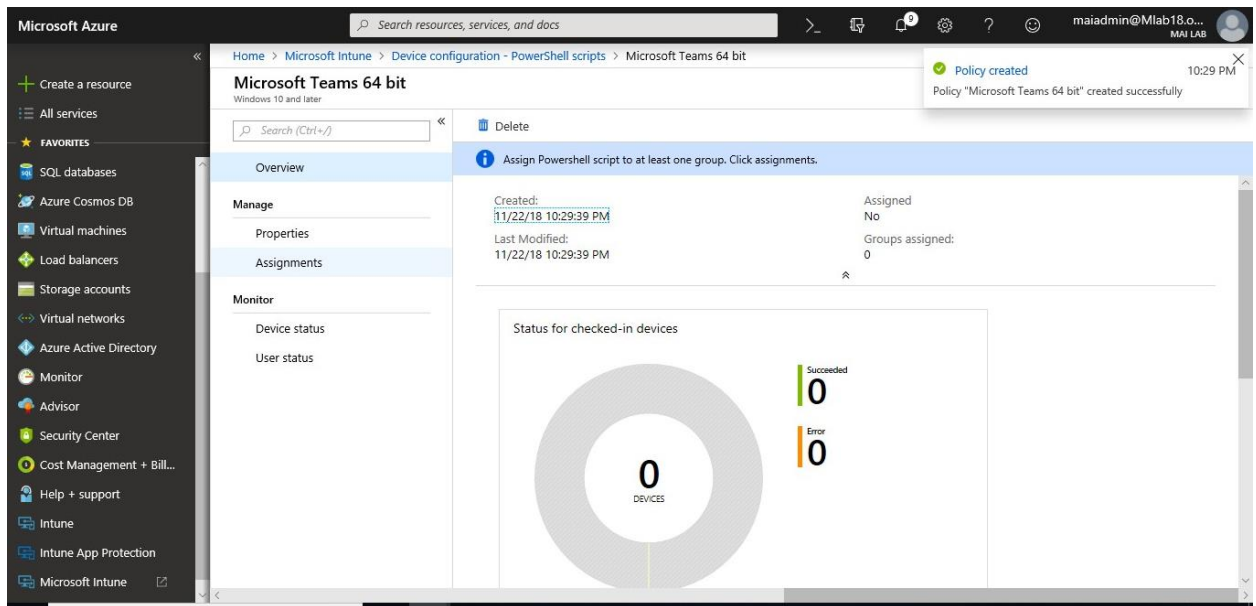
8. Select **OK**, and then **Create** to save the script.

Microsoft Intune step by step on Azure portal



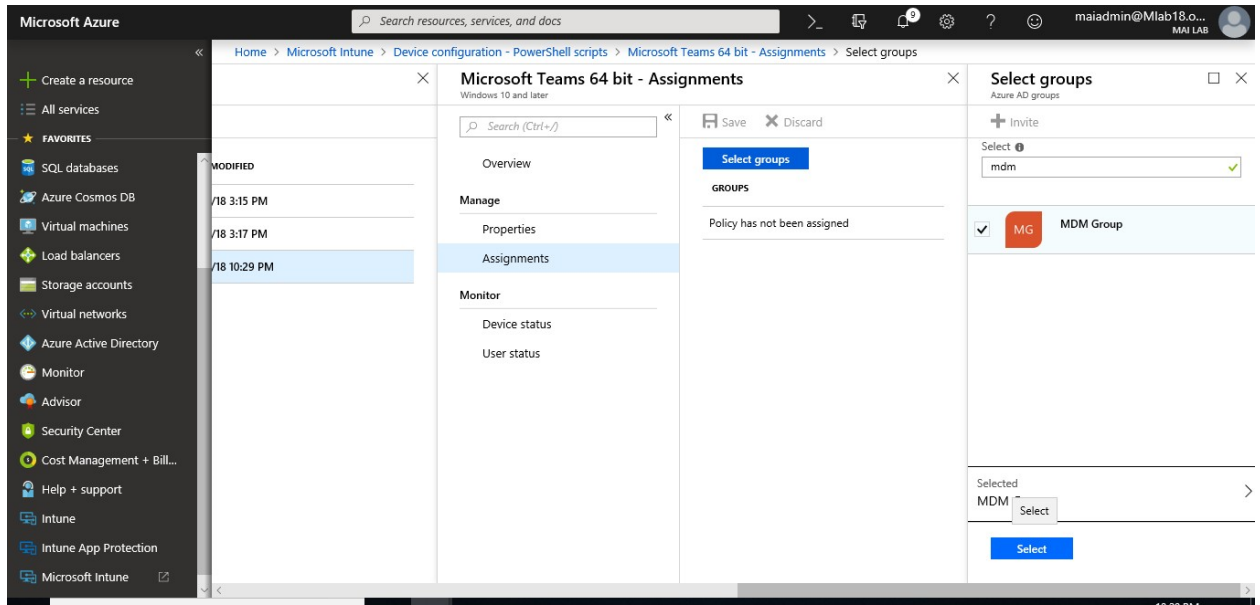
Assign a PowerShell script policy

1. In **PowerShell** scripts, select the script to assign, and then choose **Manage** > **Assignments**.

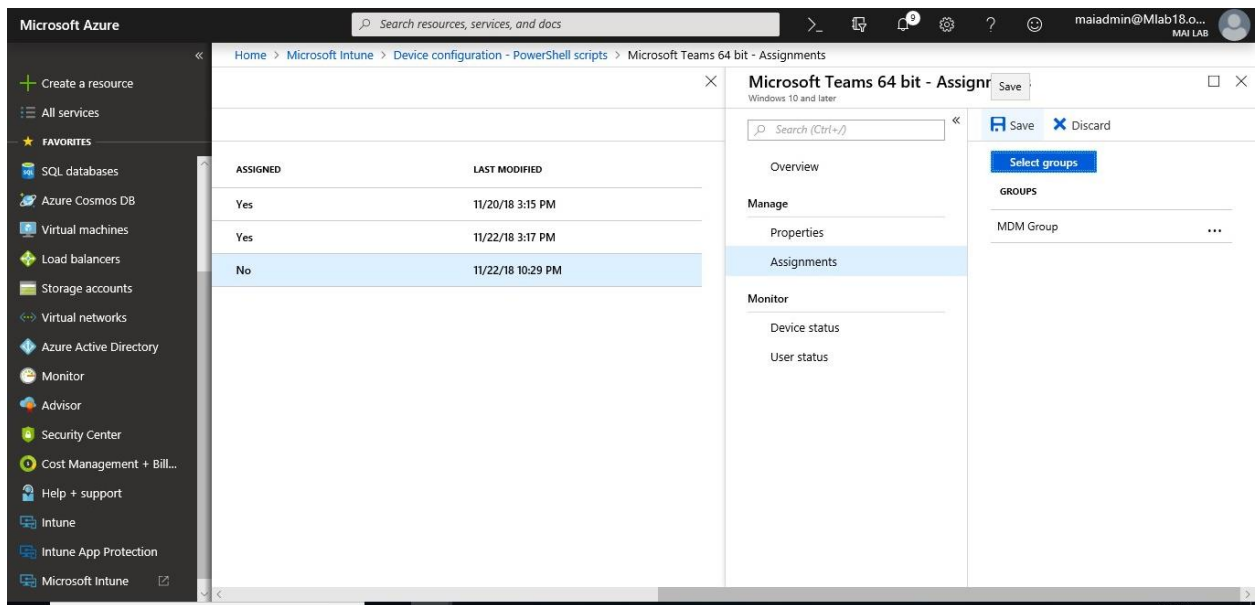


2. Choose **Select Groups** to list available Azure AD groups. Select one or more groups that contain the users whose devices receive the script. **Select** to assign the policy to the selected groups.

Microsoft Intune step by step on Azure portal



3. Click **Save**.



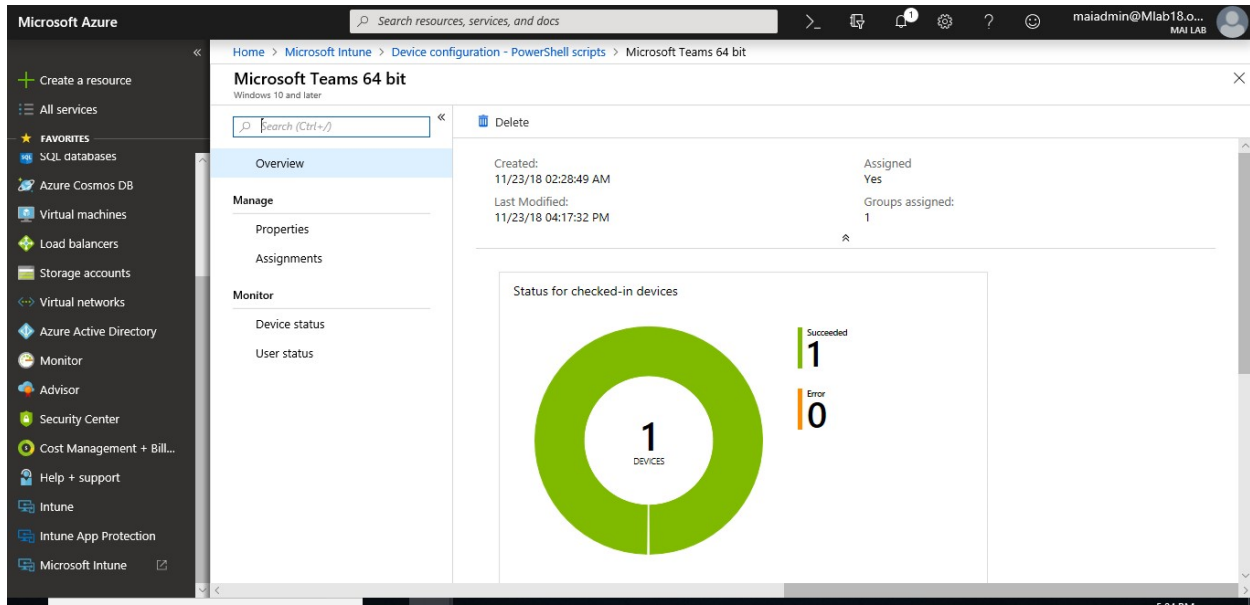
Note:

- PowerShell scripts can't be applied to computer groups.
- End users are not required to be logged in on the device to execute PowerShell scripts.
- PowerShell scripts in Intune can be targeted to AAD device security groups.

Monitor run status for PowerShell scripts

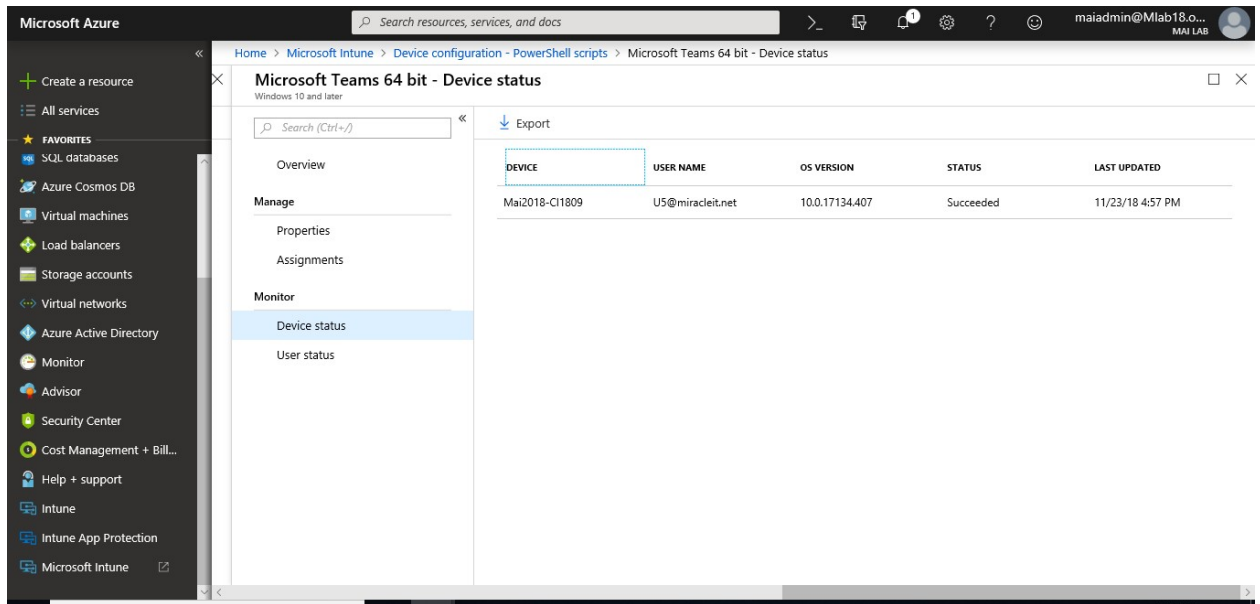
You can monitor the run status of PowerShell scripts for users and devices in the Azure portal.

Microsoft Intune step by step on Azure portal

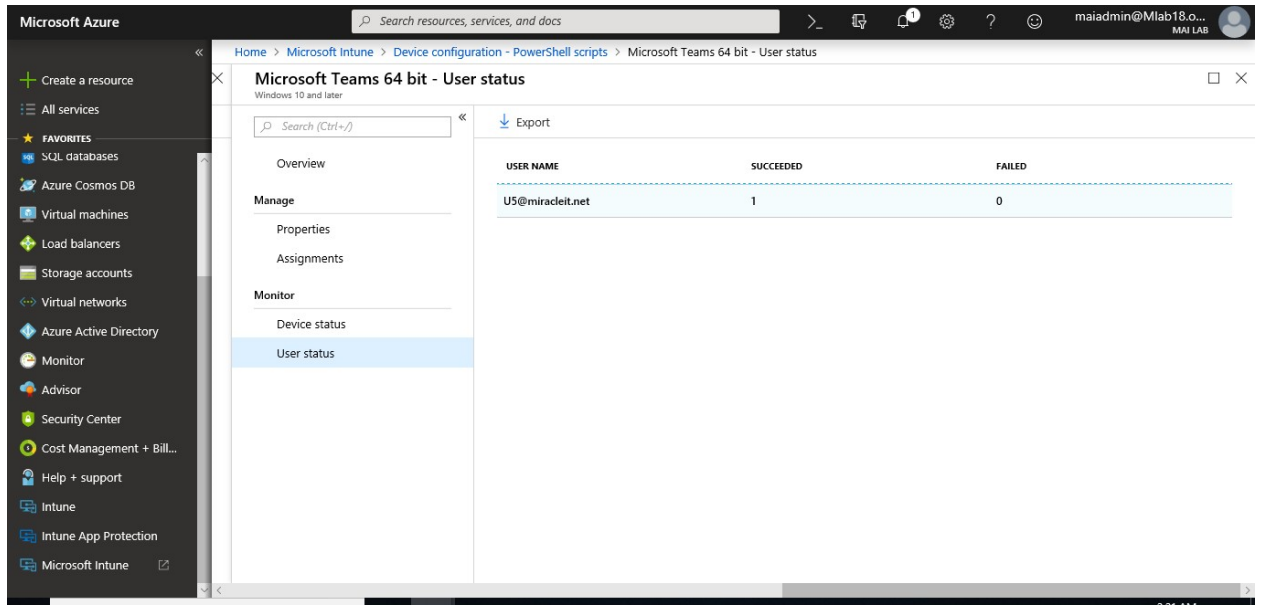


In **PowerShell scripts**, select the script to monitor, choose **Monitor**, and then choose one of the following reports:

- **Device status**



- **User status**



Note: In case Execution of PowerShell Script is failed, it will be rerun after 60 min. The agent checks **every 60 minutes** for new policies in the backend. you can troubleshoot the issue from logs “*C:\ProgramData\Microsoft\IntuneManagementExtension\Logs*”. No re-run of scripts occurs once a script is successful executed.

Deploy Application (EXE or MSI) on Windows 10 MDM

Administrators can add, install, and uninstall applications for Windows 10 users in a variety of formats such as MSIs, Setup.exe, or MSP. Intune will evaluate requirement rules before the start of app download/ install and notify end users of the status or reboot requirements using the Windows 10 Action Center.

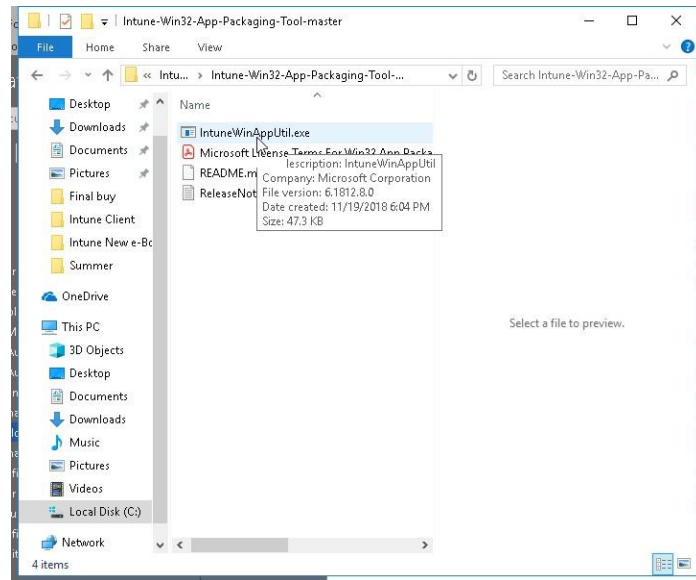
Prerequisites for public preview

- Windows 10 version 1607 or later.
- Windows 10 client needs to be:
 - joined to Azure Active Directory (AAD) or Hybrid Azure Active Directory, and
 - enrolled in Intune (MDM-managed)
- Windows application size is capped at 8 GB per app in the public preview

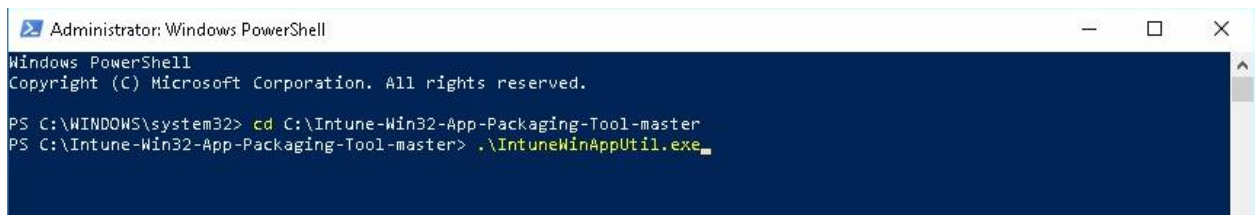
In this topic, you can package [Adobe Reader 11.x](#) using the new Intune Win32 application packaging tool on Intune tenant, you need to follow below steps

1. Download the [Microsoft Intune Win32 App Packaging Tool](#). Extract the folder.

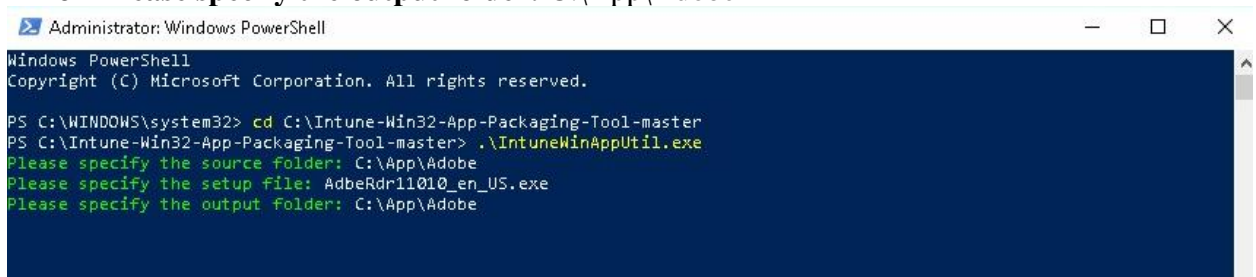
Microsoft Intune step by step on Azure portal



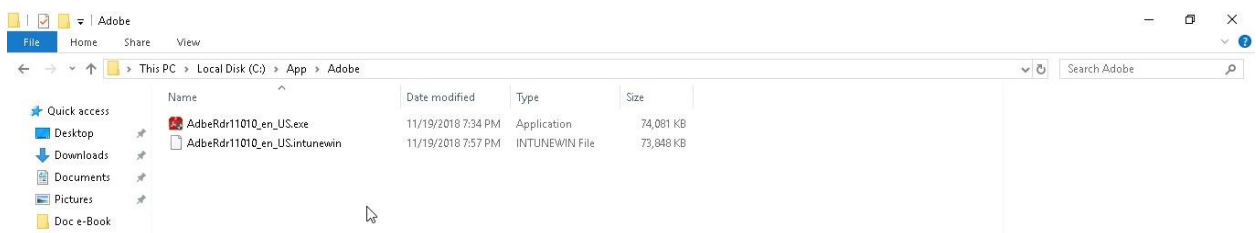
2. Open Windows PowerShell run as Administrator and navigate to the location of **IntuneWinAppUtil.exe** and Run **IntuneWinAppUtil.exe**.



3. Run **IntuneWinAppUtil.exe** and provide the following information, when requested
 - Please specify the source folder: C:\App\Adobe.
 - Please specify the setup file: AdbeRdr11010_en_US.exe
 - Please specify the output folder: C:\App\Adobe



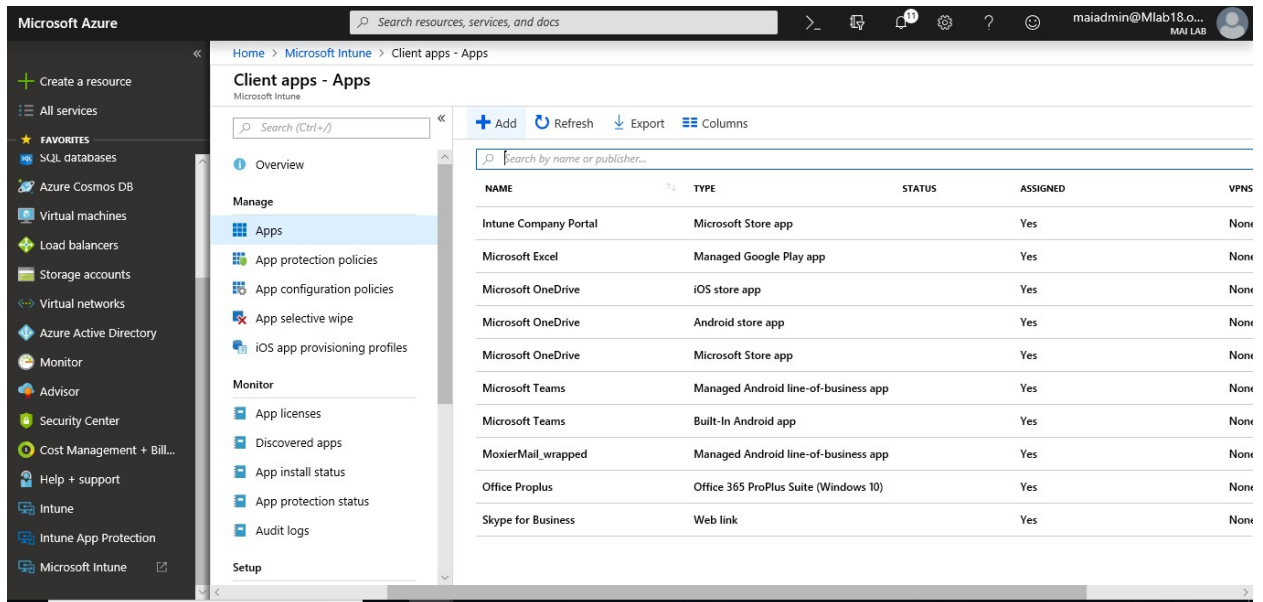
4. Once the wrapping is done. The message **Done!!!** will be shown. In my example a file named **AdbeRdr11010_en_US.intunewin** will be created in **C:\App\Adobe**.



Configure a Win32 app

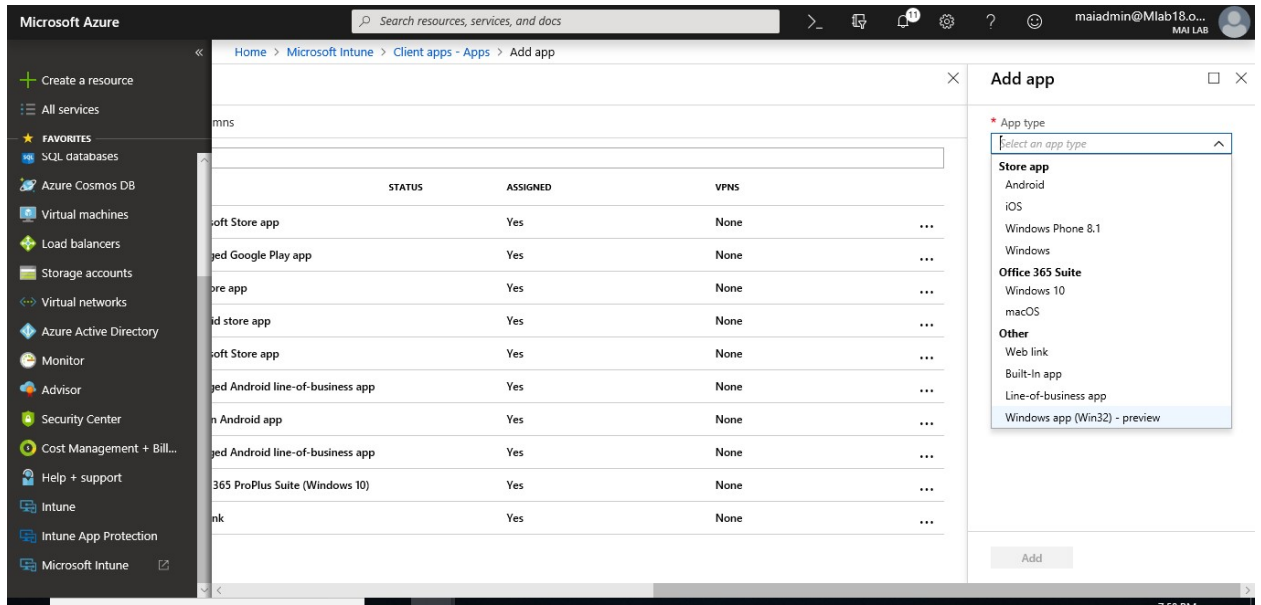
You can add a Win32 app to Microsoft Intune. This type of app is typically written in-house or by a 3rd party. The following steps provide guidance to help you add a Windows app to Intune by using the .intunewin file. After configuring the app, make sure to assign the app to a user group.

1. Open the [Azure portal](#). Select **All services > Intune**. Intune is in the **Monitoring + Management** section.
2. In the **Intune** pane, select **Client apps > Apps > Add**.

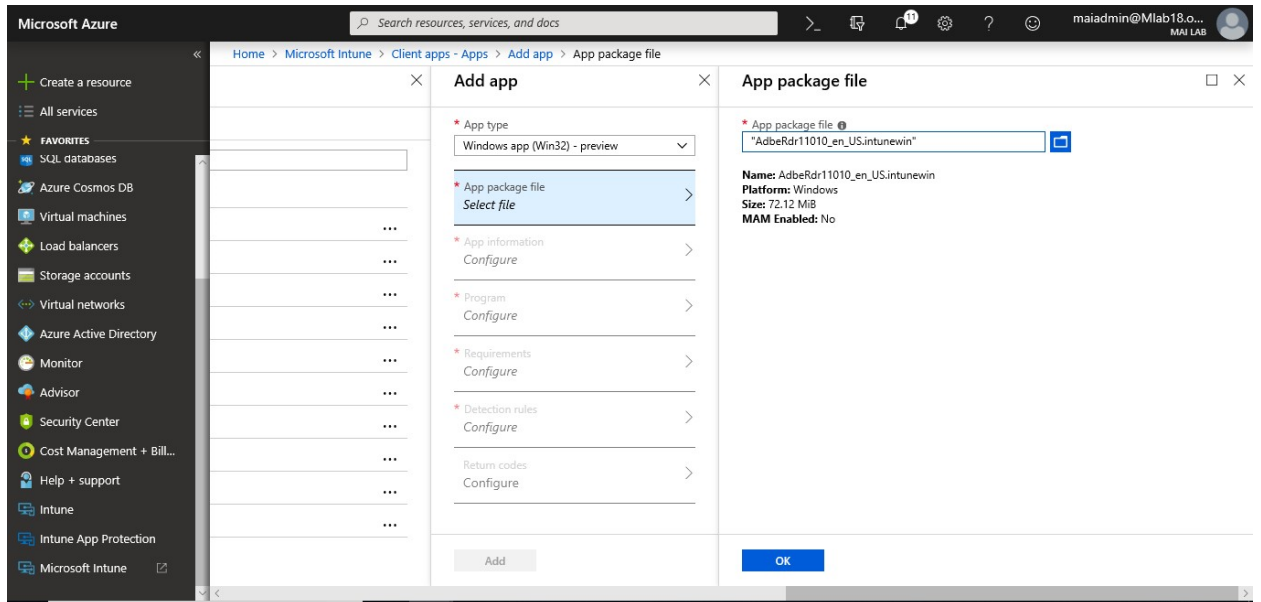


3. On the **Add app** blade, select **Windows app (Win32) – preview** from the provided drop-down list.

Microsoft Intune step by step on Azure portal

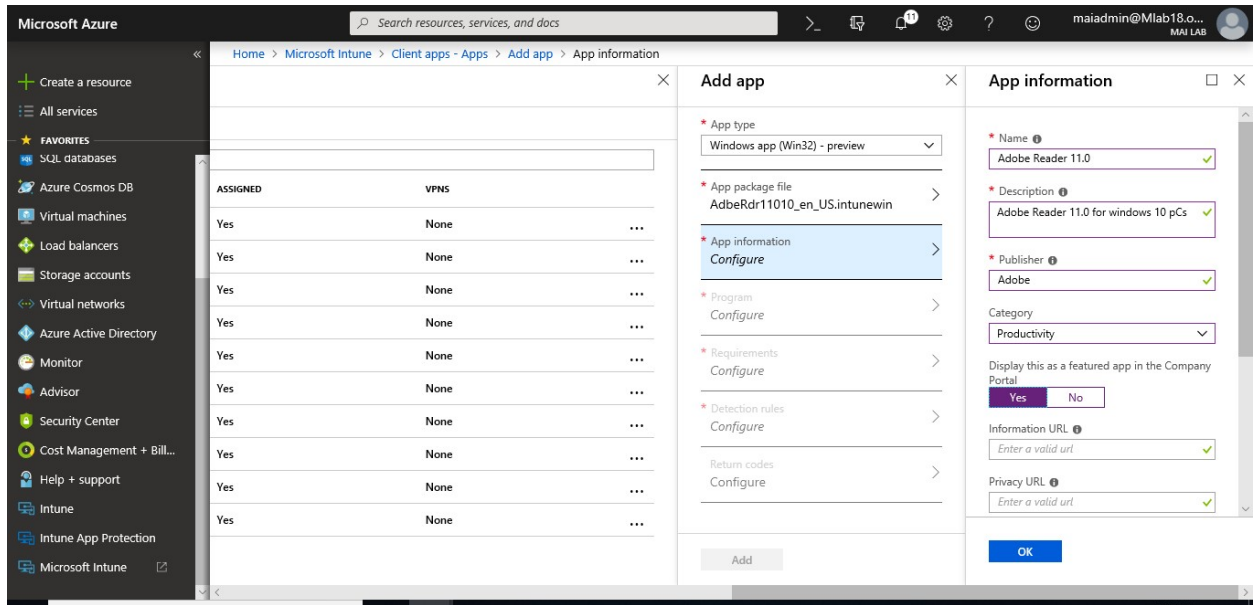


4. On the **App package file** blade, select the created **AdbRdr11010_en_US.intunewin** as **App package file** and click **OK** to return to the **Add app** blade.

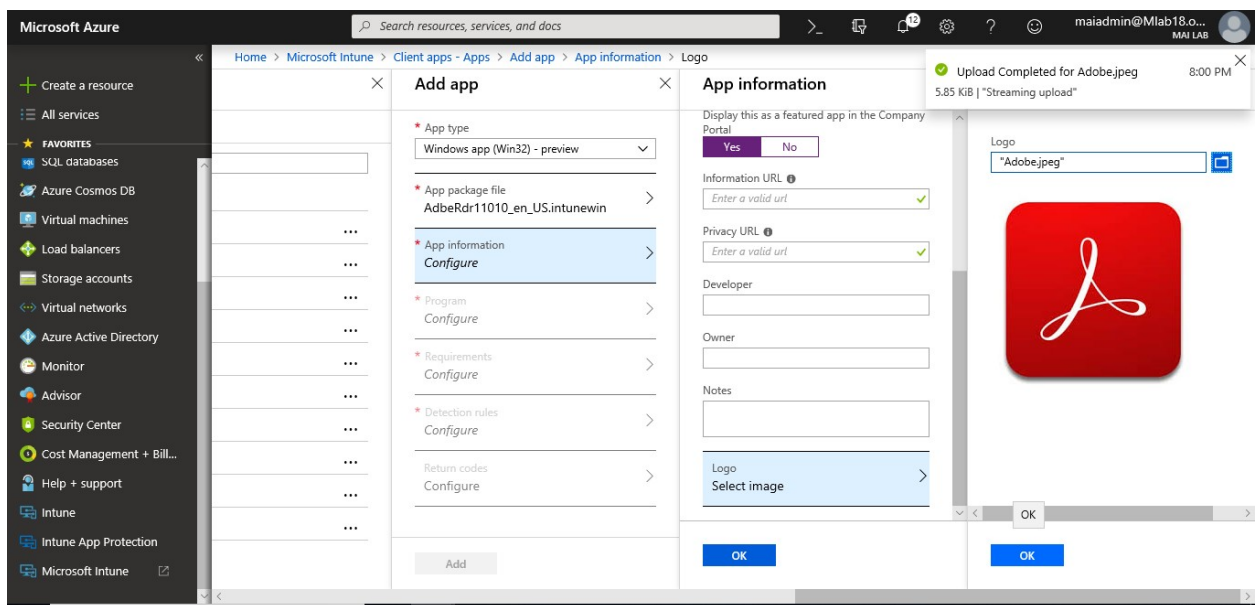


5. In the **Add app** pane, select **App information** to configure the app.
6. On the **App information** blade, provide at least the following information and click **OK** to return to the **Add app** blade.
 - **Name**: **Adobe Reader 11.0** as it appears in the company portal.
 - **Description**: Provide a description of the app
 - **Publisher**: Provide the publisher of the app

Microsoft Intune step by step on Azure portal

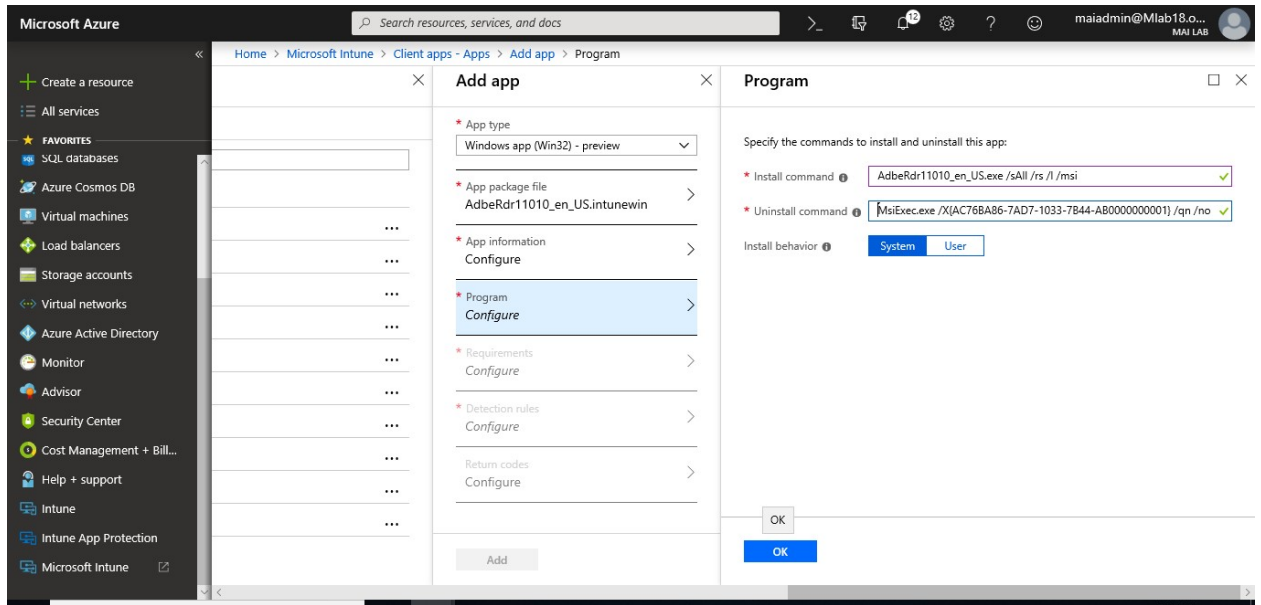


7. If you have logo of application, click **logo**, upload pic and click **OK**.



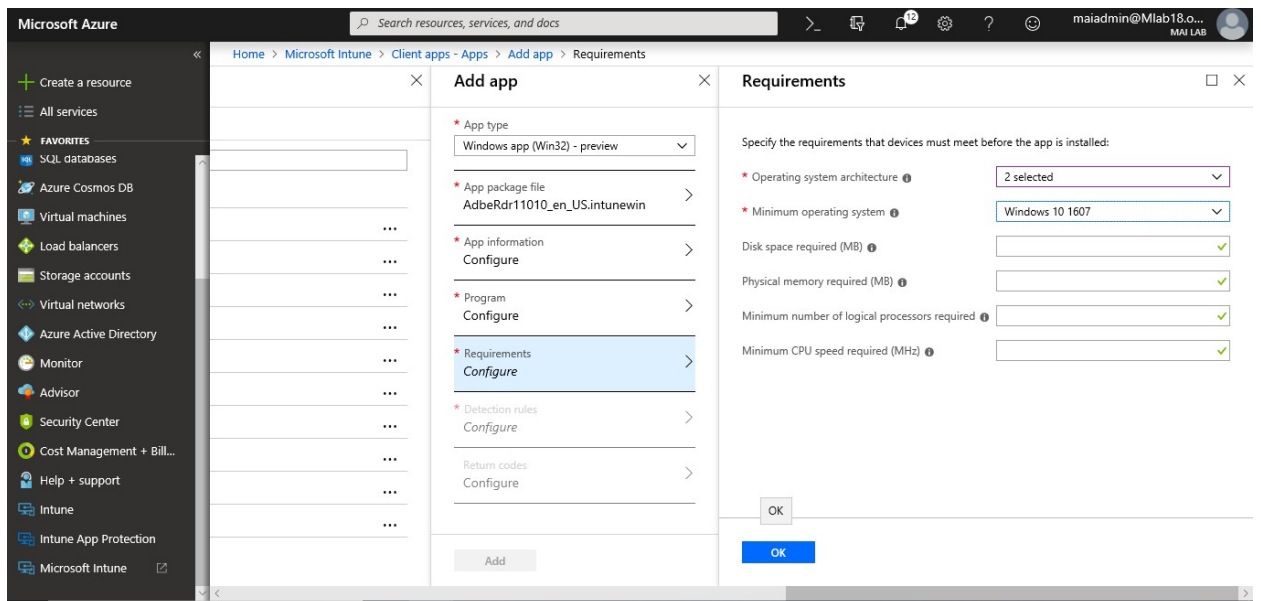
8. In the **Add app** blade, select **Program** to open the Program blade.

9. On the **Program** blade, In **Install command**, enter command to install Adobe **"AdbeRdr11010_en_US.exe /sAll /rs /l /msi"**, verify the **Uninstall command** **"MsiExec.exe /X{AC76BA86-7AD7-1033-7B44-AB0000000001} /qn /norestart"** and click **OK**.



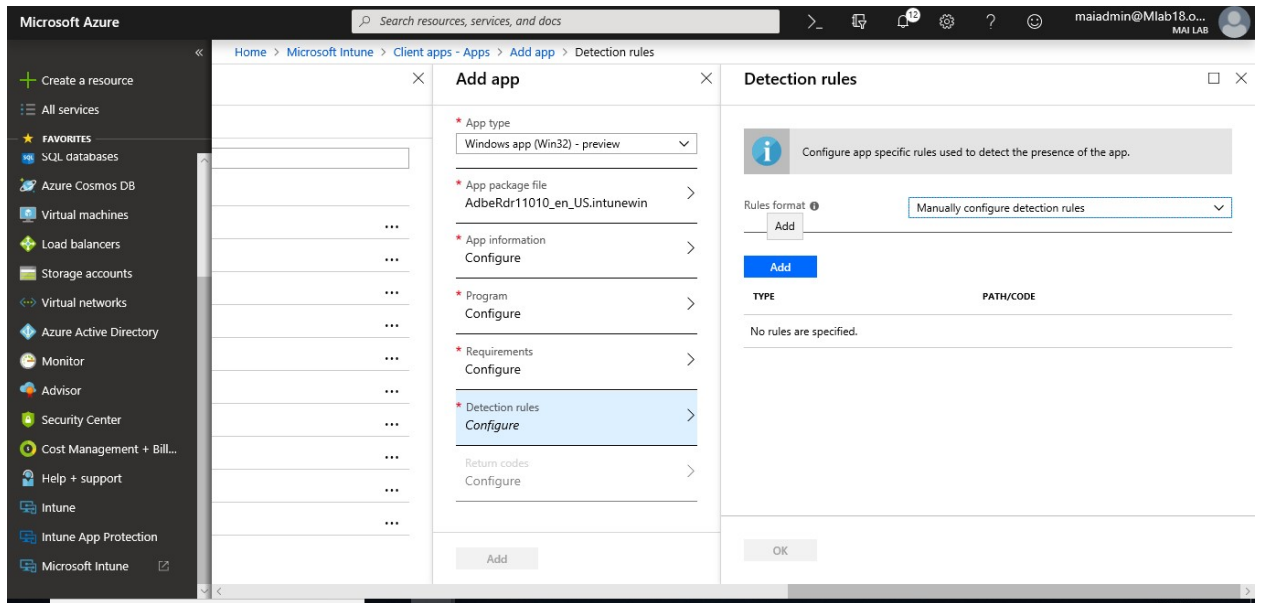
Note: You can configure a Win32 app to be installed in **User** or **System** context. **User** context refers to only a given user. **System** context refers to all users of a Windows 10 device. End users are not required to be logged in on the device to install Win32 apps.

10. In the **Add app** blade, select **Requirements** to open the **Requirements** blade.
11. On the **Requirements** blade, provide at least the following information and click **OK** to return to the **Add app** blade.
 - **Operating system architecture:** Select the applicable platforms.
 - **Minimum operating system:** Select a minimum operating system version.

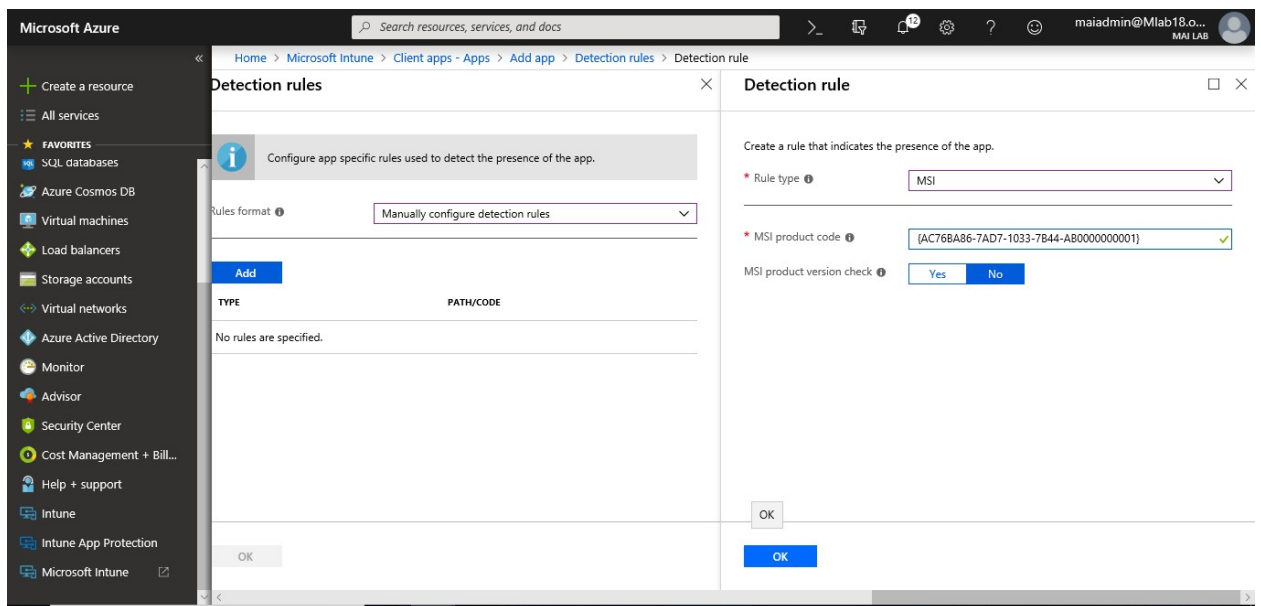


12. In the **Add app** blade, select **Detection rules** to open the **Detection rules** blade.

13. On the **Detection rules** blade, select **Manually configure detection rules** and click **Add** to open the **Detection rule** blade.

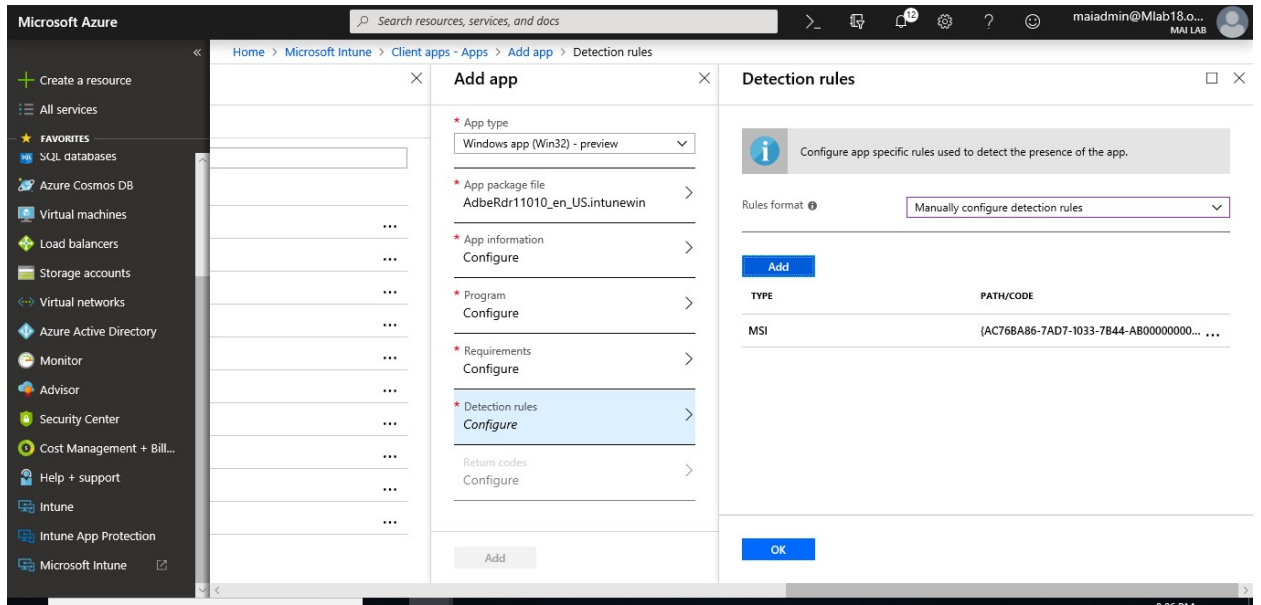


14. On the **Detection rule** blade, select **MSI** as **Rule type**, verify the pre-provisioned **MSI product code** and click **OK** to return to the **Detection rules** blade.

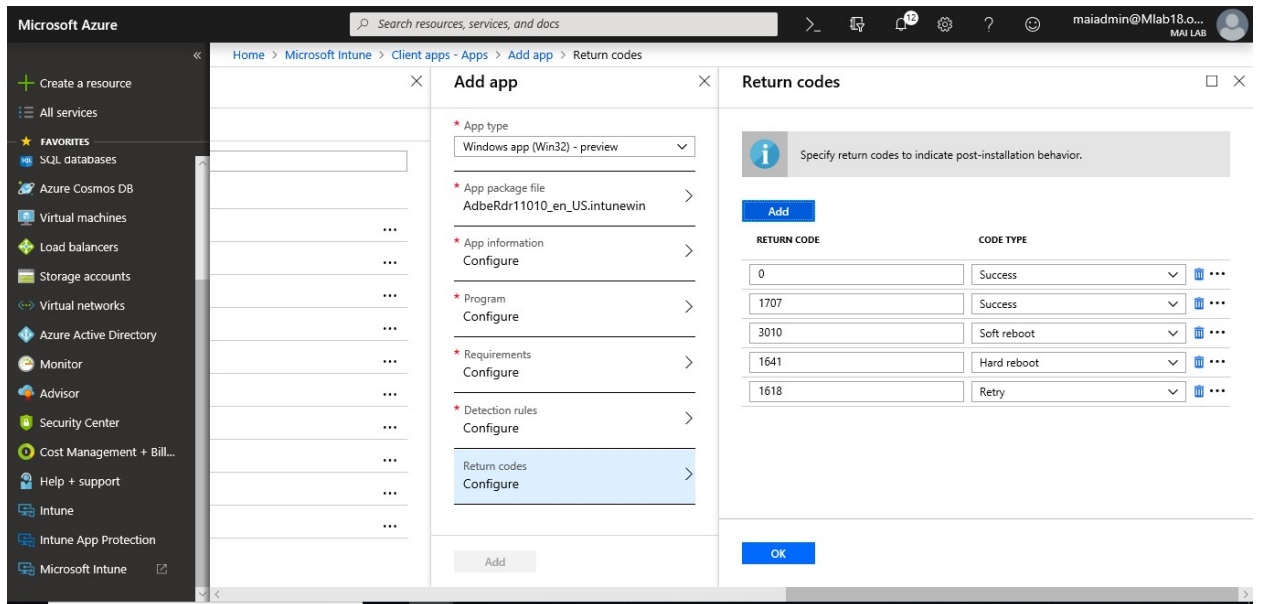


15. Back on the **Detection rules** blade, click **OK** to return to the **Add app** blade.

Microsoft Intune step by step on Azure portal

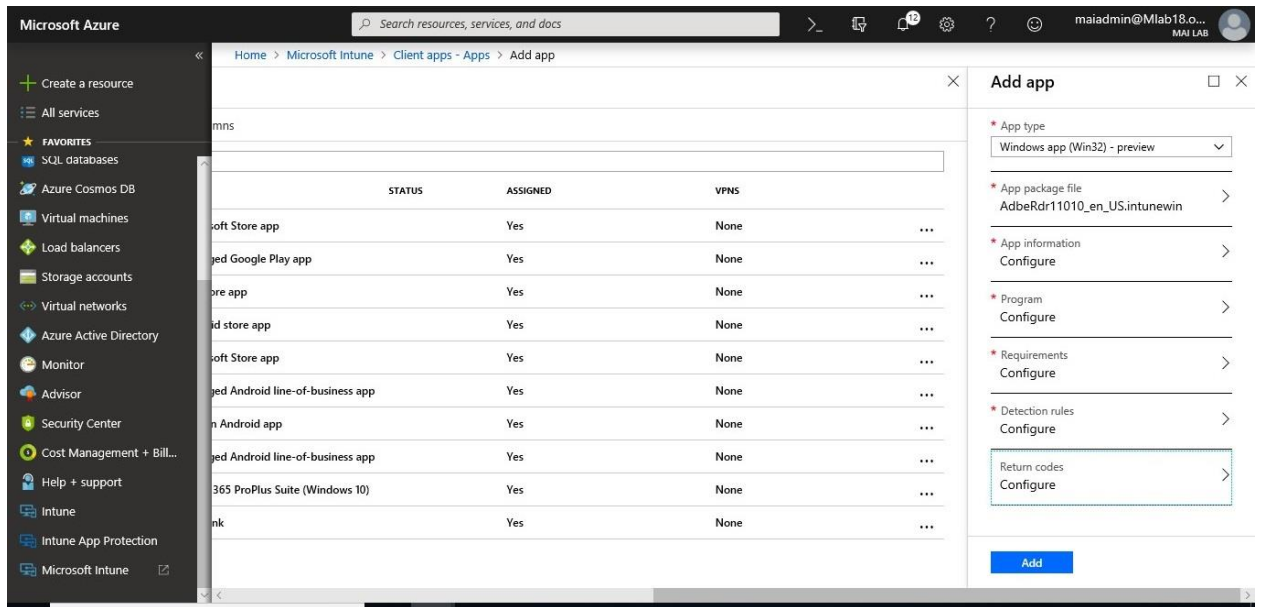


16. In the **Add app** blade, select **Return codes** to open the **Return codes** blade.
17. On the **Return codes** blade, verify the preconfigured return codes and click **OK** to return to the **Add app** blade.

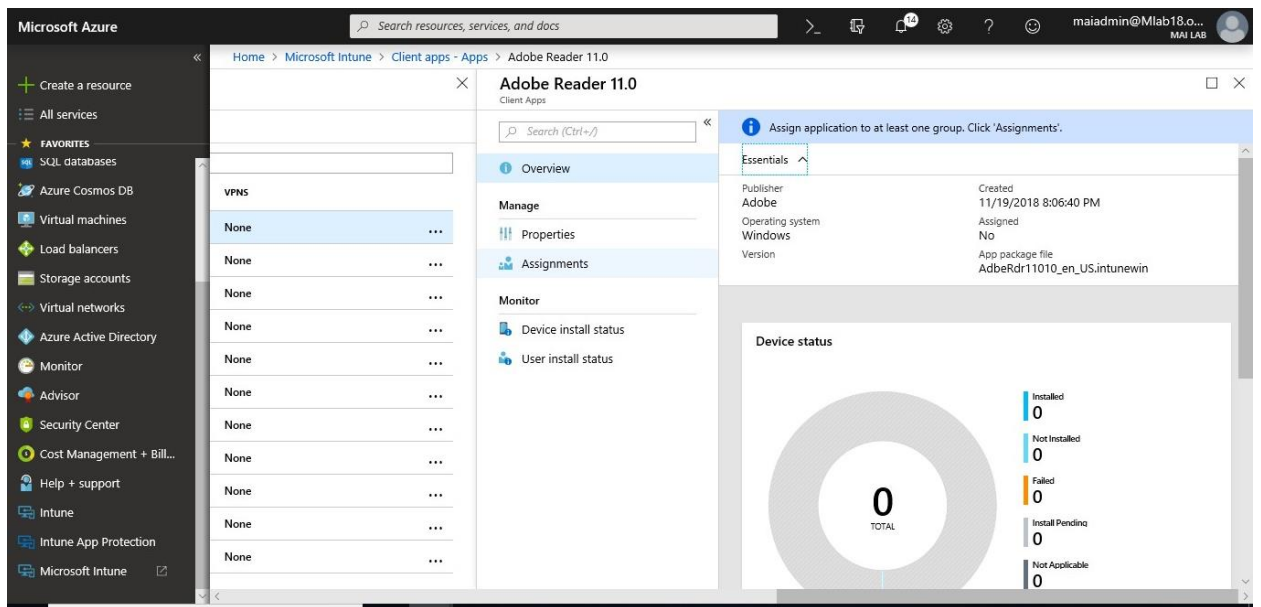


18. In the **Add app** blade, click **Add** to actually add app.

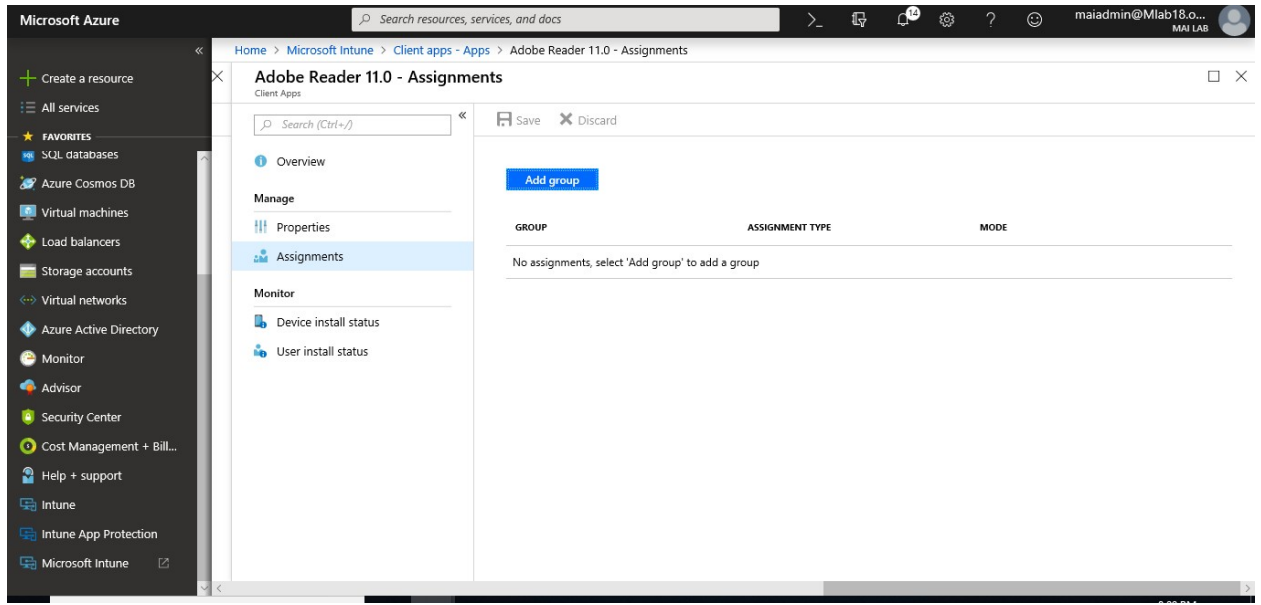
Microsoft Intune step by step on Azure portal



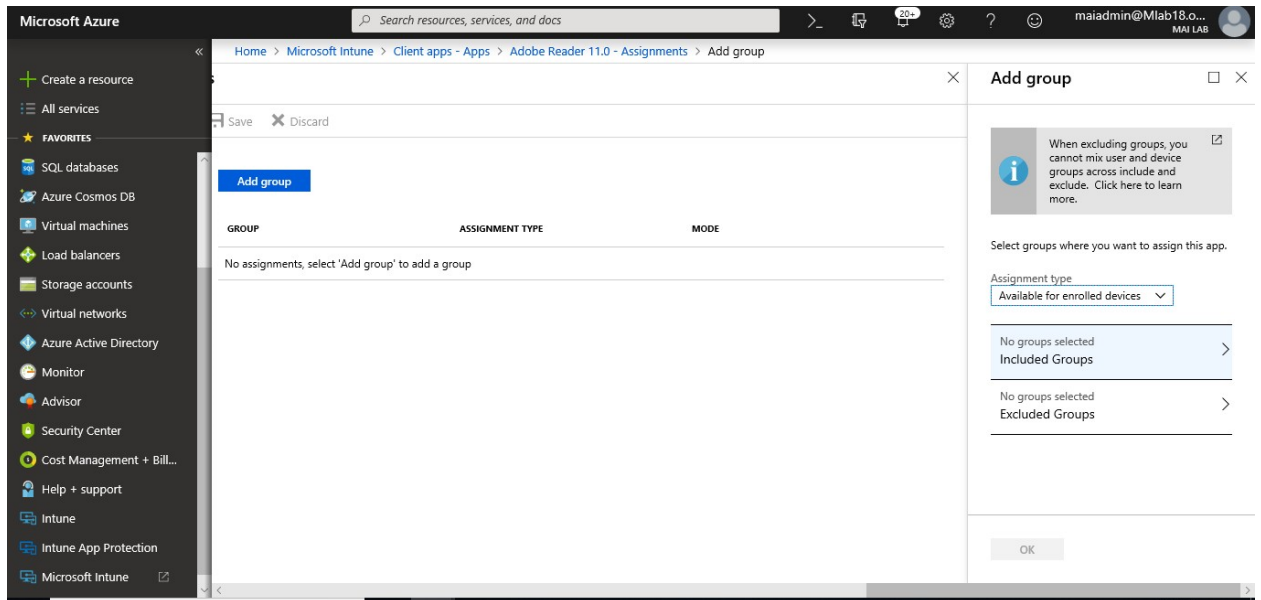
19. In the app pane, select **Assignments**.



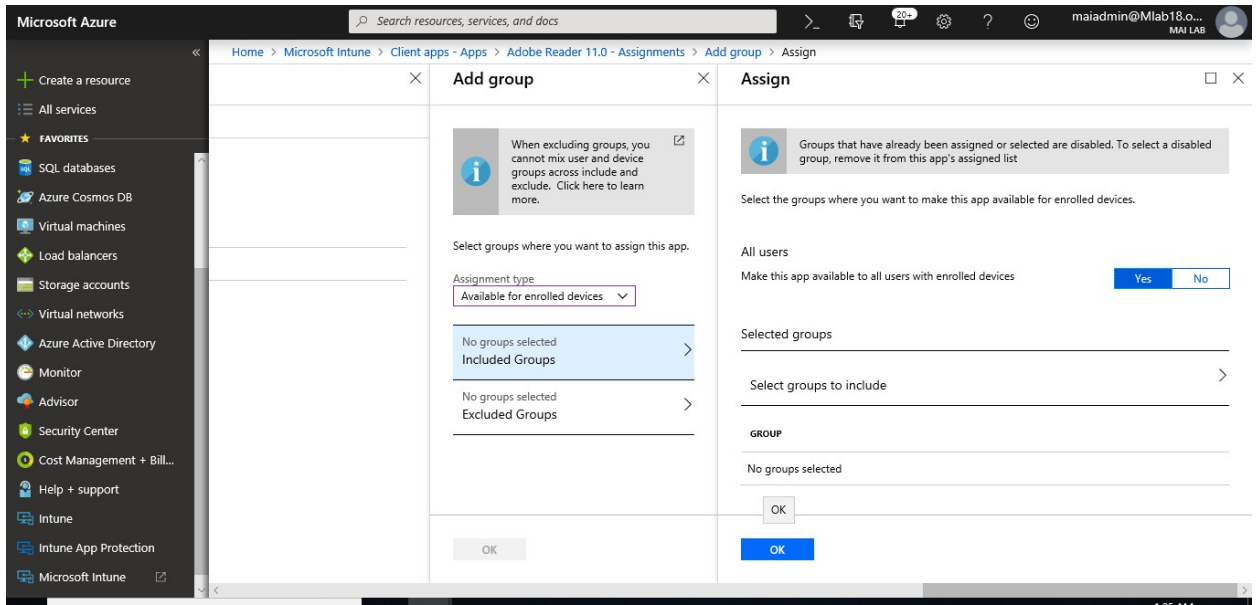
20. Select **Add Group** to open the **Add group** pane that is related to the app.



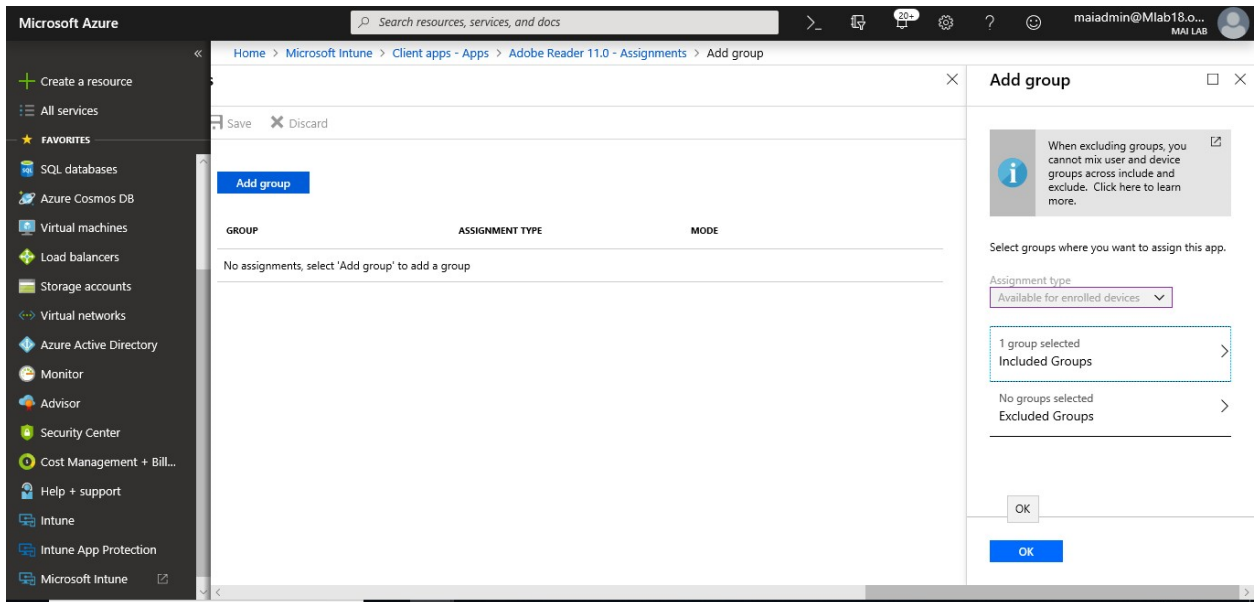
21. For the specific app, select an **assignment type**:
 - a. **Available for enrolled devices**: Users install the app from the Company Portal app or Company Portal website.
 - b. **Required**: The app is installed on devices in the selected groups.
 - c. **Uninstall**: The app is uninstalled from devices in the selected groups.
22. Select **Included Groups** and assign the groups that will use this app.



23. In the **Assign** pane, select **OK** to complete the included groups selection.

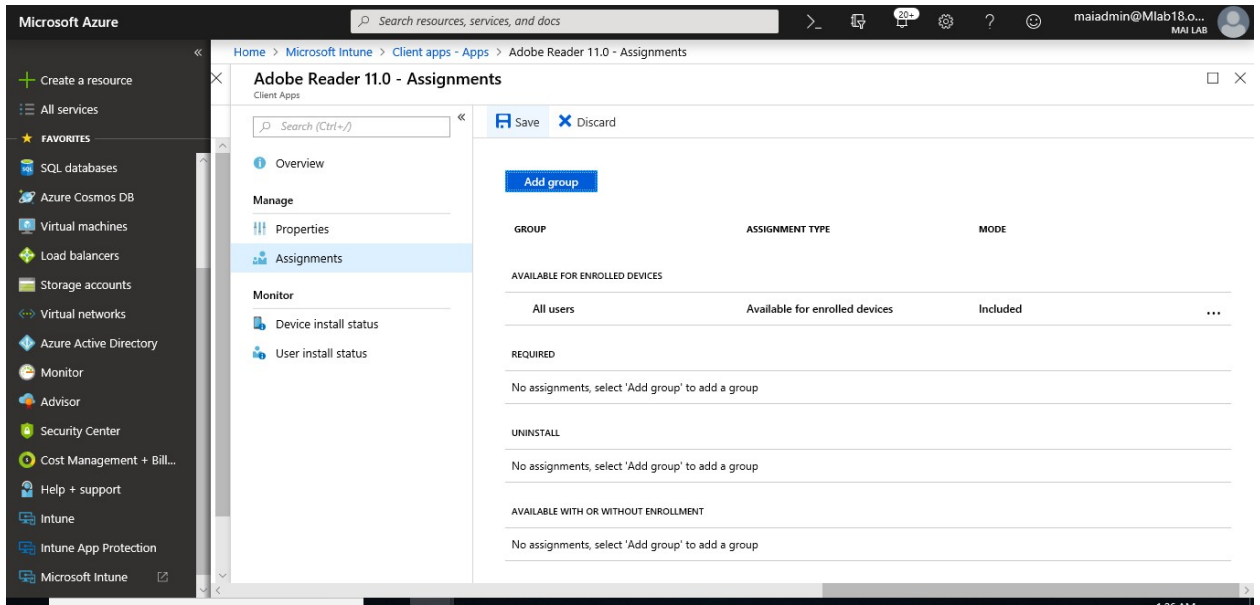


- 24. If you want to exclude any groups of users from being affected by this app assignment, select **Exclude Groups**.
- 25. In the **Add group** pane, select **OK**.

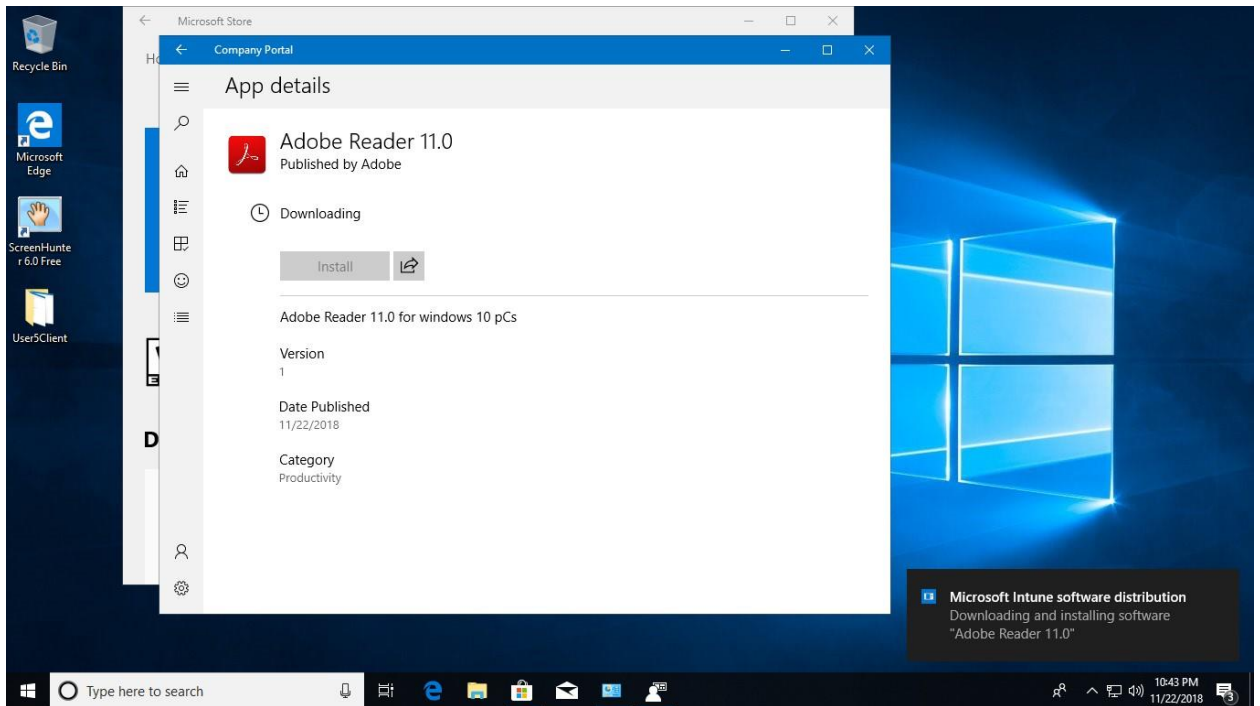


- 26. In the app **Assignments** pane, select **Save**.

Microsoft Intune step by step on Azure portal

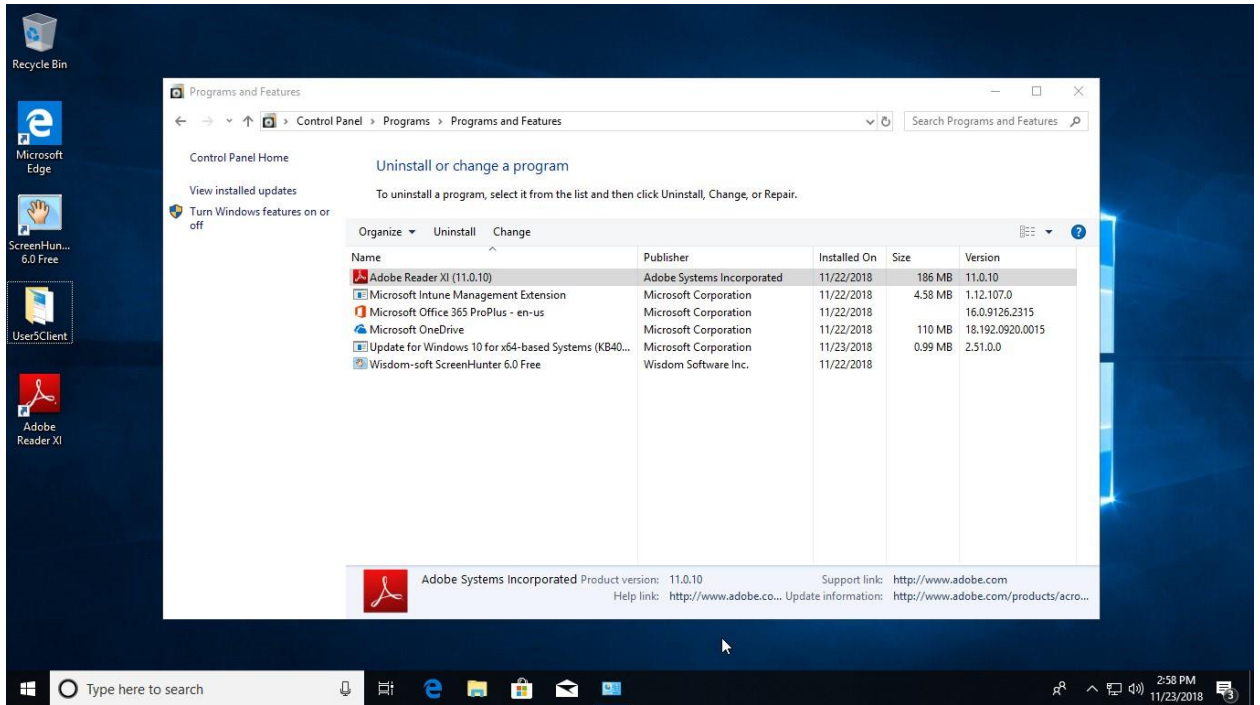


27. On Client pc, Open Company Portal, Click **Install** on Adobe.

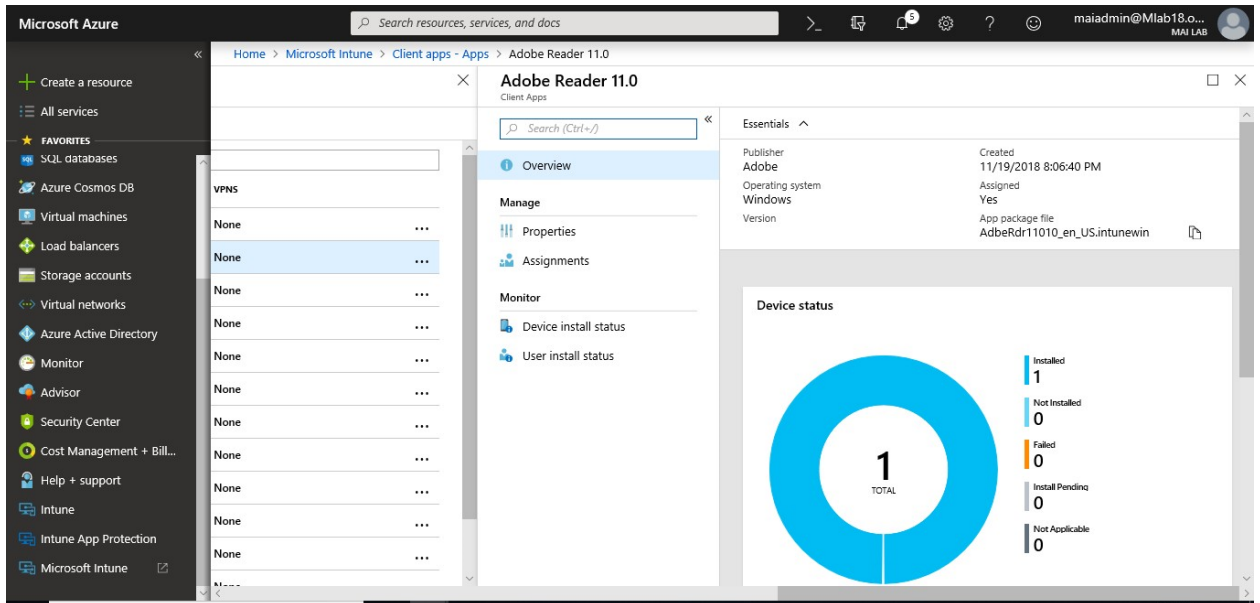


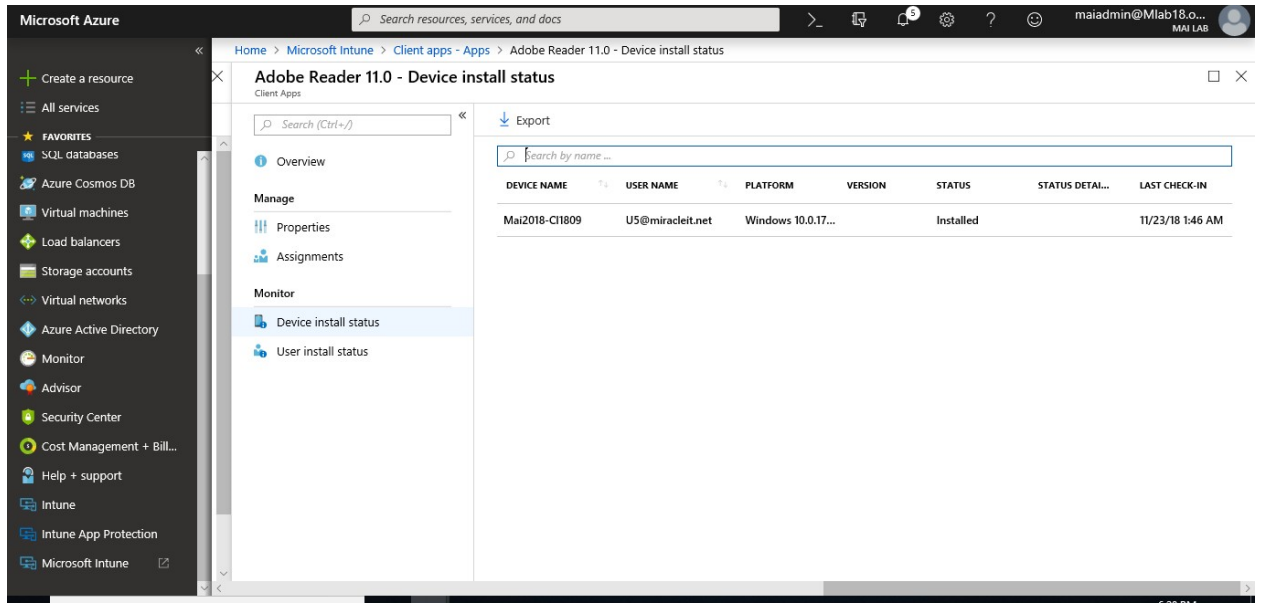
28. Once it's finished, it will appear on Desktop & control panel.

Microsoft Intune step by step on Azure portal



29. you will find on Intune admin portal that it's already installed.





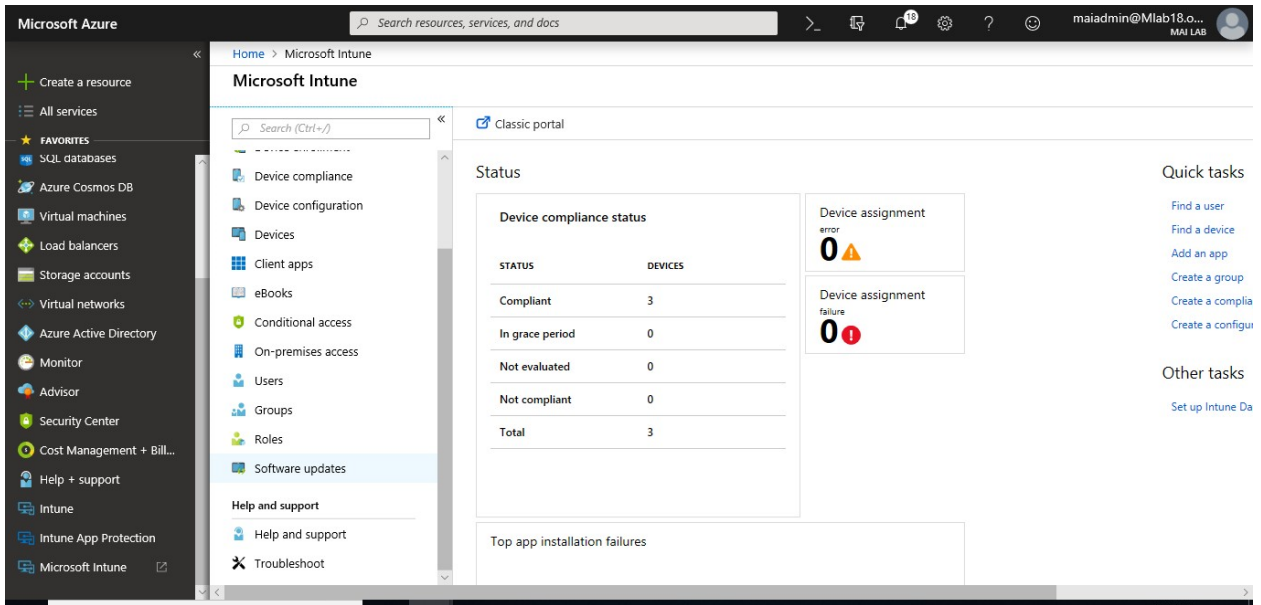
Manage Software Updates in Intune

By using Windows Update for Business, you simplify the update management experience. You don't need to approve individual updates for groups of devices. You can manage risk in your environments by configuring an update rollout strategy. Windows Update makes sure that updates are installed at the right time. Microsoft Intune provides the ability to configure update settings on devices and gives you the ability to defer update installation. Intune doesn't store the updates, but only the update policy assignment. Devices access Windows Update directly for the updates. Use Intune to configure and manage **Windows 10 update rings**. An update ring includes a group of settings that configure when and how Windows 10 updates get installed.

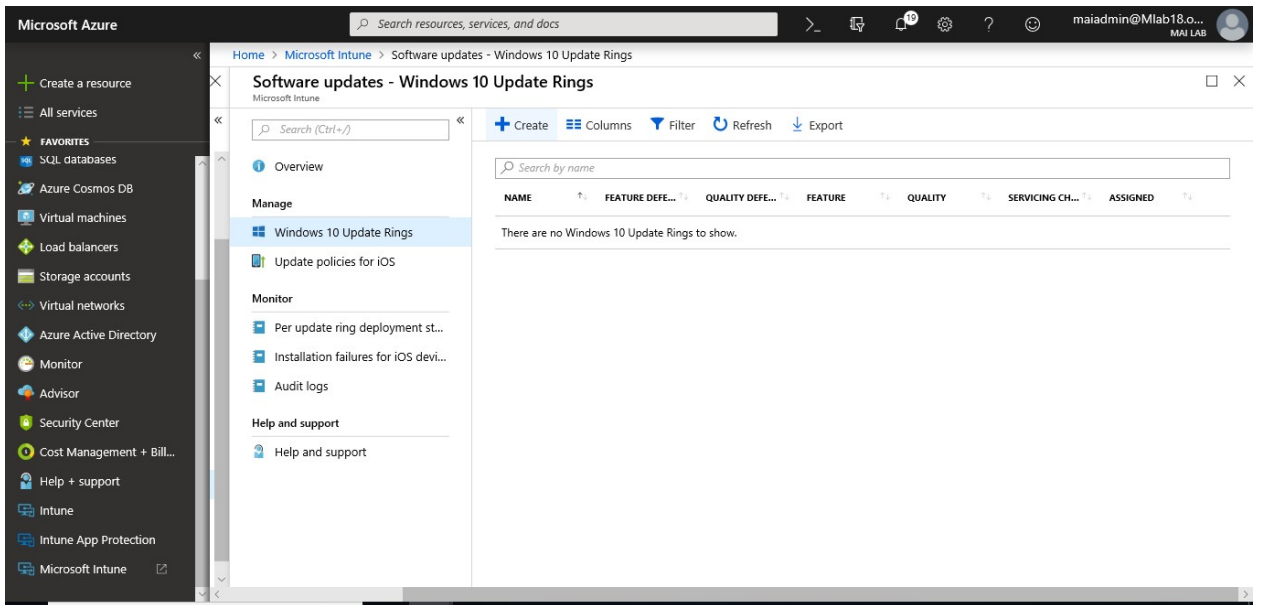
Create and assign update rings

1. Sign in to the [Azure portal](#). Select **All services**, filter on **Intune**, and then select **Microsoft Intune > Software updates**.

Microsoft Intune step by step on Azure portal

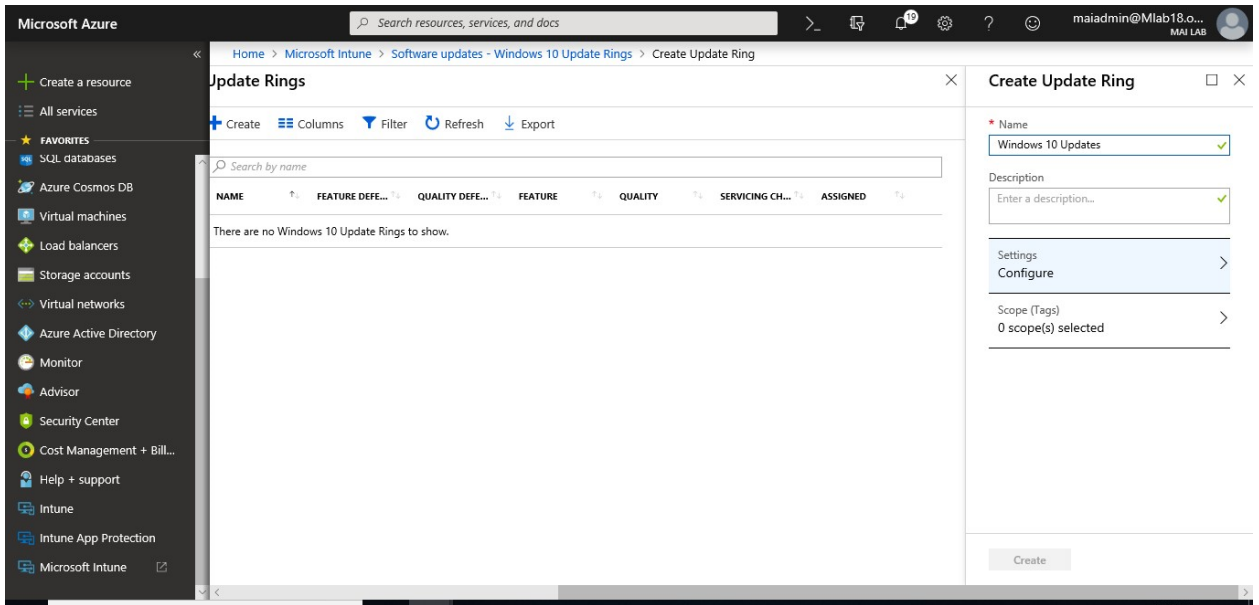


2. On Software updates > Windows 10 Update Rings > Create.

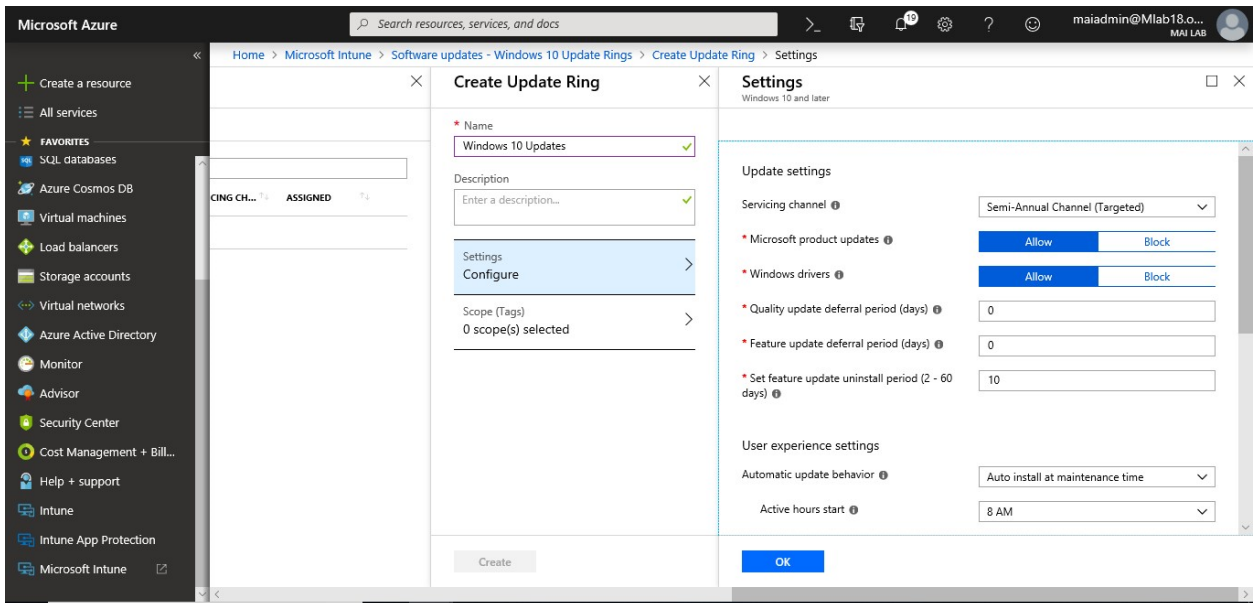


3. Enter a name, a description (optional), and then choose **Configure**.

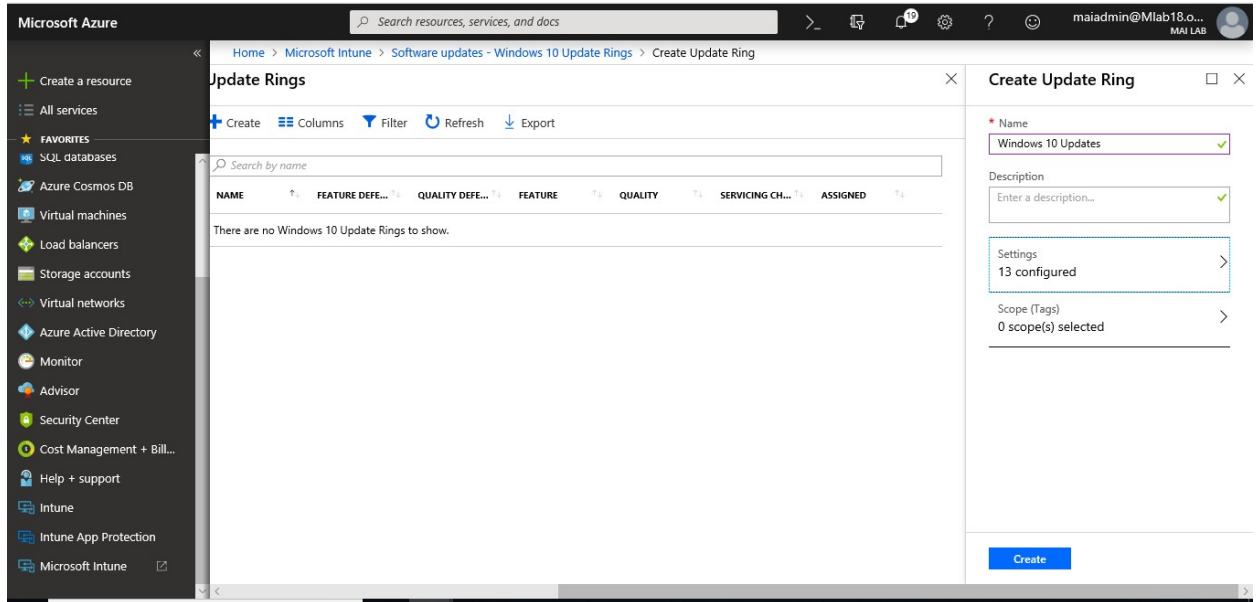
Microsoft Intune step by step on Azure portal



4. In **Settings**, enter the following information:

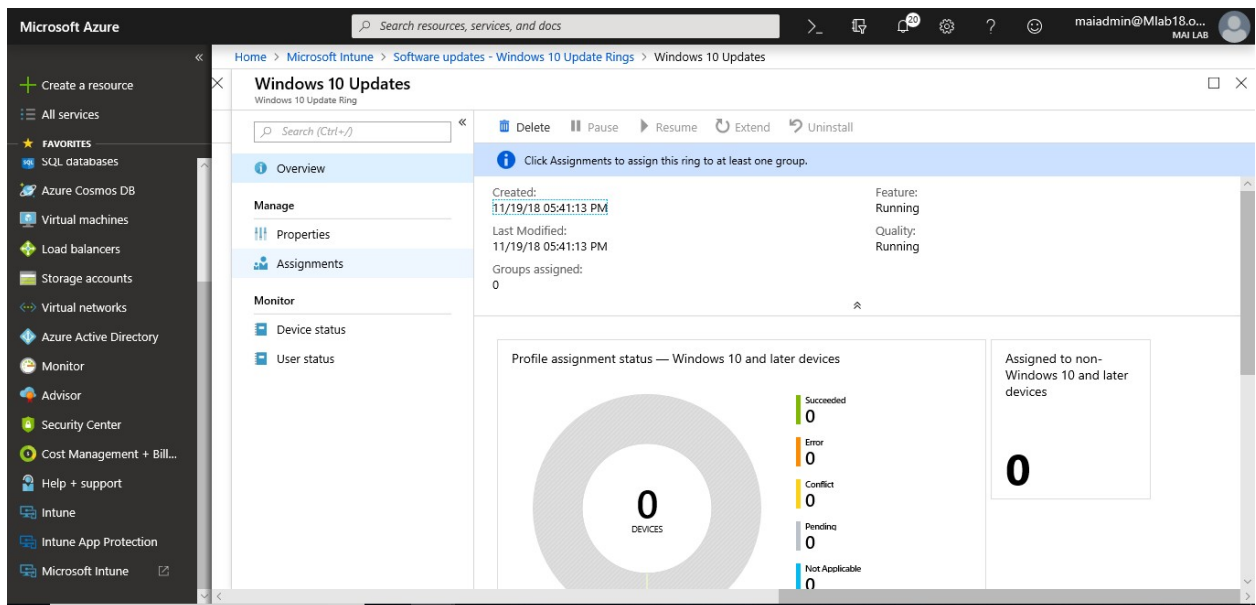


5. When done, select **OK**. In **Create Update Ring**, select **Create**.



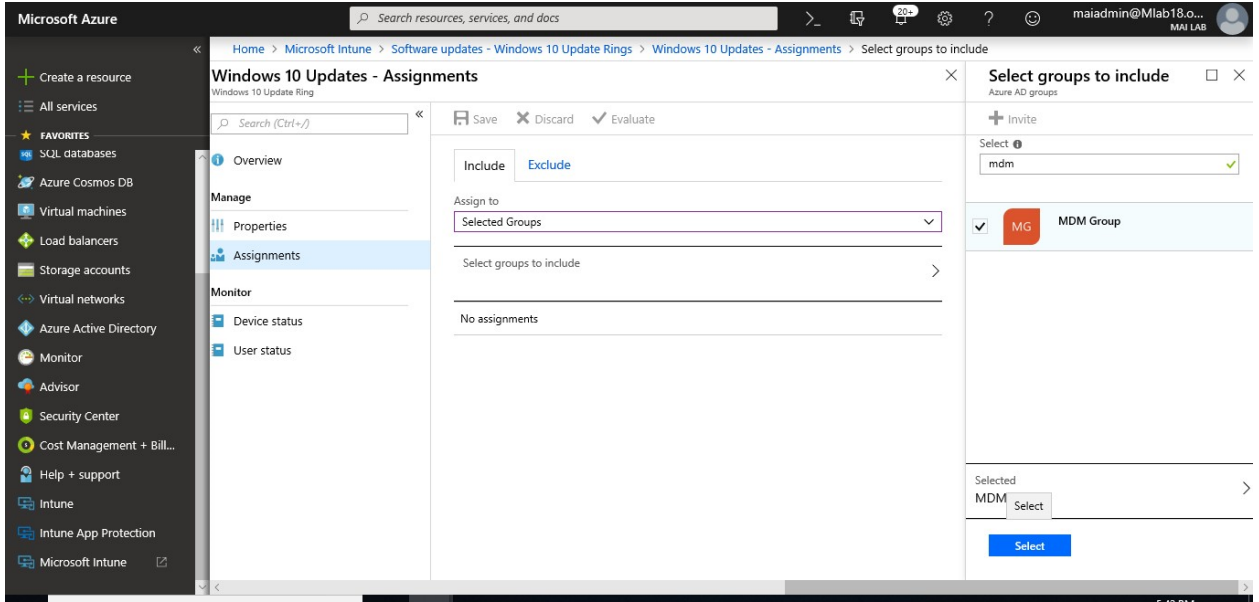
The new update ring is displayed in the list of update rings.

1. To assign the ring, in the list of update rings, select a ring, and then on the *<ring name>* tab, choose **Assignments**.

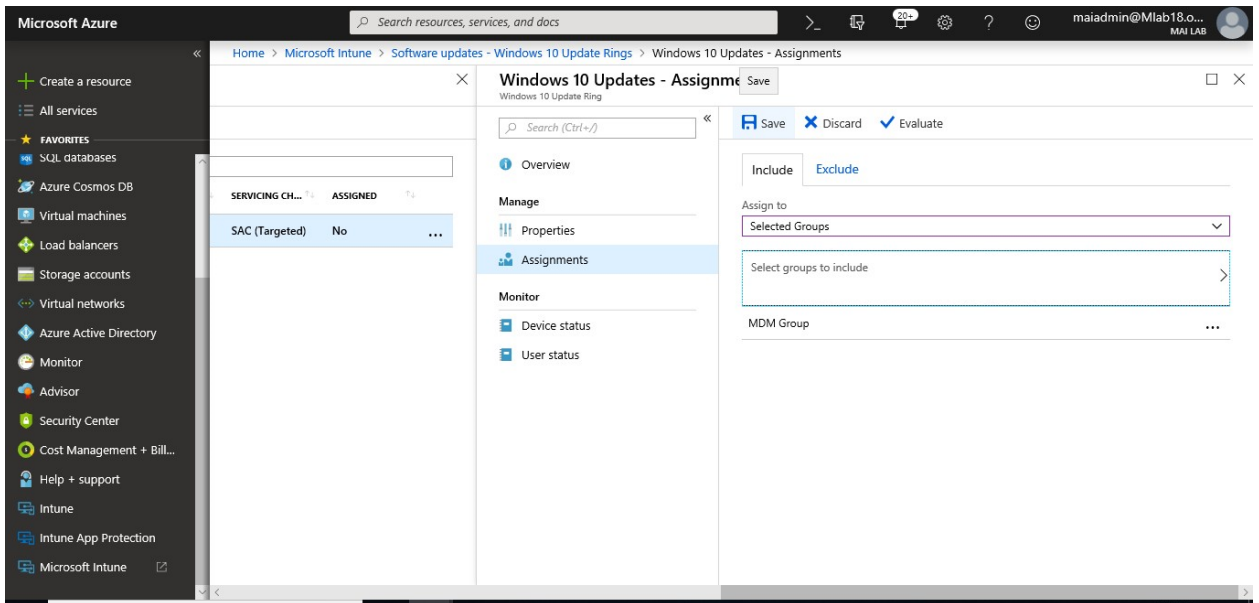


2. On the next tab, choose **Select groups to include**, and then choose the groups to which you want to assign this ring. Once you are done, choose **Select** to complete the assignment.

Microsoft Intune step by step on Azure portal

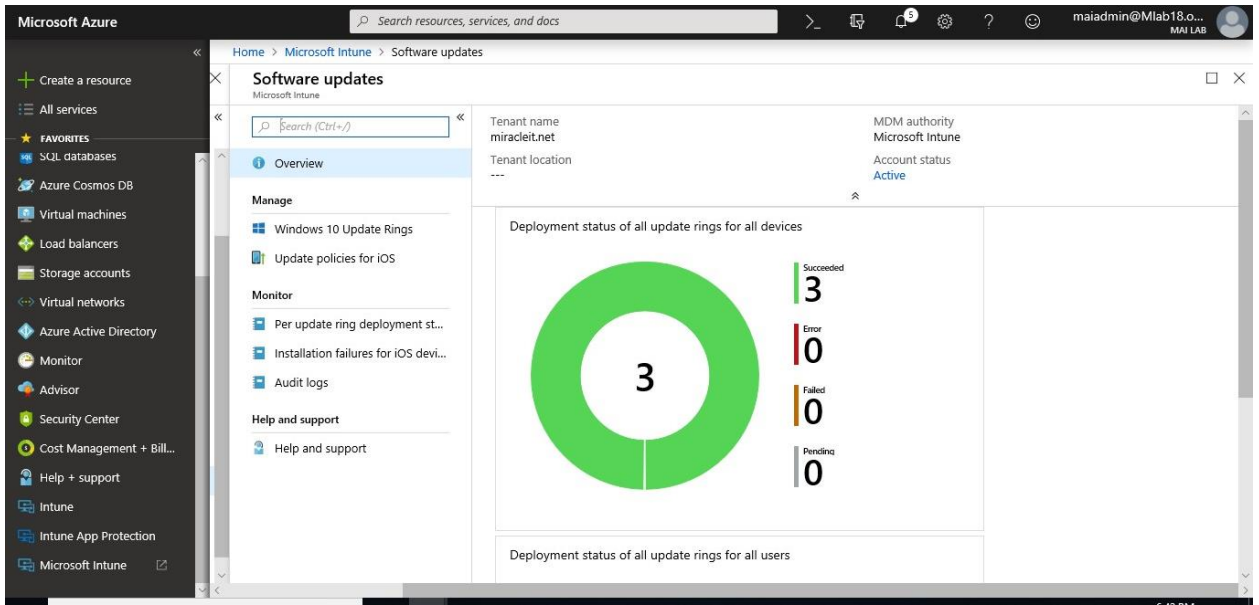


3. Click **Save**.



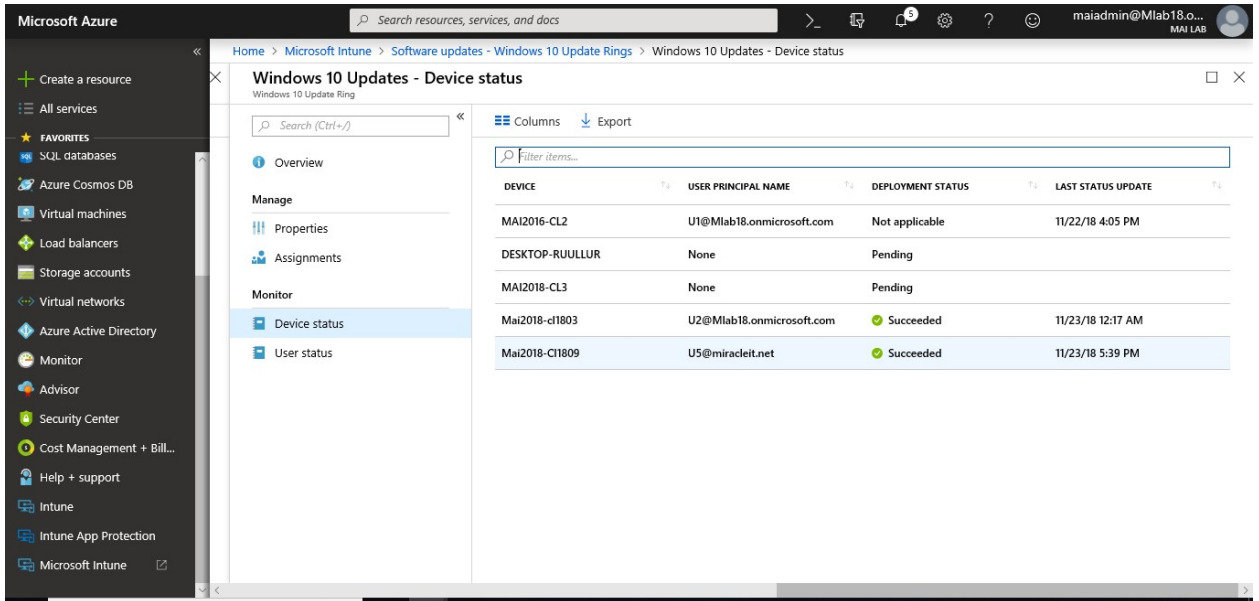
4. After 30 min., you should see update deployment started.

Microsoft Intune step by step on Azure portal



The screenshot shows the Microsoft Intune 'Software updates' overview page. The left sidebar contains navigation options like 'Overview', 'Manage', 'Monitor', and 'Help and support'. The main content area displays the 'Deployment status of all update rings for all devices' as a donut chart with a central '3'. To the right of the chart, a summary table shows: Succeeded: 3, Error: 0, Failed: 0, and Pending: 0. Metadata at the top right includes Tenant name (miracleit.net), MDM authority (Microsoft Intune), and Account status (Active).

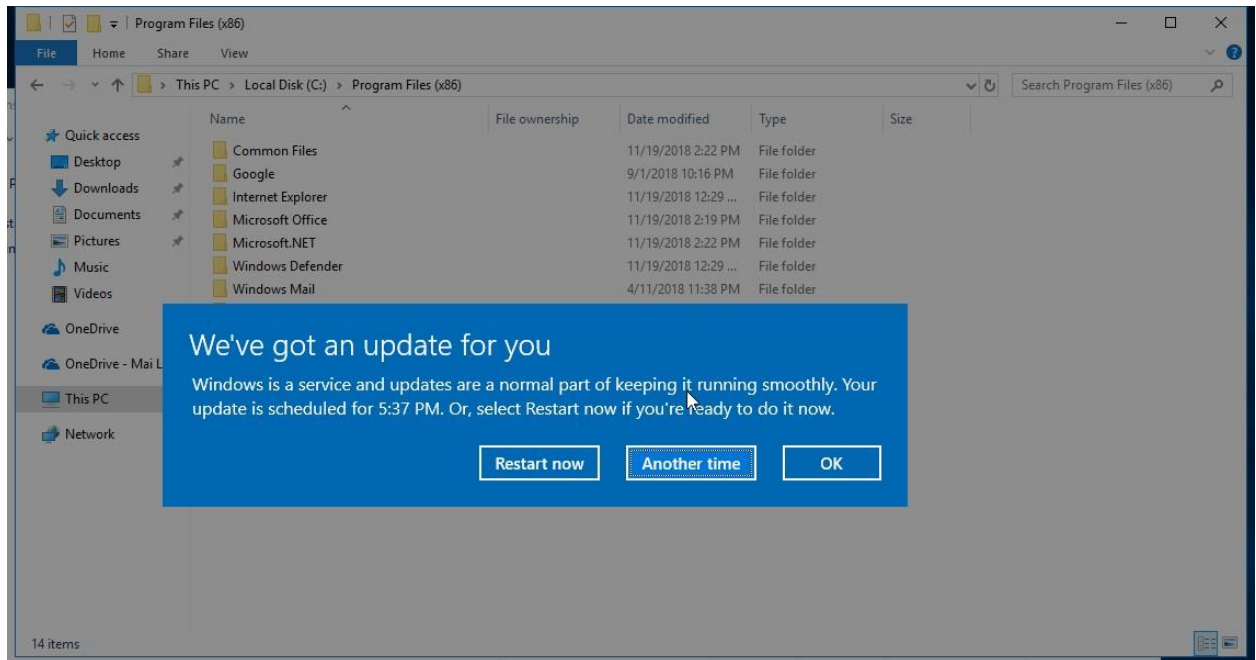
Deployment Status	Count
Succeeded	3
Error	0
Failed	0
Pending	0



The screenshot shows the 'Windows 10 Updates - Device status' page. It features a table with columns for DEVICE, USER PRINCIPAL NAME, DEPLOYMENT STATUS, and LAST STATUS UPDATE. The table contains five rows of data, with the last two rows highlighted in blue. The 'Device status' menu item is selected in the left sidebar.

DEVICE	USER PRINCIPAL NAME	DEPLOYMENT STATUS	LAST STATUS UPDATE
MAI2016-CL2	U1@Mlab18.onmicrosoft.com	Not applicable	11/22/18 4:05 PM
DESKTOP-RUULLUR	None	Pending	
MAI2018-CL3	None	Pending	
Mai2018-cl1803	U2@Mlab18.onmicrosoft.com	Succeeded	11/23/18 12:17 AM
Mai2018-CI1809	U5@miracleit.net	Succeeded	11/23/18 5:39 PM

5. On client pc., you should see update deployment started.



Configure Remote Assistance

Intune can use the [TeamViewer](#) software, purchased separately, to enable you to give remote assistance to your users who are running the Intune software client. When a user requests help from the Microsoft Intune Center, you are informed by an alert, can accept the request, and then provide assistance.

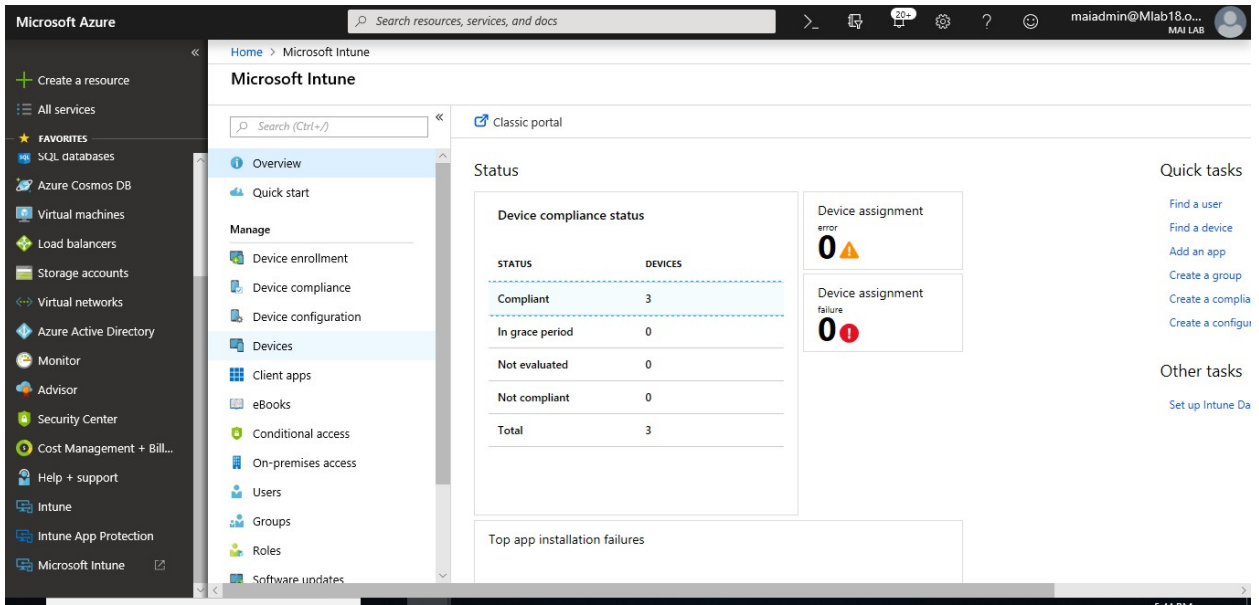
Note: TeamViewer licenses are separate licenses not related to Intune or Microsoft licenses.

Configure the TeamViewer connector

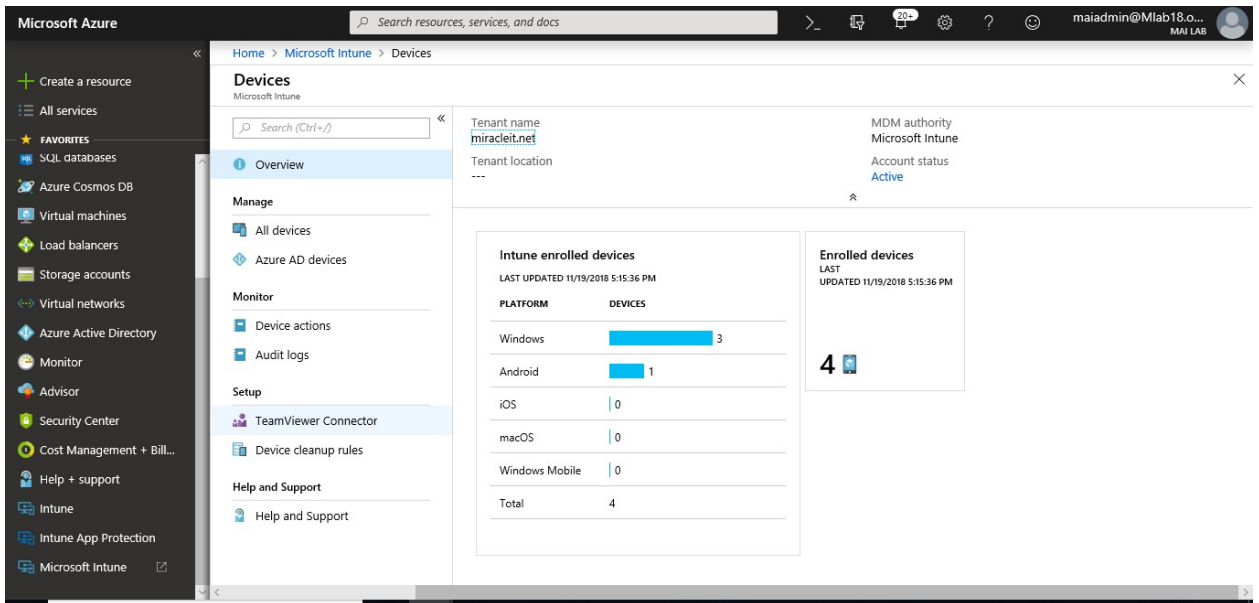
To provide remote assistance to devices, configure the Intune TeamViewer connector using the following steps:

1. In the [Azure portal](#), select **All Services**, and search for **Microsoft Intune > Devices**.

Microsoft Intune step by step on Azure portal

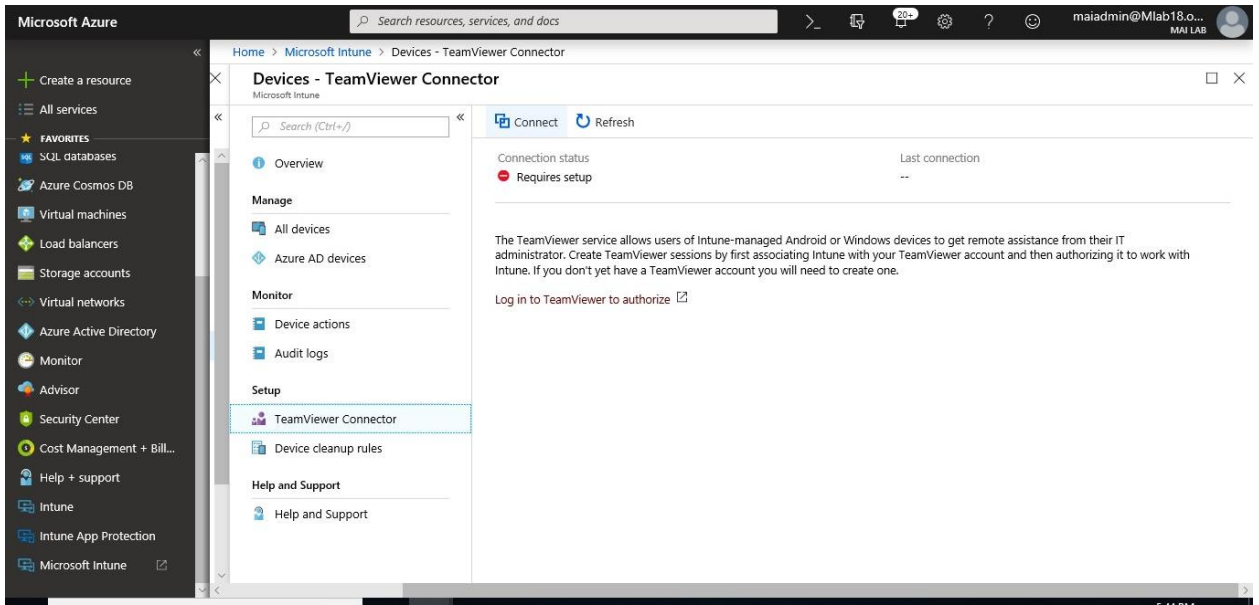


2. In Microsoft Intune, select **Devices**, and then select **TeamViewer Connector**.

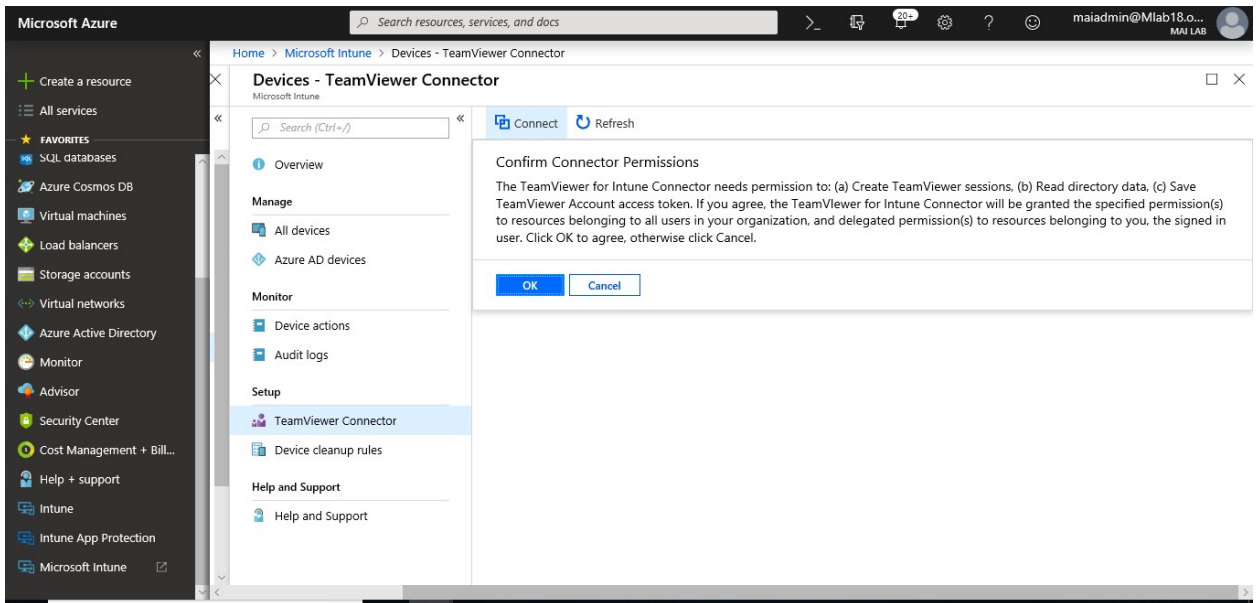


3. Select **Connect**, and then accept the license agreement.

Microsoft Intune step by step on Azure portal

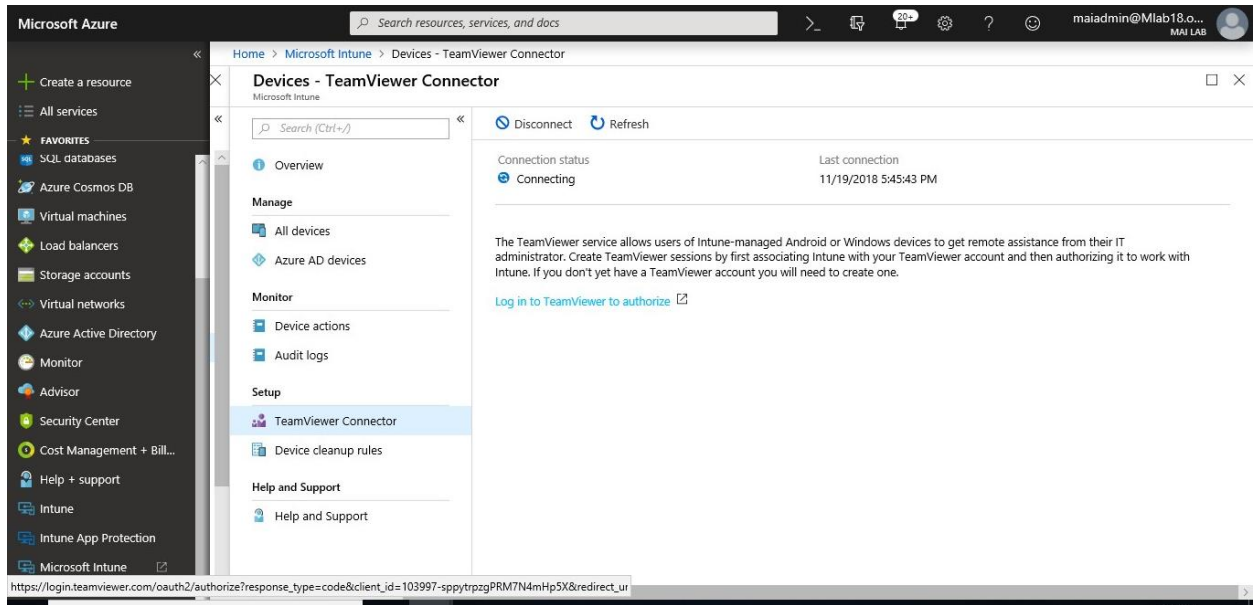


4. Confirm Connectors Permission, Click **Ok**.

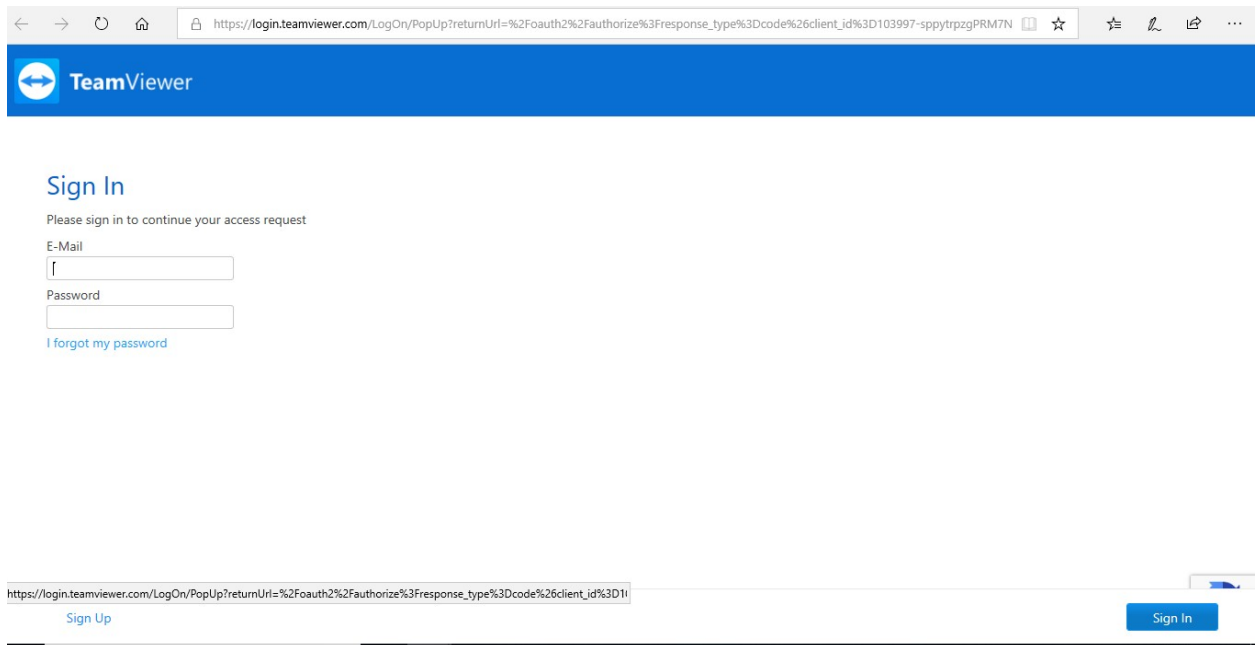


5. Select **Log in to TeamViewer to authorize**.

Microsoft Intune step by step on Azure portal

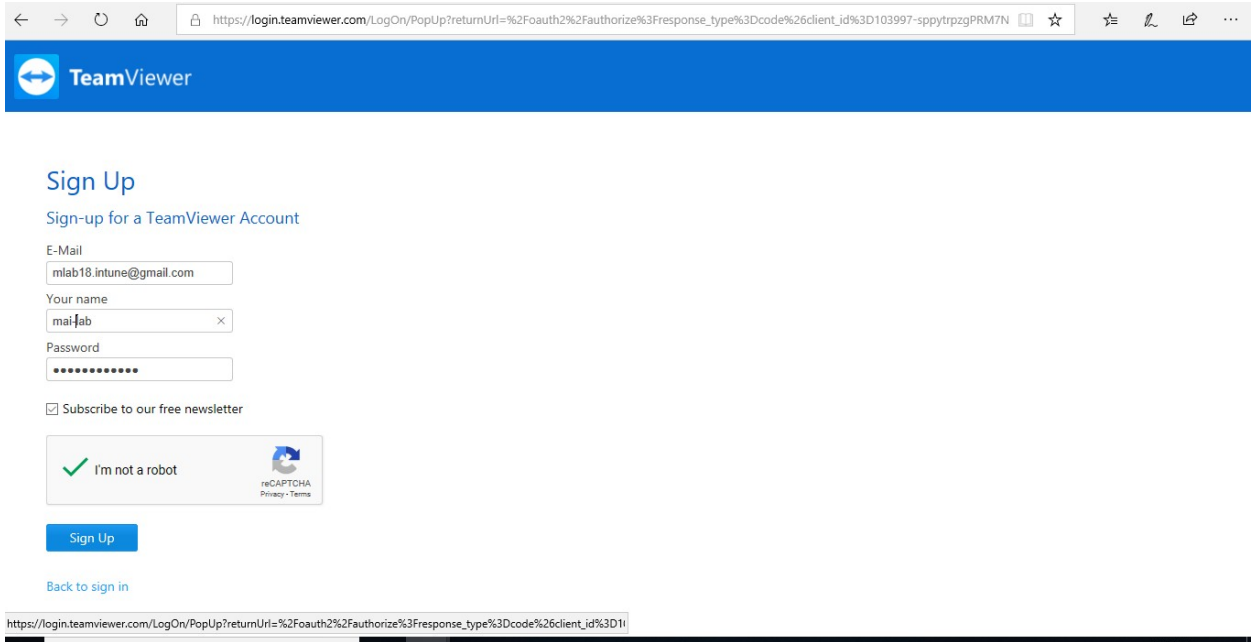


6. A web page opens to the TeamViewer site. Enter your TeamViewer license credentials, and then **Sign In**. If you don't have an account, click sign up to create a new TeamViewer account.



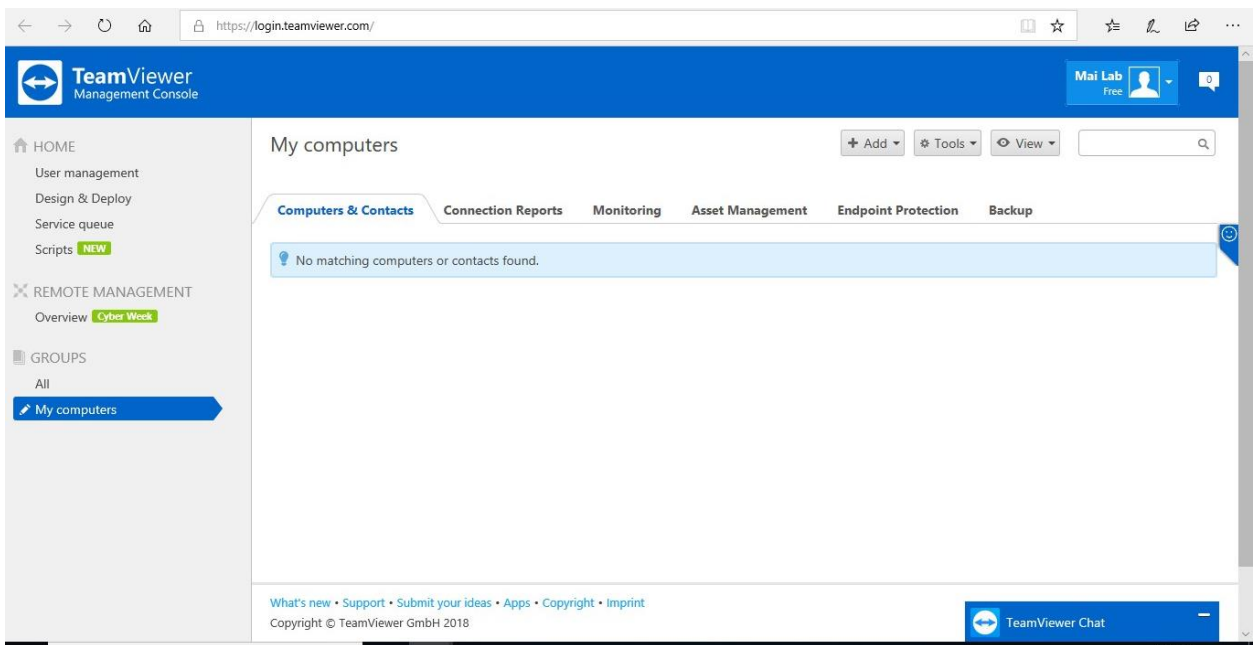
7. On **Sign up** Page, enter your information and Select **Sign up**.

Microsoft Intune step by step on Azure portal



The screenshot shows the TeamViewer Sign Up page. The browser address bar contains the URL: https://login.teamviewer.com/LogOn/PopUp?returnUrl=%2Foauth2%2Fauthorize%3Fresponse_type%3Dcode%26client_id%3D103997-sppytrpzgPRM7N. The page has a blue header with the TeamViewer logo. Below the header, the text "Sign Up" is followed by "Sign-up for a TeamViewer Account". There are four input fields: "E-Mail" with the value "mlab18.intune@gmail.com", "Your name" with the value "mai lab", and "Password" with masked characters. A checkbox for "Subscribe to our free newsletter" is checked. Below the inputs is a reCAPTCHA widget with a green checkmark and the text "I'm not a robot". A blue "Sign Up" button is at the bottom, with a link "Back to sign in" below it. The footer contains the URL: https://login.teamviewer.com/LogOn/PopUp?returnUrl=%2Foauth2%2Fauthorize%3Fresponse_type%3Dcode%26client_id%3D103997-sppytrpzgPRM7N.

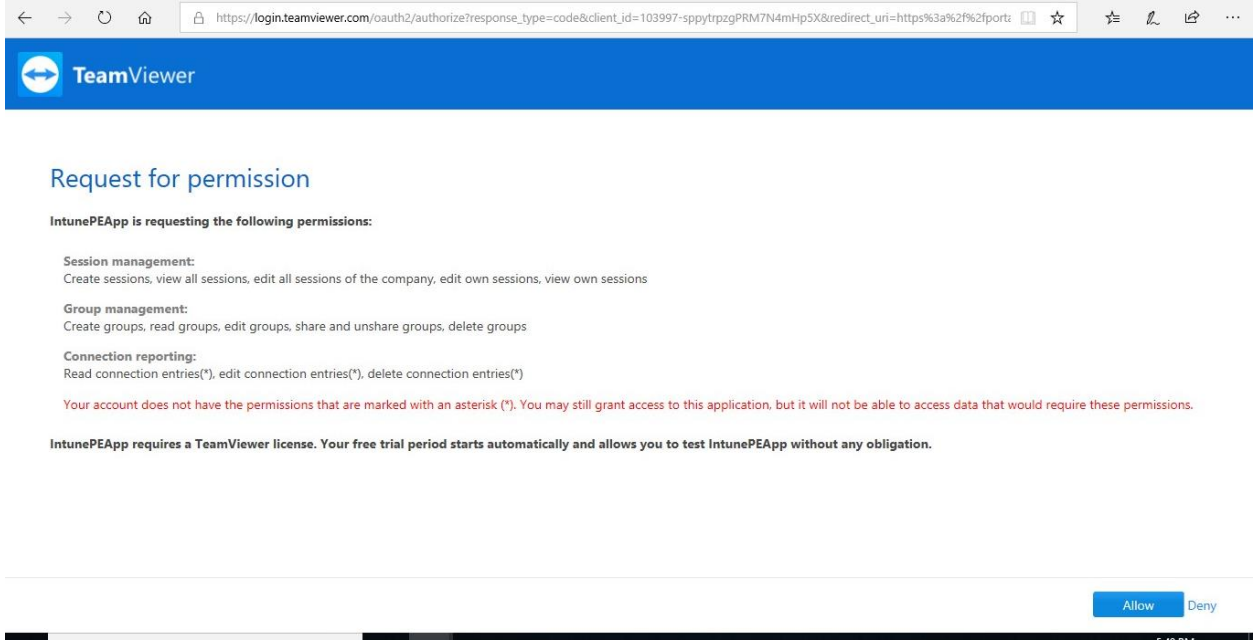
8. You will receive activation mail on your mail. Activate TeamViewer account.



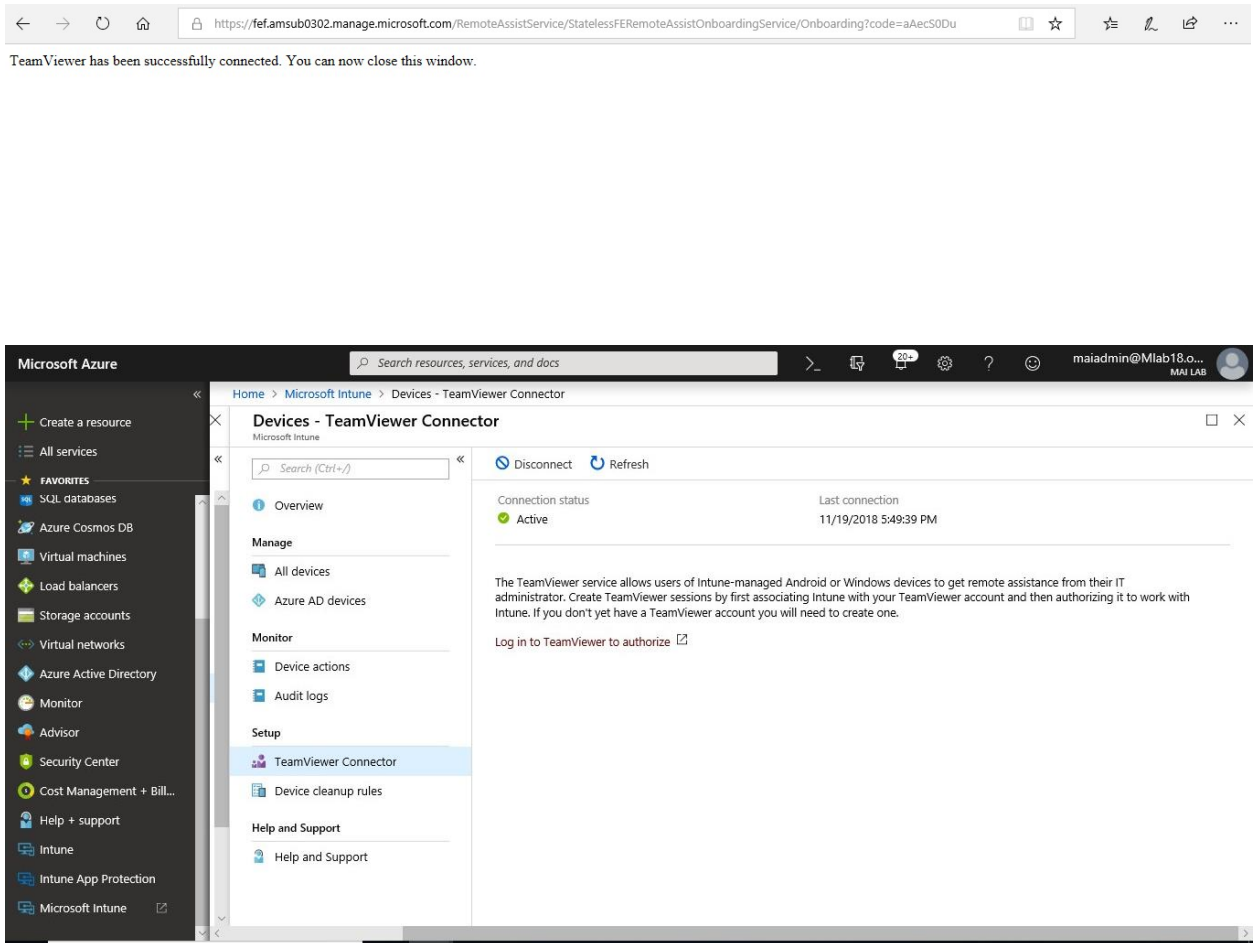
The screenshot shows the TeamViewer Management Console interface. The browser address bar contains the URL: <https://login.teamviewer.com/>. The page has a blue header with the TeamViewer logo and "Management Console". In the top right corner, there is a user profile for "Mai Lab" with a "Free" status and a chat icon. The left sidebar contains a navigation menu with sections: "HOME" (User management, Design & Deploy, Service queue, Scripts **NEW**), "REMOTE MANAGEMENT" (Overview **Cyber Week**), and "GROUPS" (All, **My computers**). The main content area is titled "My computers" and has tabs for "Computers & Contacts", "Connection Reports", "Monitoring", "Asset Management", "Endpoint Protection", and "Backup". Below the tabs, there is a message box that says "No matching computers or contacts found." At the bottom of the page, there is a footer with links for "What's new", "Support", "Submit your ideas", "Apps", "Copyright", and "Imprint", along with the copyright notice "Copyright © TeamViewer GmbH 2018". A "TeamViewer Chat" button is visible in the bottom right corner.

9. On Request for permission Page, Enter Allow.

Microsoft Intune step by step on Azure portal



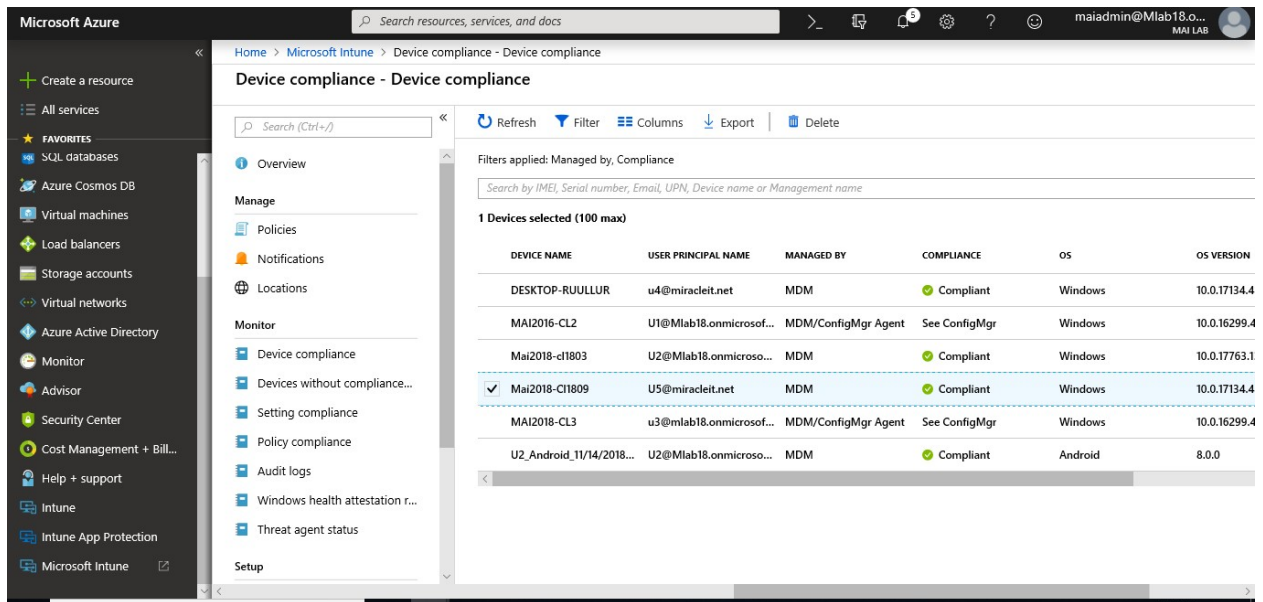
10. Now Team Viewer has connected successfully.



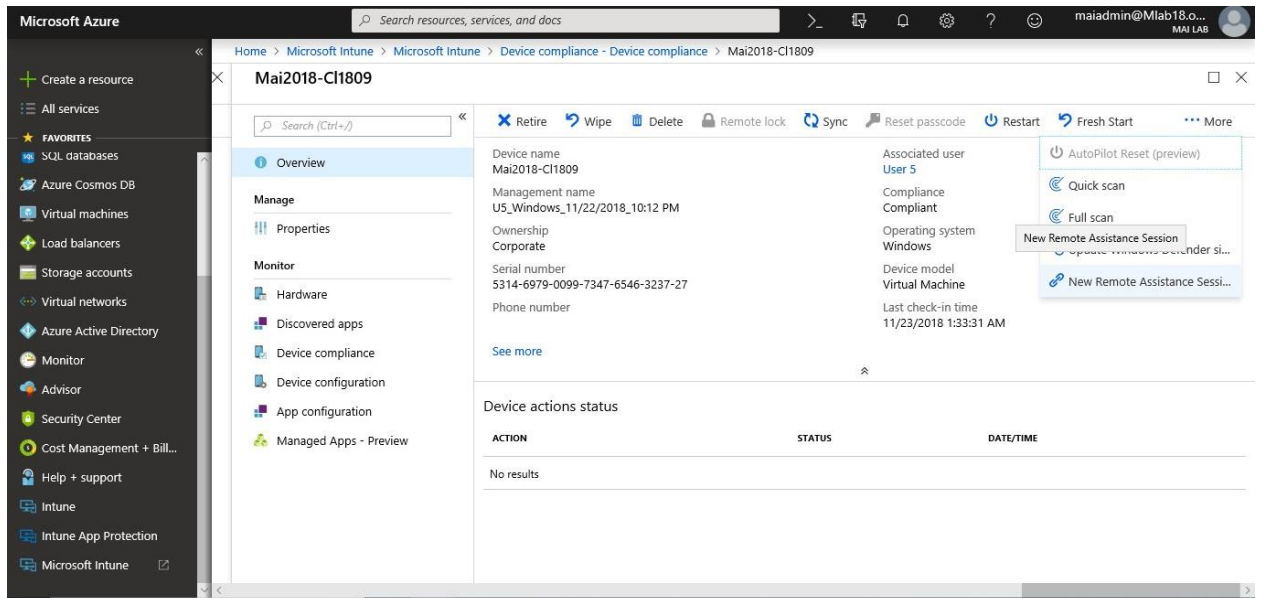
Remotely administer a device

After the connector is configured, you're ready to remotely administer a device. Use the following steps:

1. In the [Azure portal](#), select **All Services**, and search for **Microsoft Intune**.
2. In **Microsoft Intune**, select **Devices**, and then select **All devices**.
3. From the list, select the device that you want to remotely administer.

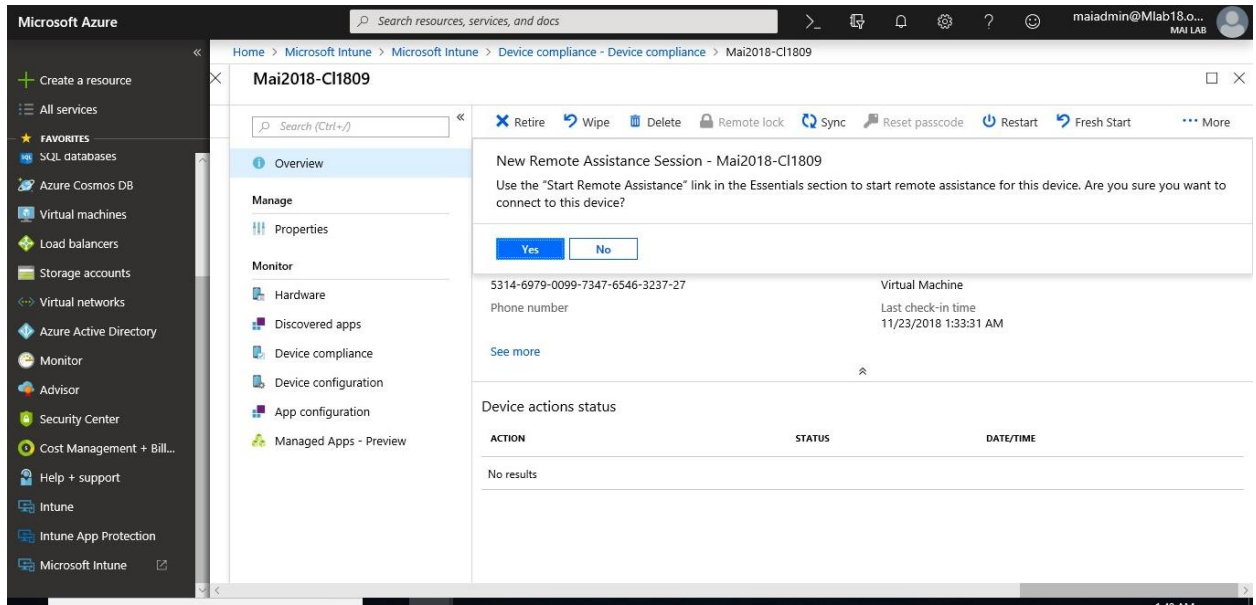


4. In the device properties, select **New Remote Assistance Session**.

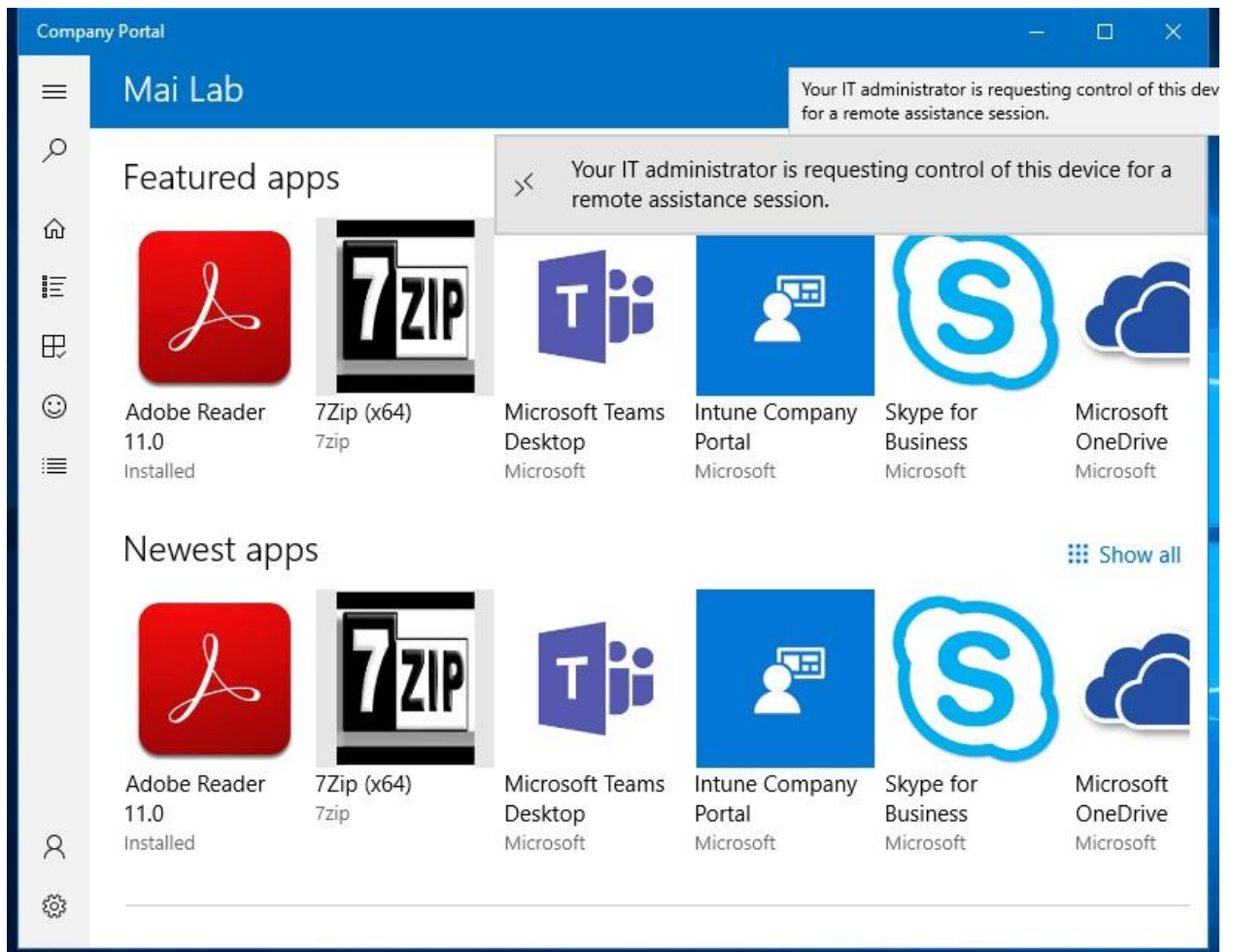


5. On **New Remote Assistance Session**, Click **Yes**.

Microsoft Intune step by step on Azure portal



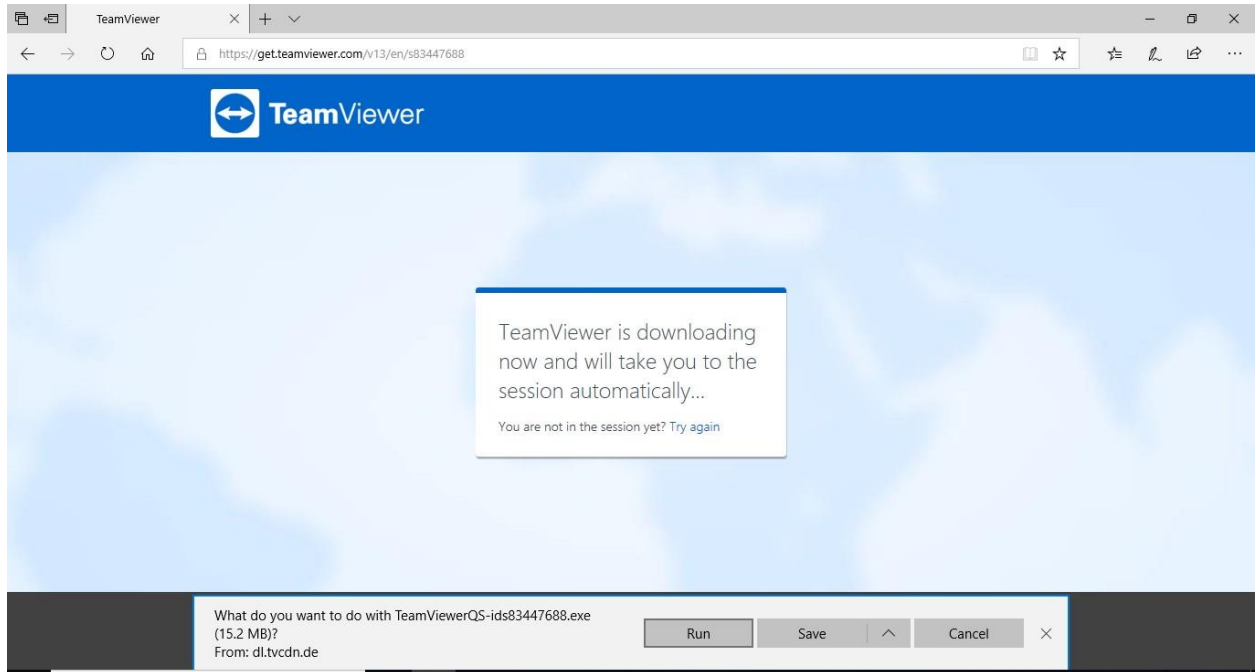
6. On Client Pc, Pop up for remote assistance.



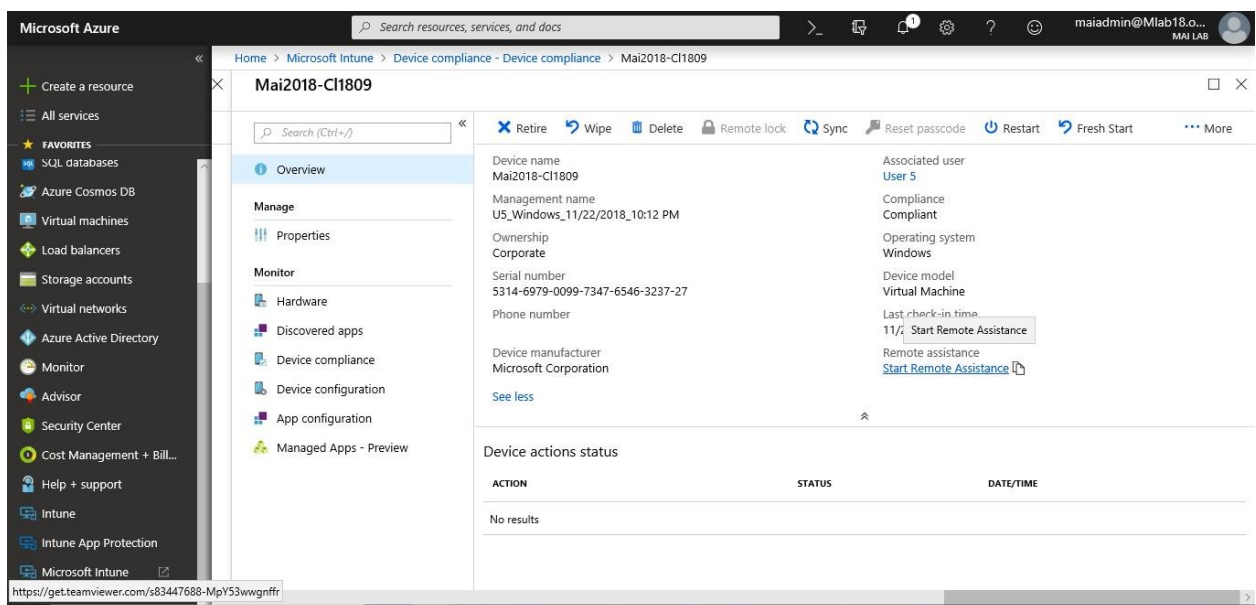
Microsoft Intune step by step on Azure portal

Note: The client should install company portal on his pc as popup for remote session appear on company portal.

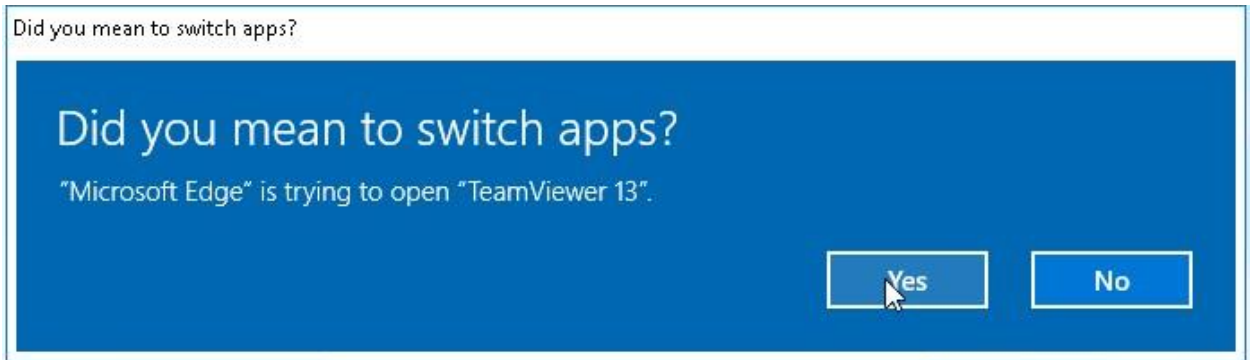
7. On Client pc, It's will open on Edge browser to run TeamViewer session, Click **Run**.



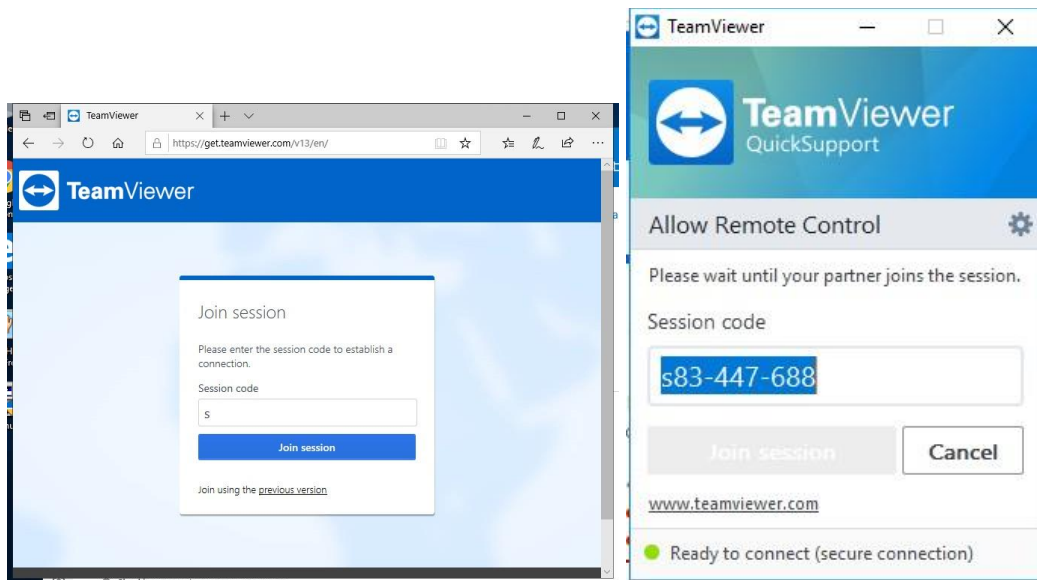
8. On Intune admin portal, you'll see some information about the device. click **start remote assistance** on administrator machine.



9. On admin machine, it will be pop up switch app. Click **Yes**.



10. On Client Pc, Click **Join**.

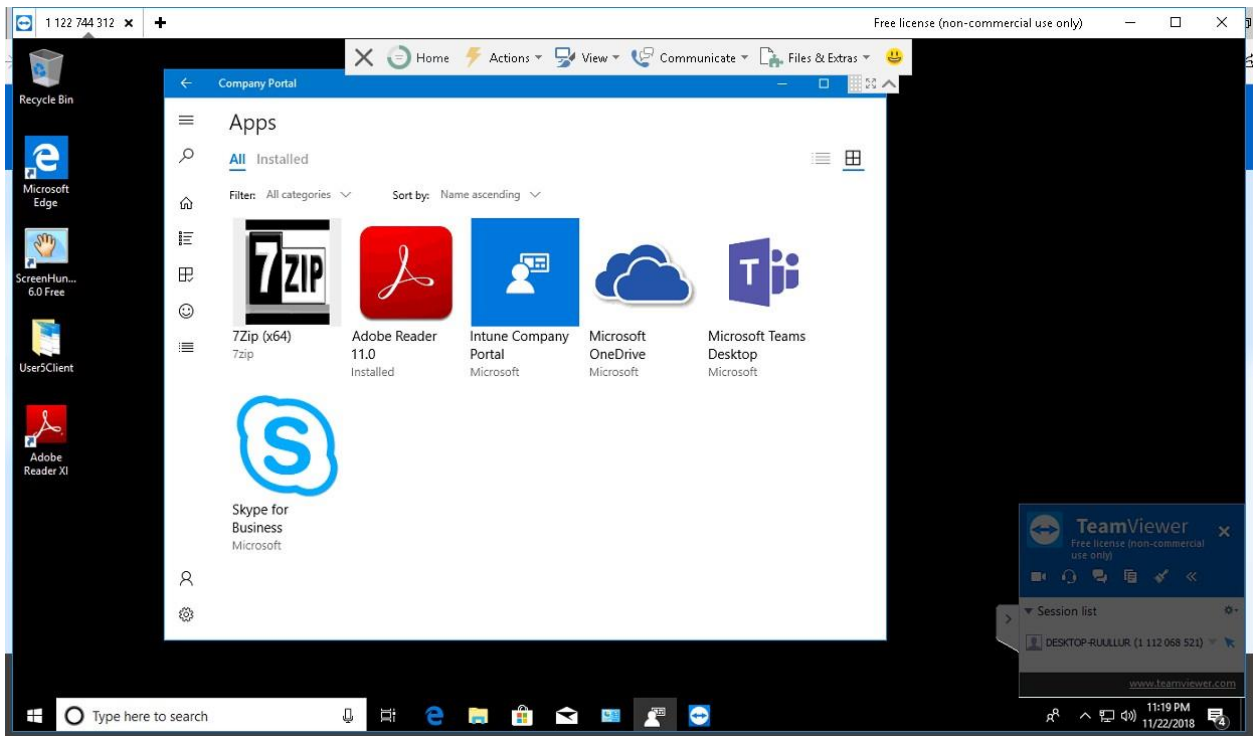


Note: End User don't need to have team viewer client because TeamViewer can open through Web browser Edge.

11. On Client Pc, Click **Allow** admin to control your client pc



12. Once end user allow control, Administrator will be able to control this pc remotely.



Protect Windows 10 MDM Using Microsoft Intune

Configure Windows Defender Antivirus

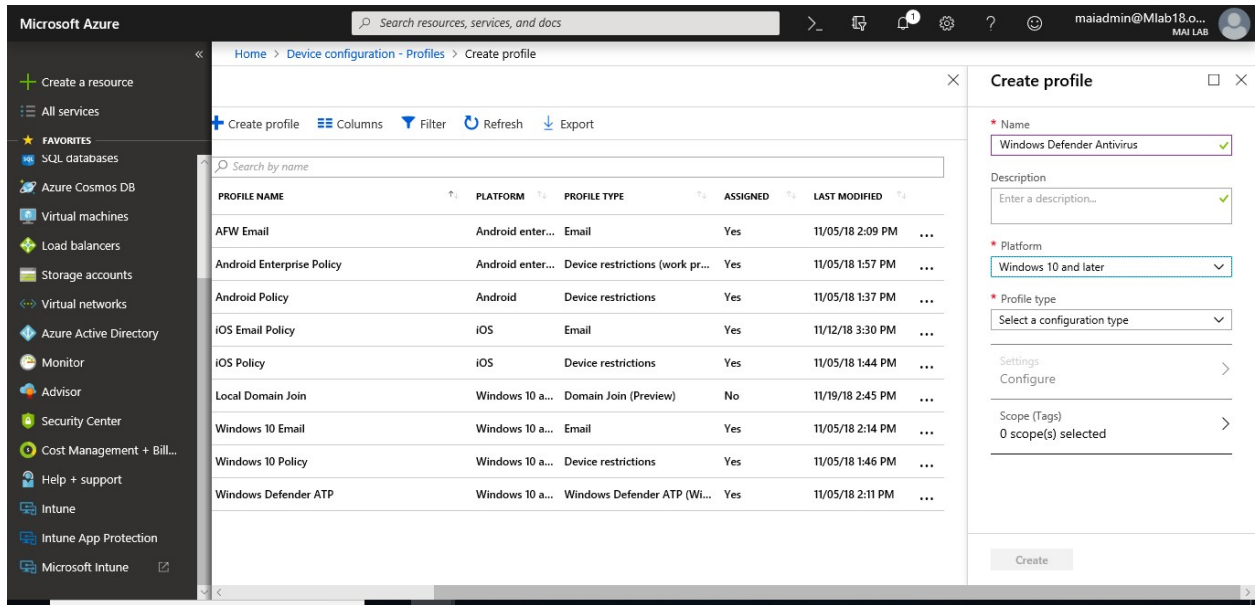
Endpoint protection lets you control different security features on your devices, including firewall, bit locker, allowing and blocking apps, Windows Defender and encryption, and more. You can configure these settings in Microsoft Intune using device profiles.

Note: In most cases, Windows 10 will disable Windows Defender Antivirus if it finds another antivirus product that is running and up-to-date. You must disable or uninstall third-party antivirus products before Windows Defender Antivirus will function. If you re-enable or install third-party antivirus products, then Windows 10 automatically disables Windows Defender Antivirus.

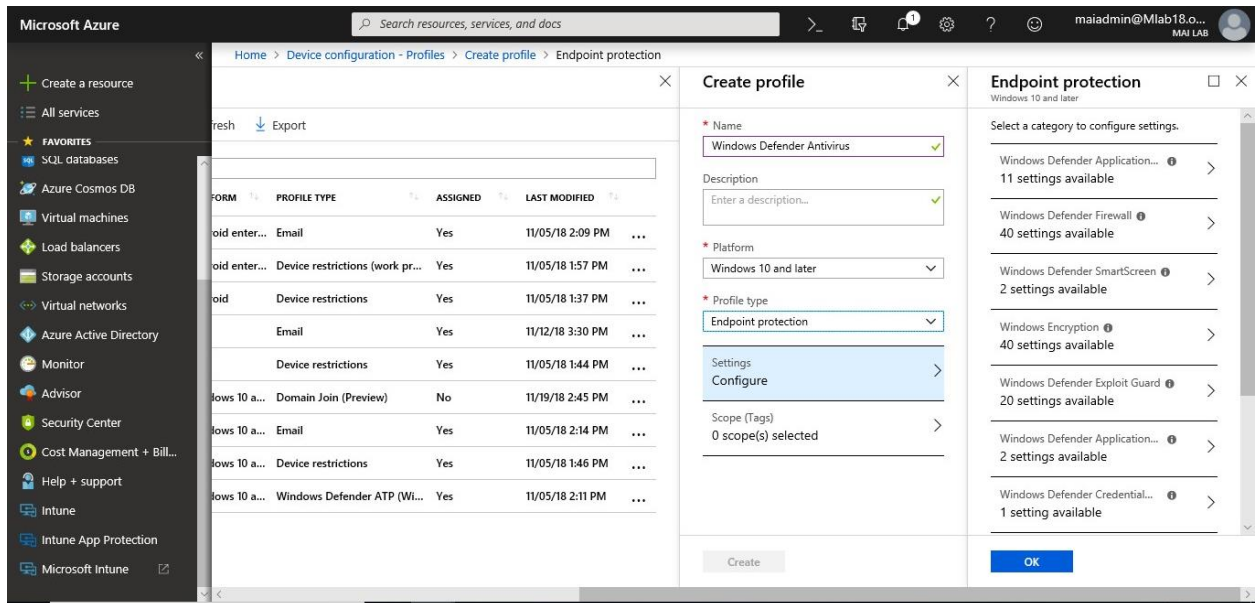
Create a device profile containing endpoint protection settings

1. Sign in to the [Azure portal](#).
2. Select **All services**, filter on **Intune**, and select **Microsoft Intune**.
3. Select **Device configuration > Profiles > Create profile**.
4. Enter a **Name** and **Description** for the endpoint protection profile.
5. From the **Platform** drop-down list, select the device platform to which you want to apply custom settings. Currently, you can choose one of the following platforms for device restriction settings:
 - **macOS**
 - **Windows 10 and later**

Microsoft Intune step by step on Azure portal



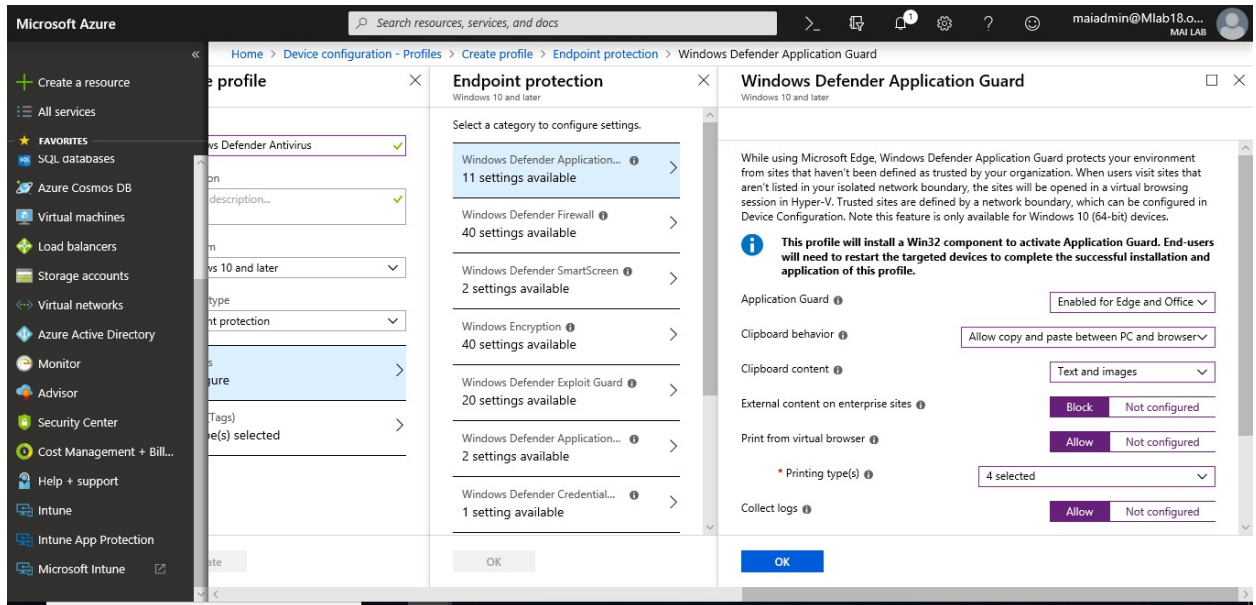
6. From the **Profile type** drop-down list, choose **Endpoint protection**.



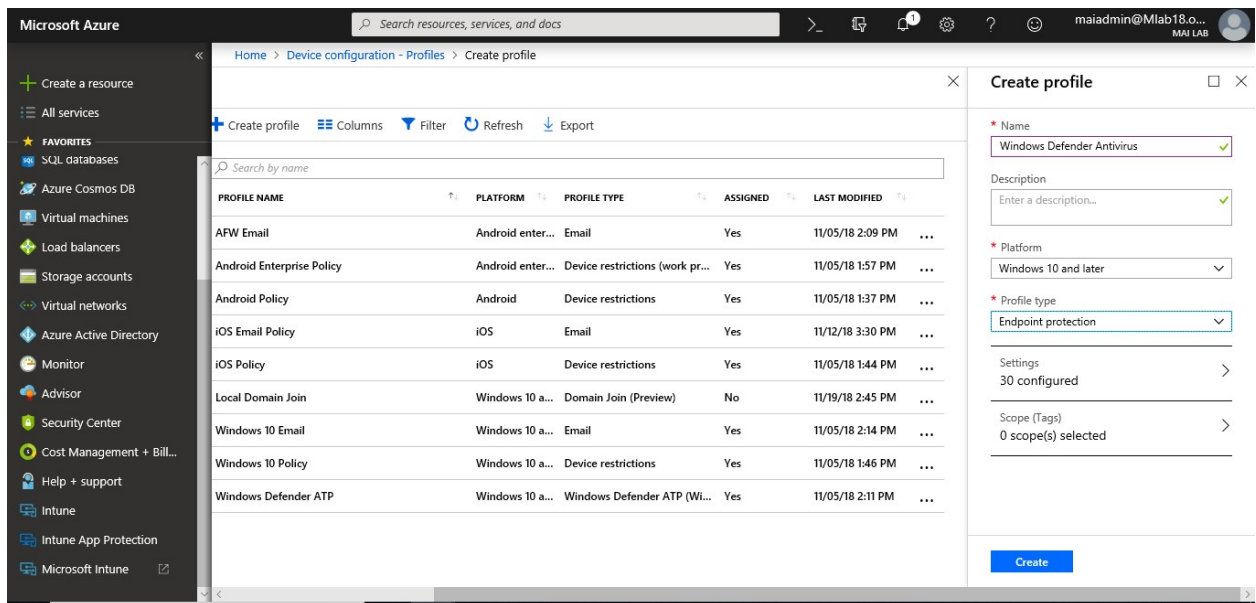
7. Depending on the platform you chose, the settings you can configure are different. Go to one of the following topics for detailed settings for each platform:

- o [macOS settings](#)
- o [Windows 10 settings](#)

Microsoft Intune step by step on Azure portal



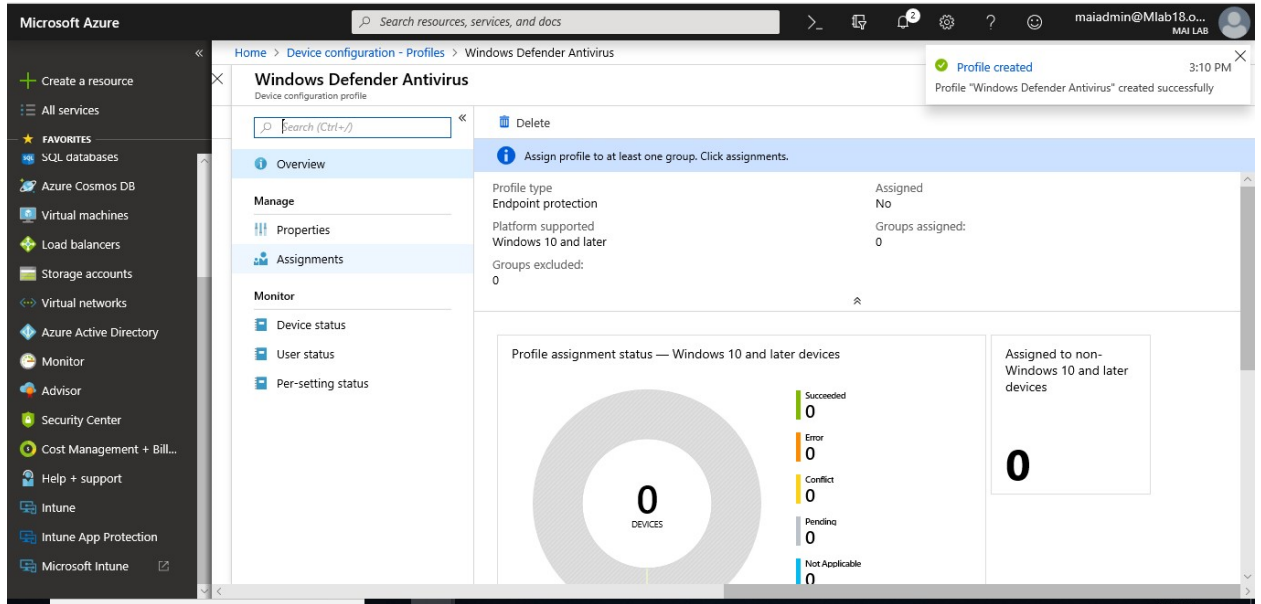
8. When you're done, go back to the **Create profile** page, and click **Create**.



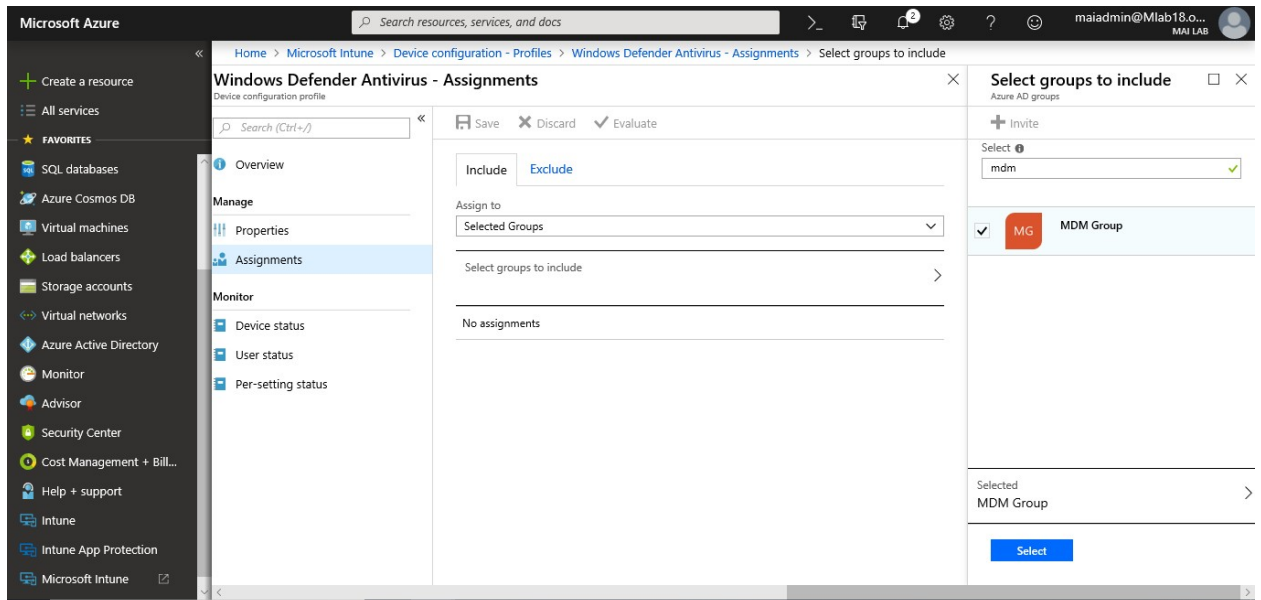
Assign a device profile

1. In the [Azure portal](#), select **All Services**, and search for **Microsoft Intune**.
2. In **Microsoft Intune**, select **Device configuration**, and select **Profiles**.
3. In the list of profiles, select the profile you want to assign, and then select **Assignments**.

Microsoft Intune step by step on Azure portal

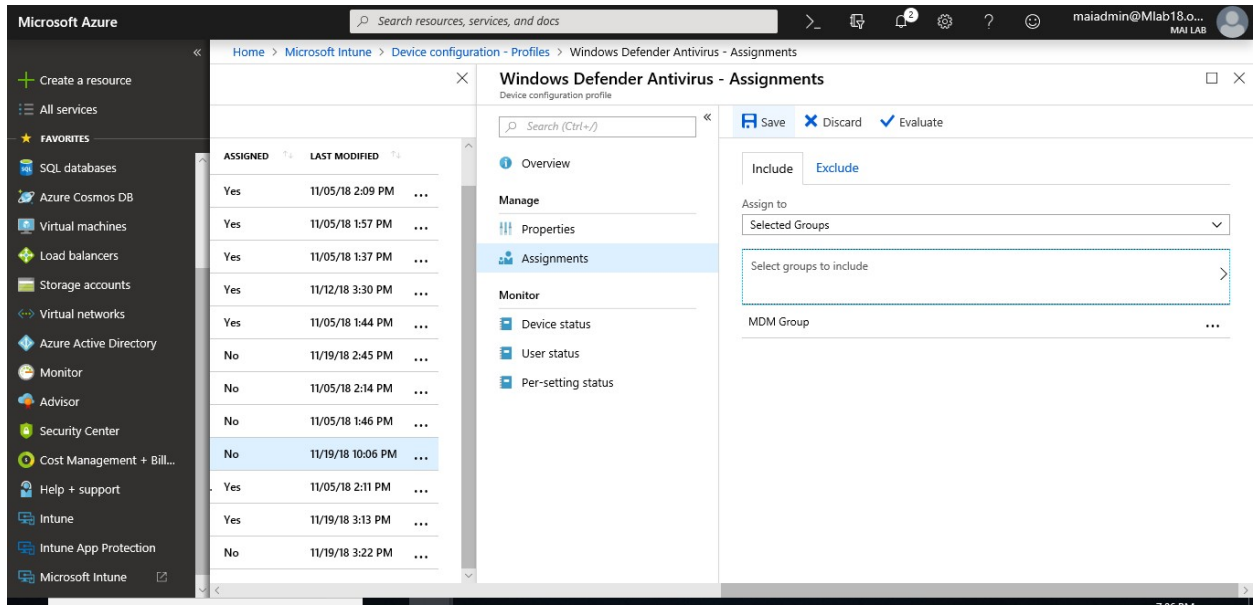


4. Choose to **Include** groups or **Exclude** groups, and then select groups.
5. When you select your groups, you're choosing an Azure AD group. To select multiple groups, hold down the **Ctrl** key.

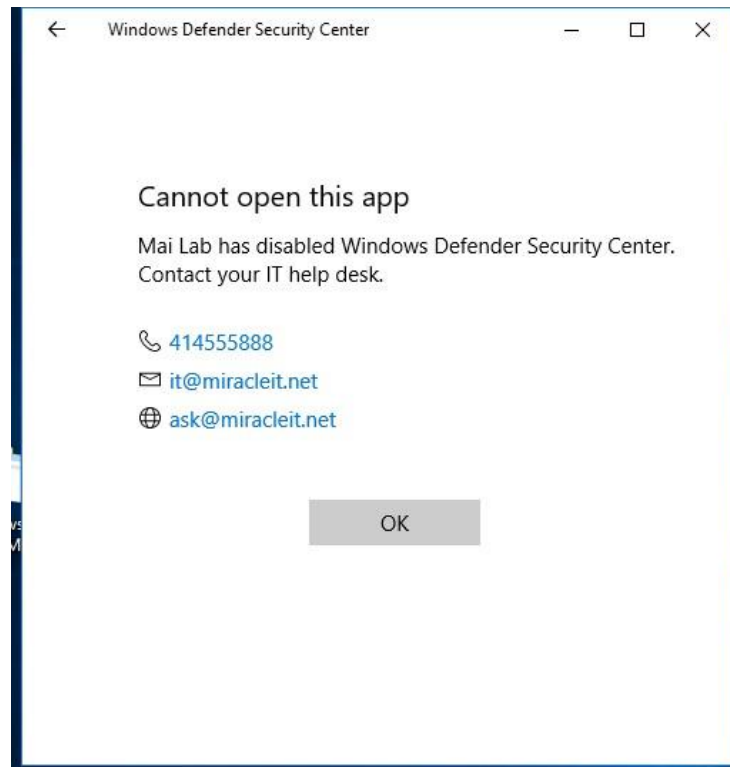


6. When you are done, select **Save**.

Microsoft Intune step by step on Azure portal



- Once policy sync, you will find windows defender will be manage by Intune on windows 10 Client.



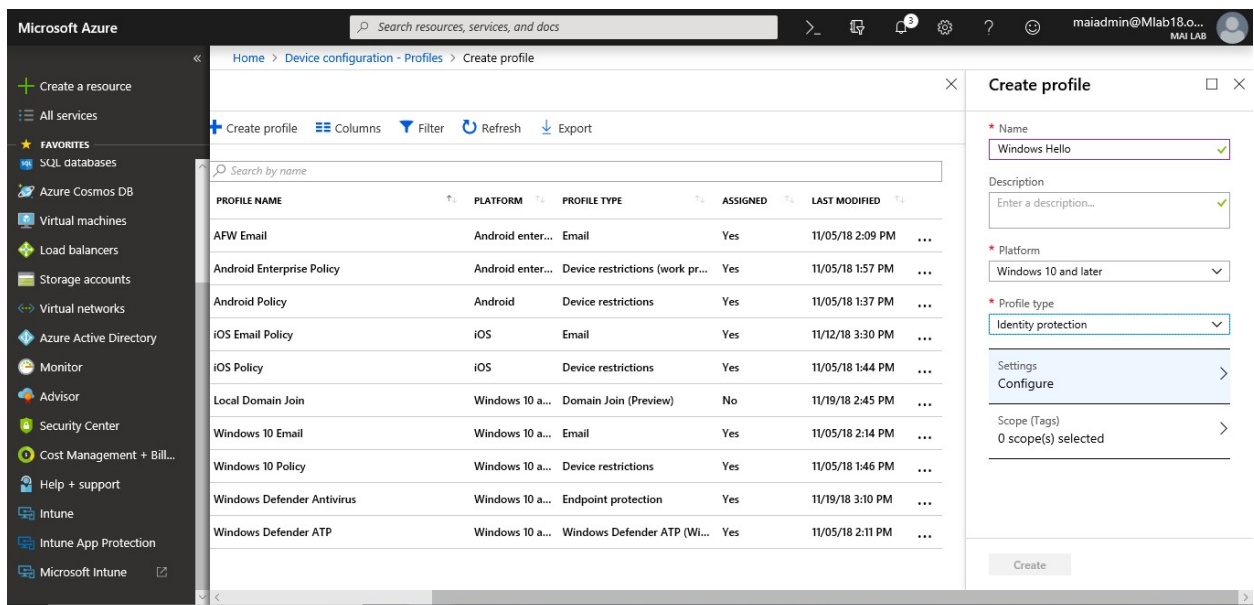
Configure Identity Protection settings in Microsoft Intune

Identity protection profiles control how Windows Hello for Business is provisioned and configured on managed Windows 10 devices. Create this profile to configure:

- Windows Hello for Business availability for devices and users.
- Device pin requirements.
- Gestures users can and can't use to sign in to their devices.

Create a device profile with identity protection settings

1. Sign in to the [Azure portal](#). Select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device configuration > Profiles > Create profile**.
3. Enter a **Name** and **Description** for the identity protection profile.
4. From the **Platform** drop-down list, select **Windows 10 and later**. Windows Hello for Business is only supported on devices running Windows 10 and later.
5. From the **Profile type** drop-down list, choose **Identity protection**.



6. On the Windows Hello for Business pane, choose from the following options for Configure Windows Hello for Business:
 - **Disabled.** If you don't want to use Windows Hello for Business, select this setting. All other settings on the screen are then unavailable.
 - **Enabled.** Select this setting if you want to configure Windows Hello for Business settings.
7. If you selected **Enabled** in the previous step, configure the required settings that are applied to targeted enrolled Windows 10 and Windows 10 Mobile devices and users.

Note: When assigning identity protection profiles to users only, the device context defaults to **Not configured**.

- **Minimum PIN length/Maximum PIN length.** Configures devices to use the minimum and maximum PIN lengths that you specify to help ensure secure sign-in. The default PIN length is six characters, but you can enforce a minimum length of four characters. The maximum PIN length is 127 characters.
- **Lowercase letters in PIN/Uppercase letters in PIN/Special characters in PIN.** You can enforce a stronger PIN by requiring the use of uppercase letters, lowercase letters, and special characters in the PIN. Choose from:
 - **Allowed.** Users can use the character type in their PIN, but it is not mandatory.
 - **Required.** Users must include at least one of the character types in their PIN. For example, it's common practice to require at least one uppercase letter and one special character.
 - **Not allowed** (default). Users must not use these character types in their PIN. (This behavior also occurs if the setting isn't configured.)
Special characters include: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~
- **PIN expiration (days).** It's a good practice to specify an expiration period for a PIN, after which users must change it. The default is 41 days.
- **Remember PIN history.** Restricts the reuse of previously used PINs. By default, the last 5 PINs cannot be reused.
- **Enable PIN recovery:** Allows the user to change their PIN by using the Windows Hello for Business PIN recovery service.
 - **Enable.** The cloud service encrypts a PIN recovery secret to store on the device. The user can change their PIN if needed.
 - **Not configured** (default). A PIN recovery secret is not created or stored. If the user's PIN is forgotten, the only way to get a new PIN is by deleting the existing PIN and creating a new one. The user will need to re-register with any services the old PIN provided access to.
- **Use a Trusted Platform Module (TPM).** A TPM chip provides an additional layer of data security. Choose one of the following values:
 - **Enable.** Only devices with an accessible TPM can provision Windows Hello for Business.
 - **Not configured.** All devices can provision Windows Hello for Business, even when there's no usable TPM. Devices will first try to use a TPM, but if one is unavailable, devices can use software encryption.
- **Allow biometric authentication.** Enables biometric authentication, such as facial recognition or fingerprint, as an alternative to a PIN for Windows Hello for Business. Users must still configure a work PIN in case biometric authentication fails. Choose from:
 - **Enable.** Windows Hello for Business allows biometric authentication.
 - **Not configured** (default). Windows Hello for Business prevents biometric authentication (for all account types).
- **Use enhanced anti-spoofing, when available.** Configures whether the anti-spoofing features of Windows Hello are used on devices that support it (for example, detecting a photograph of a face instead of a real face).
 - **Enable.** Windows requires all users to use anti-spoofing for facial features when that is supported.

Microsoft Intune step by step on Azure portal

- **Not configured** (default). Windows honors the anti-spoofing configurations on the device.
- **Certificate for on-premise resources.**
 - **Enable.** Allows Windows Hello for Business to use certificates to authenticate to resources on-premises.
 - **Not configured** (default). Prevents Windows Hello for Business from using certificates to authenticate to resources on-premises.

9. Click **OK** to save your configuration.

The screenshot shows the 'Create profile' dialog in the Microsoft Azure portal. The dialog is titled 'Create profile' and is for a 'Windows Hello for Business' profile. The 'Name' field is 'Windows Hello'. The 'Platform' is 'Windows 10 and later'. The 'Profile type' is 'Identity protection'. The 'Settings' are 'Configure'. The 'Scope (Tags)' is '0 scope(s) selected'. The 'Certificate for on-premise resources' option is set to 'Not configured'. The 'OK' button is visible at the bottom right.

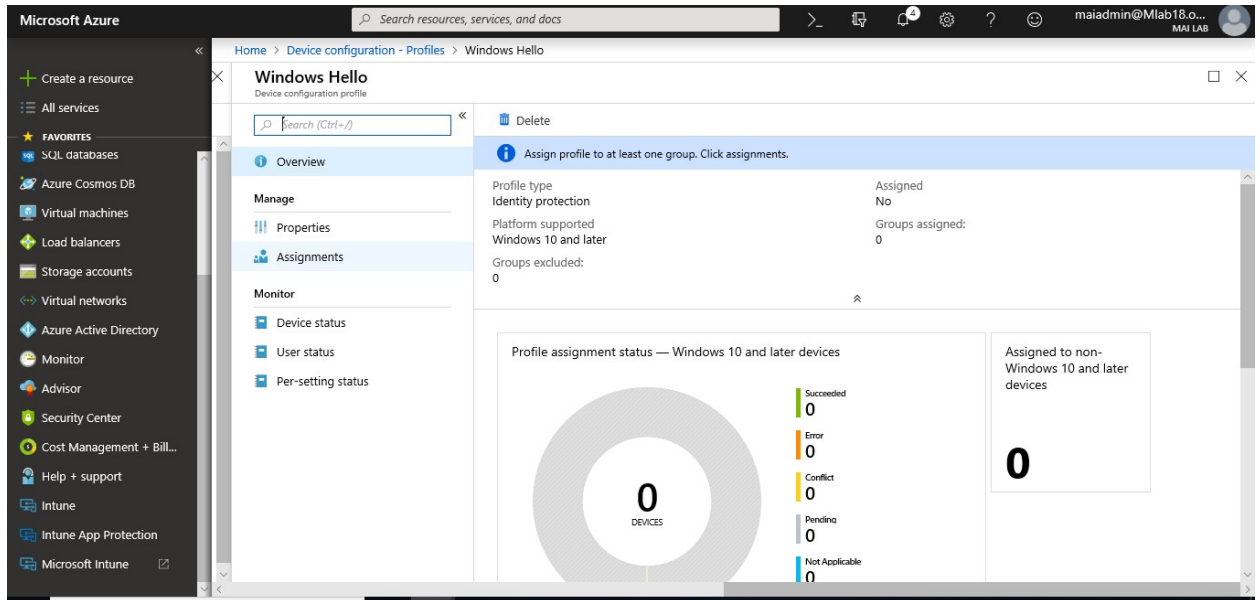
10. Click **Create** to create your profile.

The screenshot shows the 'Create profile' dialog in the Microsoft Azure portal. The dialog is titled 'Create profile' and is for a 'Windows Hello for Business' profile. The 'Name' field is 'Windows Hello'. The 'Platform' is 'Windows 10 and later'. The 'Profile type' is 'Identity protection'. The 'Settings' are '5 configured'. The 'Scope (Tags)' is '0 scope(s) selected'. The 'Create' button is visible at the bottom right.

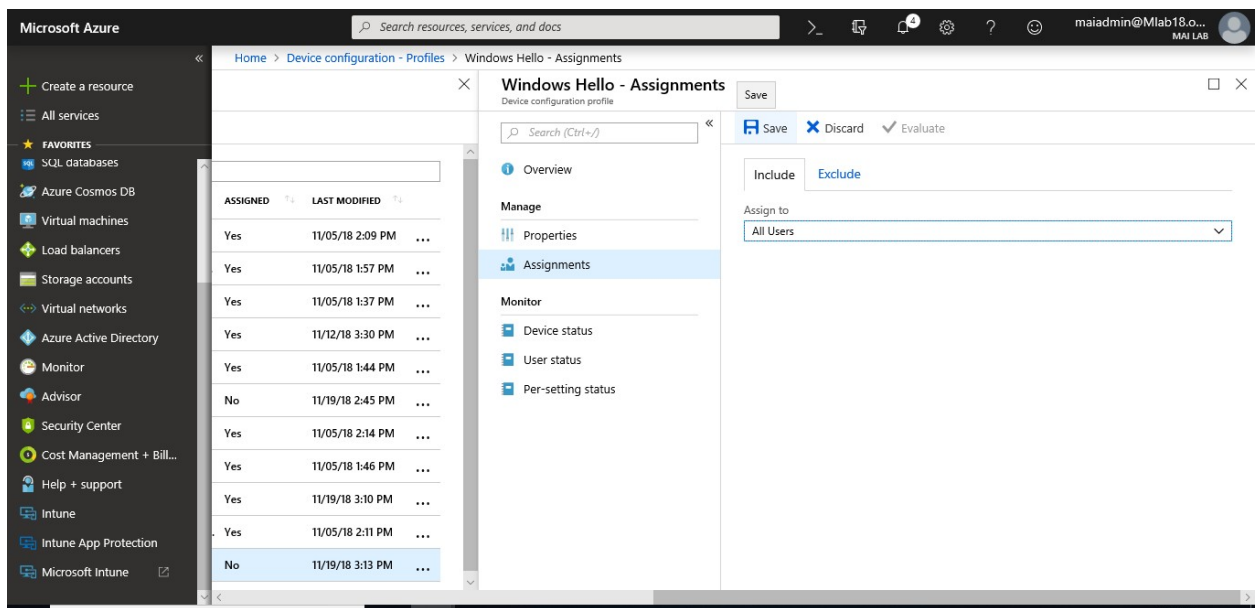
PROFILE NAME	PLATFORM	PROFILE TYPE	ASSIGNED	LAST MODIFIED
APFW Email	Android enter...	Email	Yes	11/05/18 2:09 PM
Android Enterprise Policy	Android enter...	Device restrictions (work pr...	Yes	11/05/18 1:57 PM
Android Policy	Android	Device restrictions	Yes	11/05/18 1:37 PM
iOS Email Policy	iOS	Email	Yes	11/12/18 3:30 PM
iOS Policy	iOS	Device restrictions	Yes	11/05/18 1:44 PM
Local Domain Join	Windows 10 a...	Domain Join (Preview)	No	11/19/18 2:45 PM
Windows 10 Email	Windows 10 a...	Email	Yes	11/05/18 2:14 PM
Windows 10 Policy	Windows 10 a...	Device restrictions	Yes	11/05/18 1:46 PM
Windows Defender Antivirus	Windows 10 a...	Endpoint protection	Yes	11/19/18 3:10 PM
Windows Defender ATP	Windows 10 a...	Windows Defender ATP (Wi...	Yes	11/05/18 2:11 PM

Assign a device profile

1. In the [Azure portal](#), select **All Services**, and search for **Microsoft Intune**.
2. In **Microsoft Intune**, select **Device configuration**, and select **Profiles**.
3. In the list of profiles, select the profile you want to assign, and then select **Assignments**.



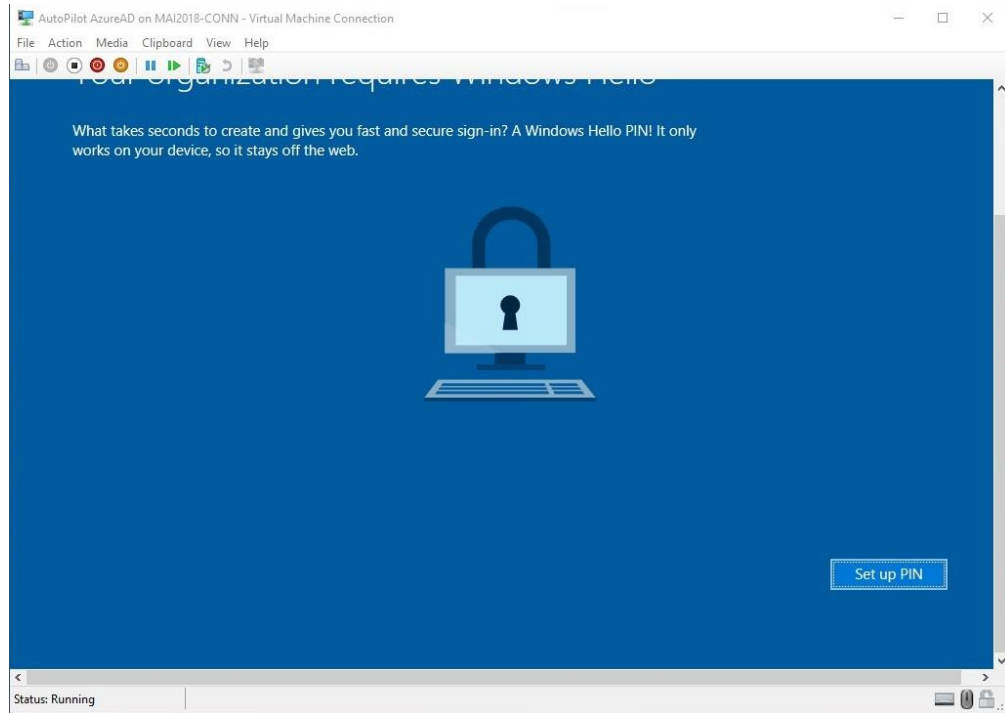
4. Choose to **Include** groups or **Exclude** groups, and then select groups.
5. When you select your groups, you're choosing an Azure AD group. To select multiple groups, hold down the **Ctrl** key.



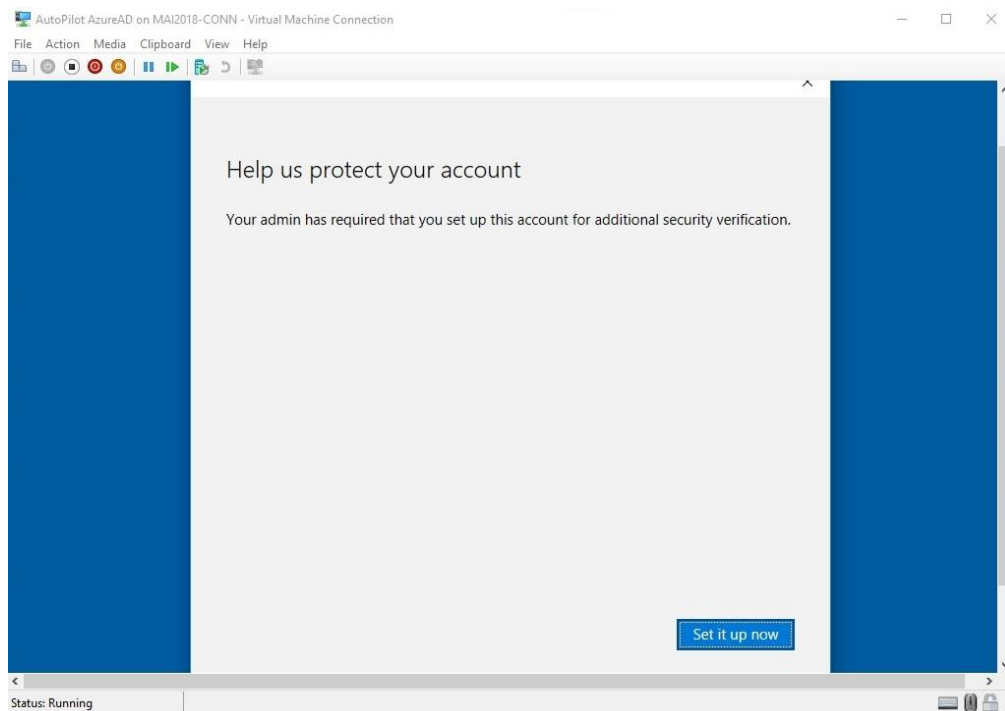
6. When you are done, select **Save**.

Push Policy on Client & Monitor it

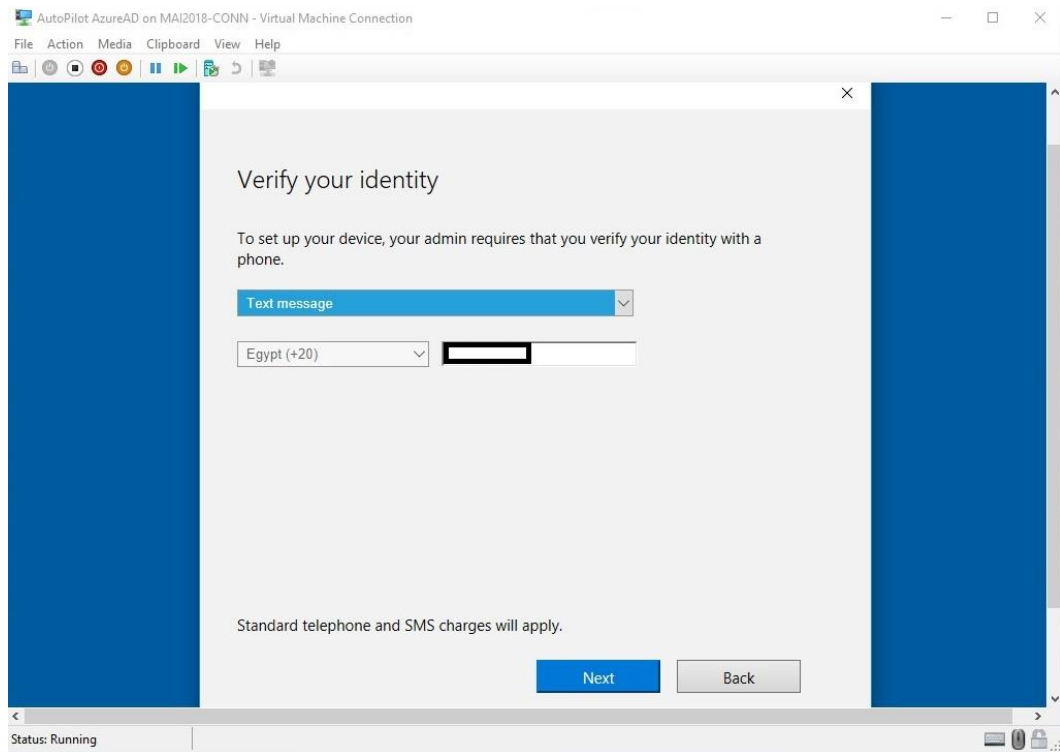
1. On Client PC, you should find PC ask you to enter PIN code for sign in instead of password. Click on **Setup PIN**.



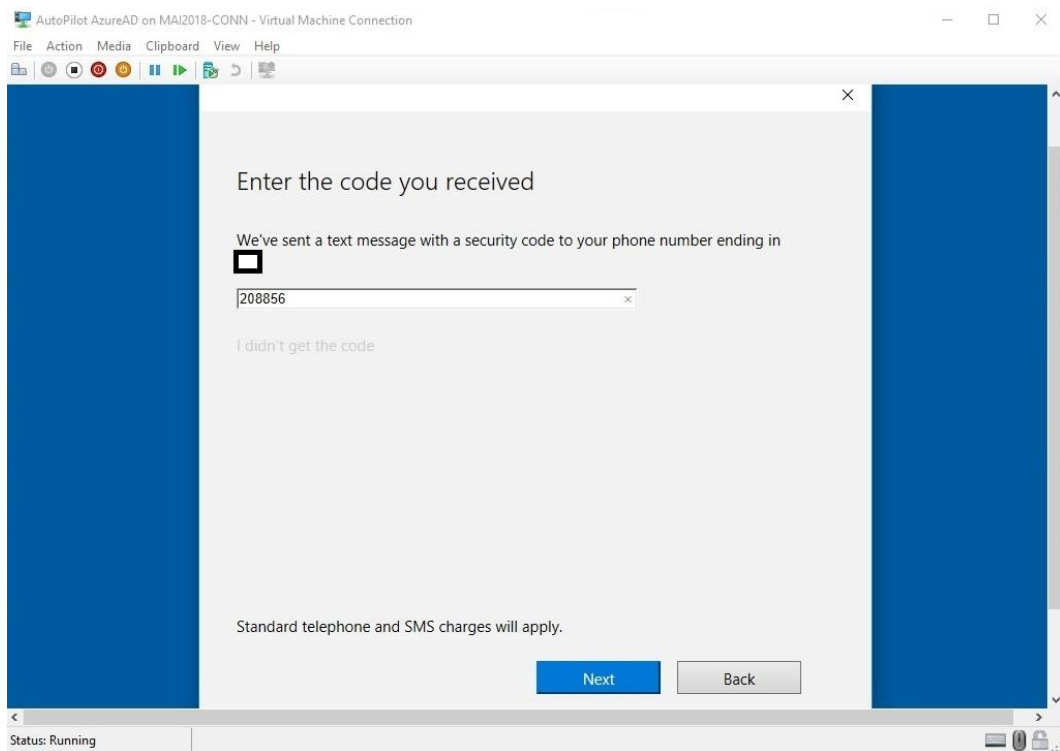
2. On **Help us protect your account** page, Click **Set it up now**.



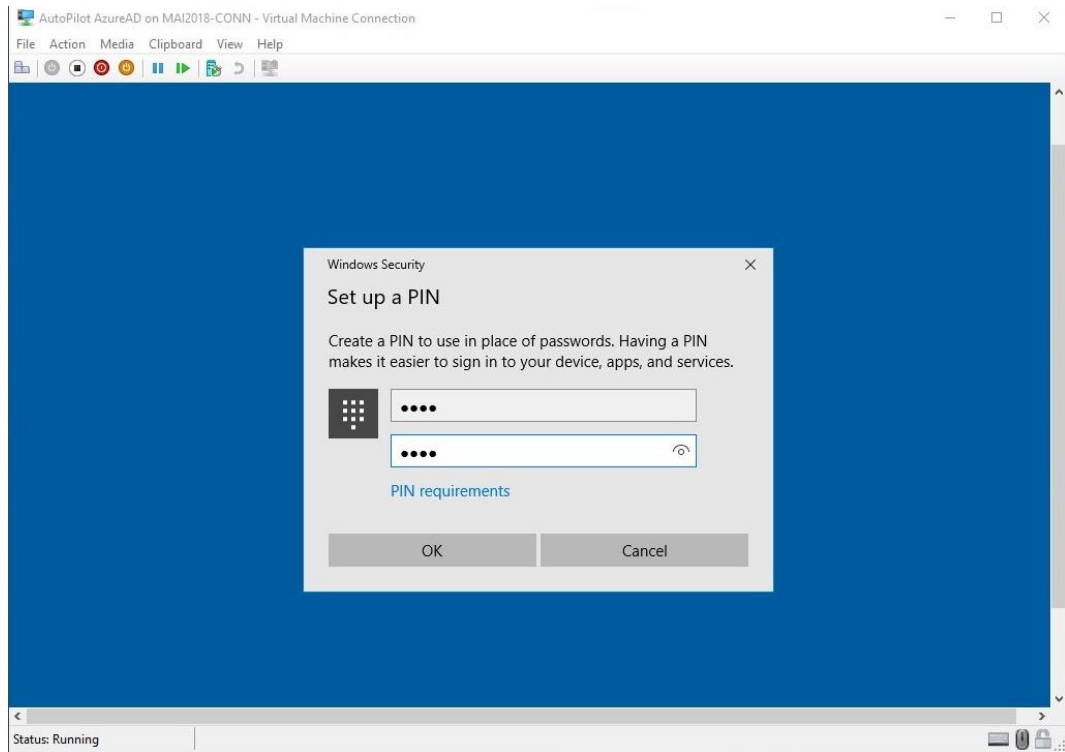
3. On **Verify your identity** Page, enter your mobile no. and method of verification text, or call, or use mobile app.



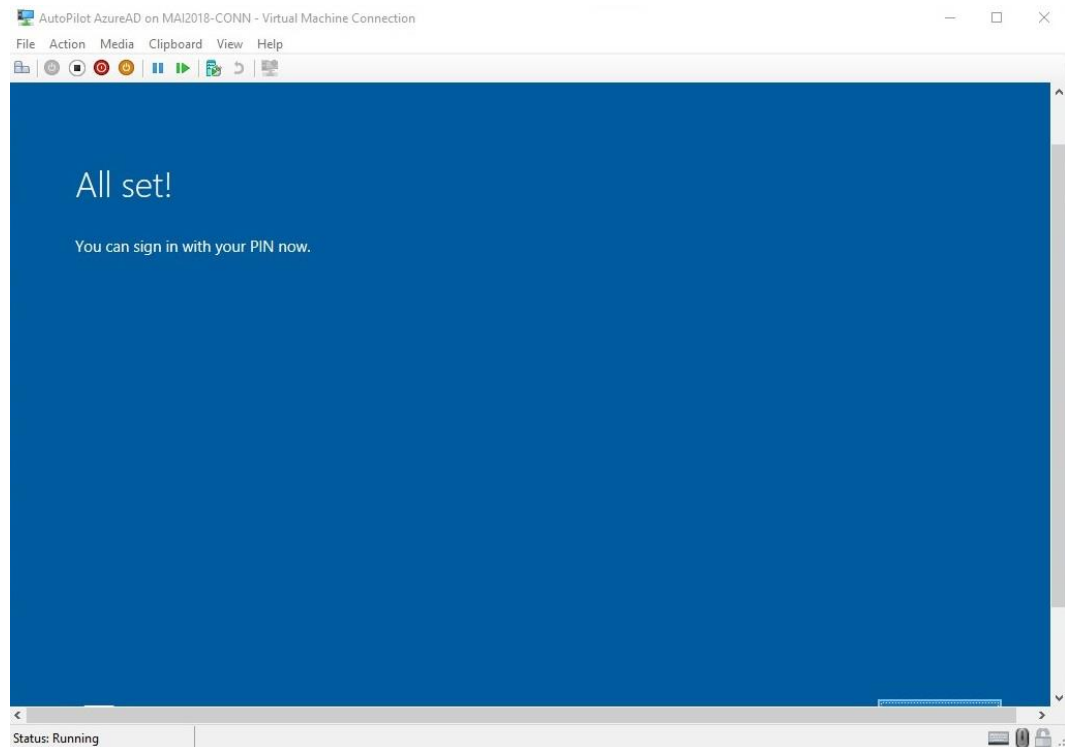
4. On **Enter the code you received** page and click **Next**.



5. On **Setup PIN** Code, enter new PIN code that you want but at least contain 4 characters as you configure on policy.

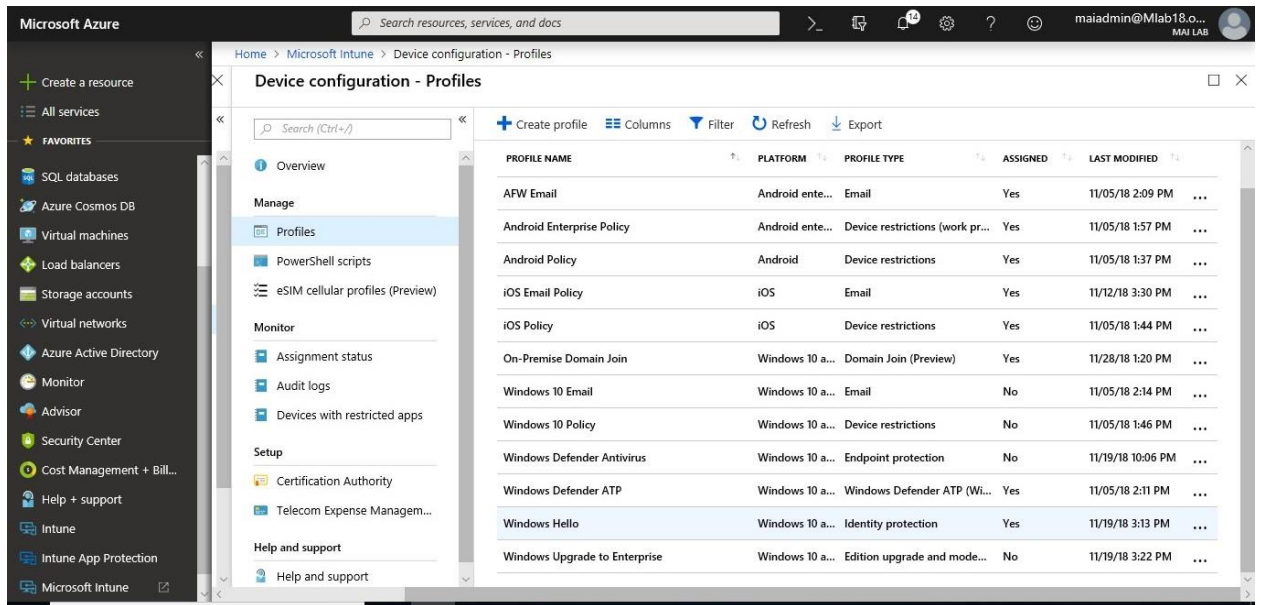


6. Now PIN code is setup.

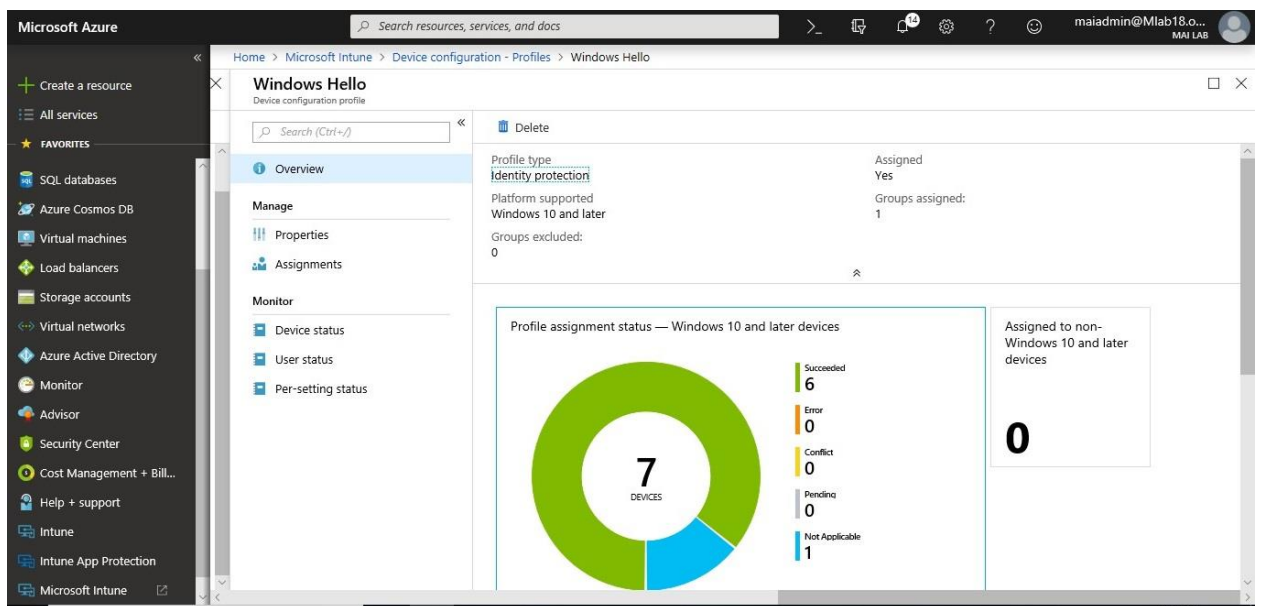


Microsoft Intune step by step on Azure portal

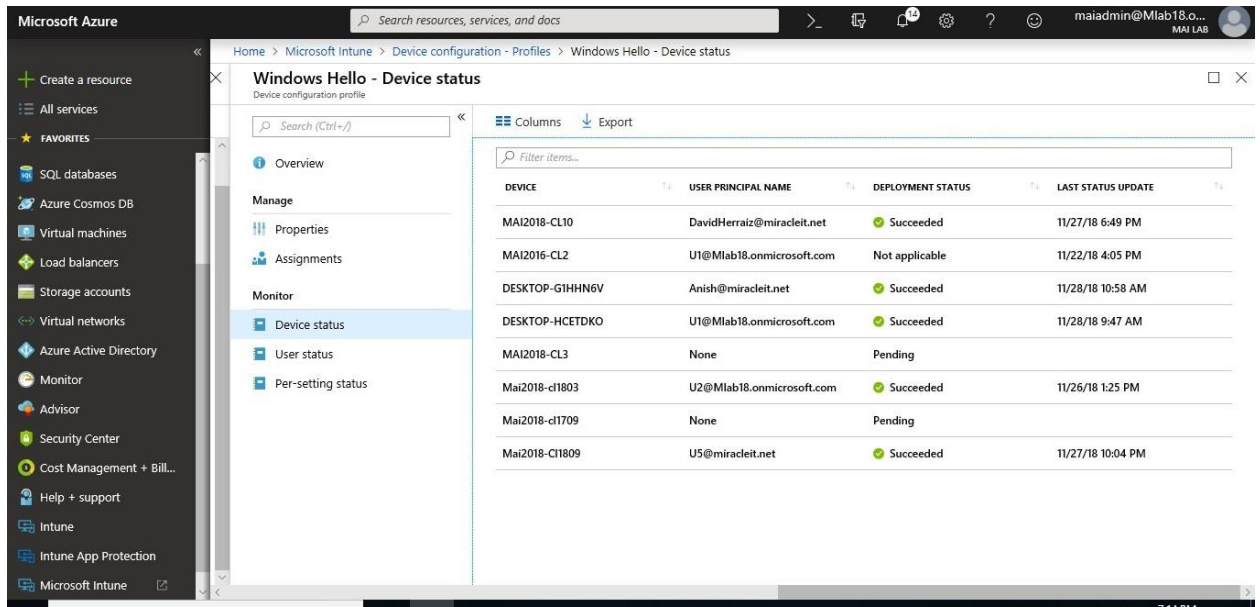
- On Intune admin Portal, Click on **Configuration Policies** > **Profile** > Click profile for identity protection that you created.



- On **Overview** Page, you should see all profile successfully pushed.



- Under **Monitor**, Click **Device Status**. You will see all devices & users who policy pushed successfully on their devices.



MDM Security Baselines – Windows 10

MDM Security baseline apply on Windows 10 MDM to put some restriction policy to secure device like block direct memory access & enable device guard. With Windows 10, version 1809, Microsoft is also releasing a Microsoft MDM security baseline that functions like the Microsoft GP-based security baseline.

Note: This feature is in preview, so it's recommended to apply any feature on preview on production until it release. You can configure it from Sign in to the [Azure portal](#) >Select **All services**, filter on **Security**, and select **Security Baselines**. OR On some tenants, you can find security Baselines on [Microsoft Intune console](#).

The MDM security baseline includes policies that cover the following areas:

- Microsoft inbox security technology (not deprecated) such as Bitlocker, Smartscreen, and DeviceGuard (virtual-based security), ExploitGuard, Defender, and Firewall
- Restricting remote access to devices
- Setting credential requirements for passwords and PINs
- Restricting use of legacy technology
- Legacy technology policies that offer alternative solutions with modern technology

Note: For devices that are fully managed in the cloud, you need to apply only the MDM security baseline. For devices that are Hybrid managed by MDM and domain joined, you need to apply the MDM security baseline via MDM and add the GPO policies included in the GPO companion list.

Retire Devices and Remove Data

When a device needs to be removed from Intune management (for example, a user leaves organization and give it to new hire), it's likely that you'll want to remove data from that device. Intune provides a range of methods to make sure your company data stays secure.

By using the **Retire** or **Wipe** actions, you can remove devices from Intune that are no longer needed, being repurposed, or missing. Users can also issue a remote command from the Intune Company Portal to personally owned devices that are enrolled in Intune.

Note: Before you remove a user from Azure Active Directory (Azure AD), use the **Wipe** or **Retire** actions for all devices that are associated with that user. If you remove users that have managed devices from Azure AD, Intune can no longer wipe or retire those devices.

Wipe

The **Wipe** action restores a device to its factory default settings. The user data is kept if you choose the **Retain enrollment state and user account** checkbox. Otherwise, the drive is securely erased.

Wipe action	Retain enrollment state and user account	Removed from Intune management	Description
Wipe	Not checked	Yes	Wipes all user accounts, data, MDM policies, and settings. Resets the operating system to its default state and settings.
Wipe	Checked	No	Wipes all MDM Policies. Keeps user accounts and data. Resets user settings back to default. Resets the operating system to its default state and settings.

The **Retain enrollment state and user account** option is **only available for Windows 10 version 1709 or later**.

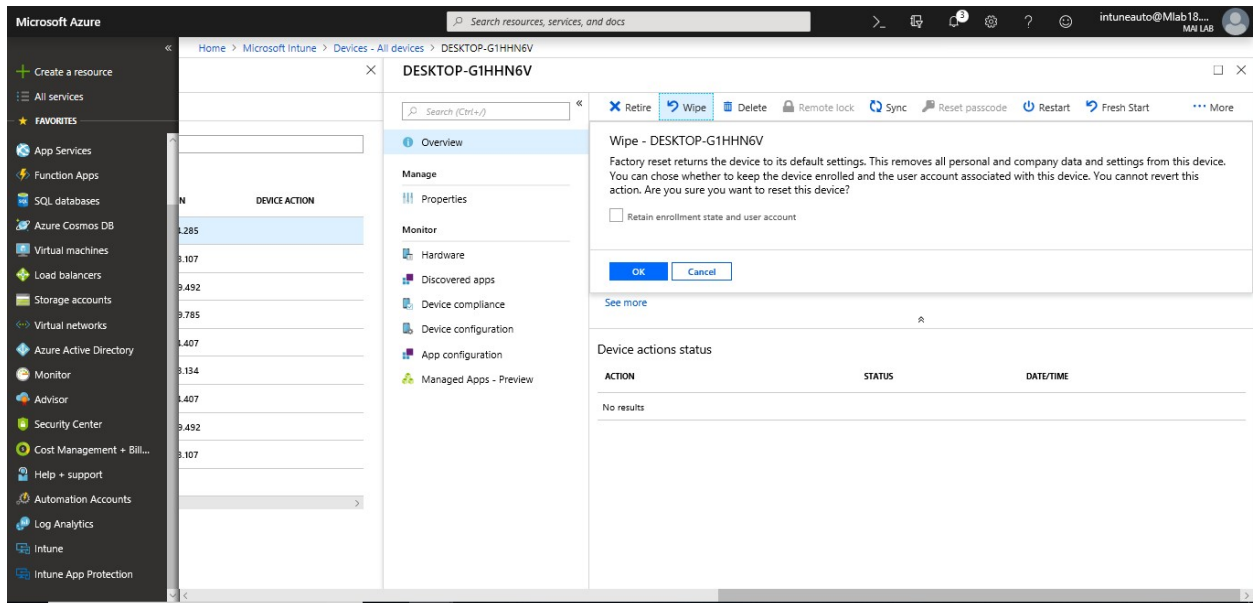
MDM policies will be reapplied the next time the device connects to Intune.

A wipe is useful for resetting a device before you give the device to a new user, or when the device has been lost or stolen. Be careful about selecting **Wipe**. Data on the device cannot be recovered.

To wipe device, you need to follow below steps:

1. Sign in to the [Azure portal](#). Select **All services**, filter on **Intune**, and select **Microsoft Intune**. Select **Devices > All devices**.
2. Select the name of the device that you want to wipe.
3. In the pane that shows the device name, select **Wipe**.
4. For Windows 10 version 1709 or later, you also have the **Retain enrollment state and user account** option.

Retained during a wipe	Not retained
User accounts associated with the device	User files
Machine state (domain join, Azure AD-joined)	User-installed apps (store and Win32 apps)
Mobile device management (MDM) enrollment	Non-default device settings
OEM-installed apps (store and Win32 apps)	
User profile	
User data outside of the user profile	
User autologon	



5. To confirm the wipe, select **Yes**.

If the device is on and connected, the **Wipe** action propagates across all device types in less than 15 minutes.

Retire

The **Retire** action removes managed app data (where applicable), settings, and email profiles that were assigned by using Intune. The device is removed from Intune management. This happens the next time the device checks in and receives the remote **Retire** action.

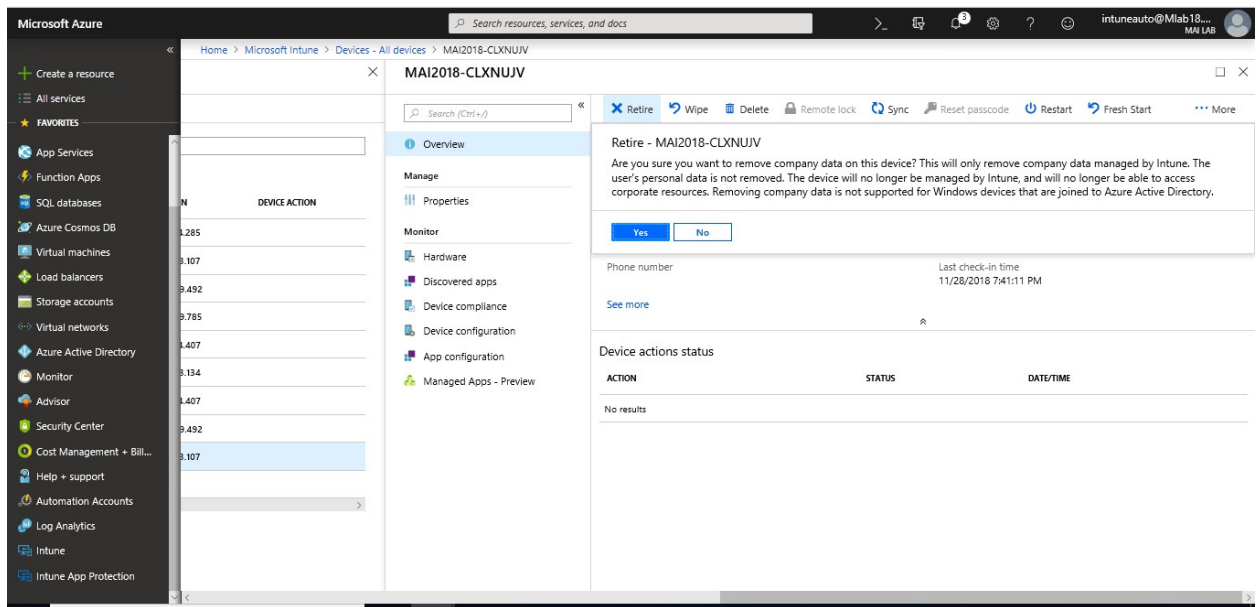
Retire leaves the user's personal data on the device.

The following tables describe what data is removed, and the effect of the **Retire** action on data that remains on the device after company data is removed.

Data type	Windows 10
Company apps and associated data installed by Intune	Apps are uninstalled. Sideloaded keys are removed. For Windows 10 version 1703 (Creators Update) and later, Office 365 ProPlus apps aren't removed.
Settings	Configurations that were set by Intune policy are no longer enforced. Users can change the settings.
Wi-Fi and VPN profile settings	Removed.
Certificate profile settings	Certificates are removed and revoked.
Email	Removes email that's EFS-enabled. This includes emails and attachments in the Mail app for Windows. Removes mail accounts that were provisioned by Intune.
Azure AD un join	Not applicable. On Windows 10, you can't retire Azure AD-joined devices.

To retire device, you need to follow below steps:

1. Sign in to the [Intune in the Azure portal](#). In the **Devices** pane, select **All devices**.
2. Select the name of the device that you want to retire.
3. In the pane that shows the device name, select **Retire**. To confirm, select **Yes**.



If the device is on and connected, the **Retire** action propagates across all device types in less than 15 minutes.

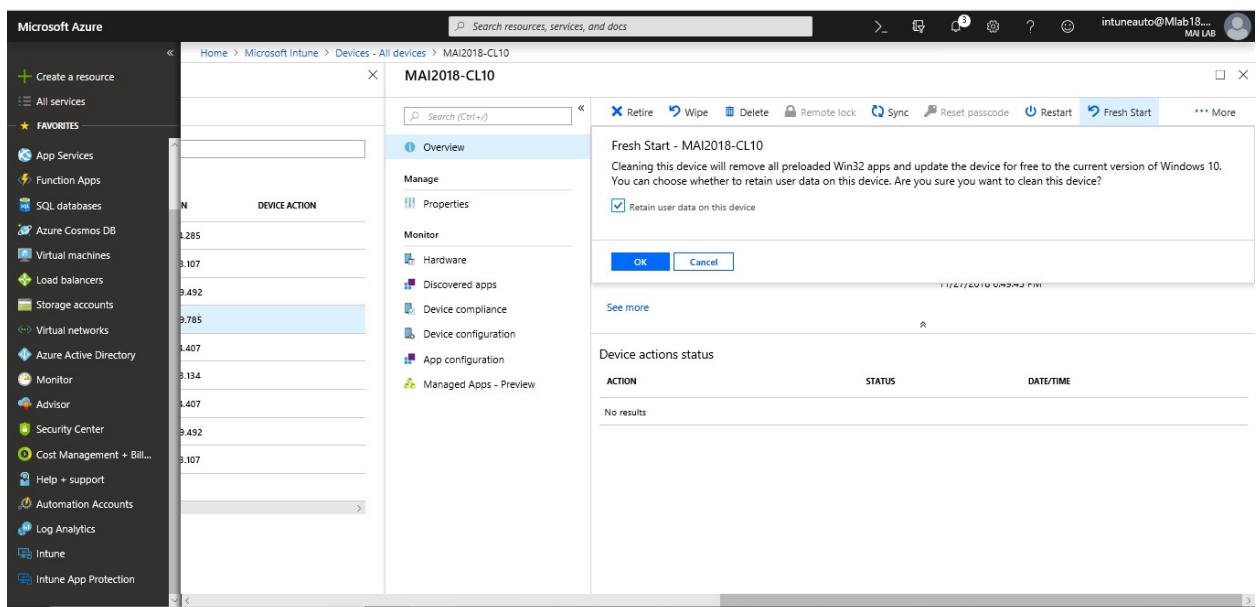
Fresh Start

The **Fresh Start** device action removes any apps that are installed on a **PC running Windows 10, version 1703 or later**. Fresh Start helps remove pre-installed (OEM) apps that are typically installed with a new PC.

1. Sign in to the [Azure portal](#) and go to > **Microsoft Intune** > **Devices** > **All devices**.
2. From the list of devices, you manage, choose a Windows 10 desktop device.
3. Click **Fresh Start**.
4. Select **Retain user data on this device** to:
 - Keep the device Azure AD joined
 - Keep the device enrolled in mobile device management
 - Keep the contents of the device user's Home folder, and remove apps and settings

Note: If you do not retain user data, the device will be restored to its out-of-box state. It will be unenrolled from Azure AD and mobile device management.

5. Click **Yes** to confirm.



6. To see the status of this action, go back to **Devices** and click **Device actions**.

Autopilot Reset

Windows Autopilot Reset removes personal files, apps, and settings and reapplies a device's original settings, maintaining its identity connection to Azure AD and its management connection to Intune so that the device is once again ready for use. Windows Autopilot Reset takes the device back to a business-ready state, allowing the next user to sign in and get productive quickly and simply.

The Windows Autopilot Reset process automatically retains information from the existing device:

- Set the region, language, and keyboard to the originally-configured values.
- Wi-Fi connection details.

Microsoft Intune step by step on Azure portal

- Provisioning packages previously applied to the device, as well as a provisioning package present on a USB drive when the reset process is initiated.
- Azure Active Directory device membership and MDM enrollment information.

Windows Autopilot Reset will block the user from accessing the desktop until this information is restored, including re-applying any provisioning packages. For devices enrolled in an MDM service, Windows Autopilot Reset will also block until an MDM sync is completed.

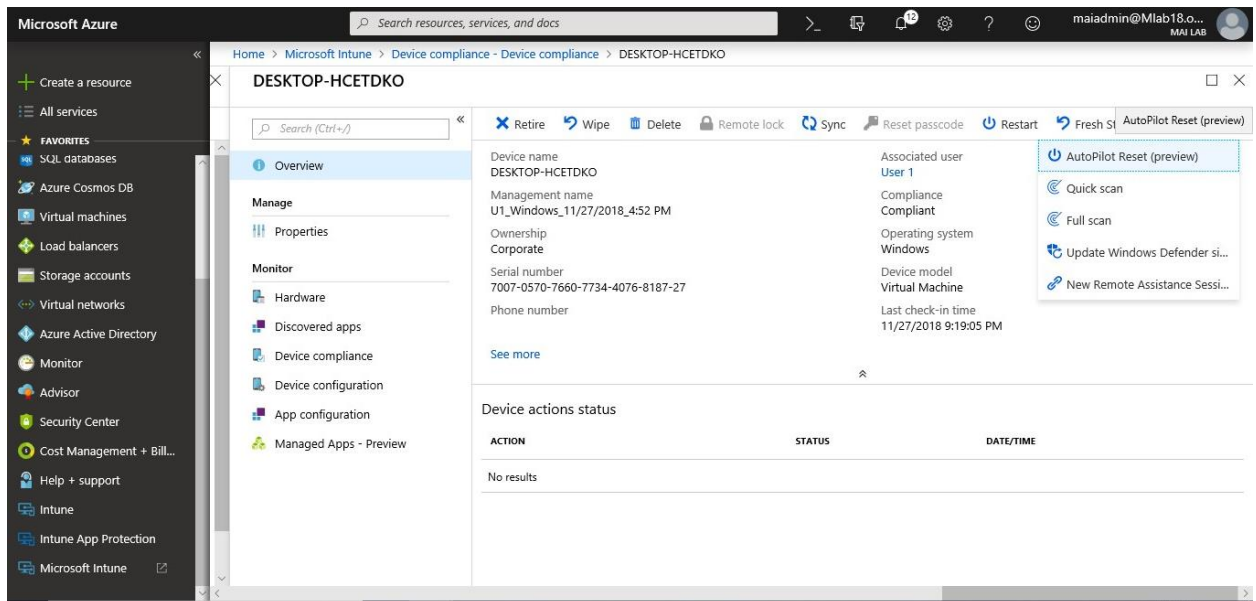
Windows Autopilot Reset supports two scenarios:

- **Local reset**, initiated by IT personnel or other administrators from the organization.
- **Remote reset**, initiated remotely by IT personnel via an MDM service such as Microsoft Intune. (Remote Autopilot reset requires Windows 10 Insider Preview Build 17672 or later).

Remote Windows Autopilot Reset

To trigger a remote Windows Autopilot Reset via Intune, follow these steps:

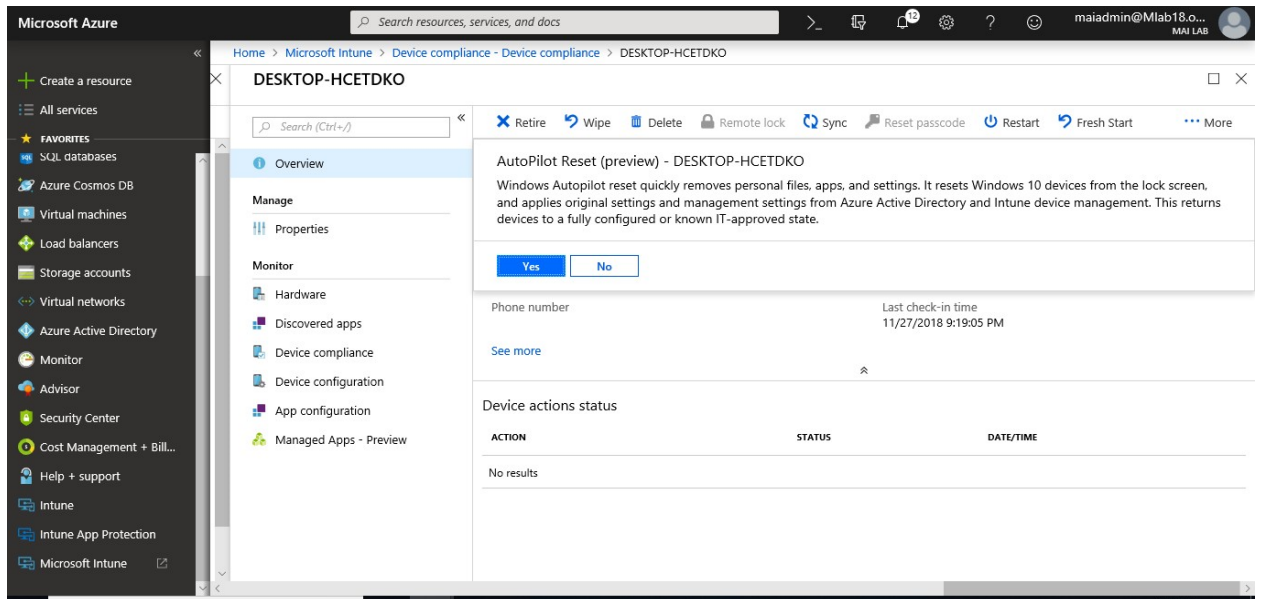
1. Sign in to the [Intune in the Azure portal](#). Navigate to **Devices** tab in the Intune console.
2. In the **All devices** view, select the targeted reset devices and then click **More** to view device actions.
3. Select **Autopilot Reset** to kick-off the reset task.



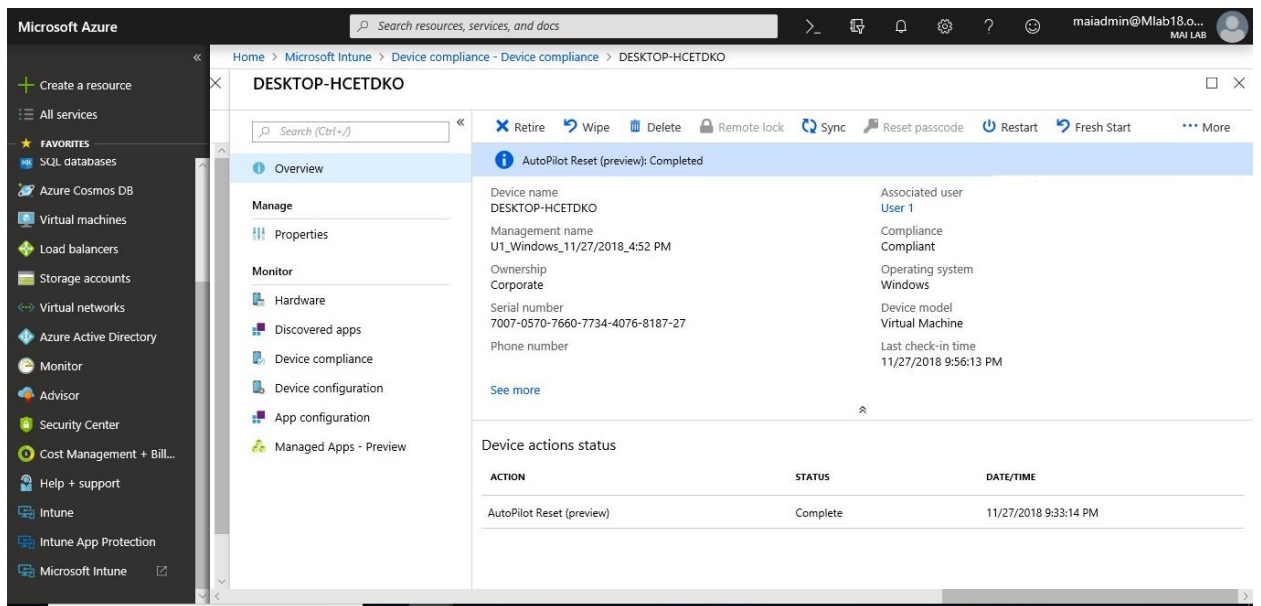
Note: The Autopilot Reset option will not be enabled in Microsoft Intune for devices not running Windows 10 build 17672 or higher.

4. Click **Yes** to confirm.

Microsoft Intune step by step on Azure portal



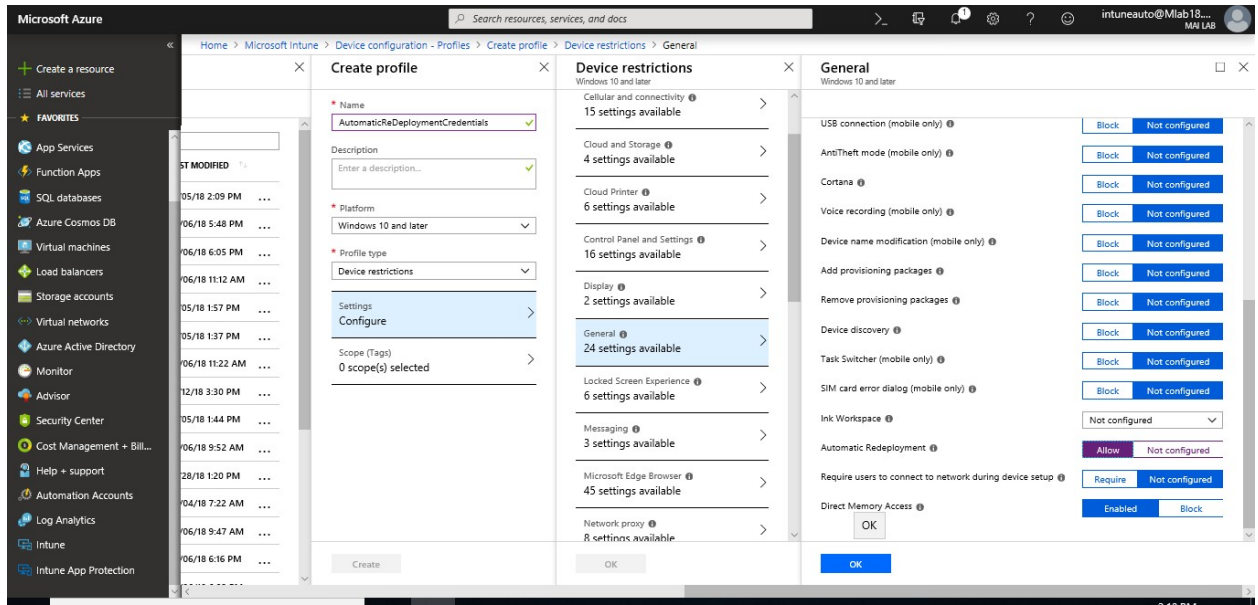
5. Once the reset is complete, the device is again ready for use



Local Windows Autopilot Reset

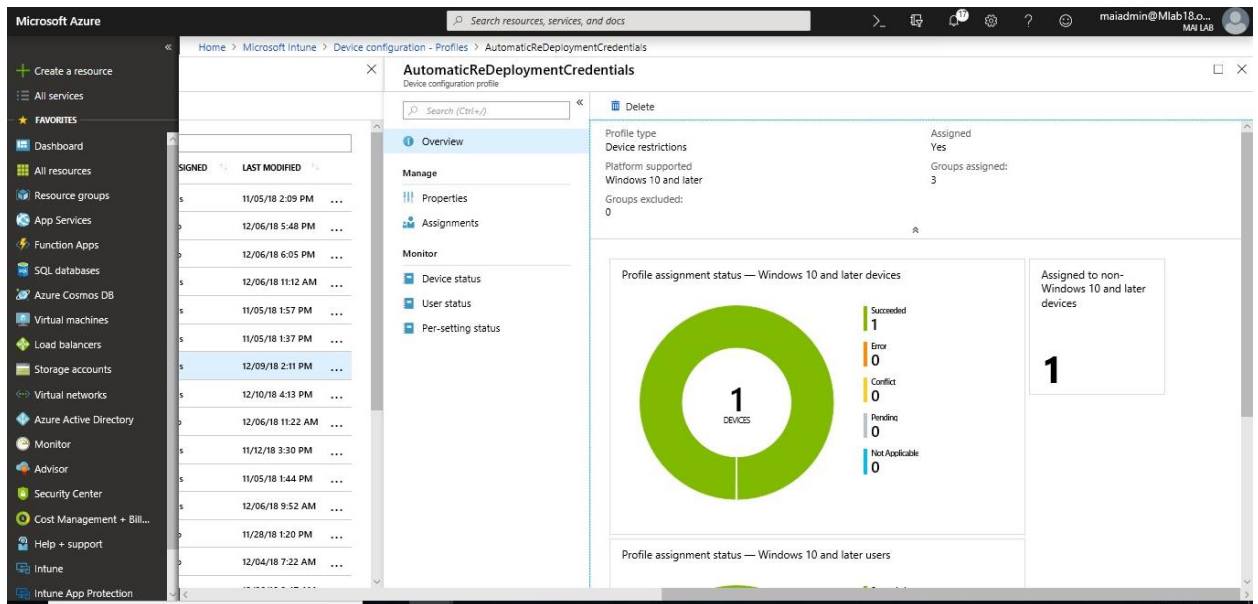
To trigger a local Windows Autopilot Reset, follow these steps:

1. Sign in to the [Intune in the Azure portal](#). Navigate to **Device Configuration** tab in the Intune console.
2. Create a new device configuration profile, specifying "**Windows 10 or later**" for the platform, "**Device restrictions**" for the profile type, and "**General**" for the settings category. The **Automatic Redeployment** setting should be set to **Allow**. Deploy this setting to all devices where a local reset should be permitted.

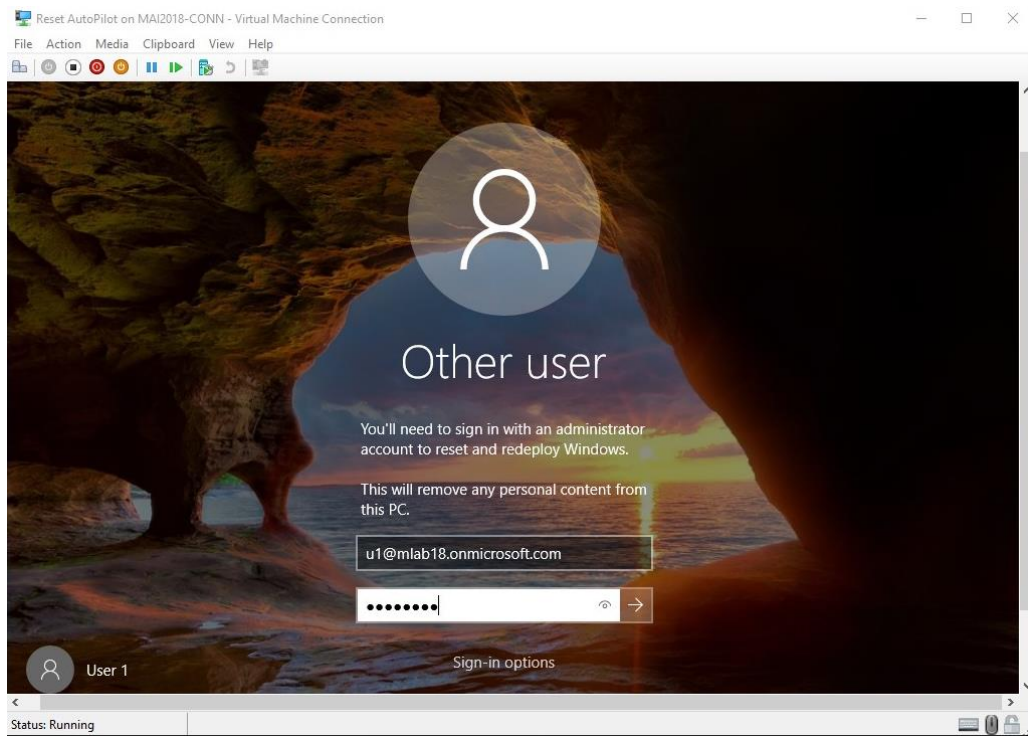


Note: To enable a local Windows Autopilot Reset, the `DisableAutomaticReDeploymentCredentials` policy must be configured.

3. You should find above policy is successfully applied to specific user. It will appear on Intune portal.

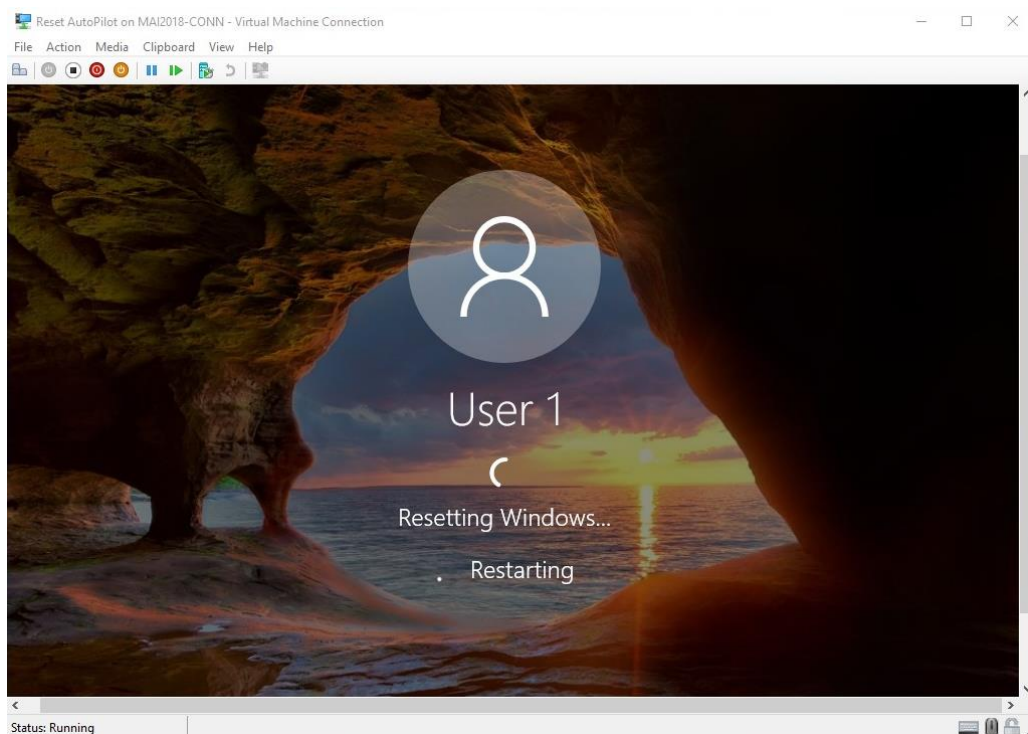


4. From the Windows device lock screen, enter the keystroke: **CTRL + Win + R**.
5. This will open up a custom login screen for the local Autopilot Reset. Confirm/verify that the end user has the right to trigger Local Autopilot Reset.



Note: Sign in with the admin account credentials. If you created a provisioning package, plug in the USB drive and trigger the **local Autopilot Reset**.

6. Once the local Autopilot Reset is triggered, the reset process starts. Once provisioning is complete, the device is again ready for use.



Chapter 10

Intune Reporting & Alerts

Use the Intune Data Warehouse

Use the Intune Data Warehouse to build reports that provide insight into your enterprise mobile environment. For example, some of the reports include:

- Trend of users enrolling in Intune, so you can optimize your license purchases
- App and OS versions breakdown so you can review that status of mobile devices
- Enrollment and device compliance trends so you can smoothly roll out policy updates

The Data Warehouse provides you access to more information about your mobile environment than the Azure portal. With the Intune Data Warehouse, you can access:

- Historical Intune data
- Data refreshed on a daily cadence
- A data model using the OData standard

Note: If you are using hybrid mobile device management (MDM) with System Center Configuration Manager and Microsoft Intune, you want to retrieve your data from SCCM. The Intune Data Warehouse only contains Intune data. You can use an SCCM Power BI dashboard for your custom reports. You should try to migrate from Intune hybrid to stand alone as Intune hybrid will be out of support by 1 September 2019.

Azure AD and Intune credential requirements

Authentication and authorization are based on Azure AD credentials and Intune role-based access control (RBAC). All global administrators and Intune service administrators for your tenant have access to the Data warehouse by default. Use Intune roles to provide access for more users by giving them access to the **Intune data warehouse** resource.

Requirements for accessing the Intune Data Warehouse (including the API) are:

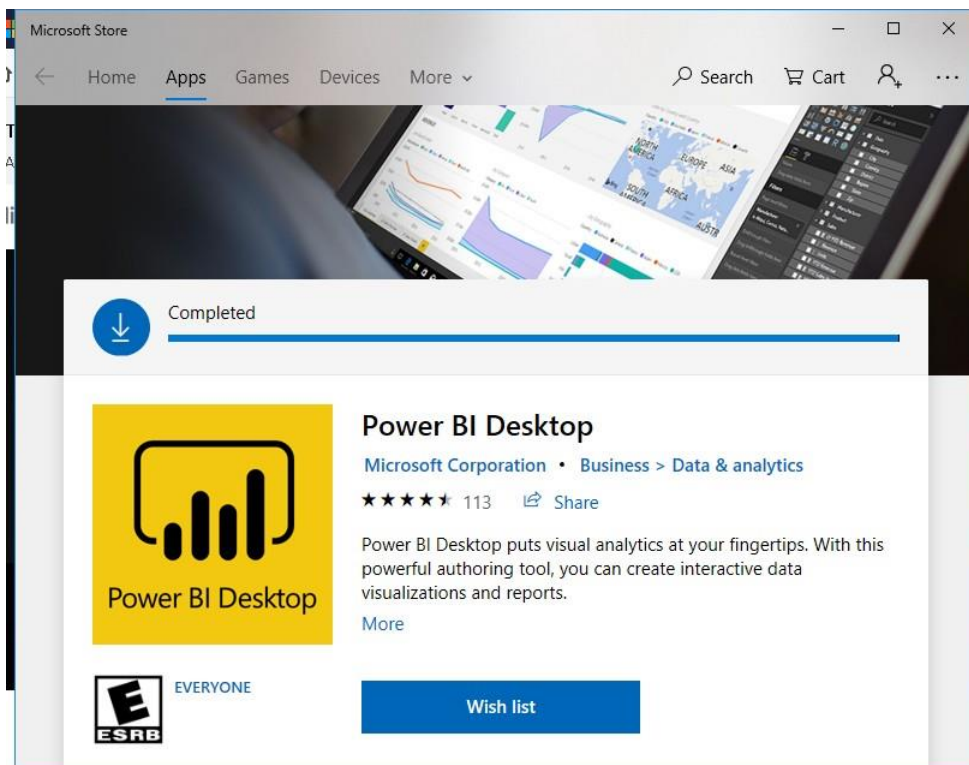
- User must be one of:
 - Azure AD global administrator
 - An Intune service administrator
 - User with role-based access to **Intune data warehouse** resource
 - User-less authentication using application-only authentication.

Microsoft Intune step by step on Azure portal

Note: You can set up an application using Azure Active Directory (Azure AD) and authenticate to the Intune Data Warehouse. you authorize your application with Azure AD using OAuth 2.0.

Install Power BI

Install the latest version of Power BI Desktop. You can download Power BI Desktop from: PowerBI.microsoft.com

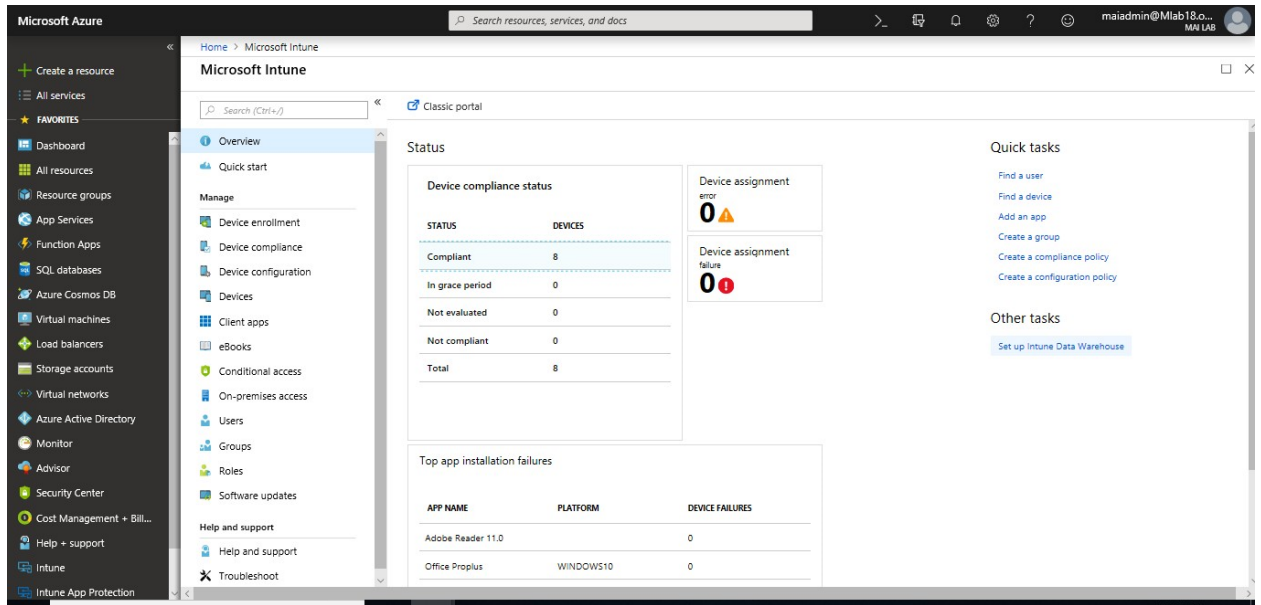


Load the data in Power BI using the OData link

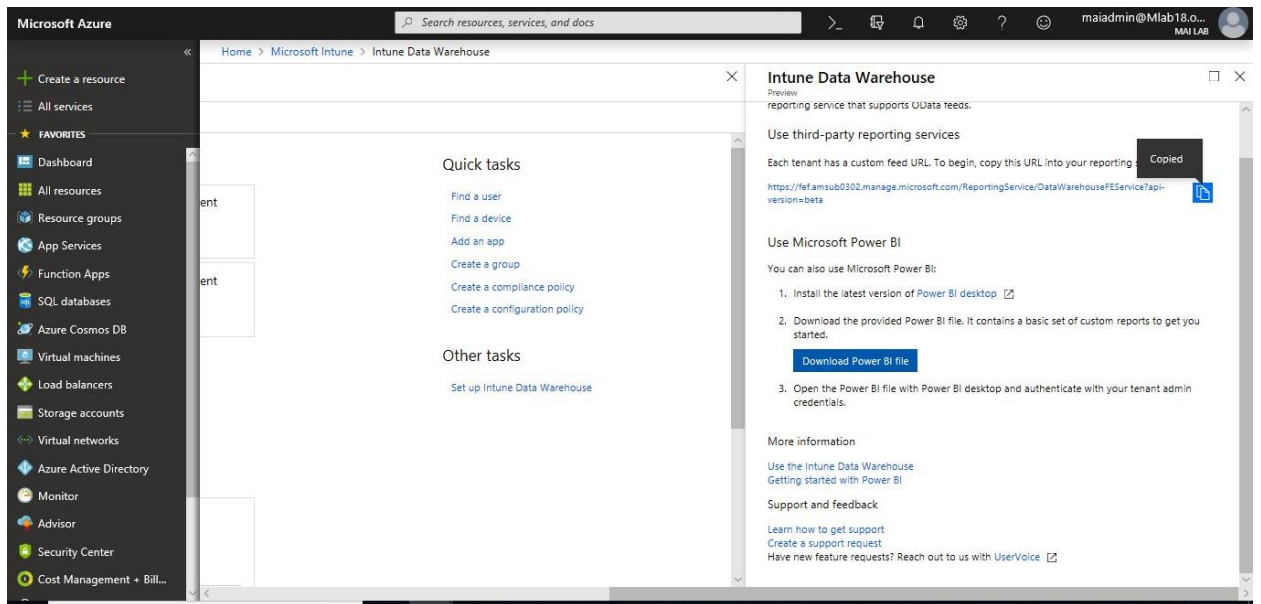
With a client authenticated to Azure AD, the OData URL connects to the RESTful endpoint in the Data Warehouse API that exposes the data model to your reporting client. Follow these instructions to use Power BI Desktop to connect and create your own reports. You are not limited to Power BI Desktop, but can use your favorite analytic tool with the OData URL provided the client supports OAUTH2.0 authentication and the OData v4.0 standard.

1. Sign in to the Azure portal and choose **Monitoring + Management > Intune**. You can also search resources for **Intune**. Click on **Setup Intune Data warehouse**.

Microsoft Intune step by step on Azure portal

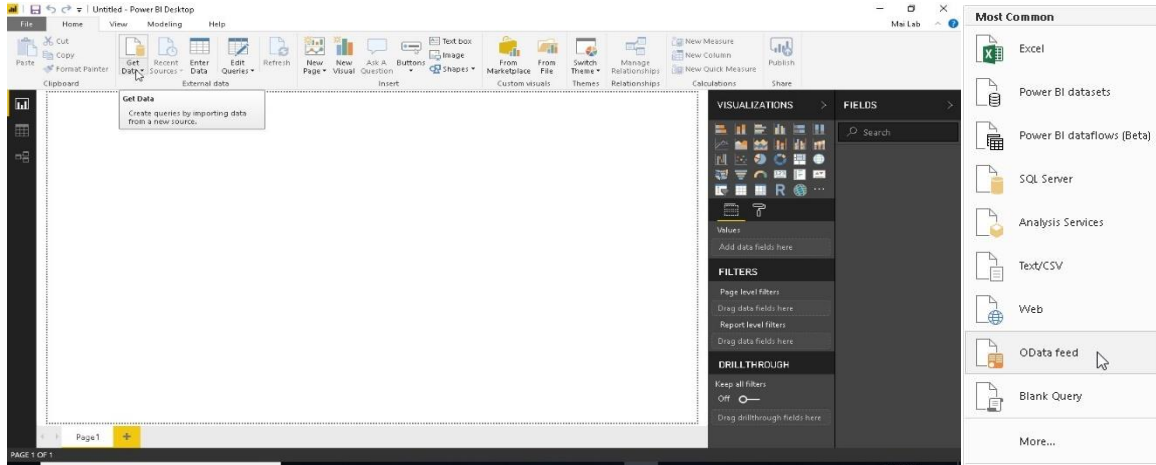


2. Open the **Microsoft Intune Data Warehouse API (Preview)** blade.
3. Retrieve the custom feed URL from the reporting blade, for example <https://fef.{yourinfo}.manage.microsoft.com/ReportingService/DataWarehouseFEService/dates?api-version=beta>



4. Open **Power BI Desktop**.
5. Choose **Home > Get Data**. Select **OData feed**.

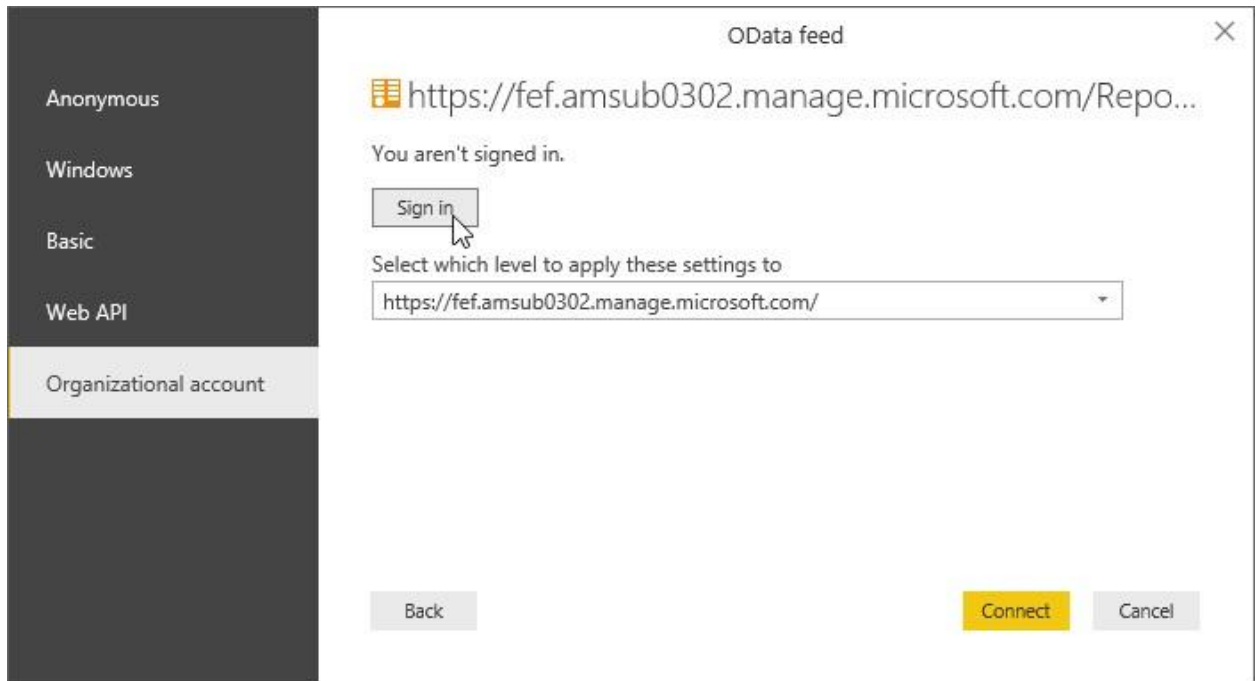
Microsoft Intune step by step on Azure portal



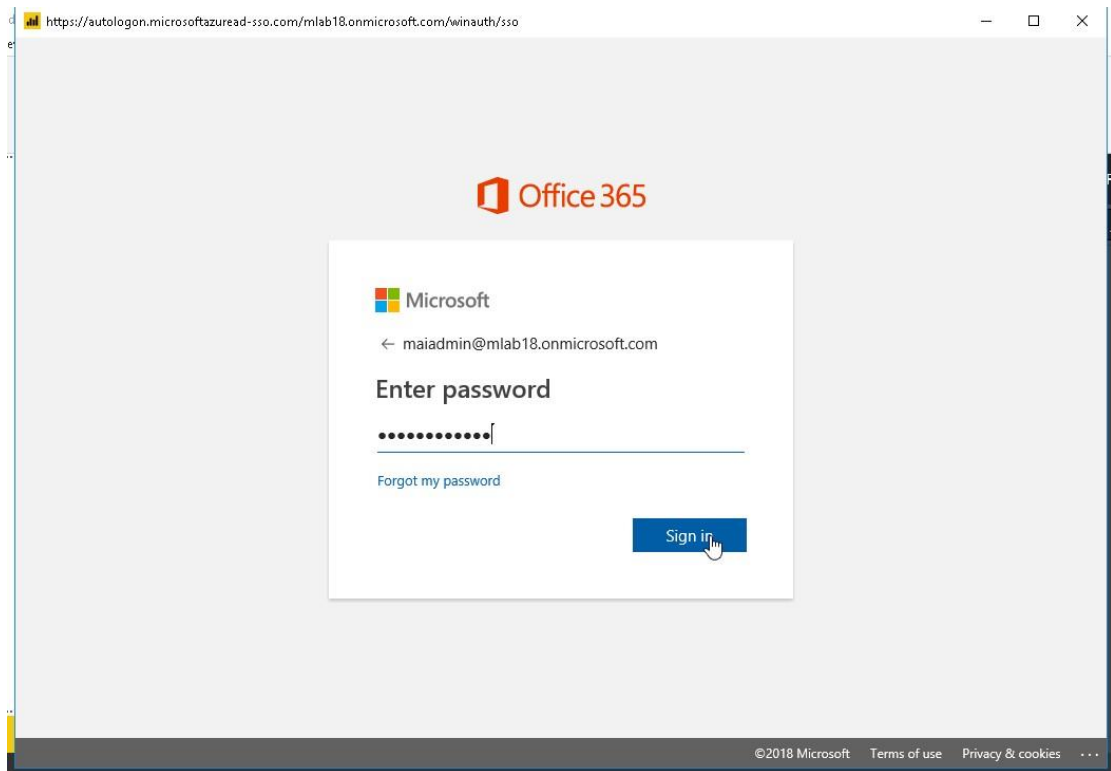
6. Choose **Basic**. Type or paste the **OData URL** into the URL box. Select **OK**.



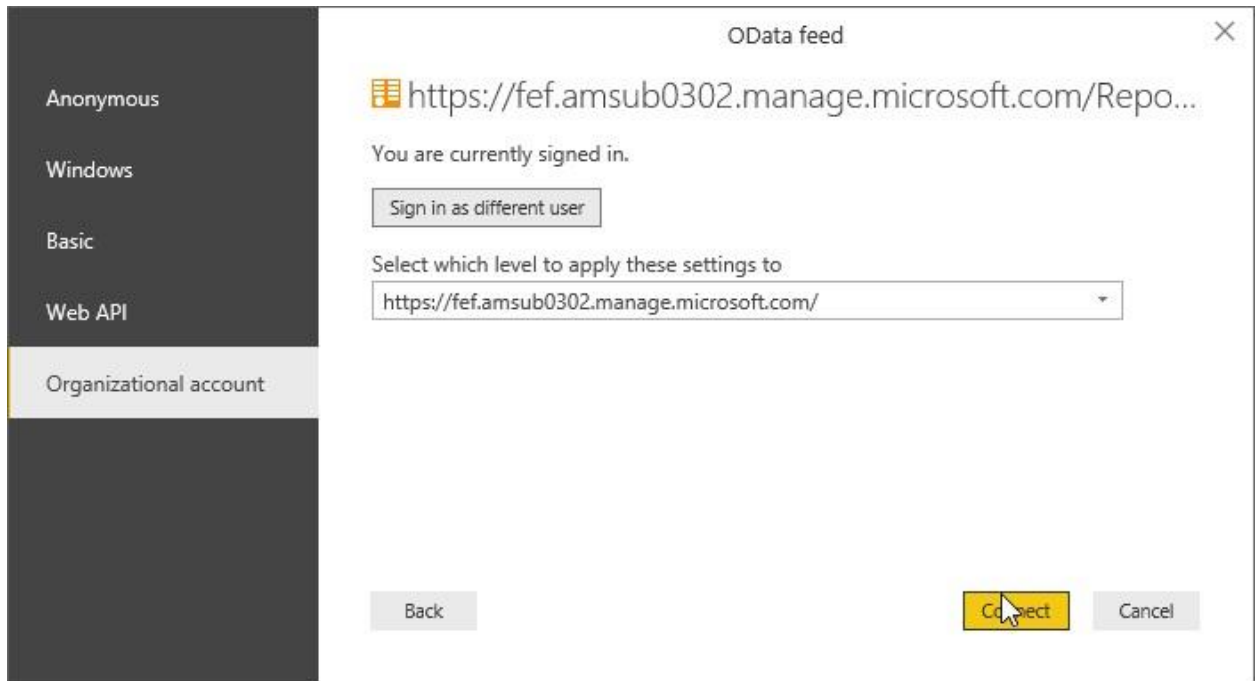
7. If you have not authenticated to Azure AD for your tenant from the Power BI desktop client, type your credentials. To gain access to your data, you must authorize with Azure Active Directory (Azure AD) using OAuth 2.0.
 - Select **Organizational account**. Select **Sign In**.



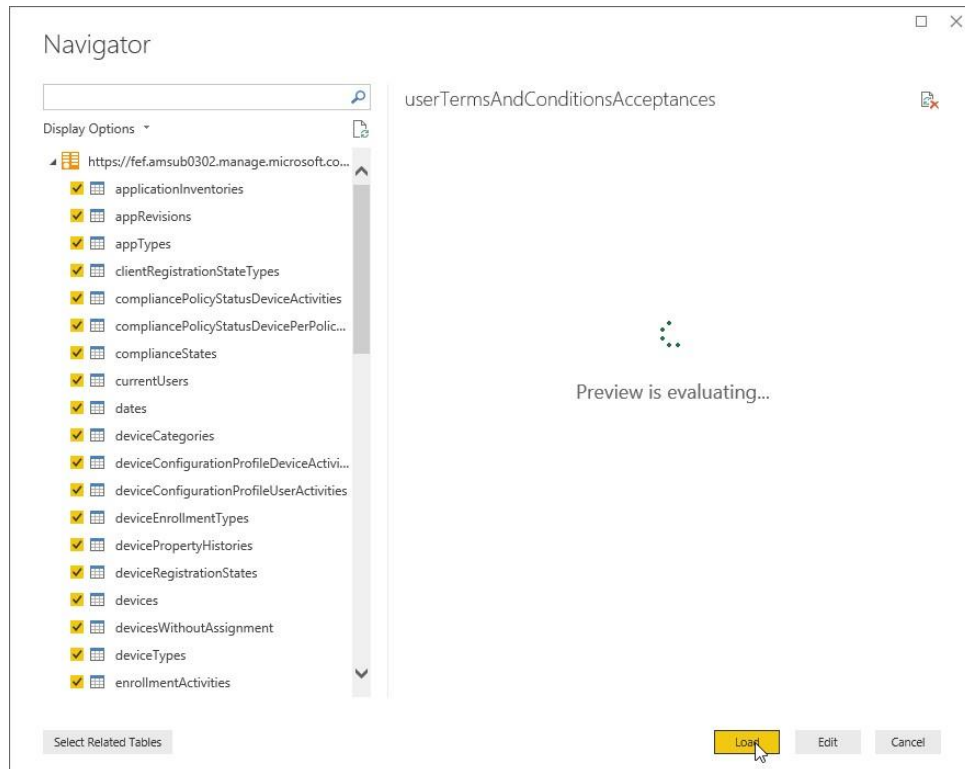
- Type your username and password. Select **Sign In**.

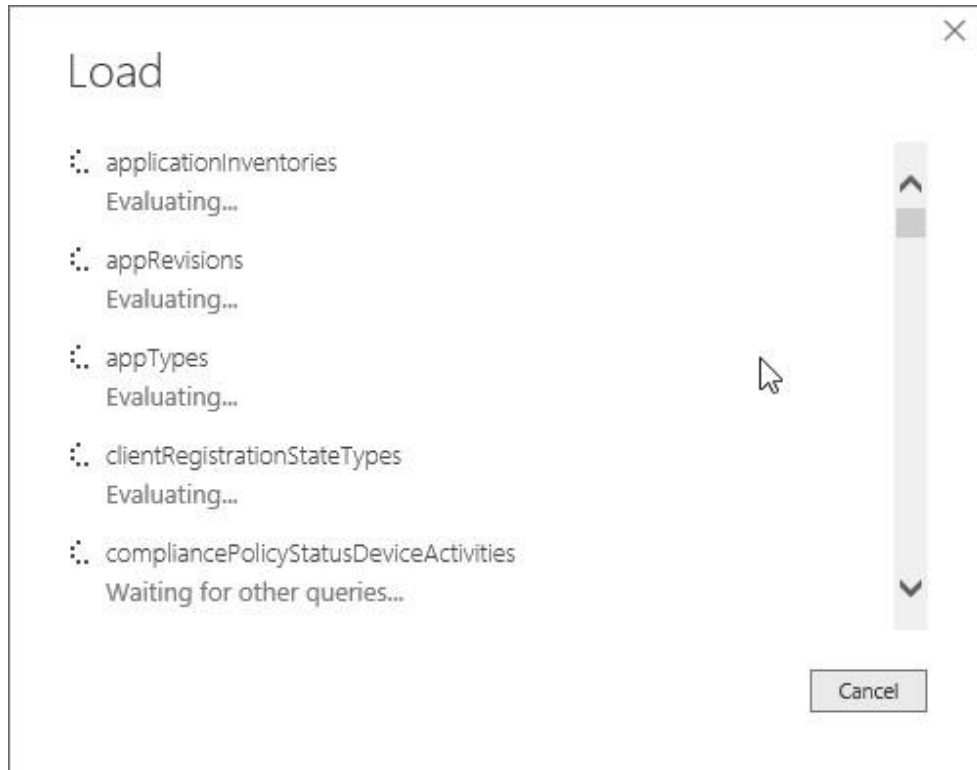


- Select **Connect**.

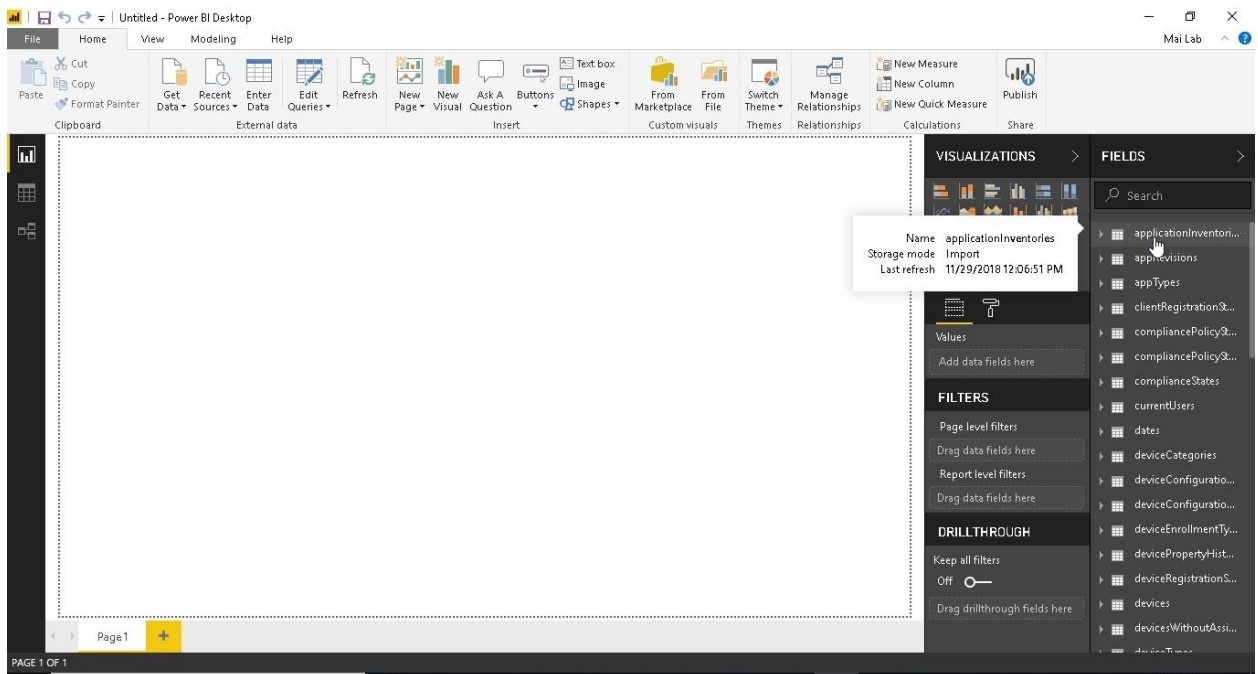


8. Select **Load**.



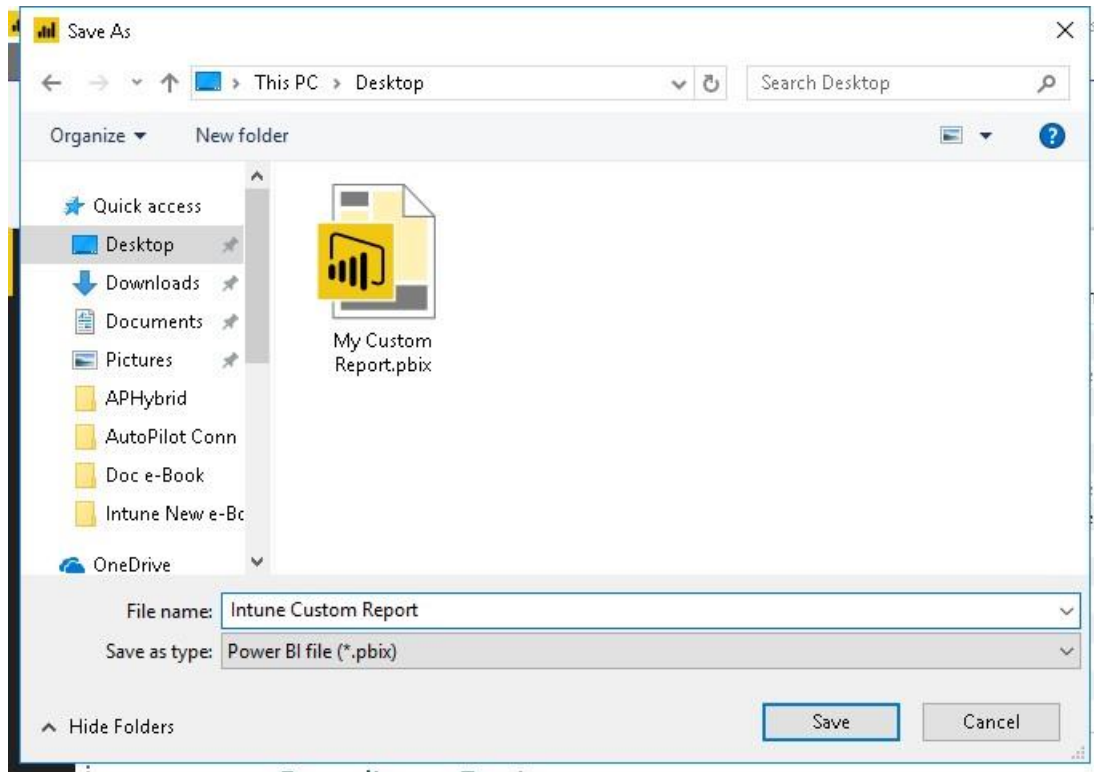


9. You will find all database uploaded and it's ready to create custom report.

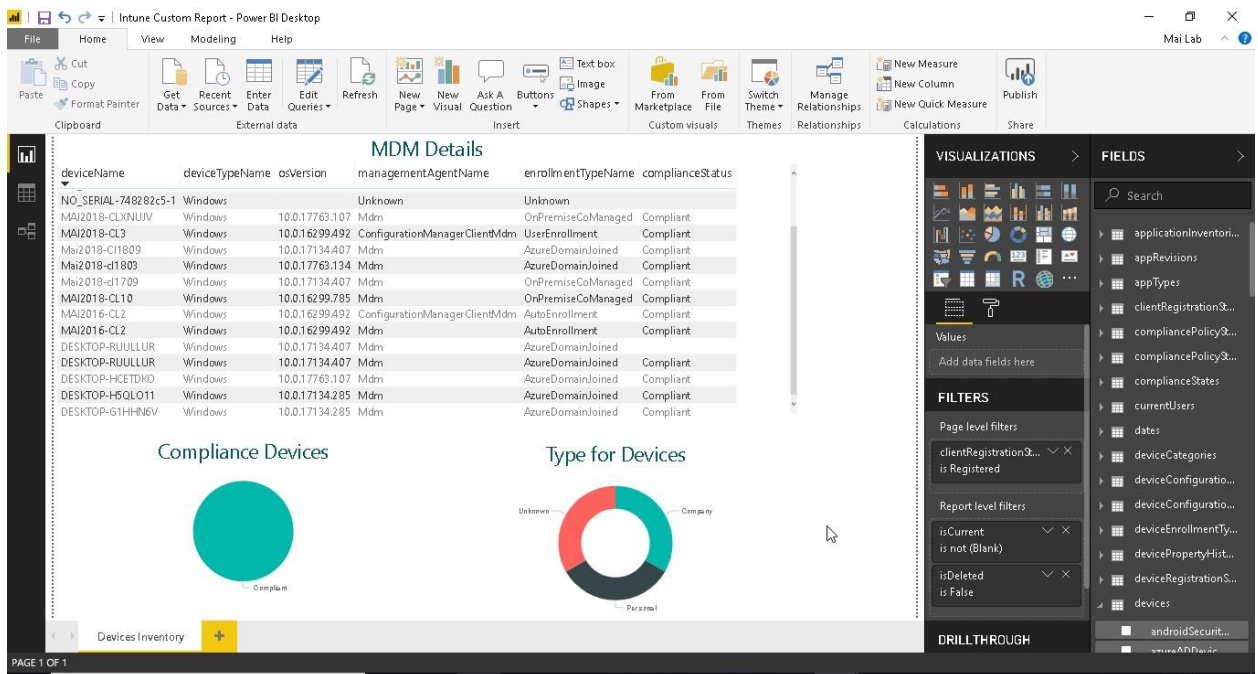


10. You can select fields that you want and create report for devices.

11. Save the report on **pbix** file.



12. Now you have Intune custom report and you can create many pages in save pbix file.

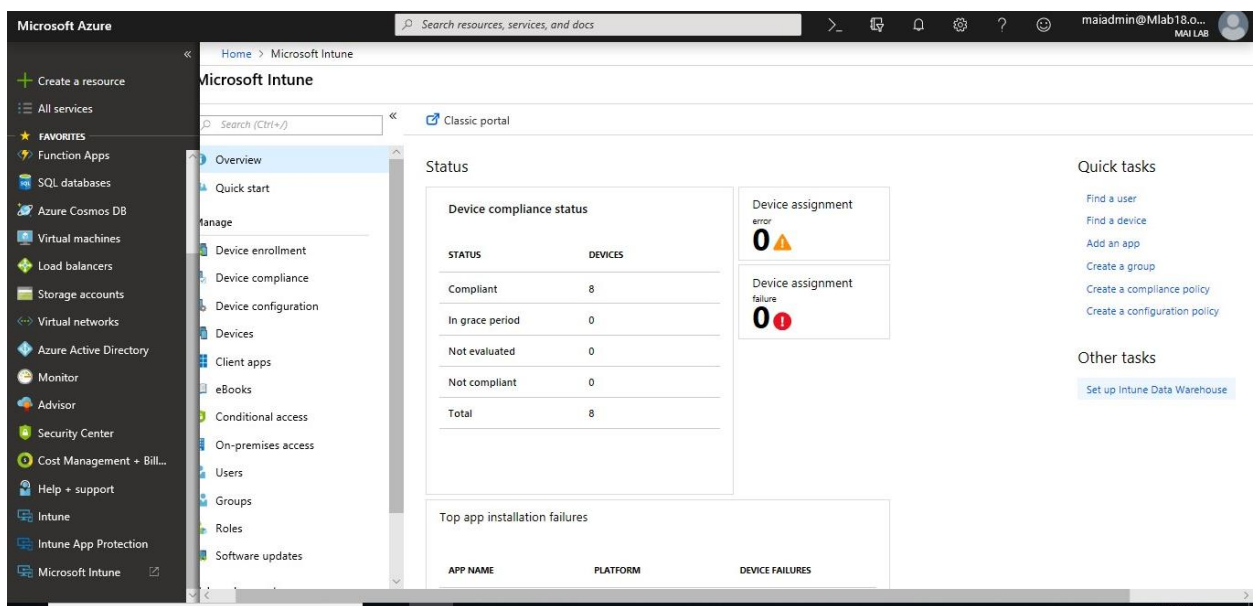


Load the data and reports using the Power BI file (pbix)

The Power BI file (pbix) contains connection information for your tenant and a set of prebuilt reports based on the Data Warehouse data model. Open the file in Power BI Desktop and sign in to the Azure AD. The report loads the data from your Intune tenant.

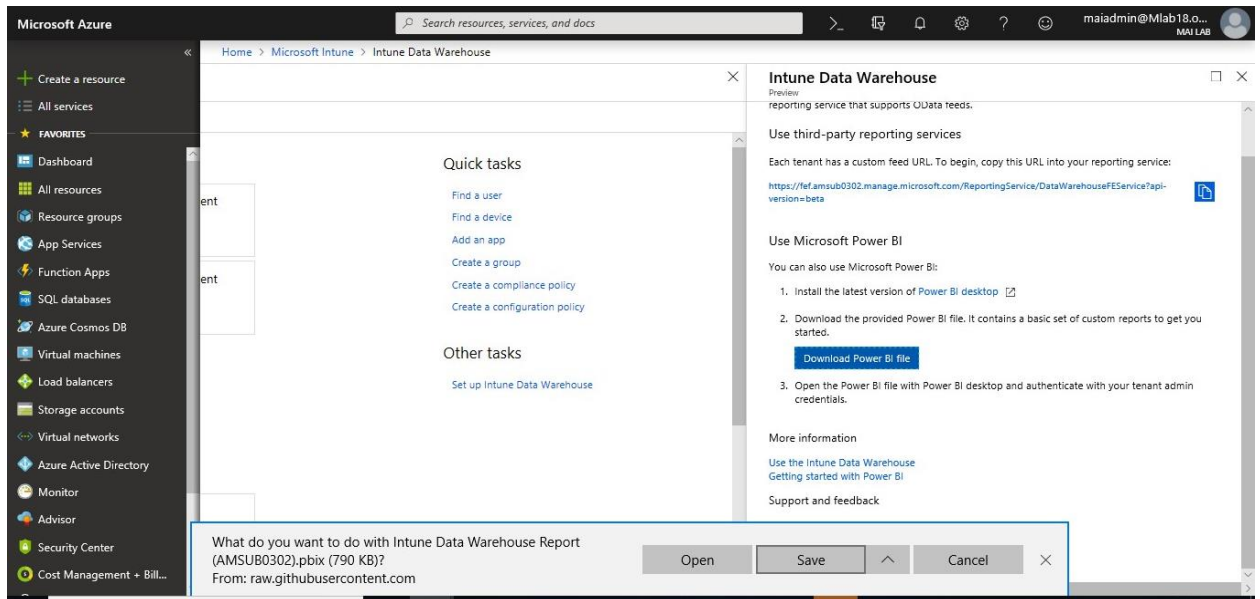
Note: Each Power BI file (pbix) may be different depending on tenant location. If you are managing multiple Intune tenants, then be sure to use the file downloaded from the Azure portal while logged in to that tenant.

1. Sign in to the Azure portal and choose **Monitoring + Management > Intune**. You can also search resources for **Intune**. Click on **Setup Intune Data warehouse**.

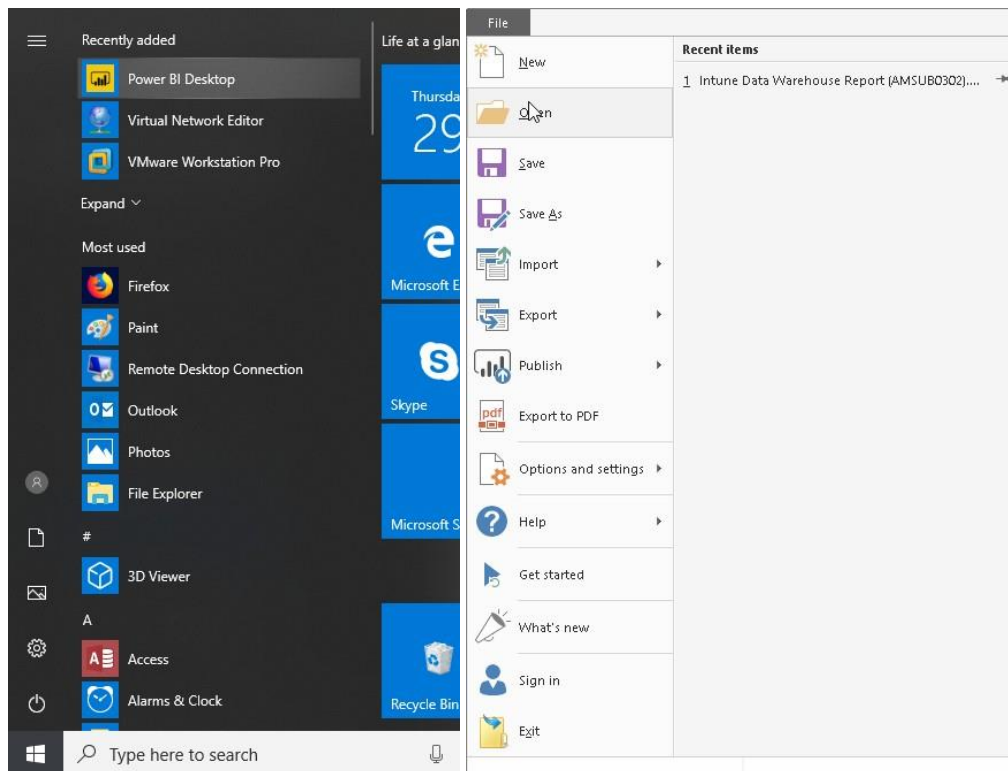


2. Open the **Microsoft Intune Data Warehouse API (Preview)** blade. Select **Download PowerBI file**. The file with a (pbix) extension downloads to the location you specified.

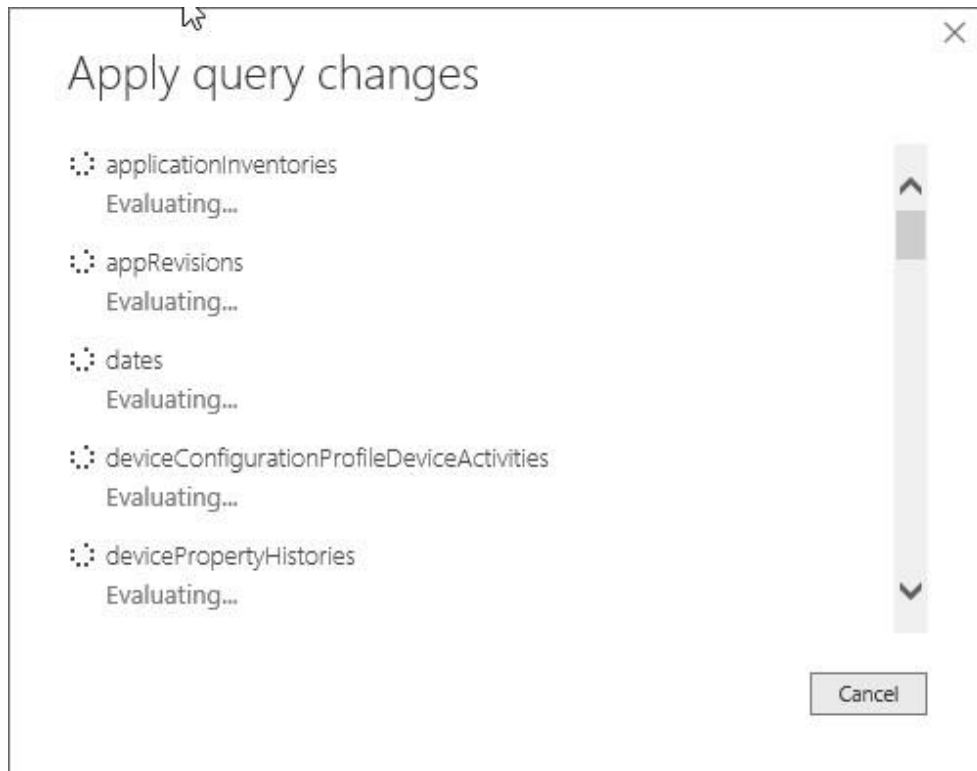
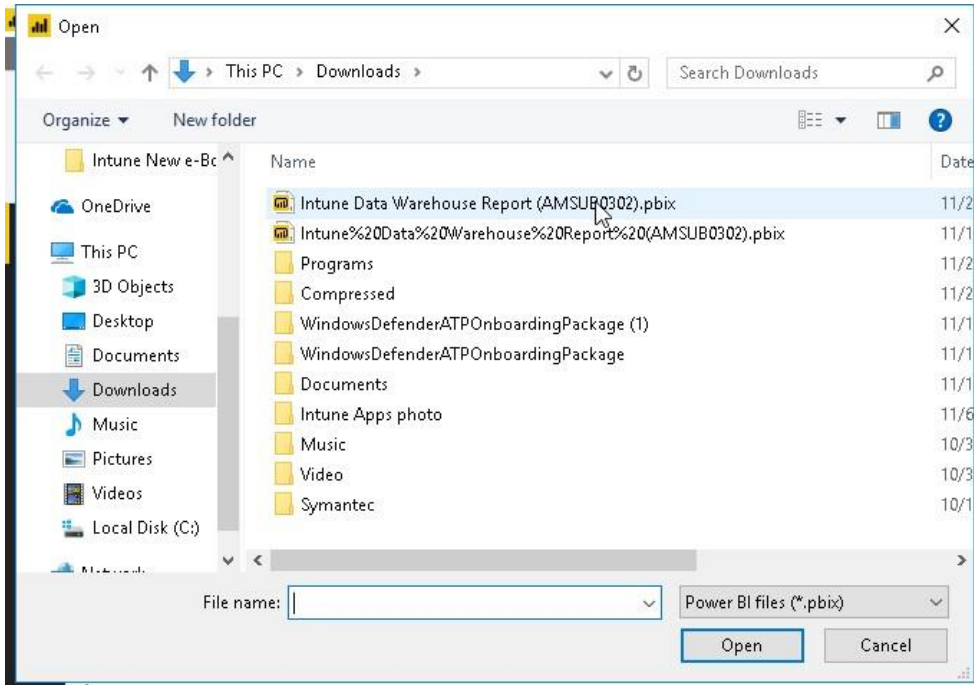
Microsoft Intune step by step on Azure portal



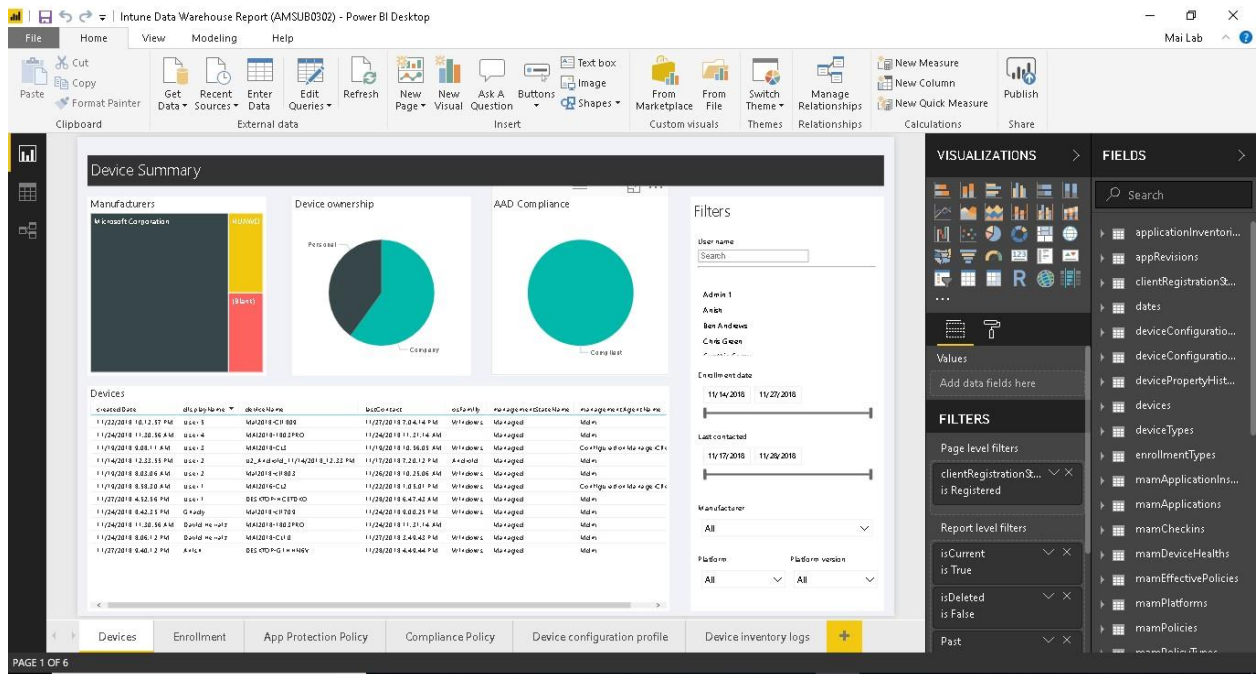
3. Open **Power BI Desktop** and Click **File > Open**.



4. Open the file with Power BI. The *Intune Data Warehouse Reports* loads but may take a second to get your tenant data.



5. Select **Refresh** to load your tenant data and review the reports.



Note: If Power BI has not authenticated with your Azure Active Directory credentials, Power BI prompts you to provide your credentials. When selecting your credentials, choose **Organizational account** as your authentication method and sign in with your global admin account.

Publish Intune Report from Power BI Desktop

When you publish a **Power BI Desktop** file to the **Power BI service**, the data in the model and any reports you created in **Report** view are published to your Power BI workspace. You'll see a new dataset with the same name, and any reports in your Workspace navigator.

Publishing from **Power BI Desktop** has the same effect as using **Get Data** in Power BI to connect to and upload a **Power BI Desktop** file.

Note: Any changes you make to the report in Power BI, for example, add, delete, or change visualizations in reports, will not be saved back to the original **Power BI Desktop** file.

To publish a Power BI Desktop dataset and reports

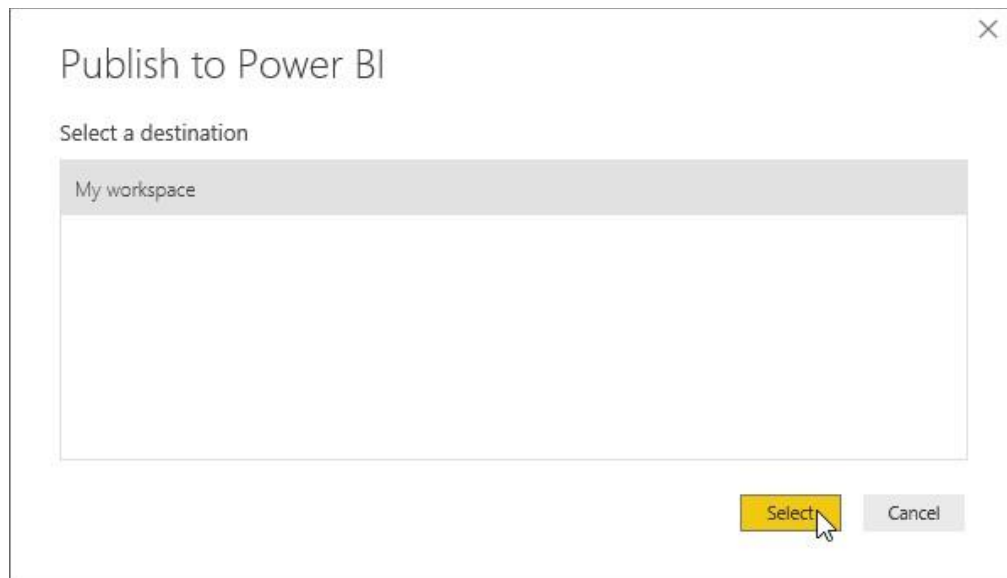
1. In Power BI Desktop > **File** > **Publish** > **Publish to Power BI** or click **Publish** on the ribbon.

Microsoft Intune step by step on Azure portal

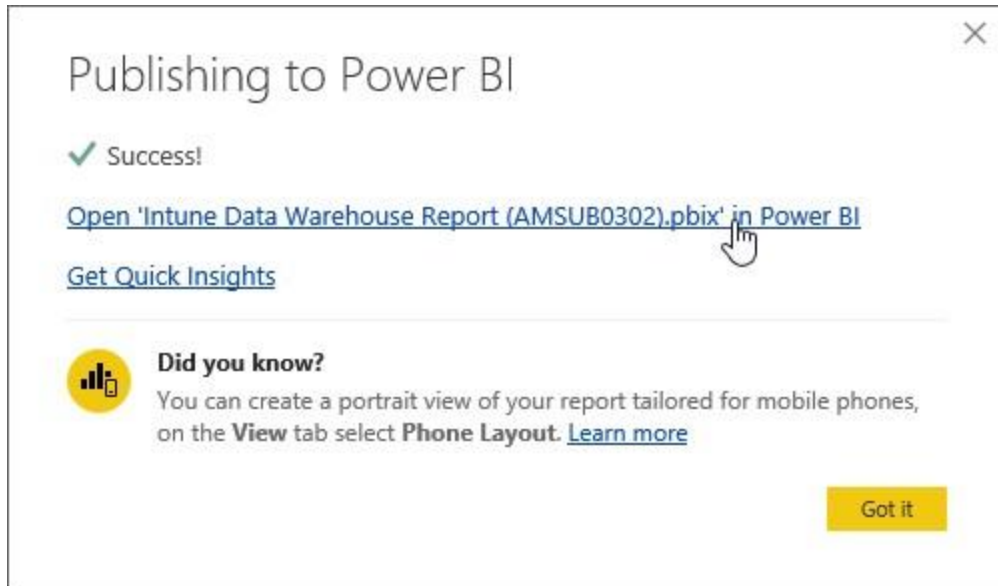
The screenshot shows the Microsoft Power BI Desktop interface. The main report, 'Device Summary', is displayed with three charts: 'Manufacturers' (a bar chart showing Microsoft Corporation and EBR), 'Device ownership' (a pie chart showing Personal and Company), and 'AAD Compliance' (a donut chart showing Compliant). Below the charts is a table of devices with columns for creation date, display name, device name, last contact, os family, management state name, and management engine name. The 'Filters' pane on the right shows filters for User name, Enrollment date, and Last contacted. The 'Visualizations' pane on the right shows the 'Publish' button and a list of data fields.

Creation date	Display name	Device name	Last contact	OS Family	Management state name	Management engine name
11/22/2018 10:12:37 PM	User 5	WAD2018-CL1009	11/27/2018 7:06:14 PM	Windows	Managed	Mid
11/24/2018 11:30:56 AM	User 4	WAD2018-1803P RO	11/24/2018 11:31:14 AM	Windows	Managed	Mid
11/19/2018 9:08:11 AM	User 3	WAD2018-CL3	11/19/2018 10:56:05 AM	Windows	Managed	Configuration Manage Cln
11/14/2018 12:33:55 PM	User 2	U2_Android_11/14/2018_12:33 PM	11/17/2018 7:20:12 PM	Android	Managed	Mid
11/19/2018 8:03:06 AM	User 2	WAD2018-clt303	11/26/2018 10:2:59 AM	Windows	Managed	Mid
11/16/2018 8:30:28 AM	User 1	WAD2018-CL2	11/22/2018 10:59:19 PM	Windows	Managed	Configuration Manage Cln
11/27/2018 4:52:56 PM	User 1	DESKTOP-HCLTDFHD	11/28/2018 6:47:43 AM	Windows	Managed	Mid
11/24/2018 8:42:35 PM	Ghady	WAD2018-clt709	11/24/2018 9:00:25 PM	Windows	Managed	Mid
11/24/2018 11:30:56 AM	David Heras	WAD2018-1803P RO	11/24/2018 11:31:14 AM	Windows	Managed	Mid
11/24/2018 8:06:12 PM	David Heras	WAD2018-CL10	11/27/2018 3:49:43 PM	Windows	Managed	Mid
11/27/2018 9:40:12 PM	Anish	DESKTOP-G1H4HNV	11/26/2018 4:49:44 PM	Windows	Managed	Mid

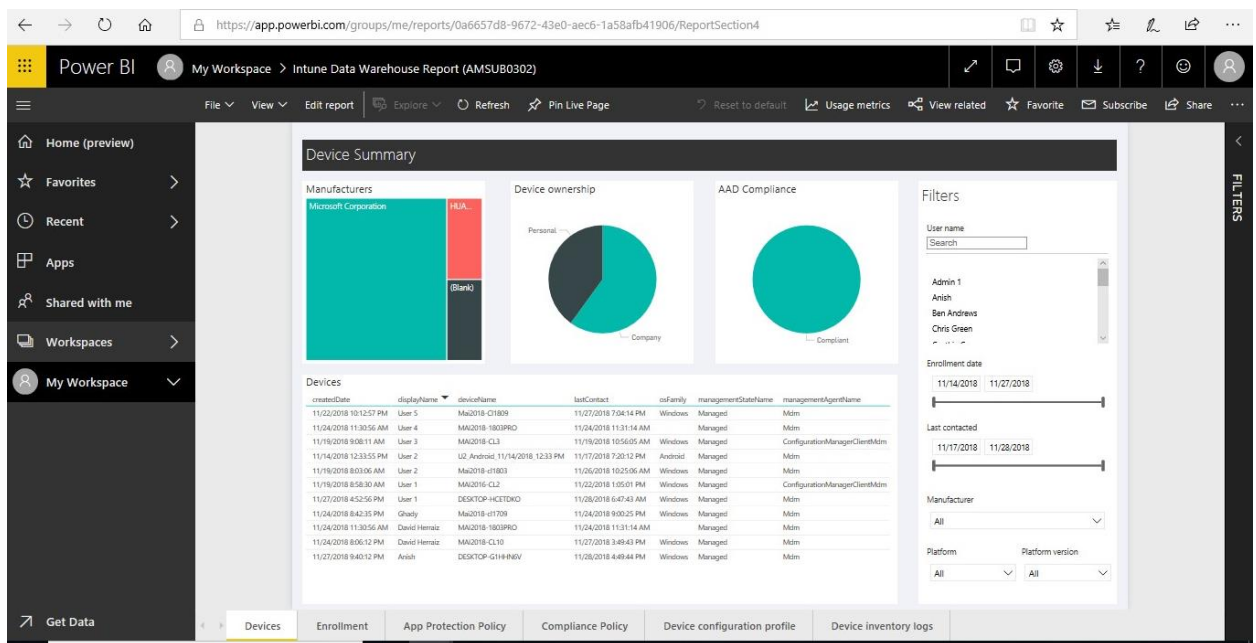
2. Sign in to **Power BI**. Select the **destination**.



3. When complete, you receive a link to your report. Click the link to open the report in your Power BI site.



4. Open Intune Report link on your web browser.

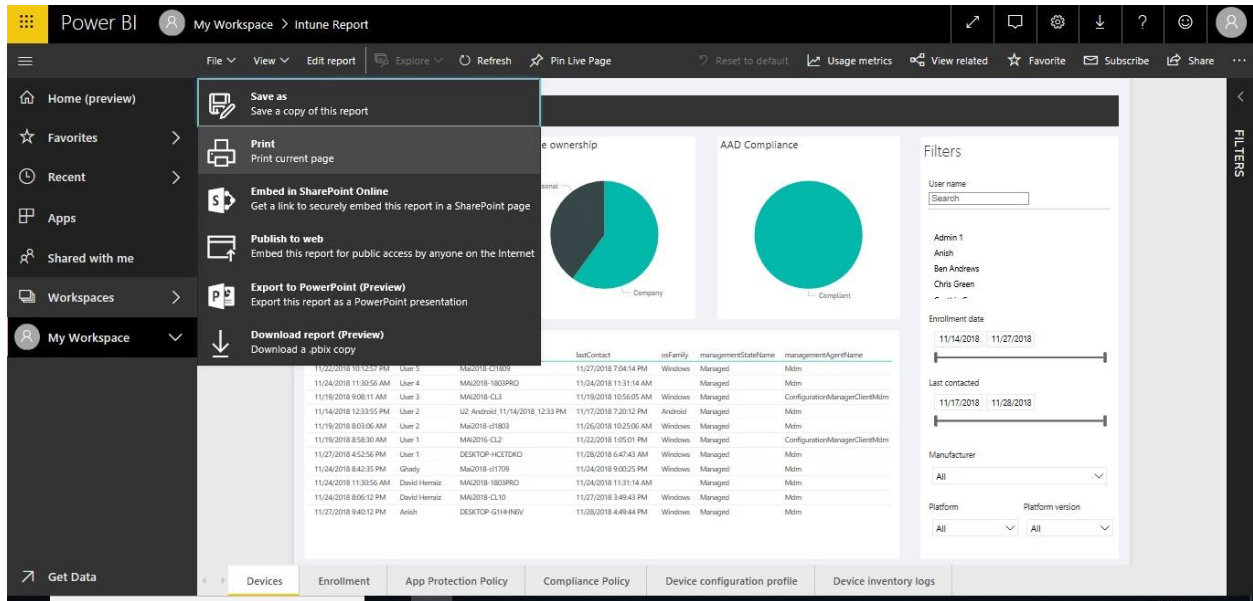


Print & Export dashboards for Reports

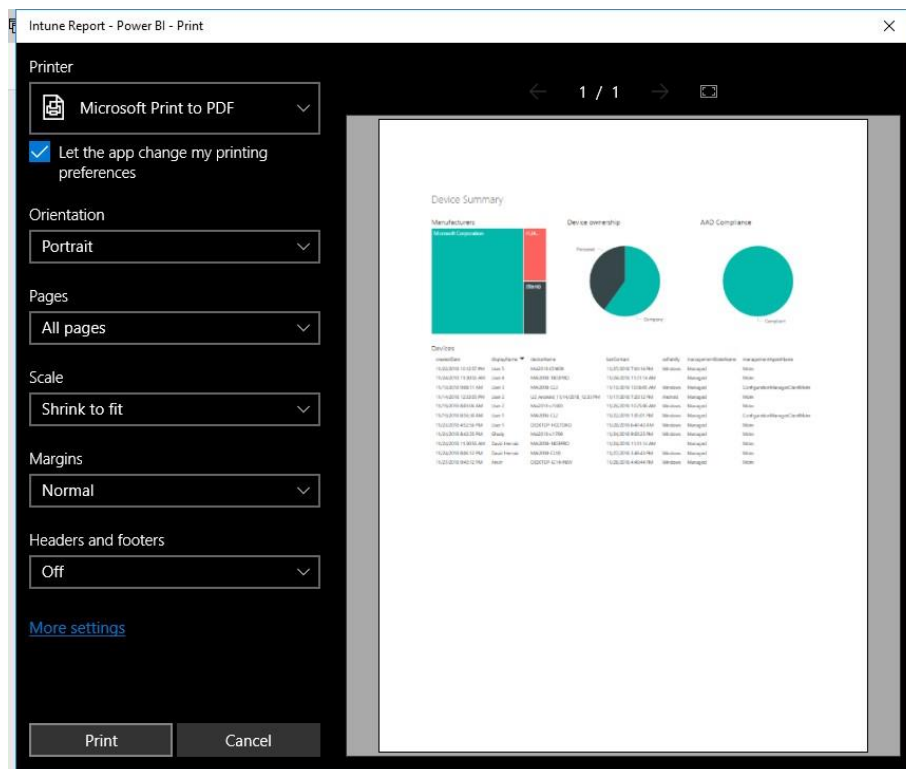
Sometimes you may want to bring a printed report or dashboard to a meeting, or so you can share it with others. With Power BI, there are a few ways you can make printouts of your visuals.

In the Power BI service, select **File > Print**, to Print dashboard.

Microsoft Intune step by step on Azure portal

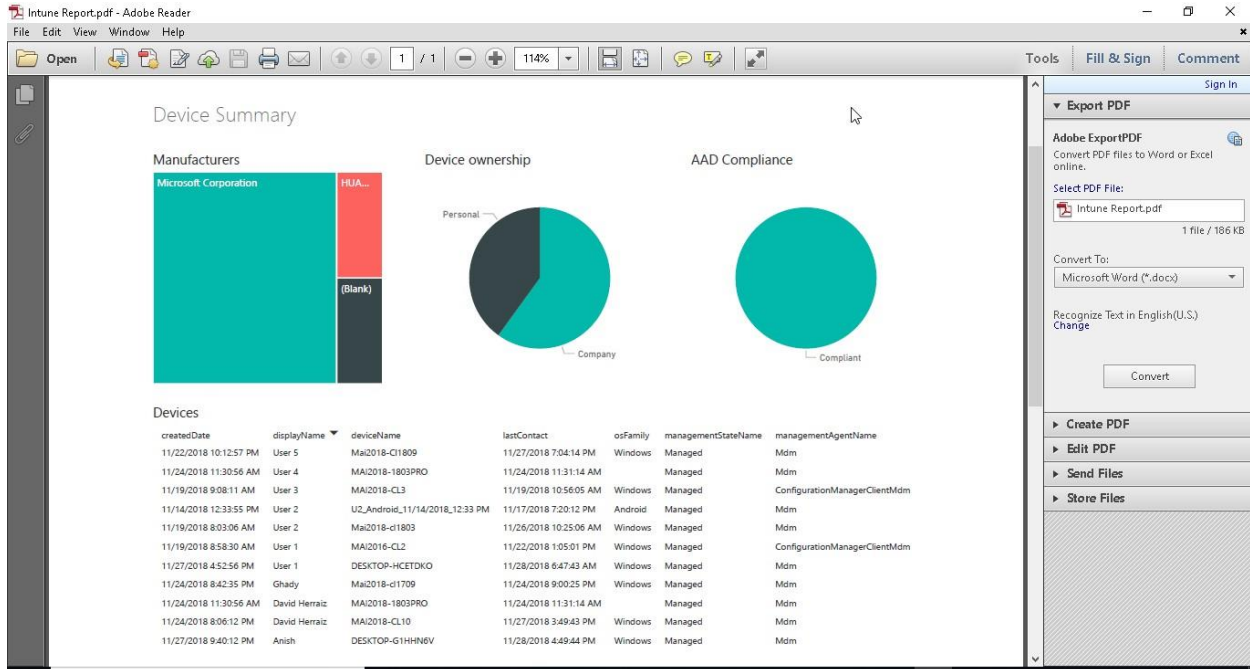


A **Print** dialog appears, where you can select the printer to which you want to send the dashboard, as well as standard print options such as *portrait* or *landscape* orientation.



You can save a report on pdf file. This is the view for PDF report.

Microsoft Intune step by step on Azure portal



Export reports from Power BI to PowerPoint

With Power BI, you can now publish your report to **Microsoft PowerPoint**, and easily create a slide deck based on your Power BI report. When you **export to PowerPoint**, the following occurs:

- Each page in the Power BI report becomes an individual slide in PowerPoint
- Each page in the Power BI report is exported as a single high-resolution image in PowerPoint
- Text boxes in the Power BI report become editable text boxes in PowerPoint
- A link is created in PowerPoint that links to the Power BI report

To export report in PowerPoint Slides, you can follow below steps:

1. In Power BI service, select **File > Export to PowerPoint (Preview)** from the menu bar.

Microsoft Intune step by step on Azure portal

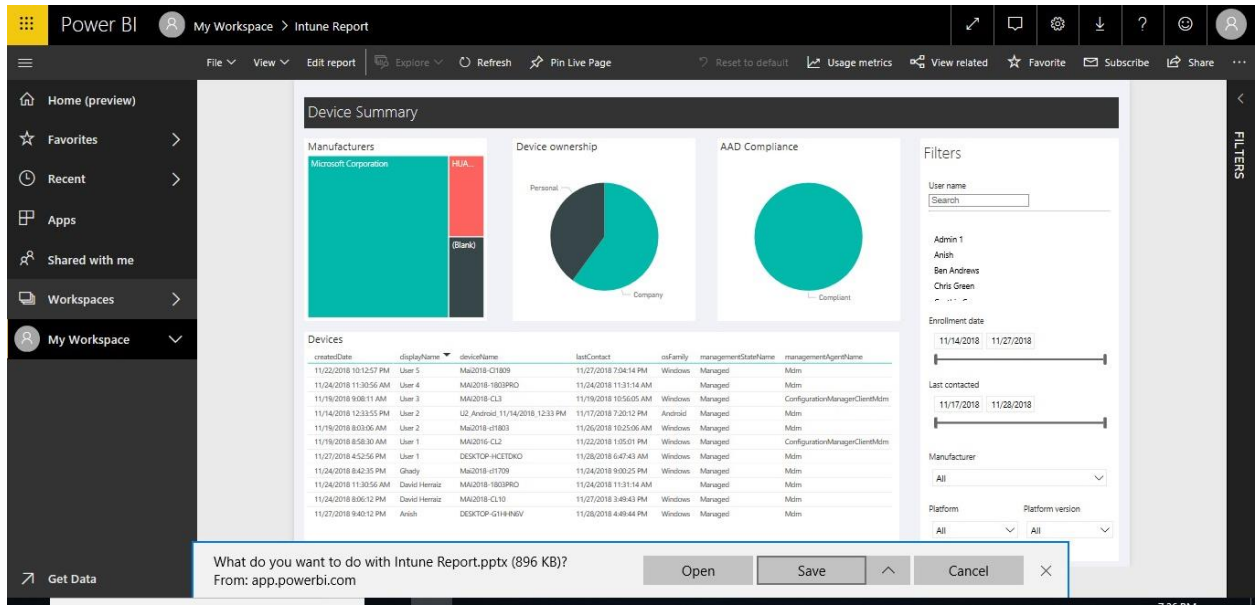
The screenshot shows the Power BI report interface for 'Intune Report'. The 'Export to PowerPoint (Preview)' option is selected in the menu, with the sub-option 'Download a .pptx copy'. The report content includes a table of device data and two pie charts: 'Device ownership' and 'AAD Compliance'. The table data is as follows:

createdDate	displayName	deviceName	lastContact	osFamily	managementStateName	managementAgentName
11/22/2018 10:12:57 PM	User 5	MA2018-CH109	11/27/2018 7:04:14 PM	Windows	Managed	Mdm
11/24/2018 11:30:56 AM	User 4	MA2018-1803PRO	11/24/2018 11:31:14 AM	Managed	Managed	Mdm
11/19/2018 9:08:11 AM	User 3	MA2018-CL3	11/19/2018 10:56:05 AM	Windows	Managed	ConfigurationManagerClientMdm
11/14/2018 12:33:55 PM	User 2	U2_Android_11/14/2018_12:33 PM	11/17/2018 7:20:12 PM	Android	Managed	Mdm
11/18/2018 8:03:06 AM	User 2	MA2018-rt1803	11/26/2018 10:25:06 AM	Windows	Managed	Mdm
11/18/2018 8:58:30 AM	User 1	MA2018-CL2	11/22/2018 1:05:01 PM	Windows	Managed	ConfigurationManagerClientMdm
11/27/2018 4:52:56 PM	User 1	DESKTOP-HCETDKO	11/28/2018 6:47:43 AM	Windows	Managed	Mdm
11/24/2018 8:42:35 PM	Ghady	MA2018-rt1709	11/24/2018 9:00:25 PM	Windows	Managed	Mdm
11/24/2018 11:30:56 AM	David Hernandez	MA2018-1803PRO	11/24/2018 11:31:14 AM	Managed	Managed	Mdm
11/24/2018 8:06:12 PM	David Hernandez	MA2018-CL10	11/27/2018 3:49:43 PM	Windows	Managed	Mdm
11/27/2018 9:40:12 PM	Anish	DESKTOP-G114-RWV	11/28/2018 4:49:44 PM	Windows	Managed	Mdm

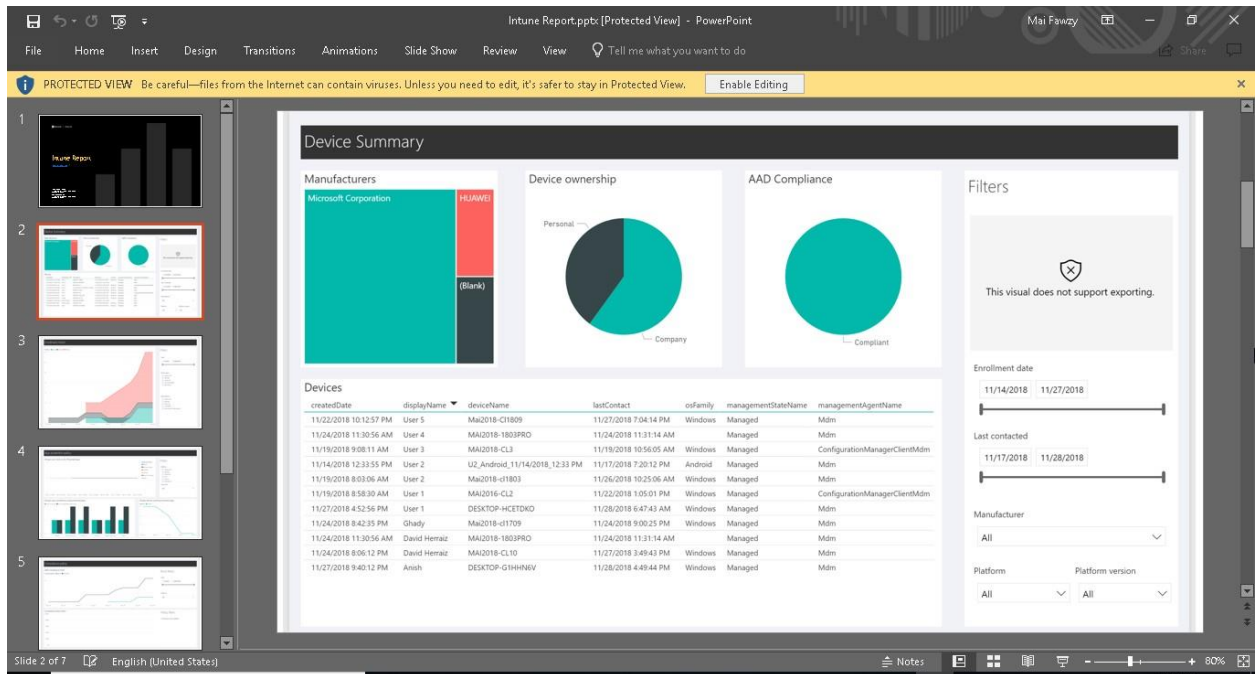
- You'll see a notification banner in the upper right corner of the Power BI service browser window that the report is being exported to PowerPoint. This might take a few minutes, and you can continue to work in Power BI while the report is being exported.

The screenshot shows the same Power BI report interface, but with a notification banner in the upper right corner that reads: 'Export to PowerPoint in progress. Your report Intune Report is being exported to a PowerPoint file. This might take a few minutes.' The report content is the same as in the previous screenshot.

- Once complete, the notification banner changes to let you know that the Power BI service has finished the export process. Our file is then available where your browser displays downloaded files.



4. When you open the PowerPoint file that Power BI exported, you find a few cool and useful elements. PowerPoint opens in normal mode. A static image of each Power View is centered on a separate slide.

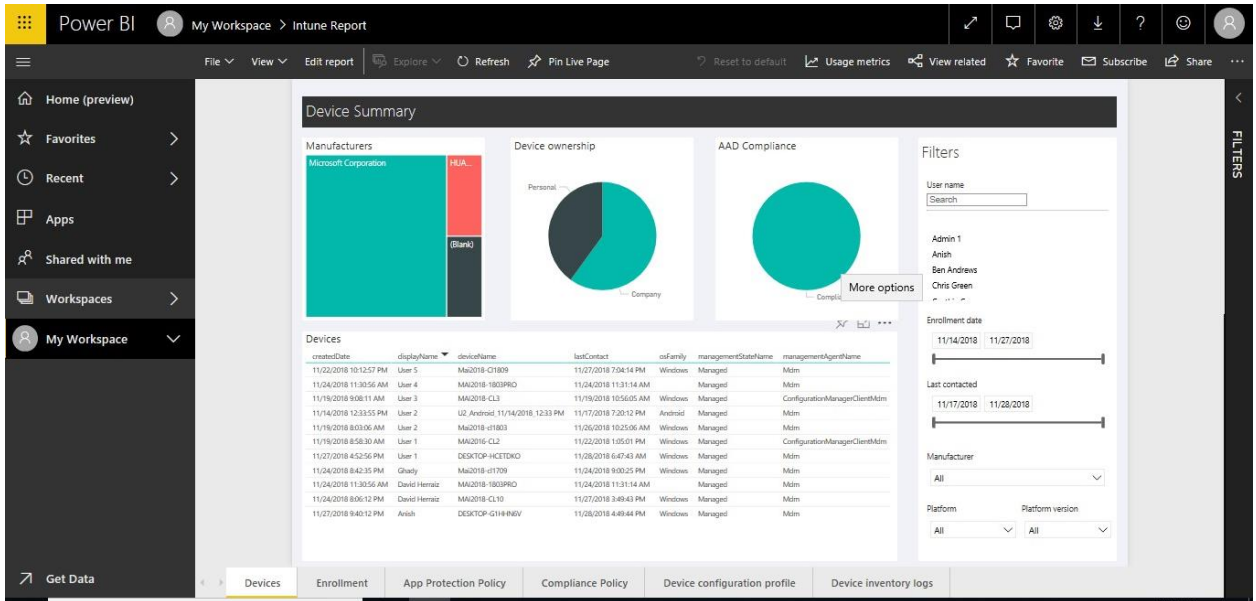


Export data from a visual

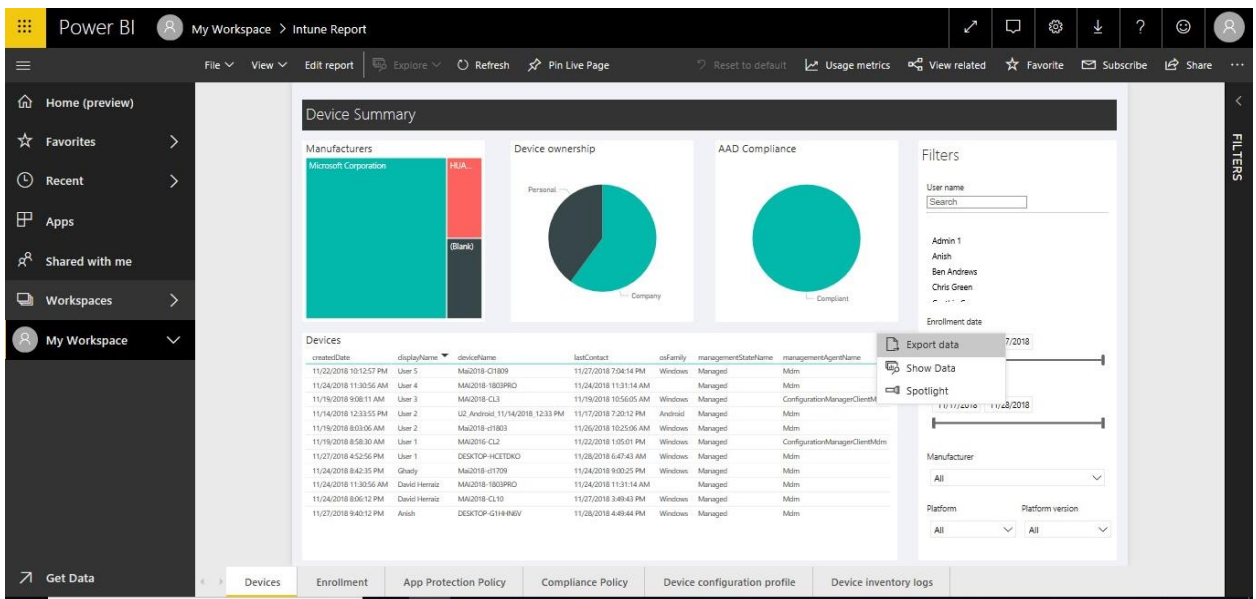
You can also export the data from any visual in the Power BI service. Just select the ellipses on any visual, and then select the **Export data** button (the middle button). When you do so, a .CSV file is created and downloaded to your local computer, and a message appears on your browser (just like any other browser-initiated download) letting you know the download is complete.

From a visualization on a Power BI dashboard

1. Select the ellipses in the top right corner of the visualization.

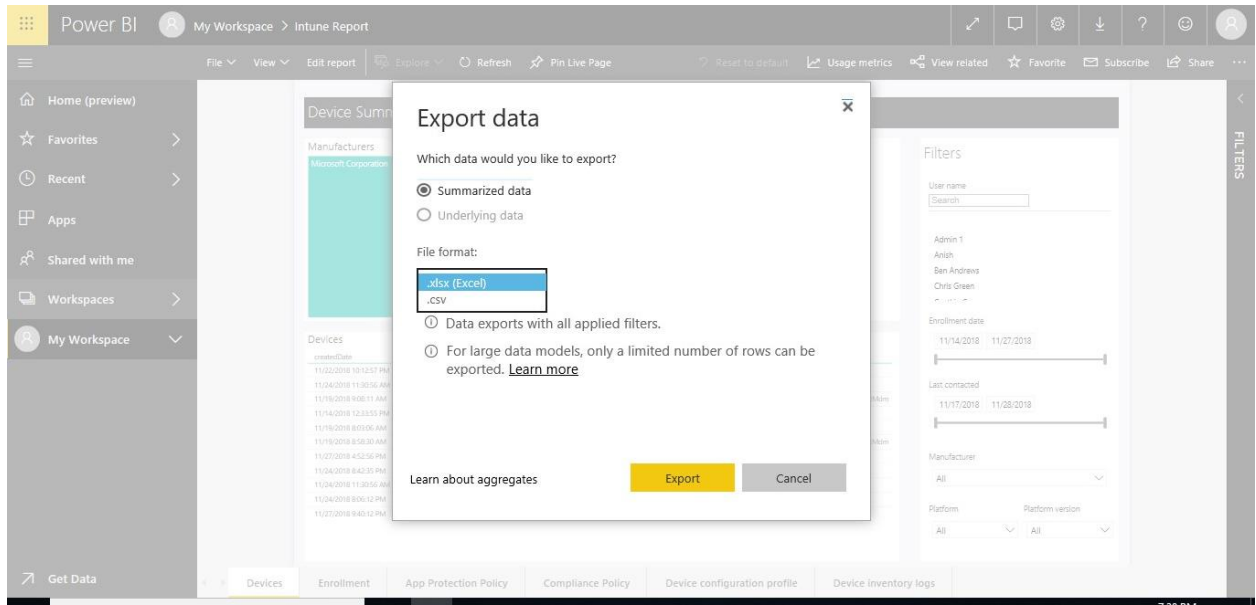


2. Choose the **Export data** icon.

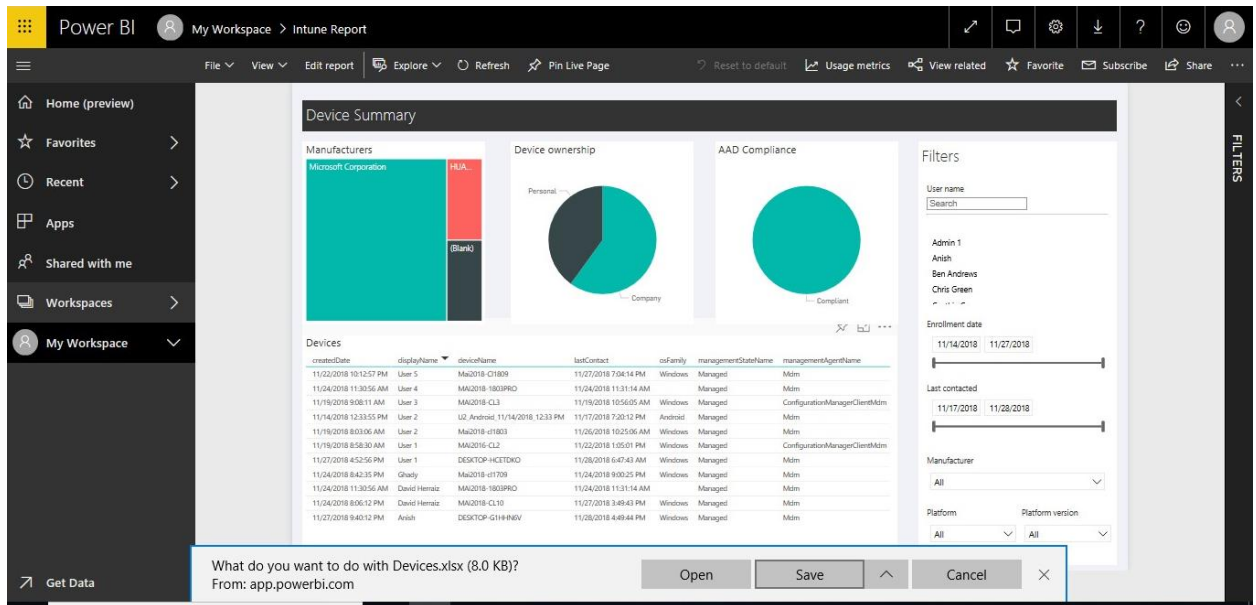


3. The data is exported to excel file. If the visual is filtered, then the downloaded data will also be filtered.

Microsoft Intune step by step on Azure portal

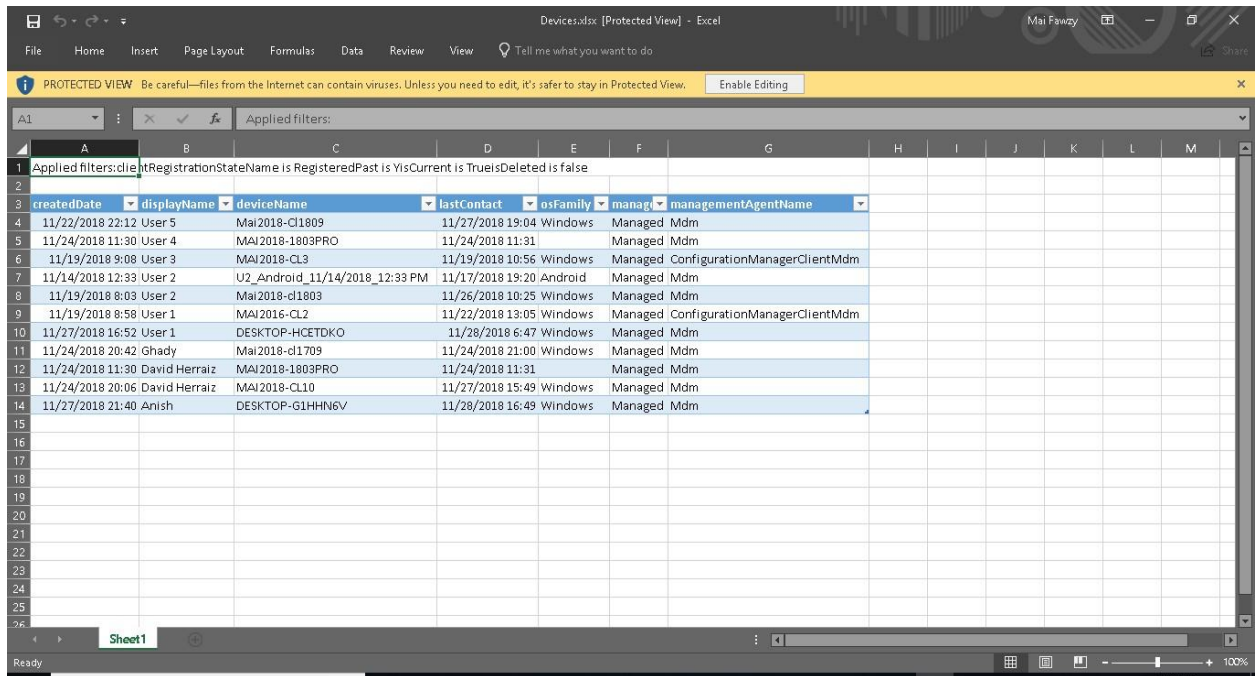


4. Your browser will prompt you to save the file.



5. Once saved, open the Excel file.

Microsoft Intune step by step on Azure portal



Applied filters: displayName is RegisteredPast is YesCurrent is TrueIsDeleted is false

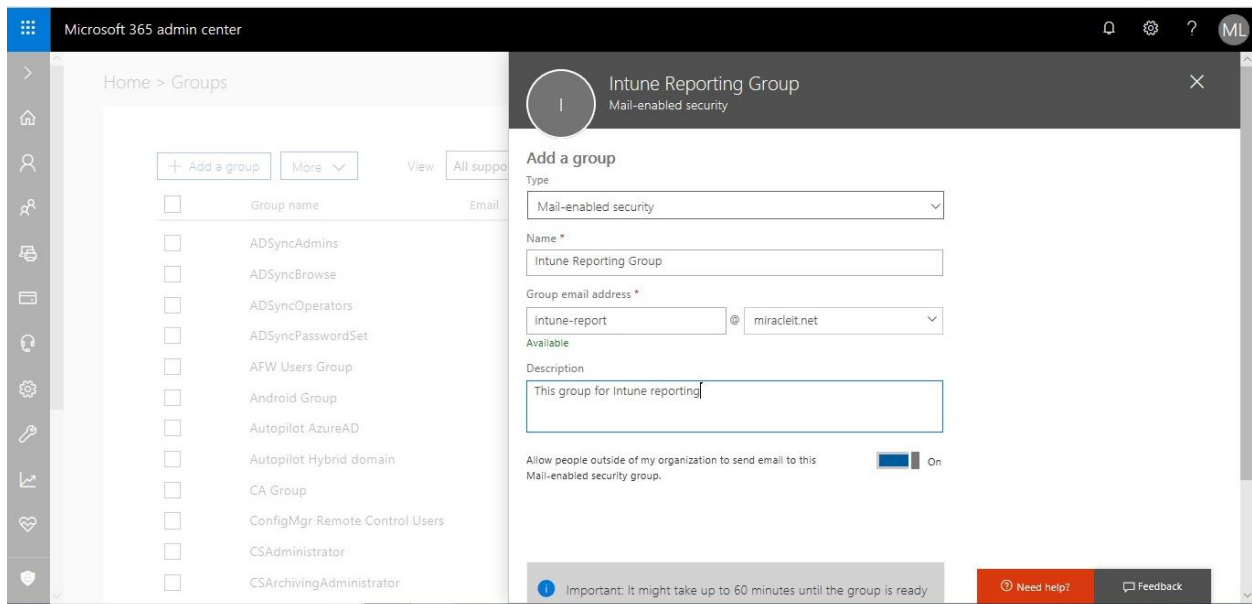
createdDate	displayName	deviceName	lastContact	osFamily	managementAgentName
11/22/2018 22:12	User 5	MAI2018-CL1809	11/27/2018 19:04	Windows	Managed Mdm
11/24/2018 11:30	User 4	MAI2018-1803PRO	11/24/2018 11:31	Managed	Mdm
11/19/2018 9:08	User 3	MAI2018-CL3	11/19/2018 10:56	Windows	Managed ConfigurationManagerClientMdm
11/14/2018 12:33	User 2	U2_Android_11/14/2018_12:33 PM	11/17/2018 19:20	Android	Managed Mdm
11/19/2018 8:03	User 2	MAI2018-cl1803	11/26/2018 10:25	Windows	Managed Mdm
11/19/2018 8:58	User 1	MAI2016-CL2	11/22/2018 13:05	Windows	Managed ConfigurationManagerClientMdm
11/27/2018 16:52	User 1	DESKTOP-HCETDKO	11/28/2018 6:47	Windows	Managed Mdm
11/24/2018 20:42	Ghady	MAI2018-cl1709	11/24/2018 21:00	Windows	Managed Mdm
11/24/2018 11:30	David Herraiz	MAI2018-1803PRO	11/24/2018 11:31	Managed	Mdm
11/24/2018 20:06	David Herraiz	MAI2018-CL10	11/27/2018 15:49	Windows	Managed Mdm
11/27/2018 21:40	Anish	DESKTOP-G1HHN6V	11/28/2018 16:49	Windows	Managed Mdm

You have multiple method to export Intune Report on files or publish it on SharePoint.

Share and collaborate with colleagues in Power BI

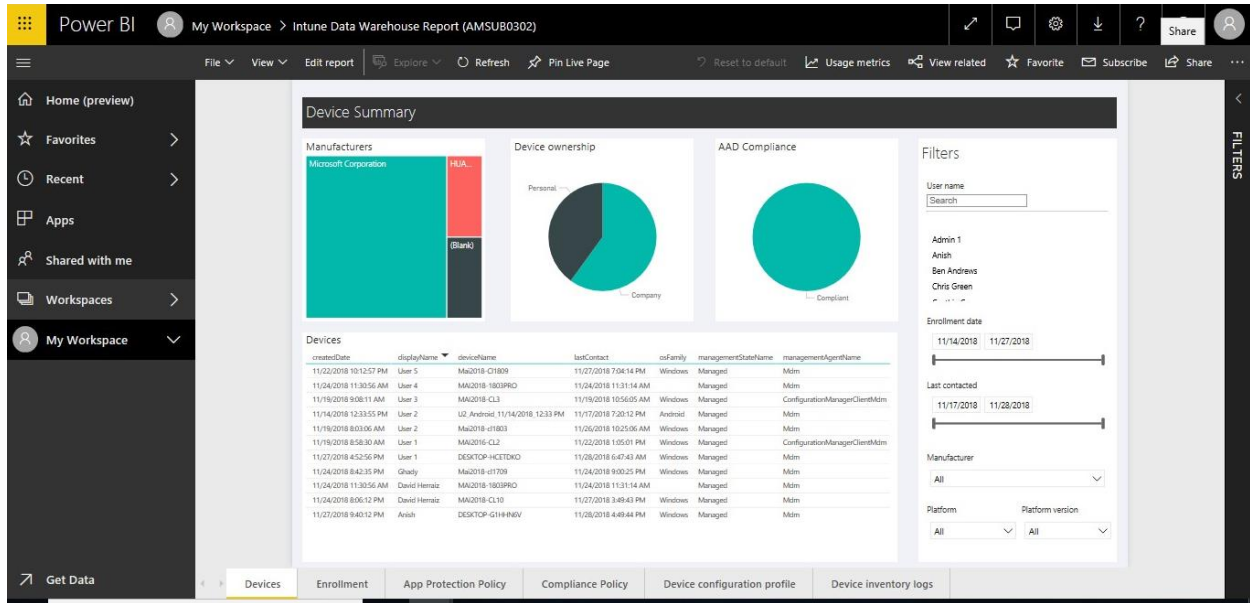
We cover the various ways Power BI offers for sharing and collaborating with your colleagues on your dashboards, reports, and data. we start by creating a *group*. A **group** defines a set of users who have access to specific dashboards, reports, and data.

You can security group or Mail-enabled security group and share Power BI report with them.



Microsoft Intune step by step on Azure portal

In Power BI service, select report or dashboard that you want to share with your colleagues > select **Share**.

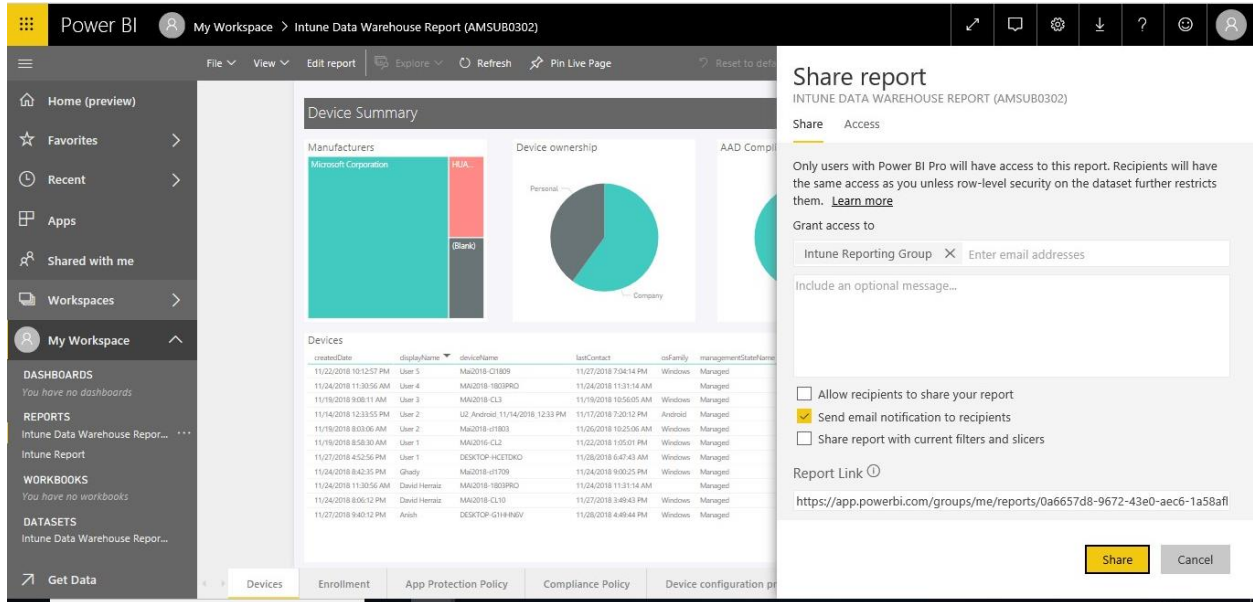


Type email for your colleague and Click **Share**.

The screenshot shows the 'Share report' dialog box for the 'Device Summary' report. The dialog box has a title bar 'Share report' and a subtitle 'INTUNE DATA WAREHOUSE REPORT (AMSUB0302)'. It has two tabs: 'Share' and 'Access'. The 'Share' tab is active. The dialog box contains the following text: 'Only users with Power BI Pro will have access to this report. Recipients will have the same access as you unless row-level security on the dataset further restricts them. [Learn more](#)'. Below this is a section 'Grant access to' with a search box containing 'David Herratz' and a placeholder 'Enter email addresses'. Below the search box is a text area containing 'This is Report for MDM Devices'. At the bottom of the dialog box, there are two checkboxes: 'Allow recipients to share your report' (checked) and 'Send email notification to recipients' (checked). Below the checkboxes is a 'Report Link' section with a URL: 'https://app.powerbi.com/groups/me/reports/0a6657d8-9672-43e0-aec6-1a58afi'. At the bottom right of the dialog box, there are two buttons: 'Share' and 'Cancel'.

If you want to expand My Workspace, you can share it with specific Group > select **Share**. Type email for Mail-enabled Security Group and Click **Share**.

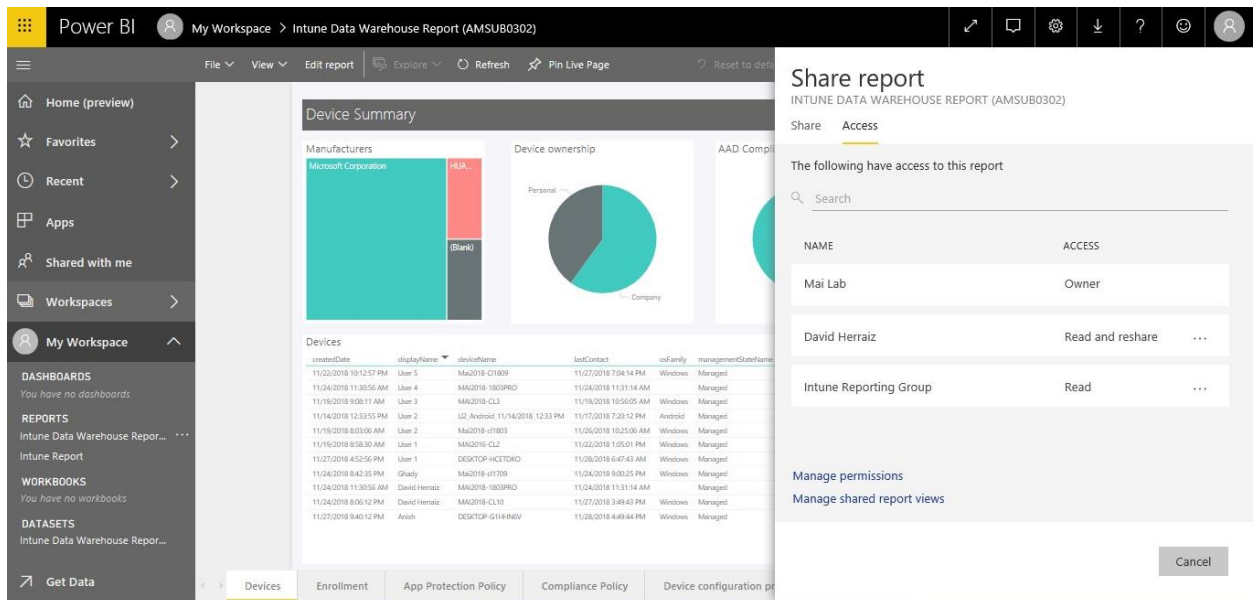
Microsoft Intune step by step on Azure portal



The screenshot shows the Power BI interface with a report titled "Device Summary" (INTUNE DATA WAREHOUSE REPORT (AMSUB0302)). The report displays two charts: "Manufacturers" (a bar chart showing Microsoft Corporation and HUAWEI) and "Device ownership" (a pie chart showing Personal and Company). Below the charts is a table of devices with columns for createDate, displayName, deviceIdName, lastContact, osFamily, and managementStateName.

The "Share report" dialog is open, showing the "Share" tab. It includes a "Grant access to" field with "Intune Reporting Group" selected, a "Share" button, and a "Cancel" button. The "Report Link" is displayed as <https://app.powerbi.com/groups/me/reports/0a6657d8-9672-43e0-aec6-1a58af1>.

To check that report already read by other user, Click on **Share > Access**. You will find all users who access this report.



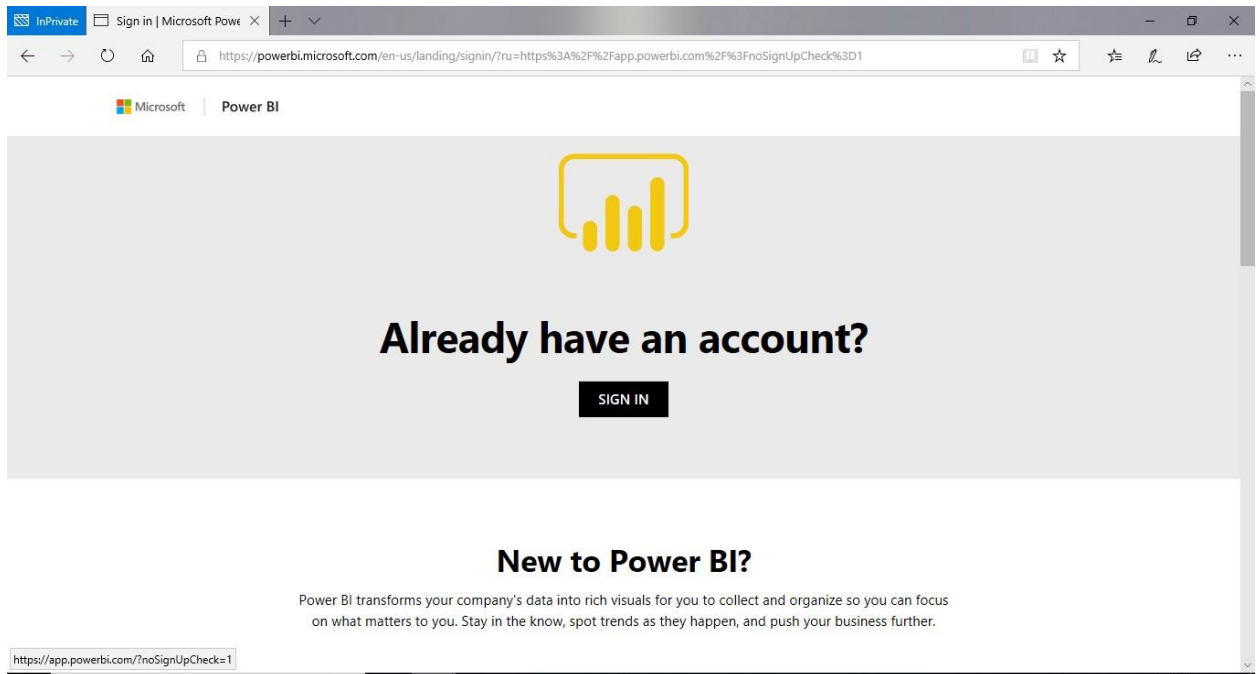
The screenshot shows the Power BI interface with the "Device Summary" report. The "Share report" dialog is open, showing the "Access" tab. It displays a list of users with access to the report:

NAME	ACCESS
Mai Lab	Owner
David Herraiz	Read and reshare
Intune Reporting Group	Read

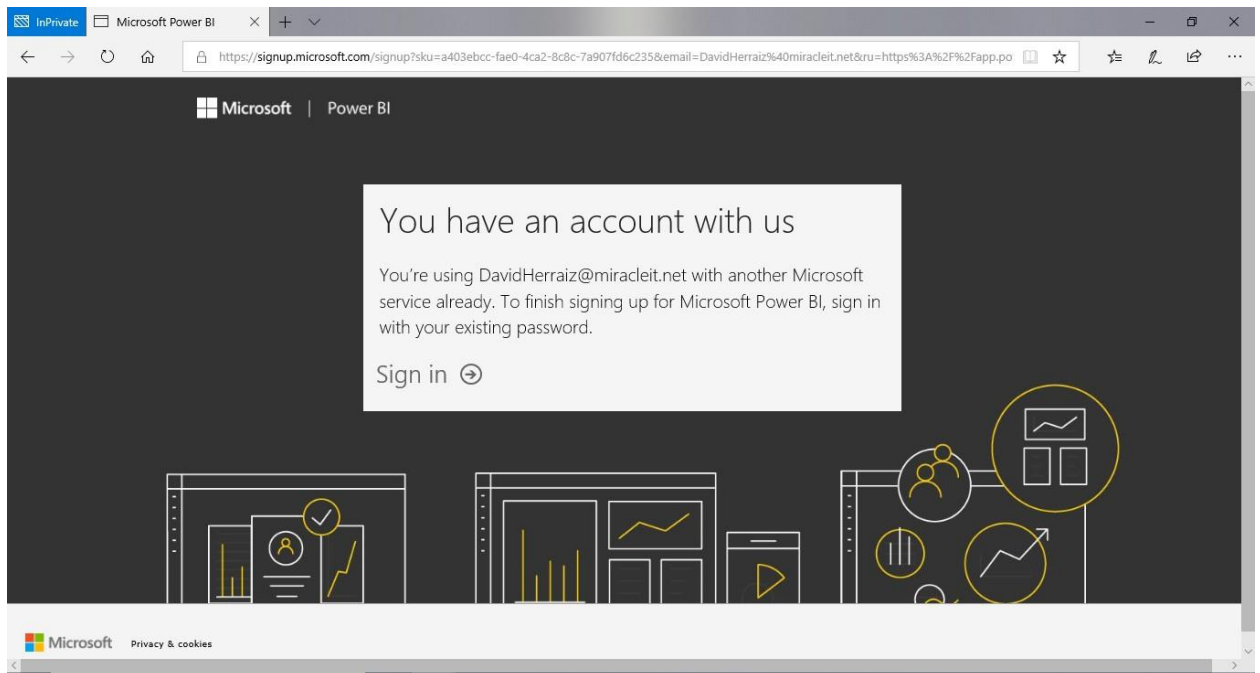
Below the list are options for "Manage permissions" and "Manage shared report views". A "Cancel" button is at the bottom right.

To view report from end user, you need to follow below steps:

1. Login to **Power BI** from one of those users "https://app.powerbi.com".

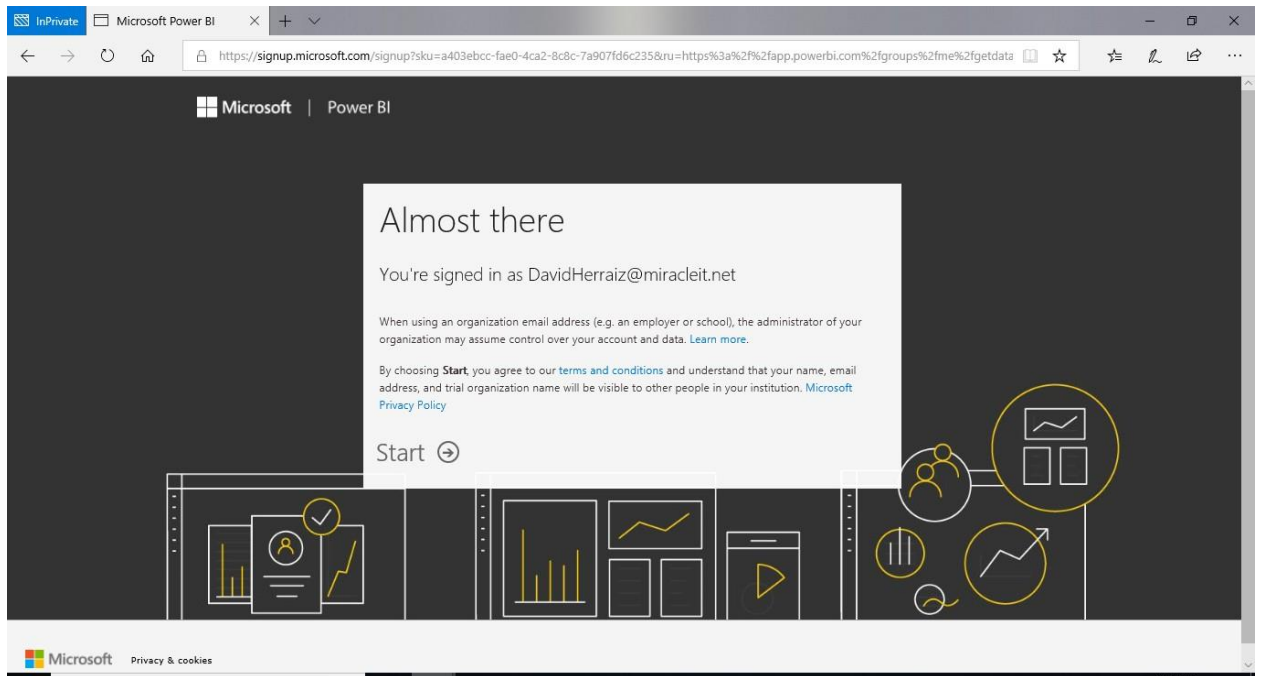


2. Click **Sign In**. Enter credential
3. If This is first time to use Power BI, it will pop up message to finish Sign up once you sign in on power BI site. Click **Sign In**.

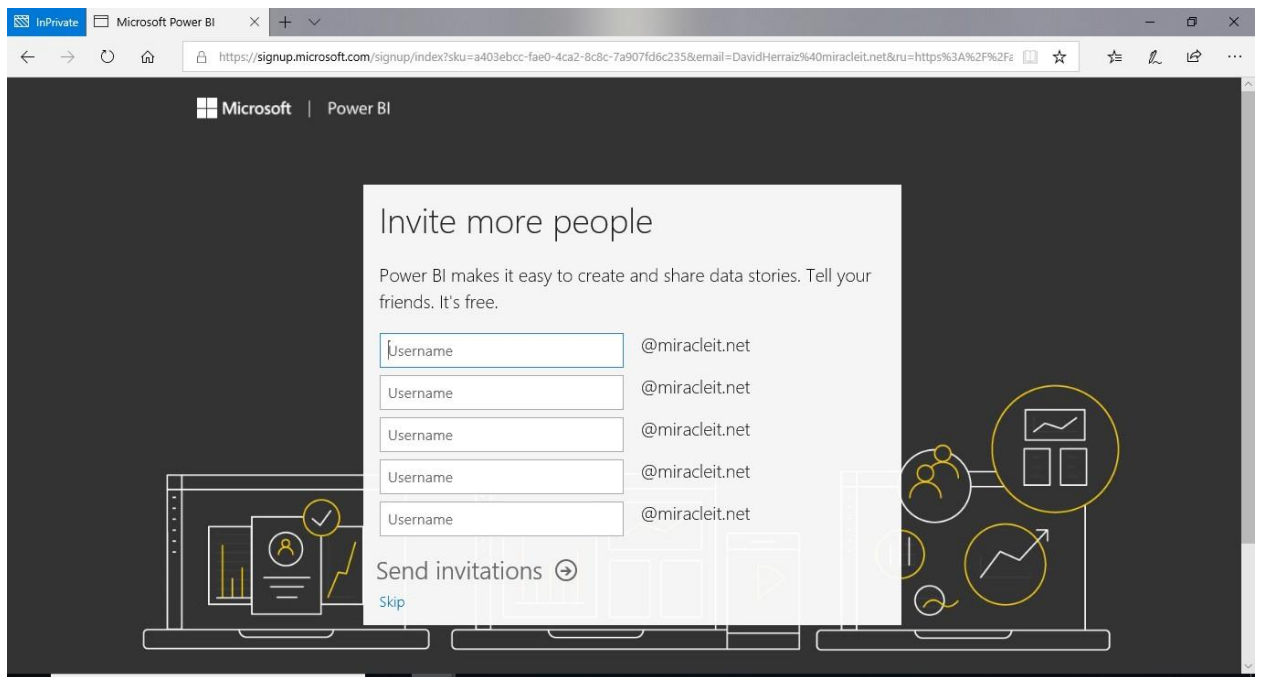


4. Click **Start**.

Microsoft Intune step by step on Azure portal

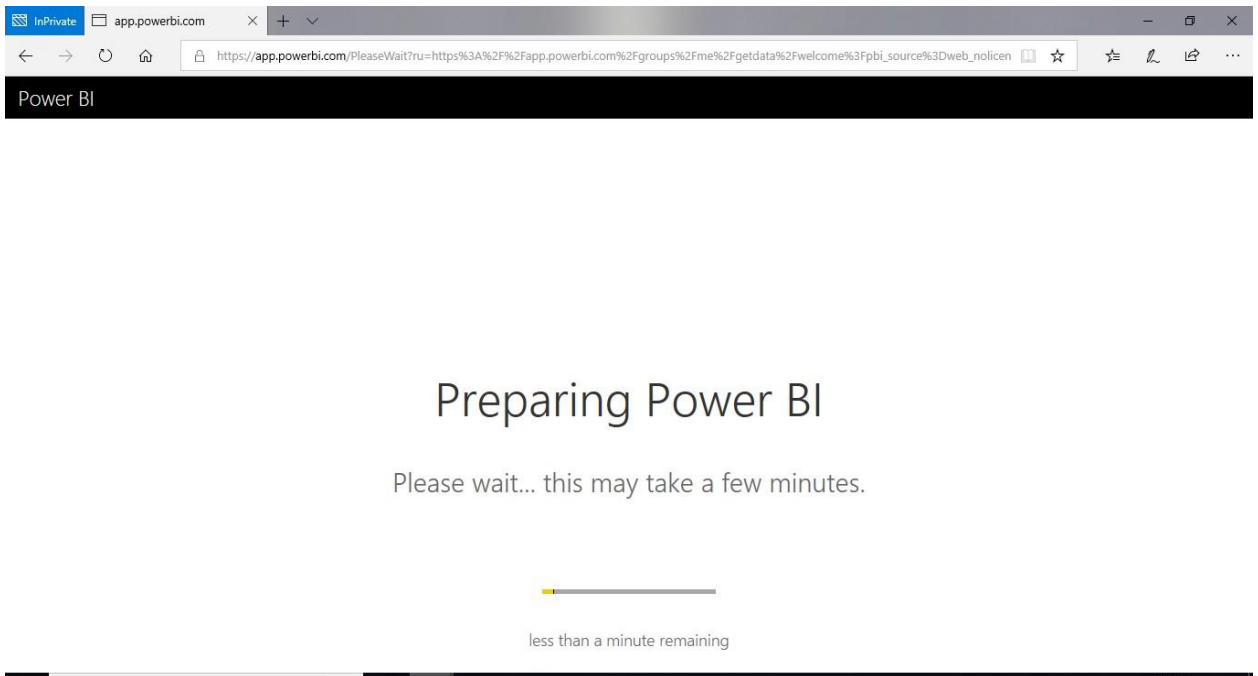


5. Click **Skip** for invite more users.

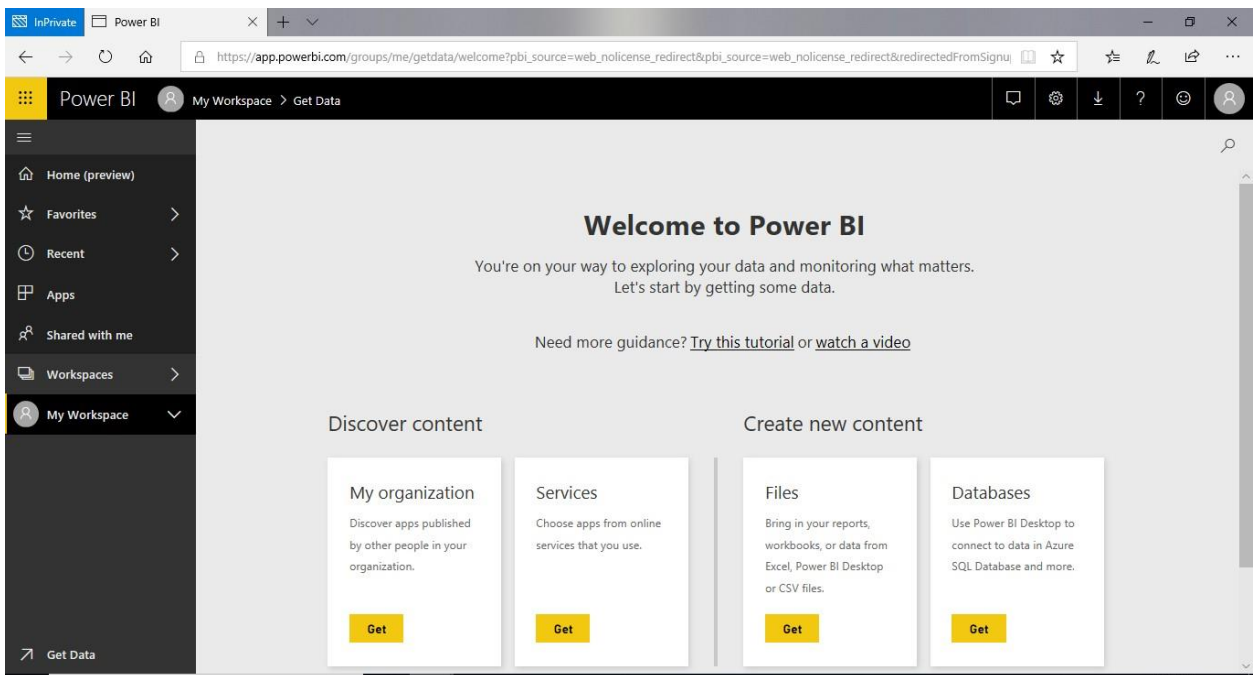


6. Now start preparing Power BI.

Microsoft Intune step by step on Azure portal

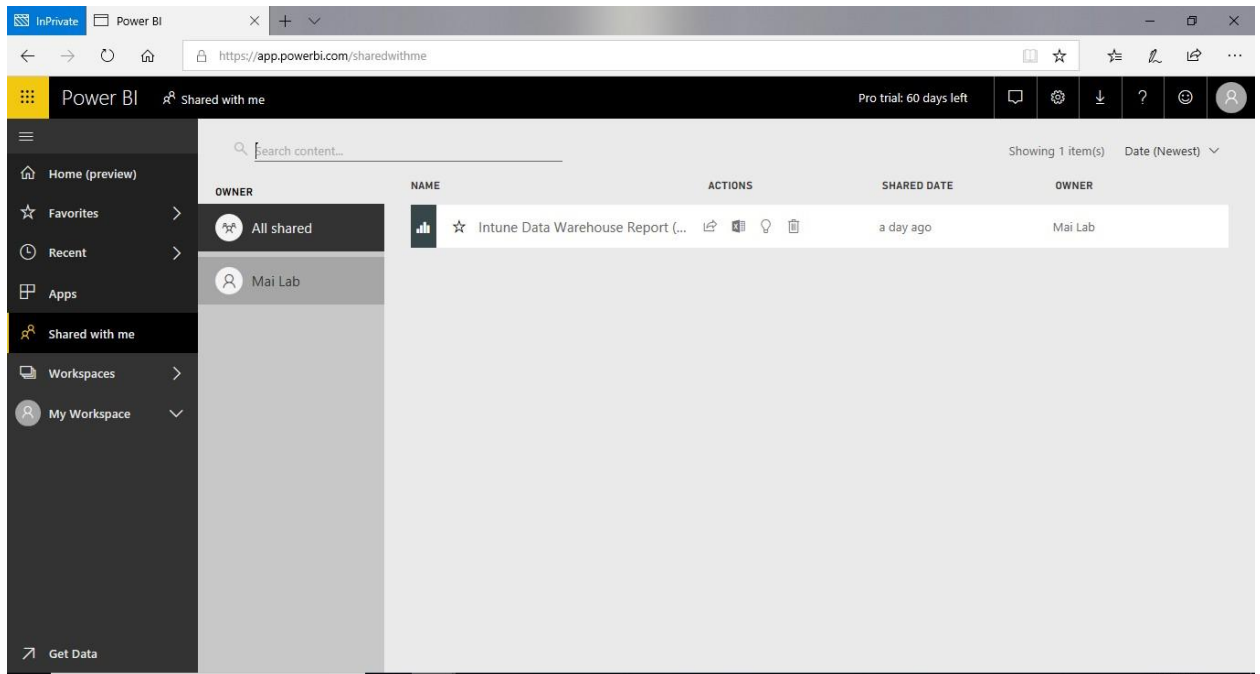


7. On Power BI console, Click **Shared with me**.



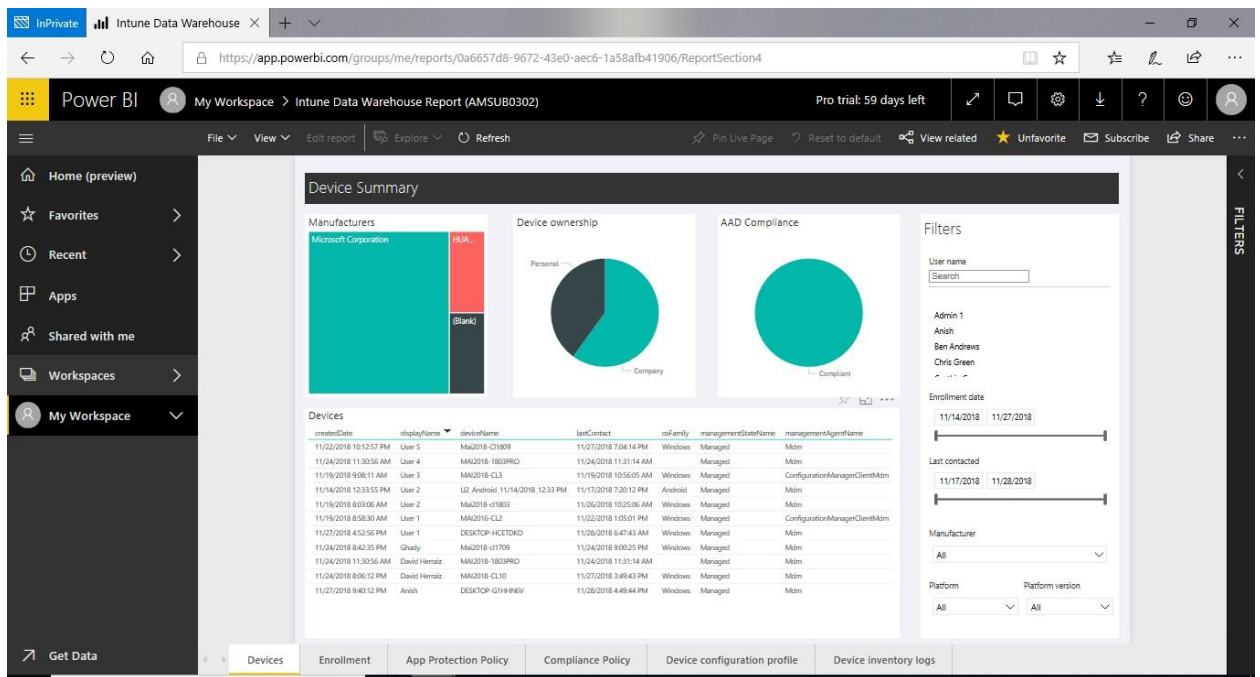
8. On Shared with me blade, you will find all reports share to you. You can select star to add it to favorite.

Microsoft Intune step by step on Azure portal



Note: you need to have license Power BI Pro to access Power BI reports.

9. You can open this report.



Intune APIs in Microsoft Graph

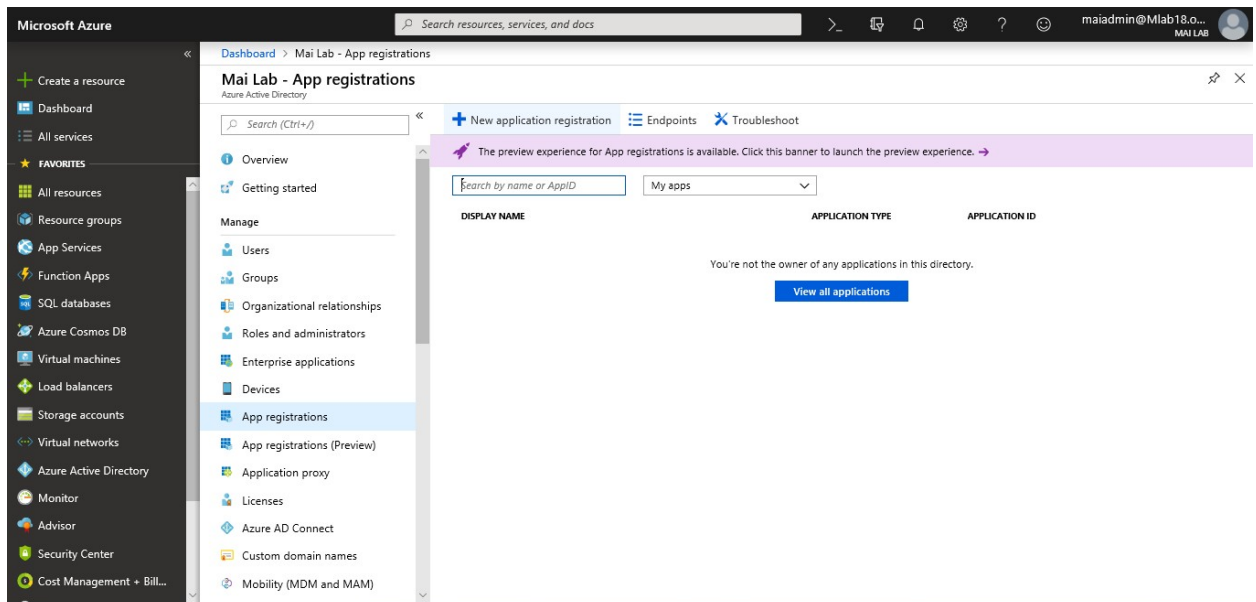
The Microsoft Graph Security API enables managing security alerts from all Microsoft security products, known as Microsoft Graph Security providers, through a single REST endpoint. Some organizations may already ingest Azure-specific log data through Azure Monitor into SIEM

solutions. To simplify integration, the security alerts available through the Microsoft Graph Security API can also be provisioned by the customer to their subscription via Azure Monitor. Intune APIs in Microsoft Graph can also provide detailed user, device, and application information to other IT asset management systems. You could build custom experiences which call Microsoft Graph to configure Intune controls and policies and unify workflows across multiple services.

To configure integration between Intune & Graph API, you need to follow below steps:

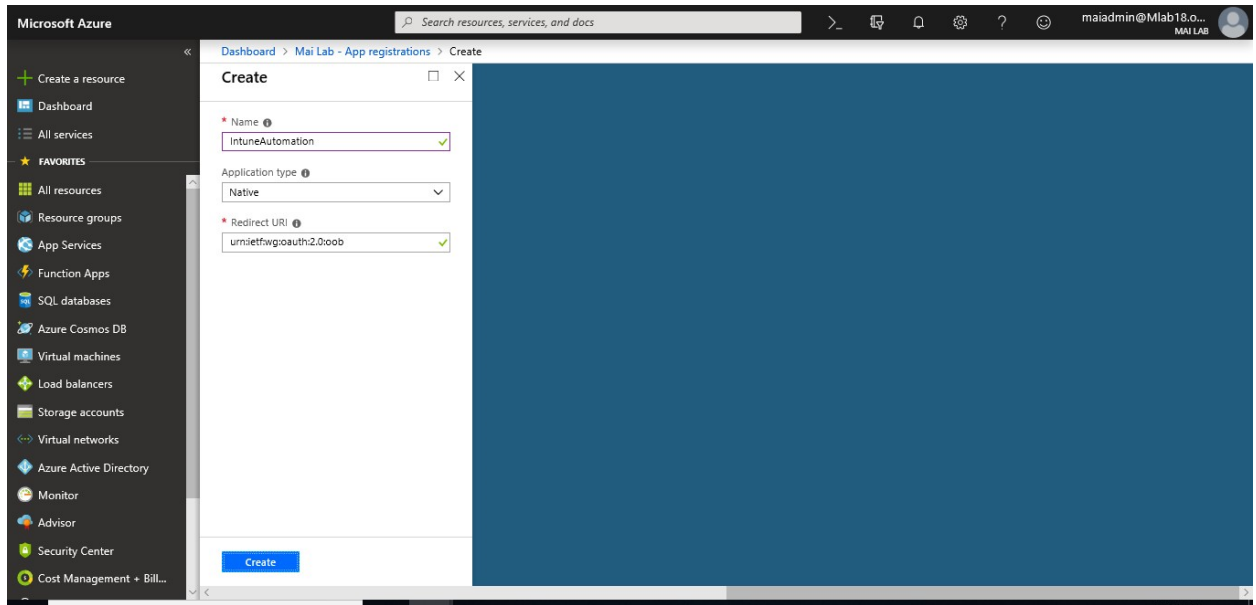
Step 1: Register Native App. In Azure AD

1. Sign into the [Azure portal](#) using administrative credentials.
2. From the menu, choose **Azure Active Directory** > **App Registrations**.



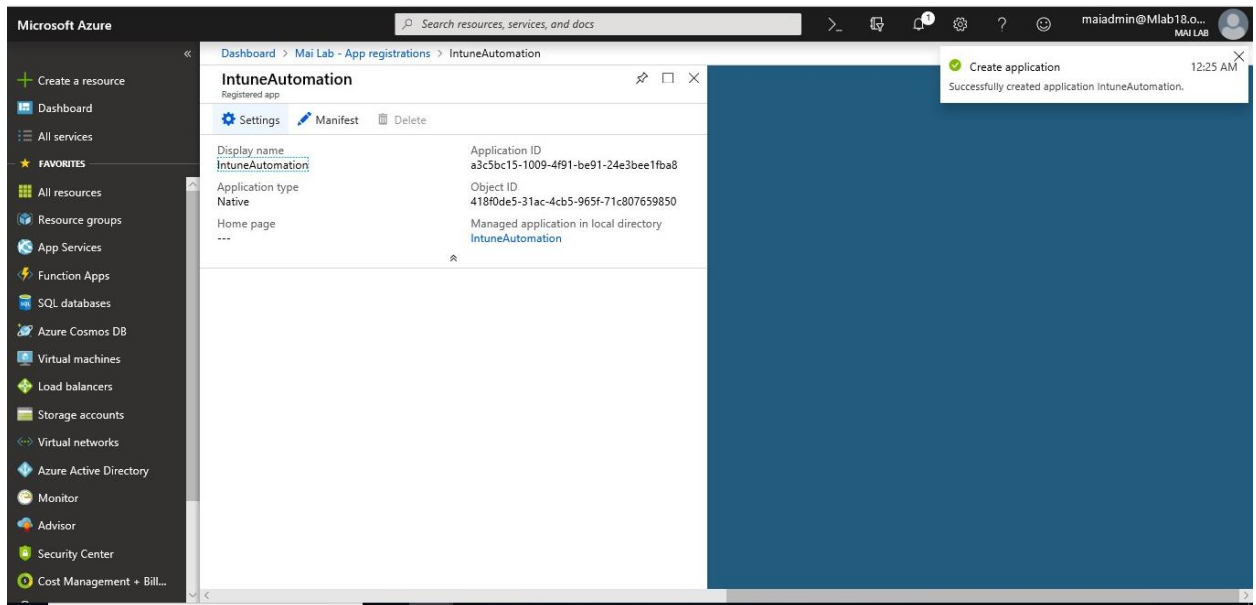
3. Either choose **New application registration** to create a new application or choose an existing application. (If you choose an existing application, skip the next step.)
4. On the **Create** blade, specify the following:
 - A **Name** for the application (displayed when users sign in).
 - The **Application type** and **Redirect URI** values. These vary according to your requirements. For example, if you're using an Azure AD Authentication Library (ADAL), set **Application Type** to Native and **Redirect URI** to **urn:ietf:wg:oauth:2.0:oob**.

Microsoft Intune step by step on Azure portal



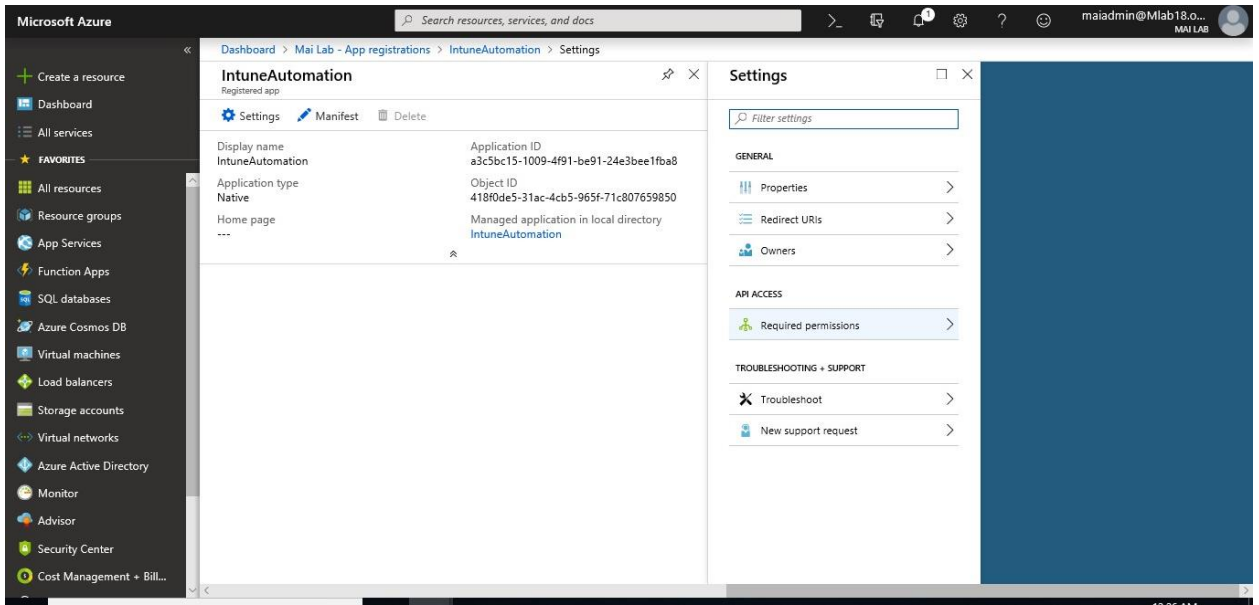
Step 2: Assign permissions to the registered application

1. From the application blade: Choose **Settings**

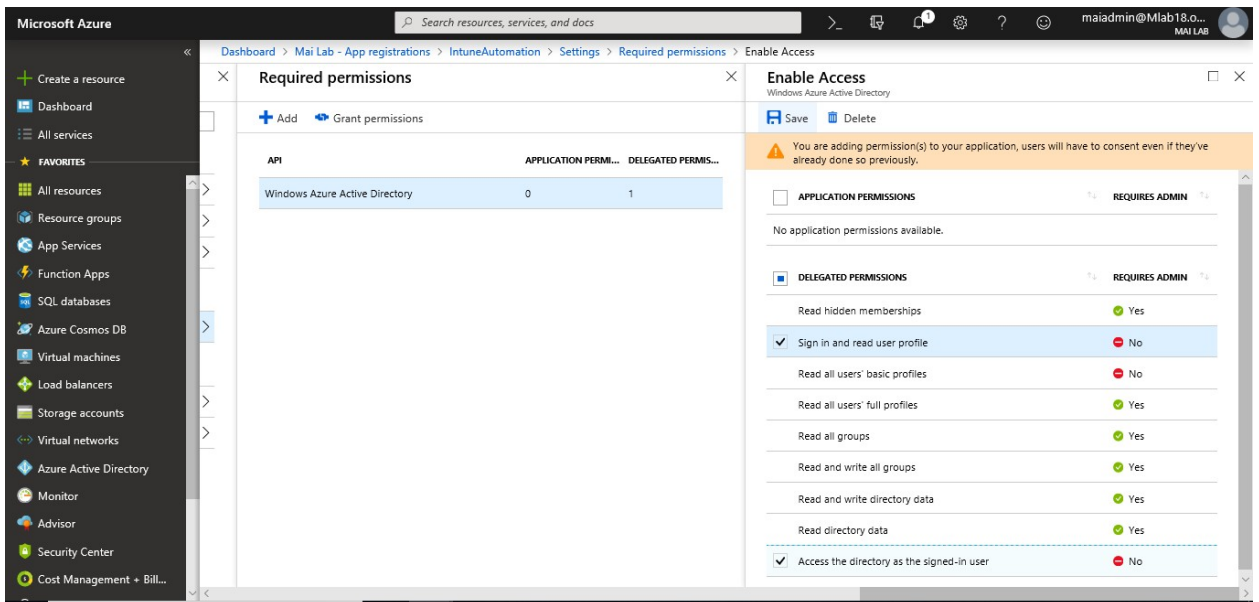


2. Choose **Settings** > **API access** > **Required permissions**.

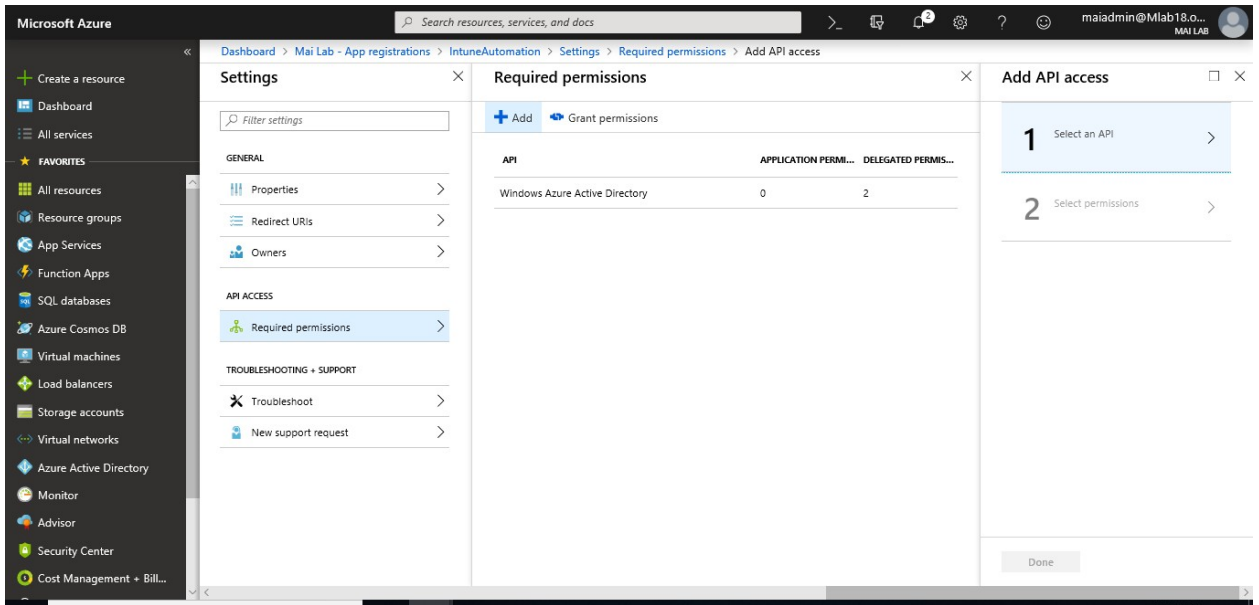
Microsoft Intune step by step on Azure portal



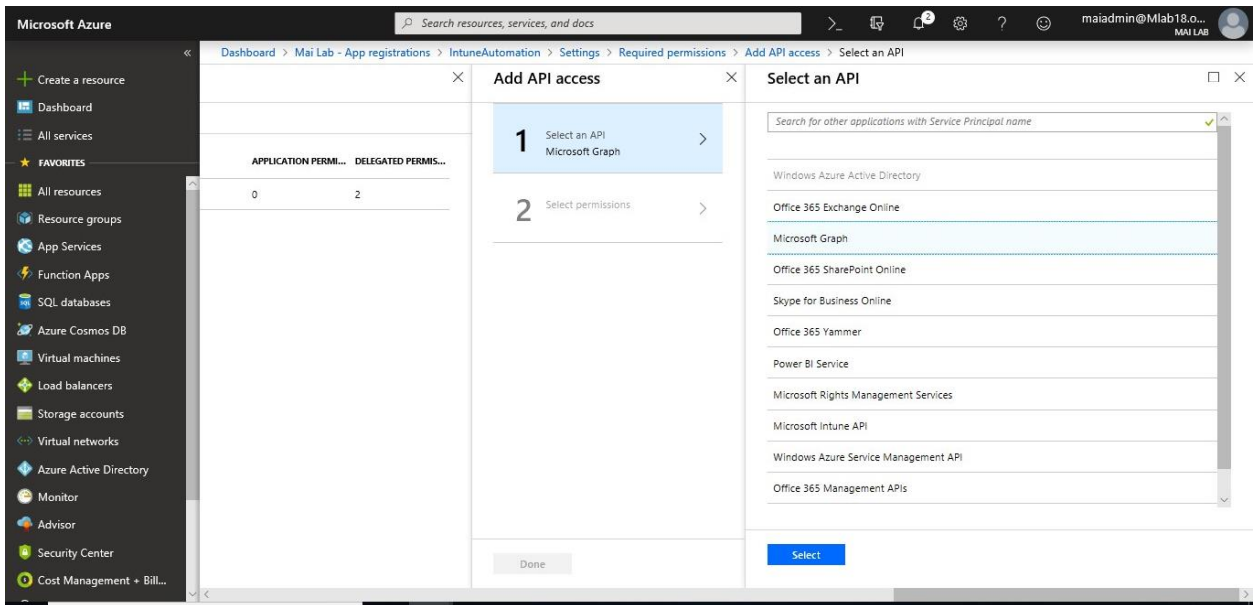
3. From the **Required Permissions** blade, Select **Windows Azure Active Directory** > Select **Access the directory as the signed-in user**.



4. From the **Required Permissions** blade, choose **Add** > **Add API access** > **Select an API**.



5. From the **Select an API** blade, choose **Microsoft Graph** > **Select**.

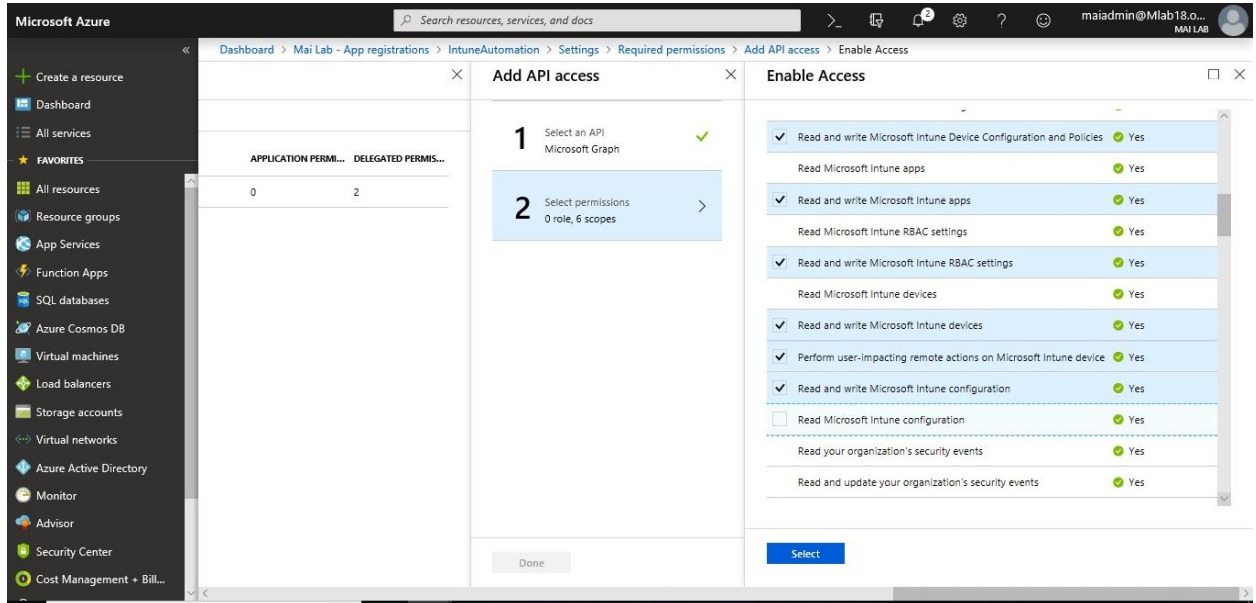


6. The **Enable access** blade opens and [lists permission scopes for GraphApi](#) available to your application. Microsoft Intune PowerShell needs permission to:

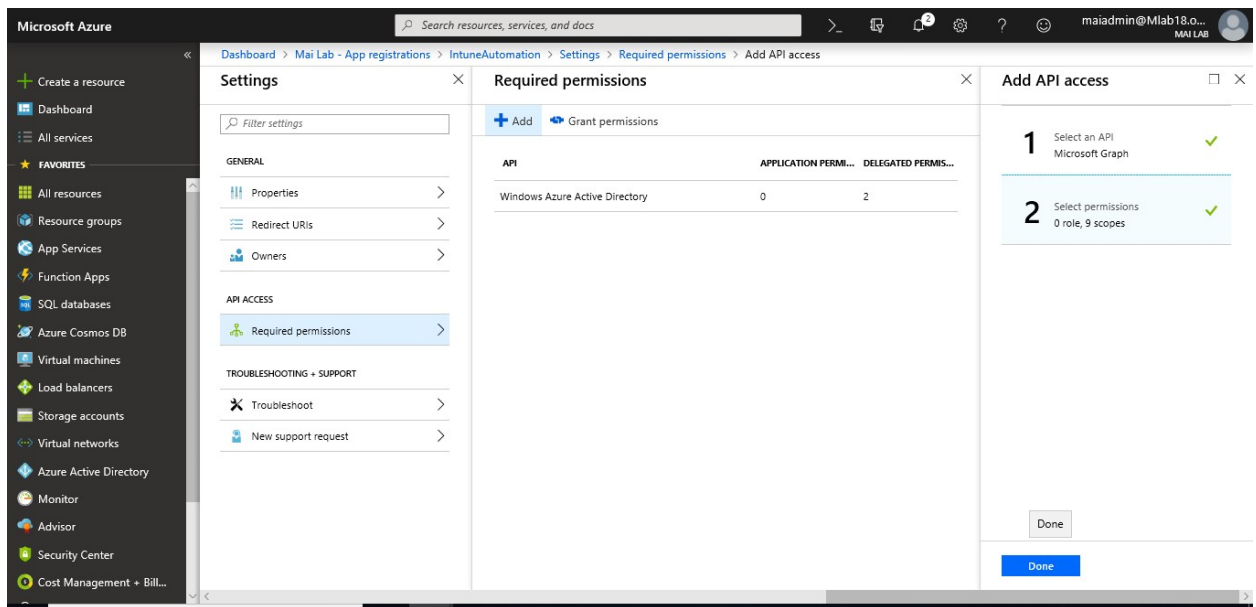
- Sign you in and read your profile
- Read all groups
- Read directory data
- Read and write Microsoft Intune Device Configuration and Policies (preview)
- Read and write Microsoft Intune RBAC settings (preview)
- Perform user-impacting remote actions on Microsoft Intune devices (preview)
- Sign in as you

Microsoft Intune step by step on Azure portal

- Read and write Microsoft Intune devices (preview)
- Read and write all groups
- Read and write Microsoft Intune configuration (preview)
- Read and write Microsoft Intune apps (preview)



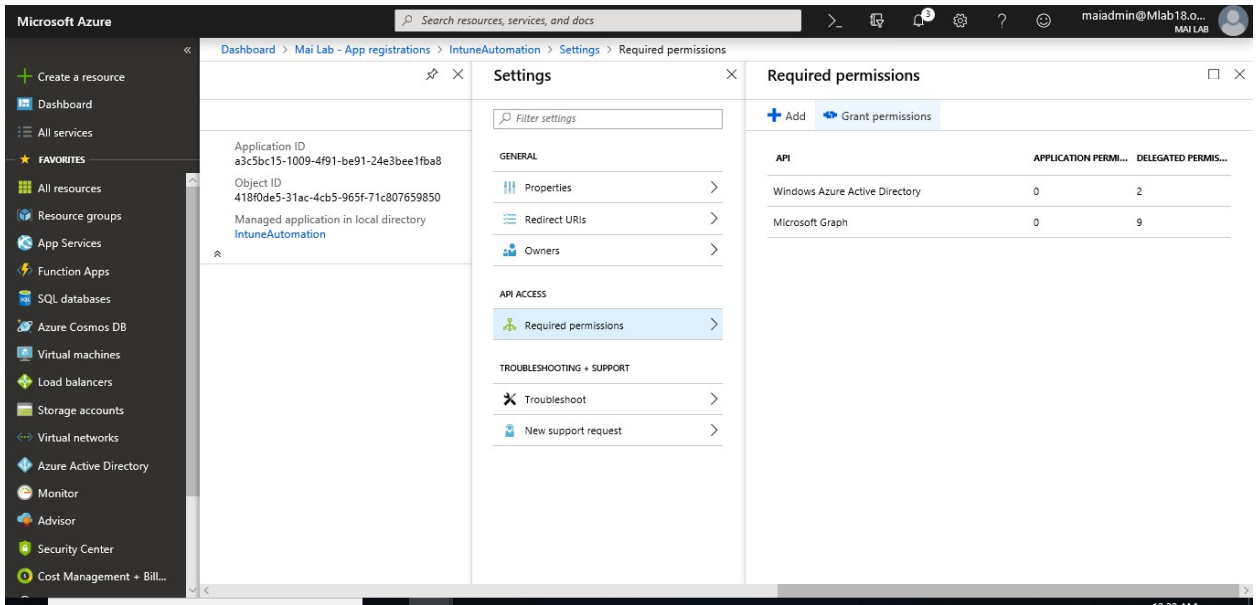
7. Click **Done** once you finished the Enable Access.



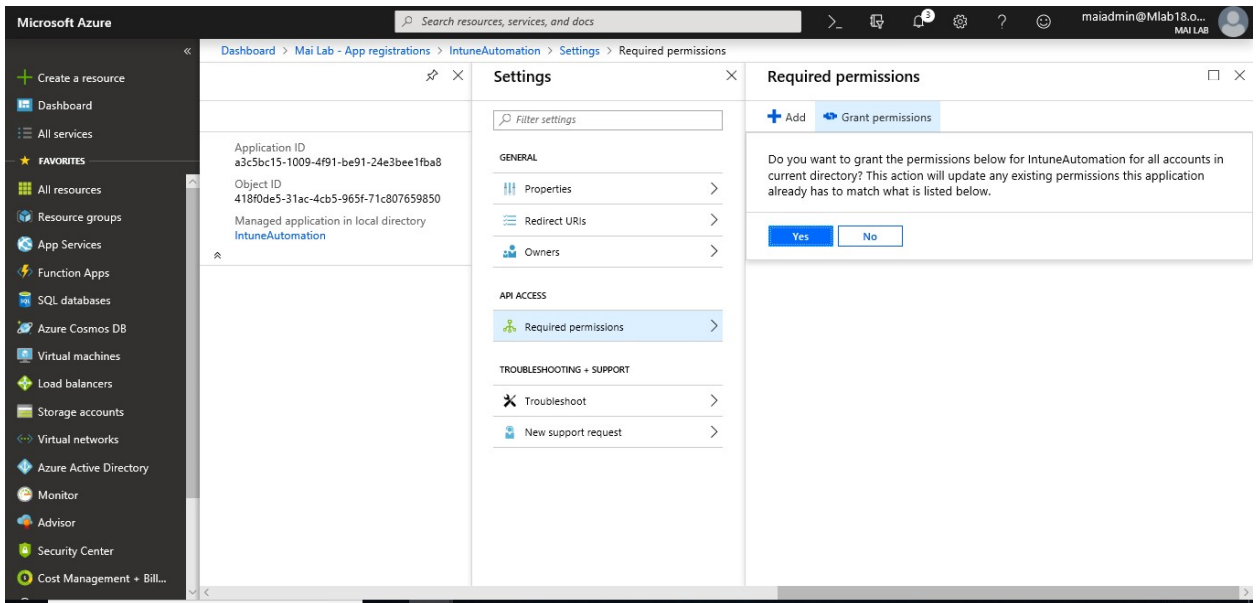
Step 3: Grant permissions to the registered application

- i. Choose to grant permission for all tenant accounts to use the app without providing credentials.

Microsoft Intune step by step on Azure portal



ii. To do so, choose **Grant permissions** and accept the confirmation prompt.



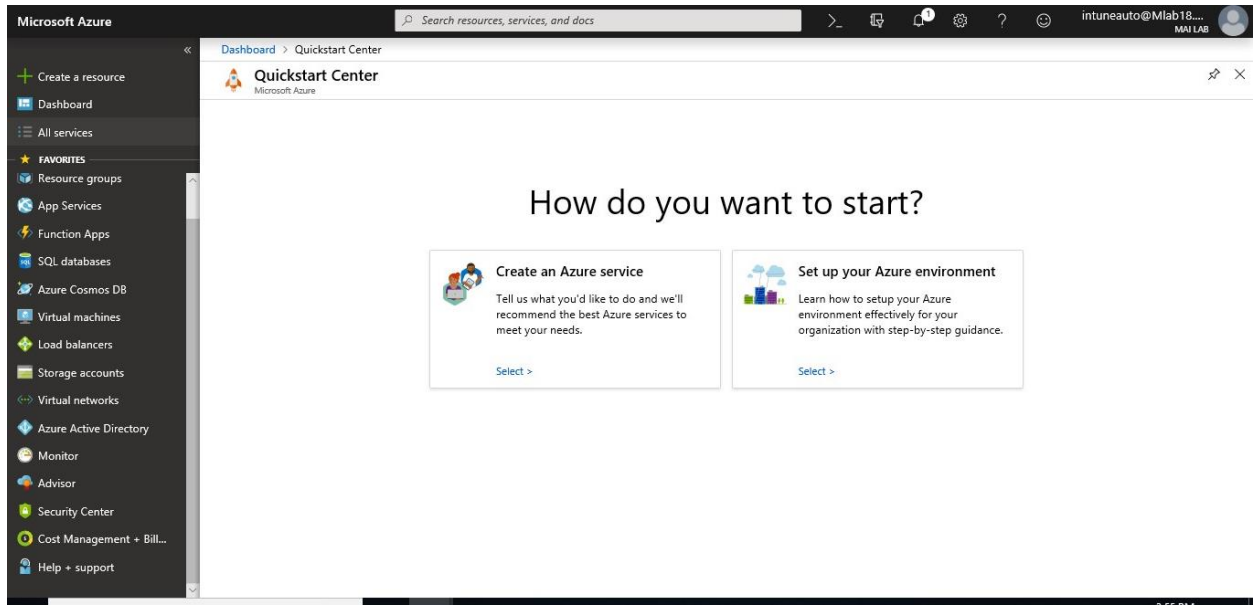
iii. When you run the application for the first time, you're prompted to grant the app permission to perform the selected roles.

Step 4: Create Azure Automation Account

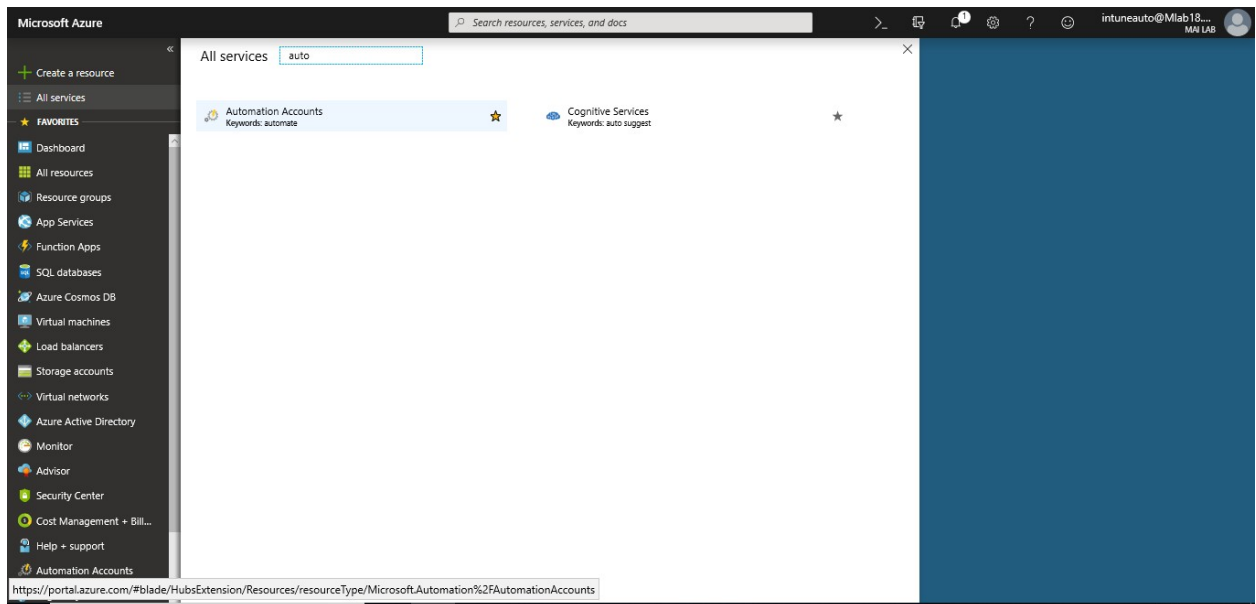
To create an Azure Automation account in the Azure portal, complete the following steps:

1. Sign in to the [Azure portal](#) with an account that's a member of the subscription Administrators role and a coadministrator of the subscription.
2. Select **+ Create a Resource**.

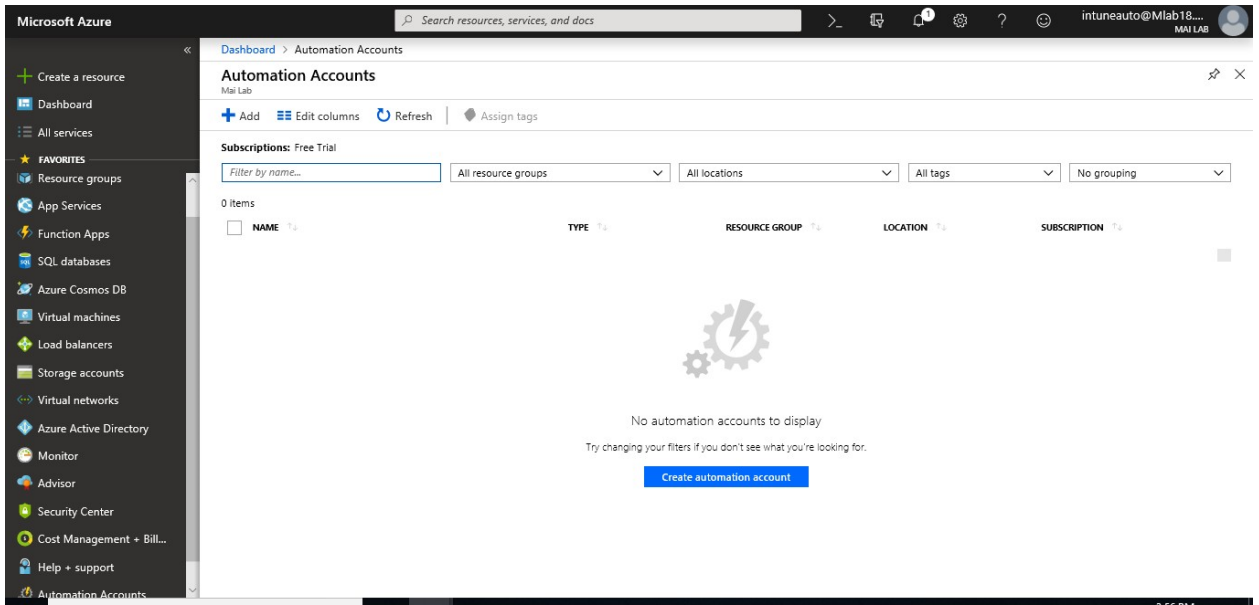
Microsoft Intune step by step on Azure portal



3. Search for **Automation**. In the search results, select **Automation Accounts**. Click on start to appear on favorite bar.

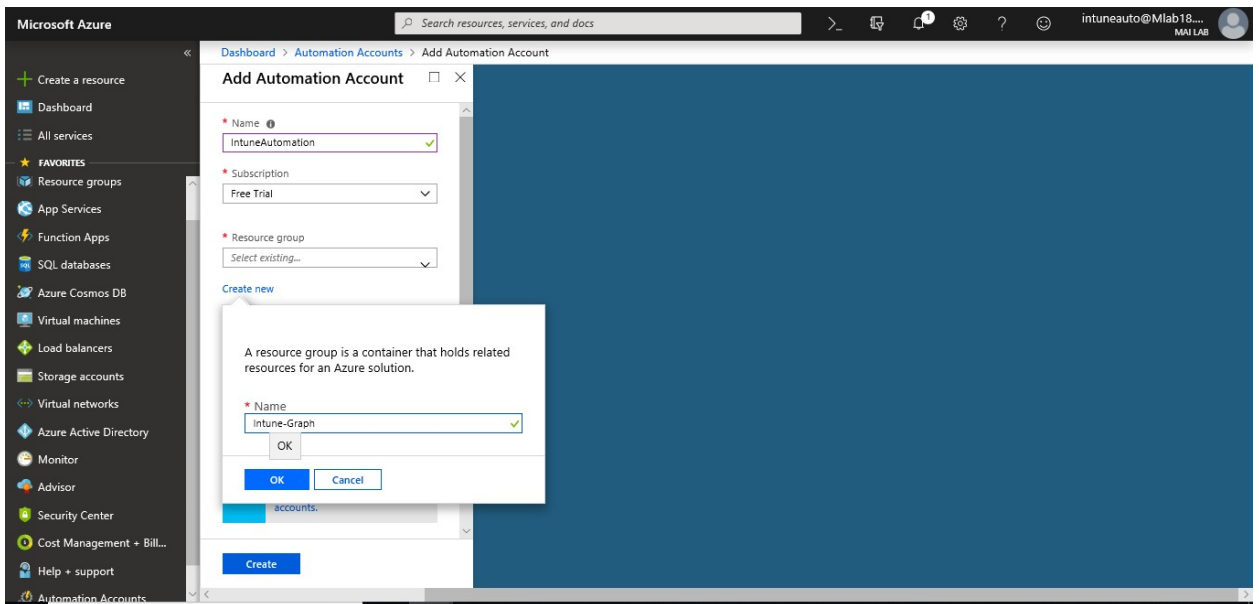


4. On the next screen select **Create**.



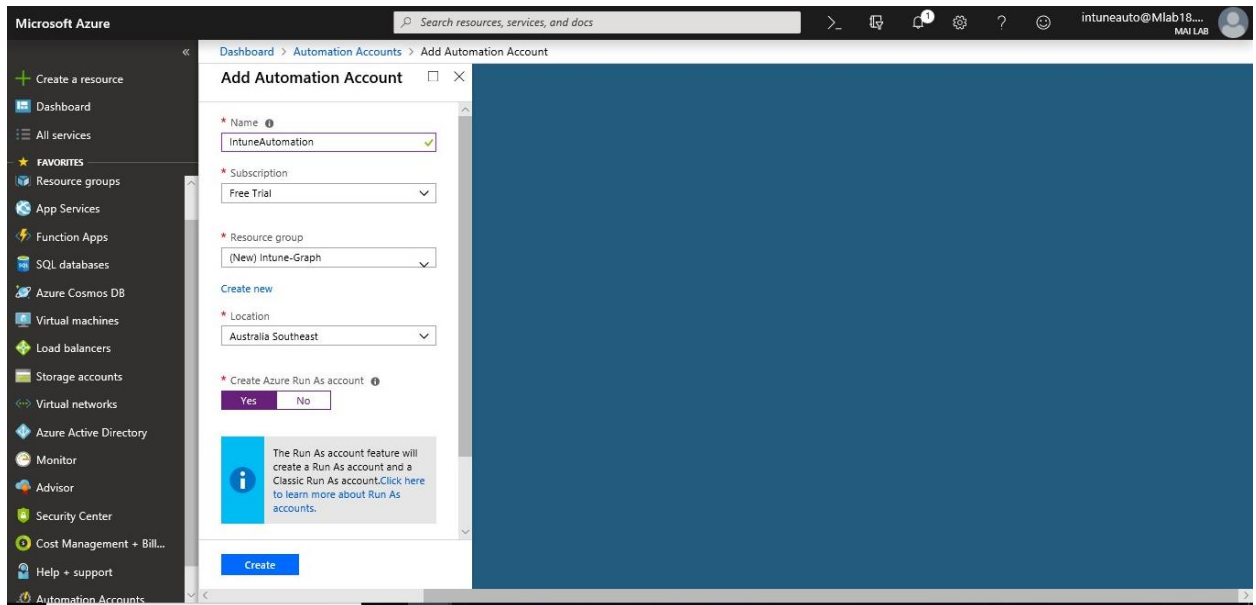
Note: To Add Automation Account, your account should be a member of the subscription Administrators role or a coadministrator of the subscription.

5. In the **Add Automation Account** pane, in the **Name** box, enter a name for your new Automation account. This name cannot be changed after it is chosen. **Automation Account names are unique per region and resource group.**



6. If you have more than one subscription, in the **Subscription** box, specify the subscription you want to use for the new account.
7. For **Resource group**, enter or select a new or existing resource group.
8. For **Location**, select an Azure datacenter location.

9. For the **Create Azure Run As account** option, ensure that **Yes** is selected, and then select **Create**.



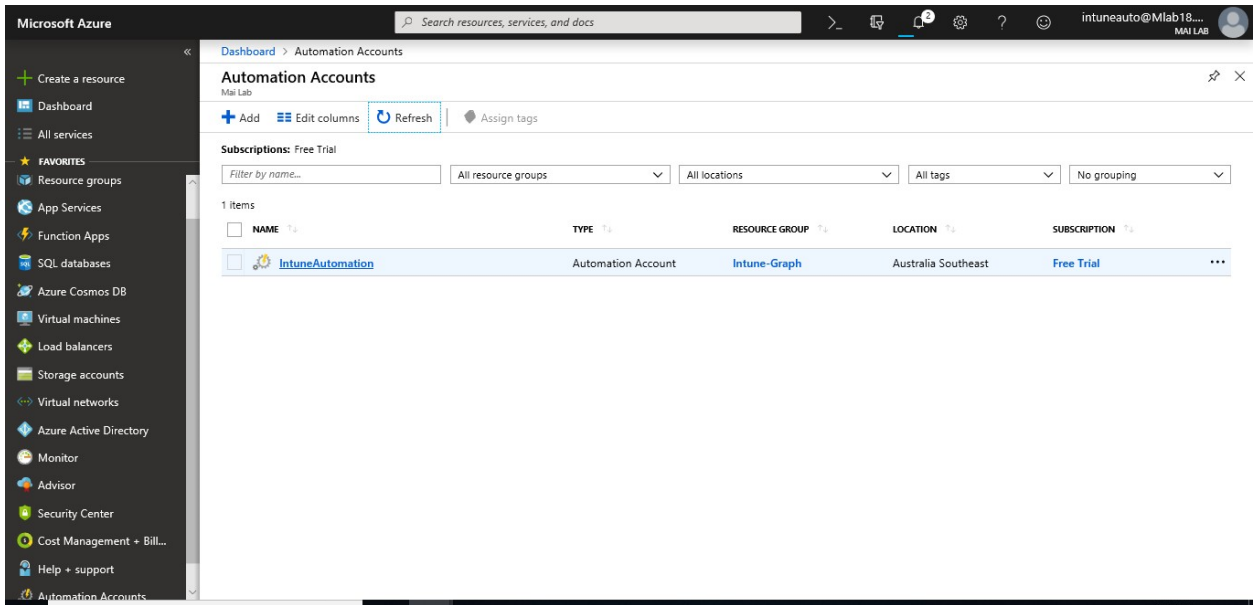
Note: If you choose not to create the Run As account by selecting **No** for **Create Azure Run As account**. Although the account is created in the Azure portal, the account doesn't have a corresponding authentication identity in your classic deployment model subscription or in the Azure Resource Manager subscription directory service. Therefore, the Automation account doesn't have access to resources in your subscription. This prevents any runbooks that reference this account from being able to authenticate and perform tasks against resources in those deployment models. When the service principal is not created, the Contributor role is not assigned.

Step 5: Import PSIntuneAuth & Azure AD module to the Azure Automation Account

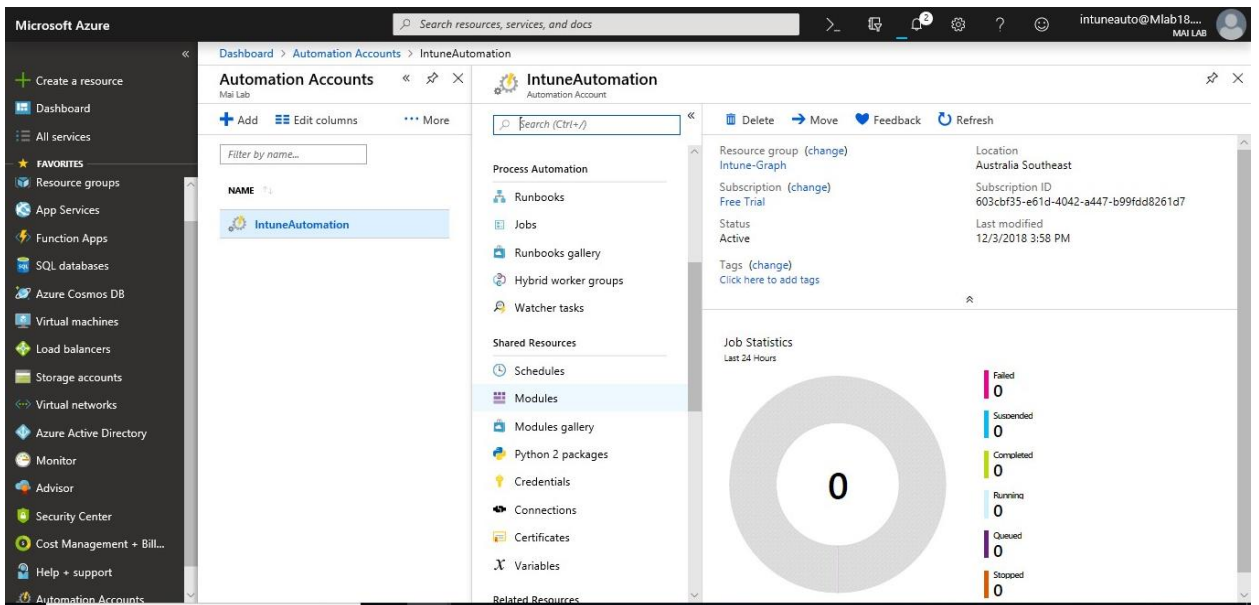
To import a module from the Automation Module Gallery with the Azure portal

1. In the [Azure portal](#), Select **All Service**, select **Automation Accounts**.
2. On **Automation accounts** blade, open your Automation account.

Microsoft Intune step by step on Azure portal

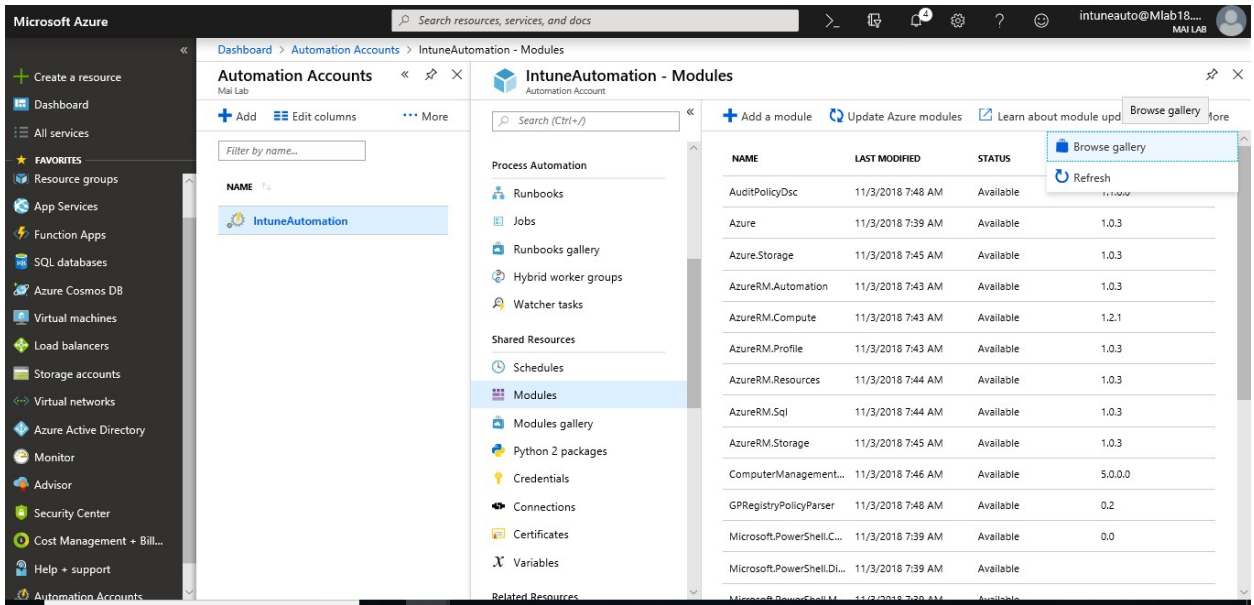


3. On your Automation account, Select **Modules** under **Shared Resources** to open the list of modules.

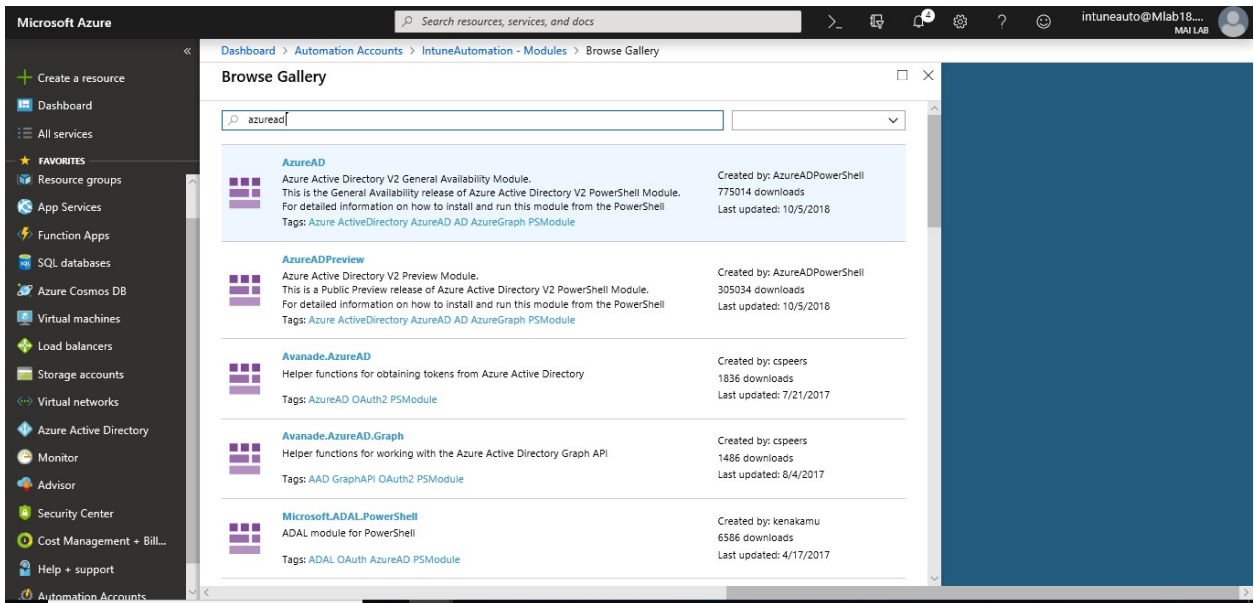


4. Click on **More (...)** > Click **Browse gallery** from the top of the page.

Microsoft Intune step by step on Azure portal

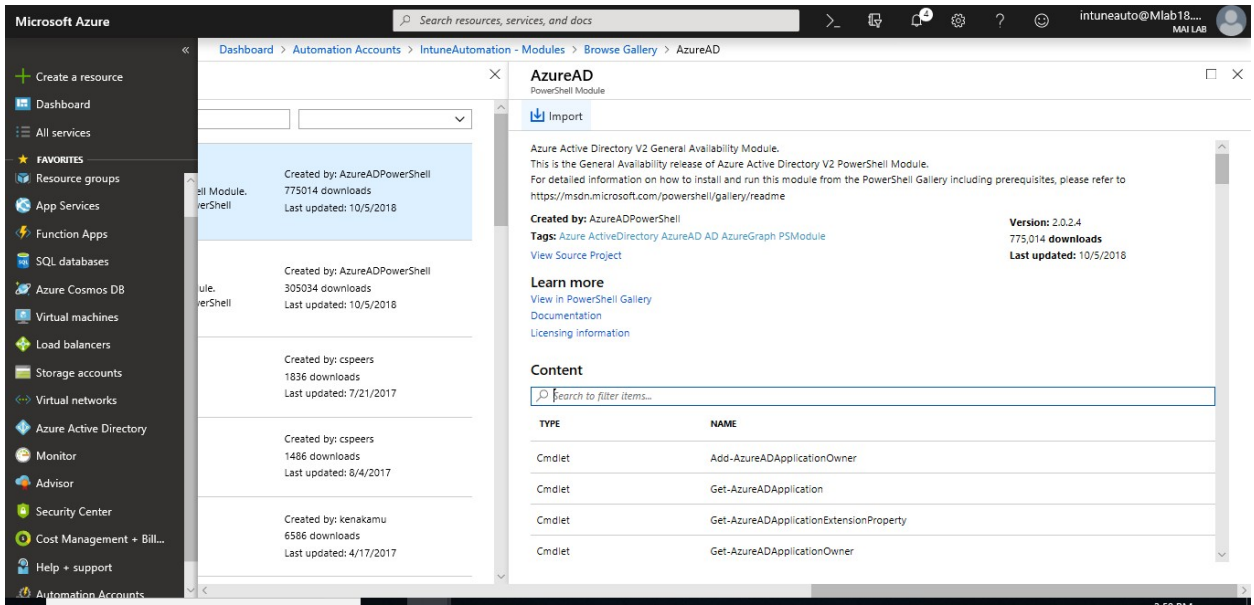


5. On the **Browse gallery** page, type on search **AzureAD**.

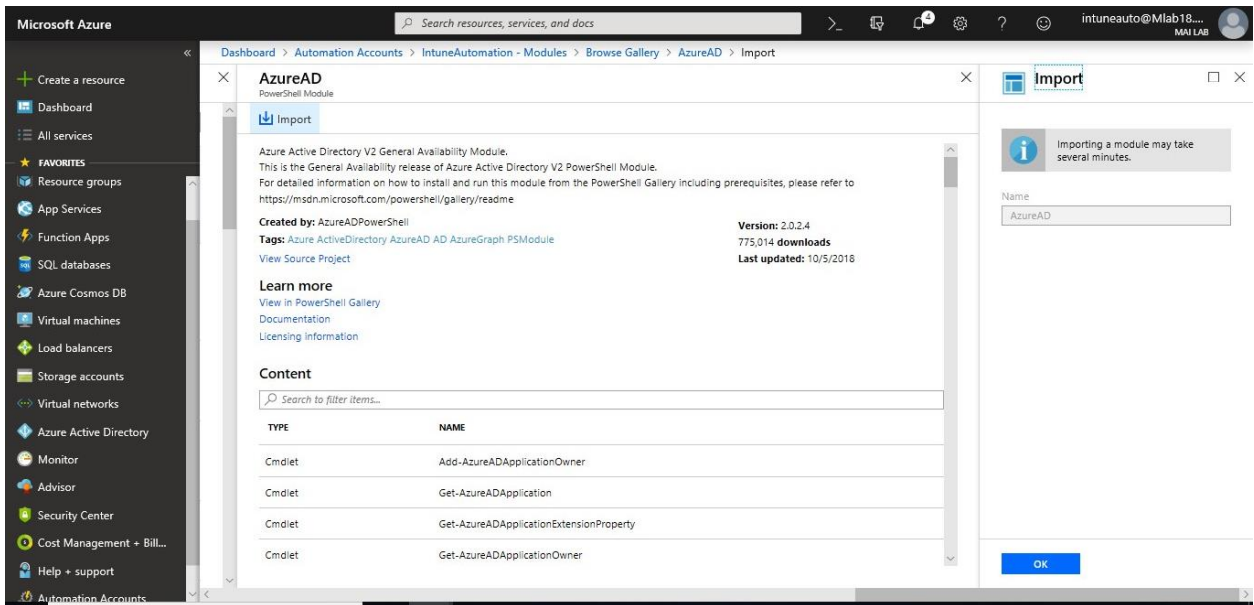


6. To install the module directly into Azure Automation, click the **Import** button.

Microsoft Intune step by step on Azure portal

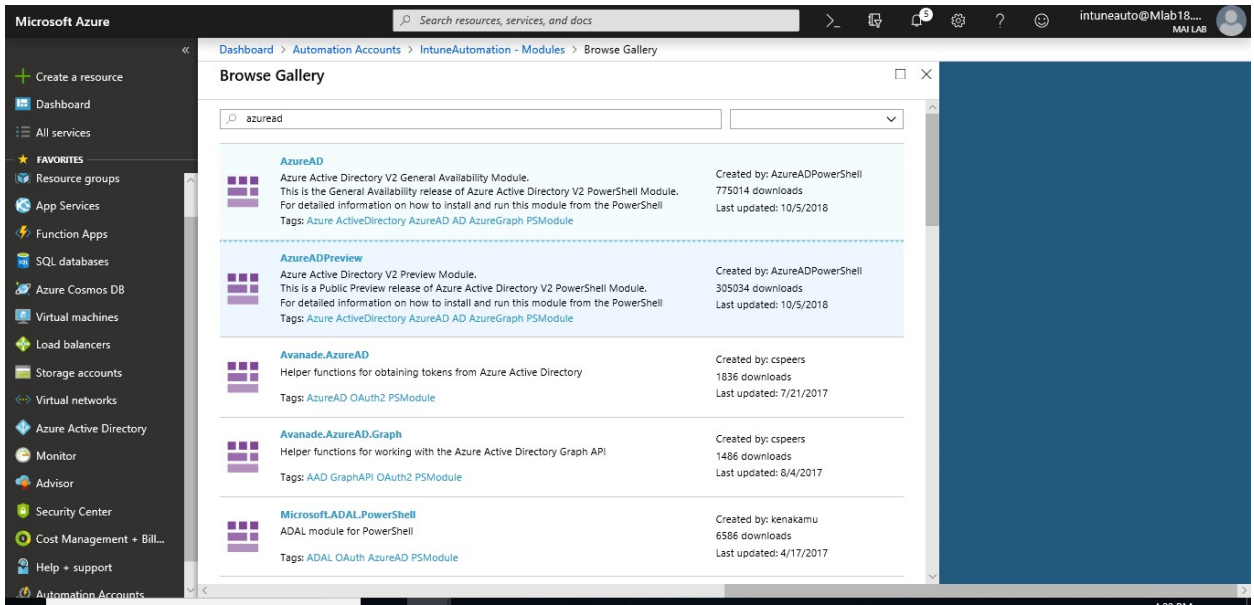


7. On the **Import** page, click **OK** to import the module.

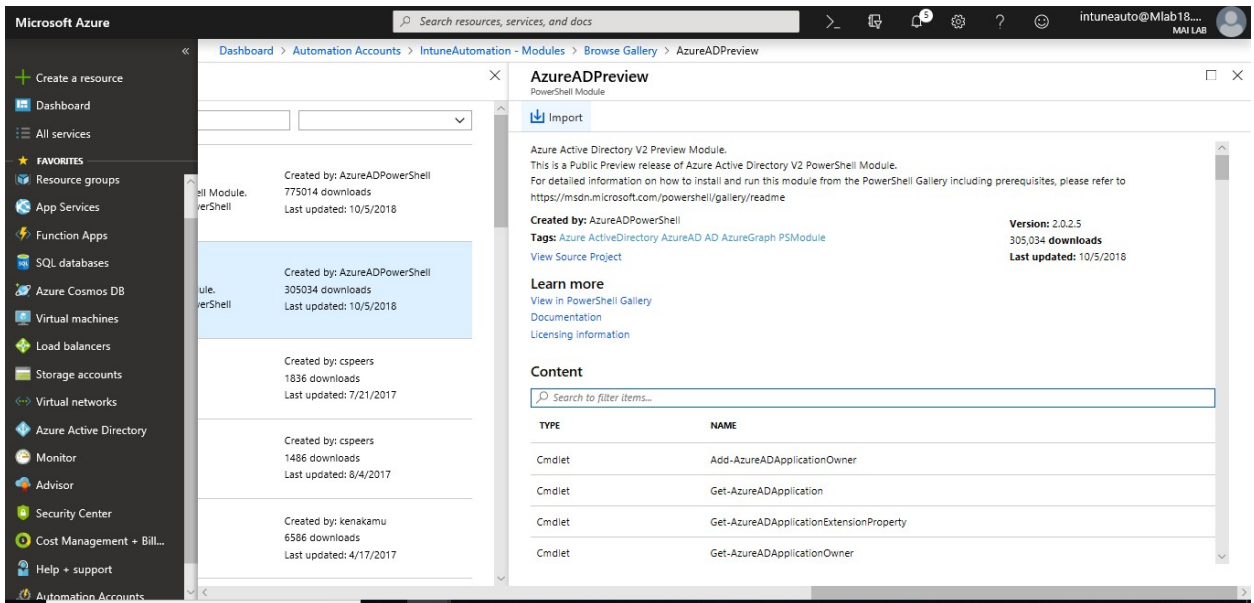


8. On the **Browse gallery** page, type on search **AzureADPreview**.

Microsoft Intune step by step on Azure portal

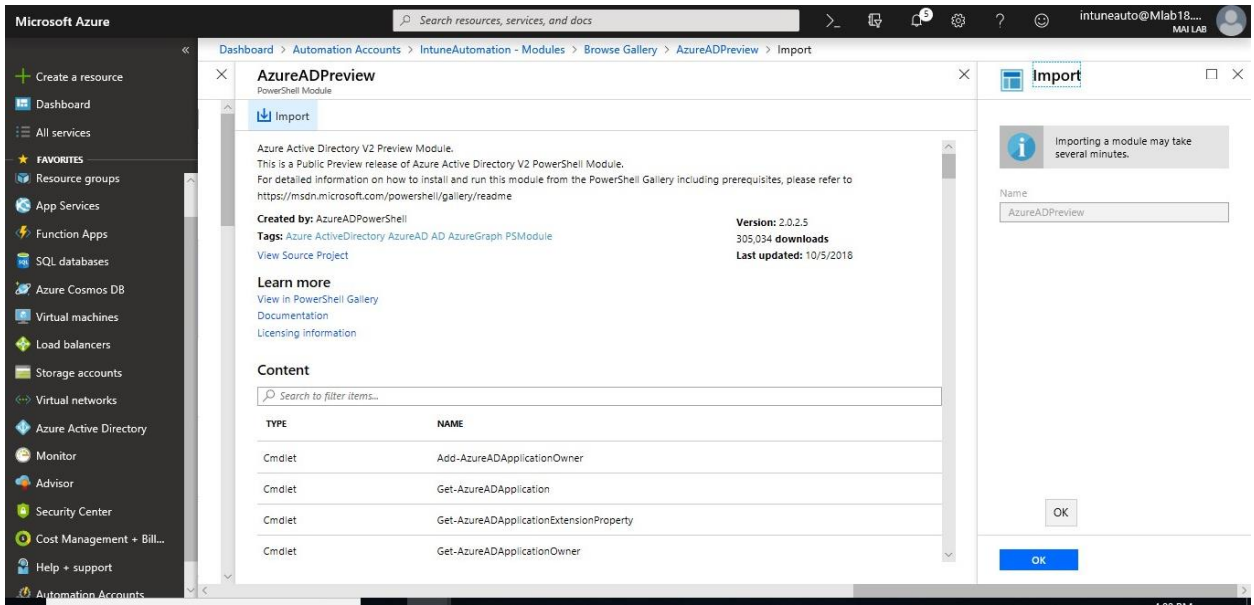


9. To install the module directly into Azure Automation, click the **Import** button.

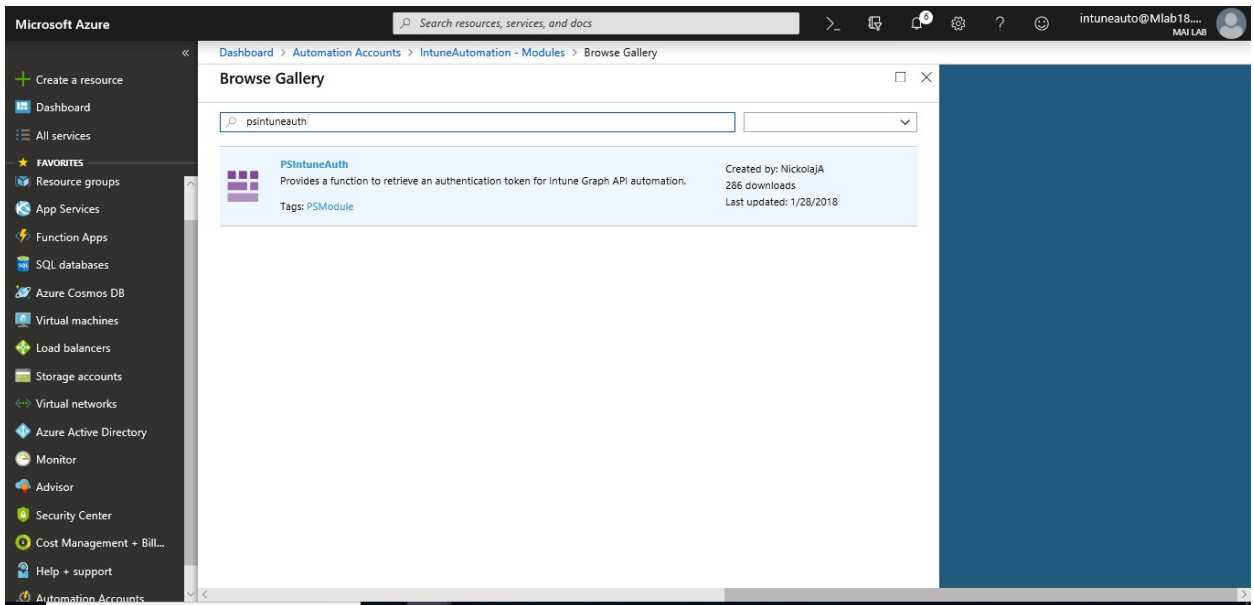


10. On the **Import** page, click **OK** to import the module.

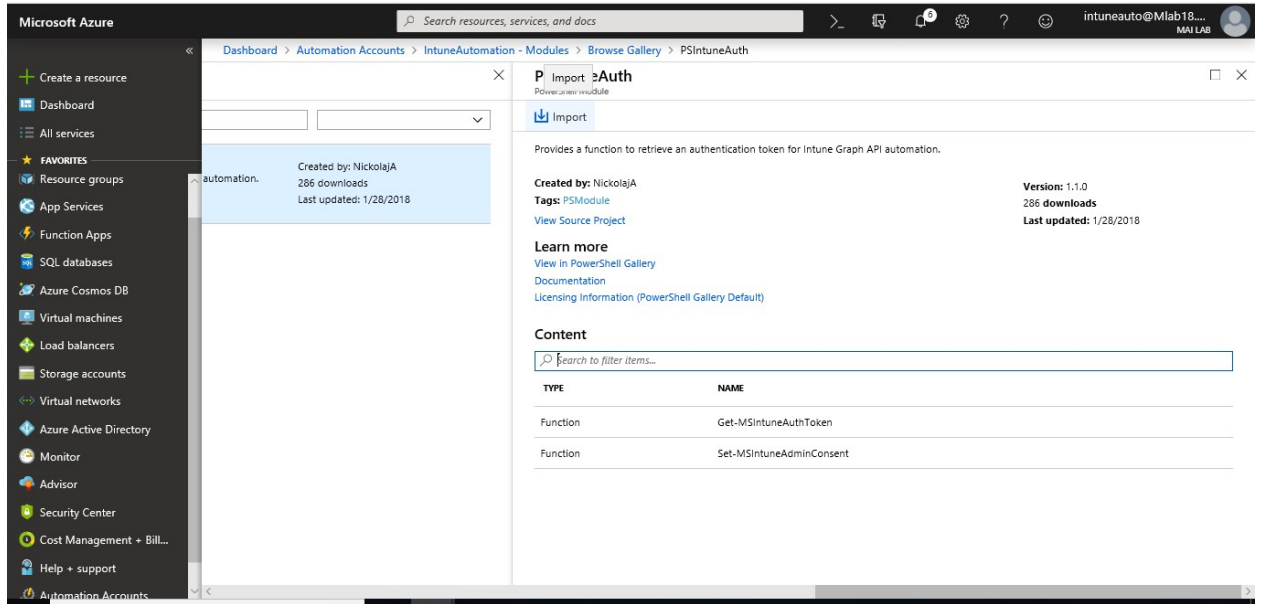
Microsoft Intune step by step on Azure portal



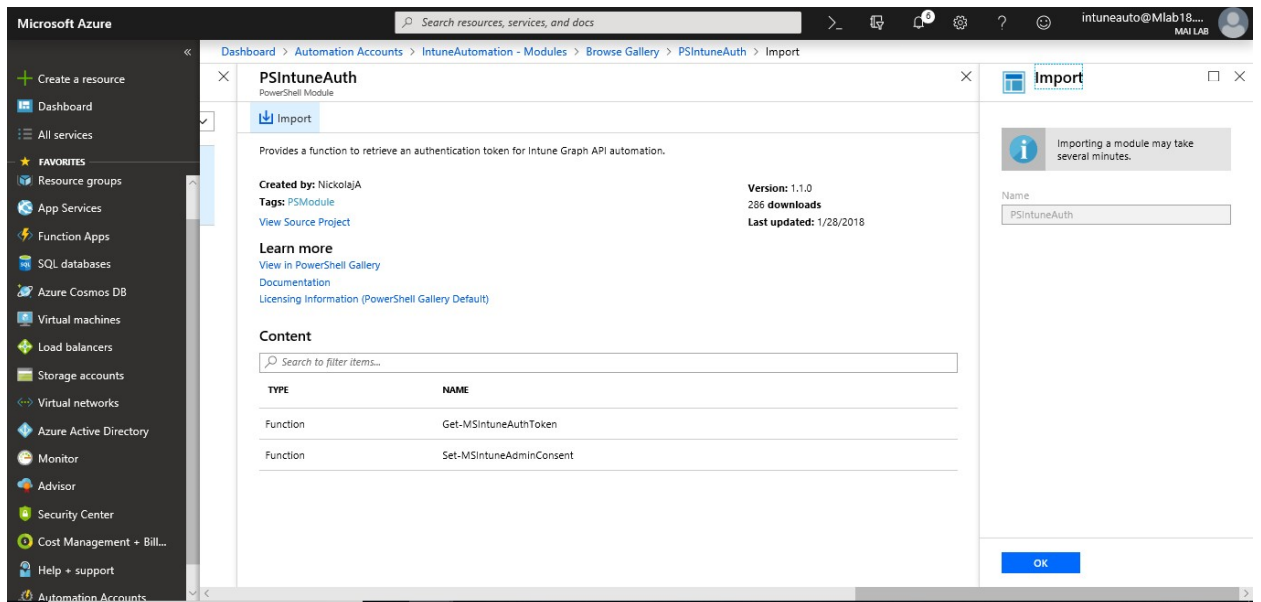
11. On the **Browse gallery** page, type on search **PSIntuneAuth**



12. To install the module directly into Azure Automation, click the **Import** button.

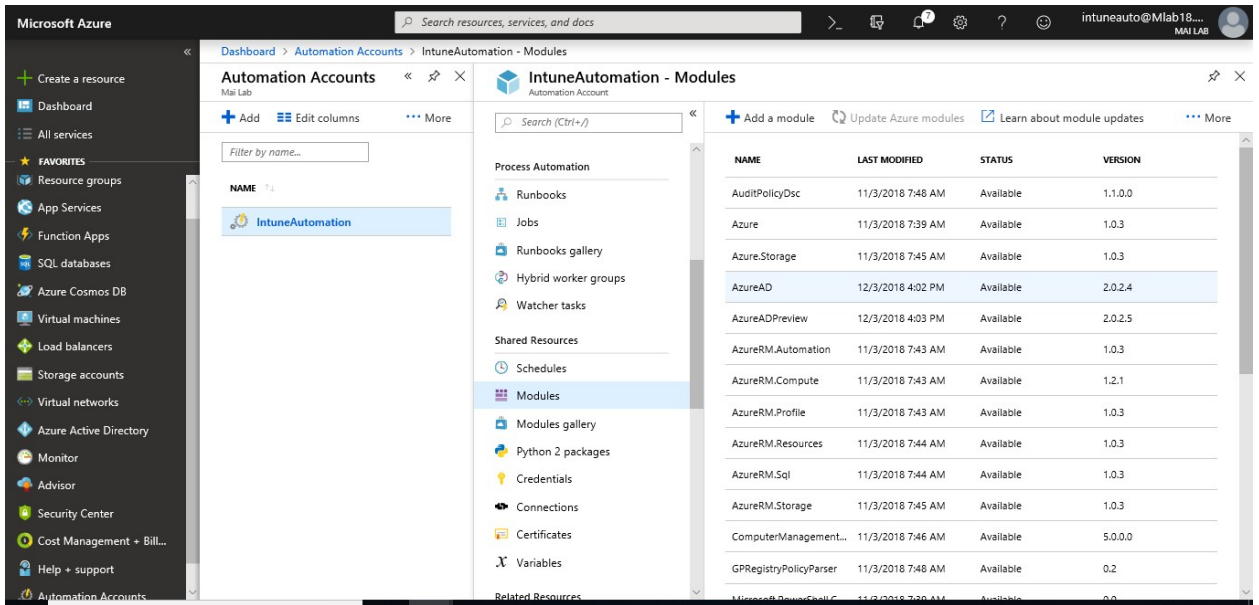


13. When you click the Import button, on the **Import** pane, you see the module name that you are about to import. If all the dependencies are installed, the **OK** button is activated. If you are missing dependencies, you need to import those before you can import this module.
14. On the **Import** page, click **OK** to import the module. While Azure Automation imports a module to your account, it extracts metadata about the module and the cmdlets. This may take a couple of minutes since each activity needs to be extracted.



15. You receive an initial notification that the module is being deployed and another notification when it has completed.
16. After the module is imported, you can see the available activities, and you can use its resources in your runbooks and Desired State Configuration.

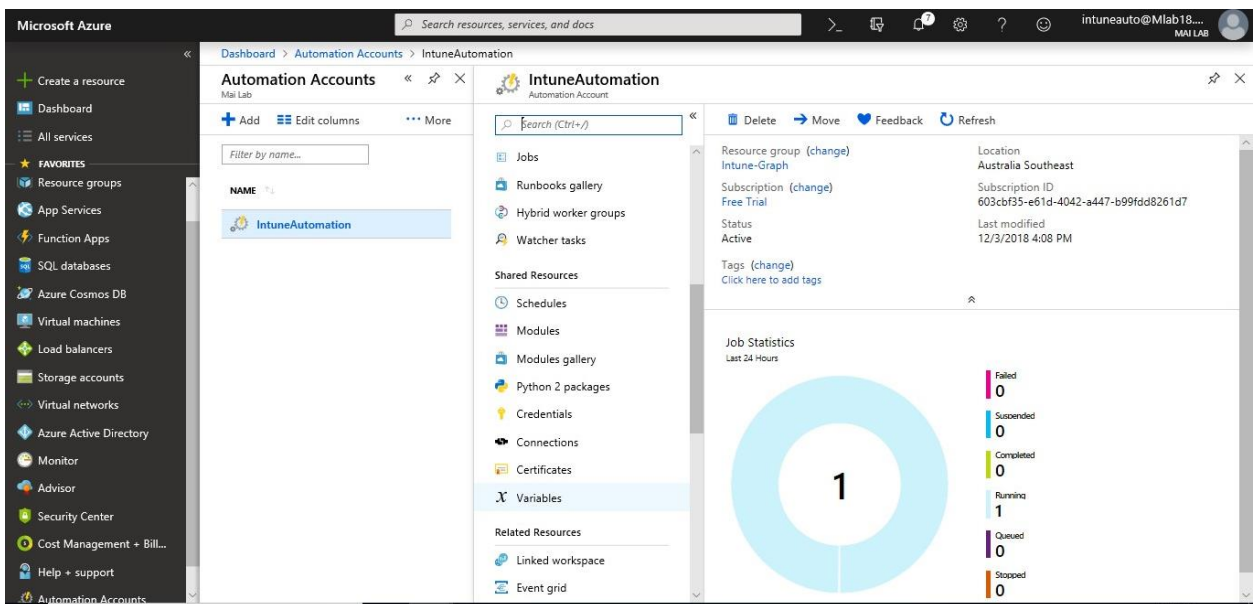
Microsoft Intune step by step on Azure portal



Step 6: Add variables Assets in Azure Automation

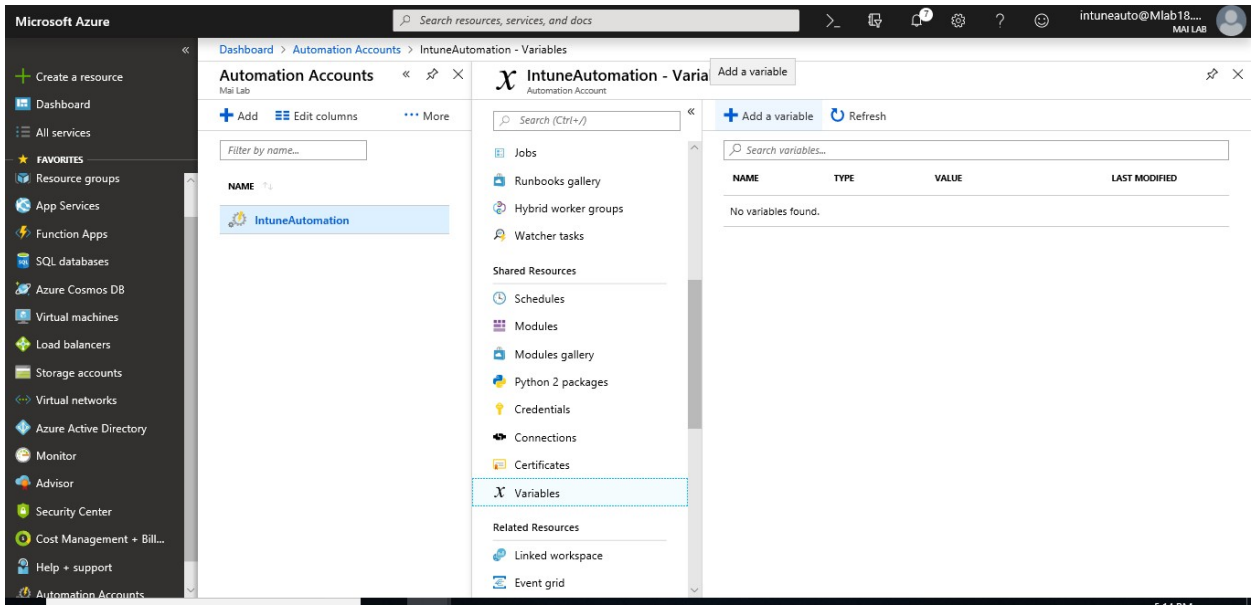
To create a new variable with the Azure portal, you need to follow below steps:

1. From your Automation account, on the **Shared Resources** blade, select **Variables**.

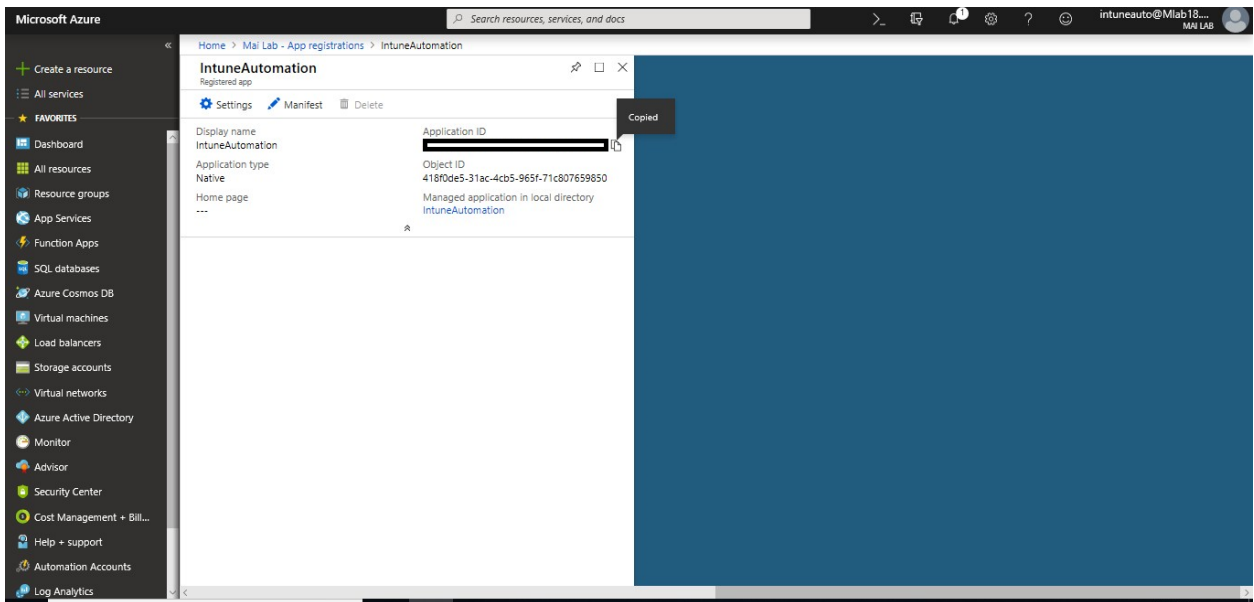


2. On the **Variables** tile, select **Add a variable**.

Microsoft Intune step by step on Azure portal

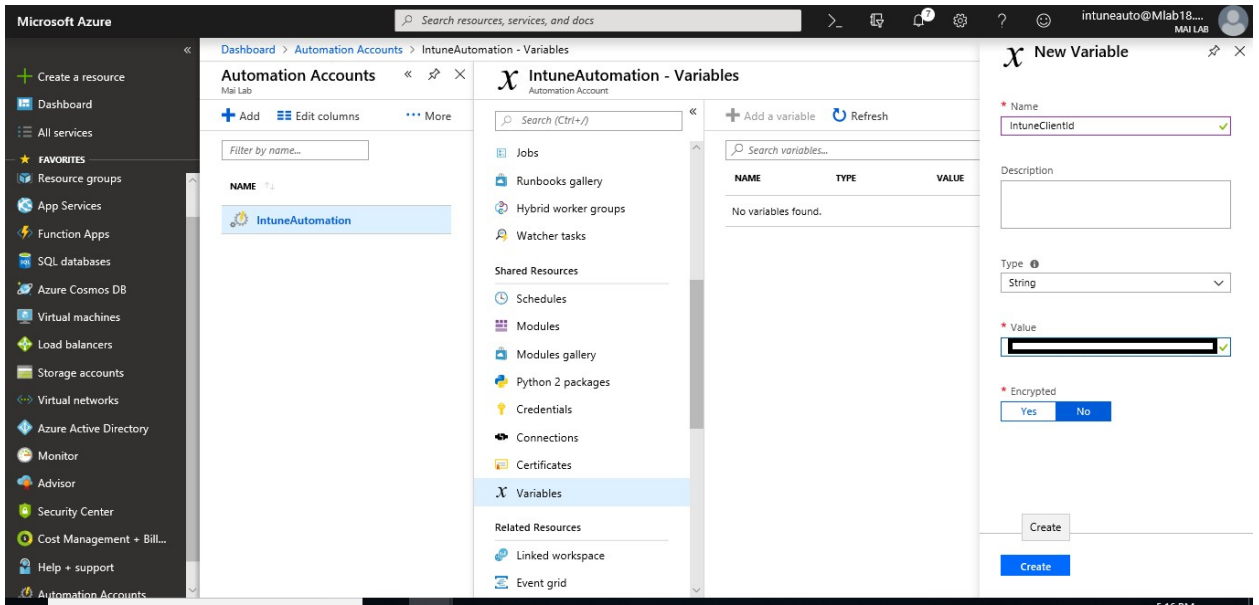


3. Create New Variable for IntuneClientId which is point to native App that you create on Step 1.

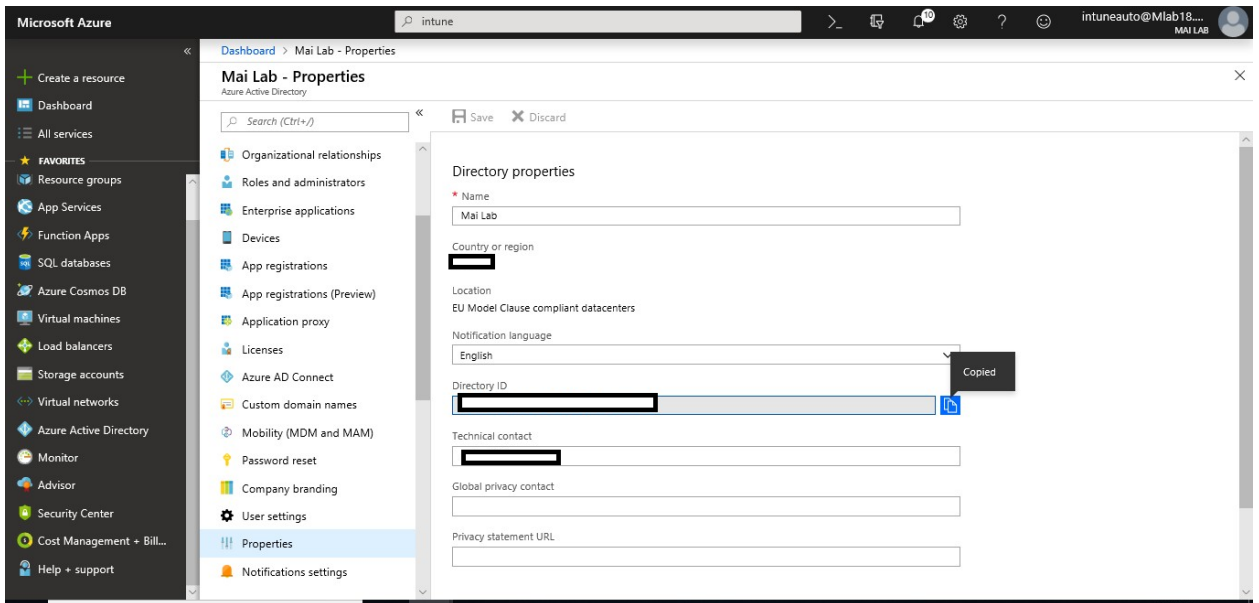


4. Complete the options on the **New Variable** blade and click **Create** save the new variable.

Microsoft Intune step by step on Azure portal

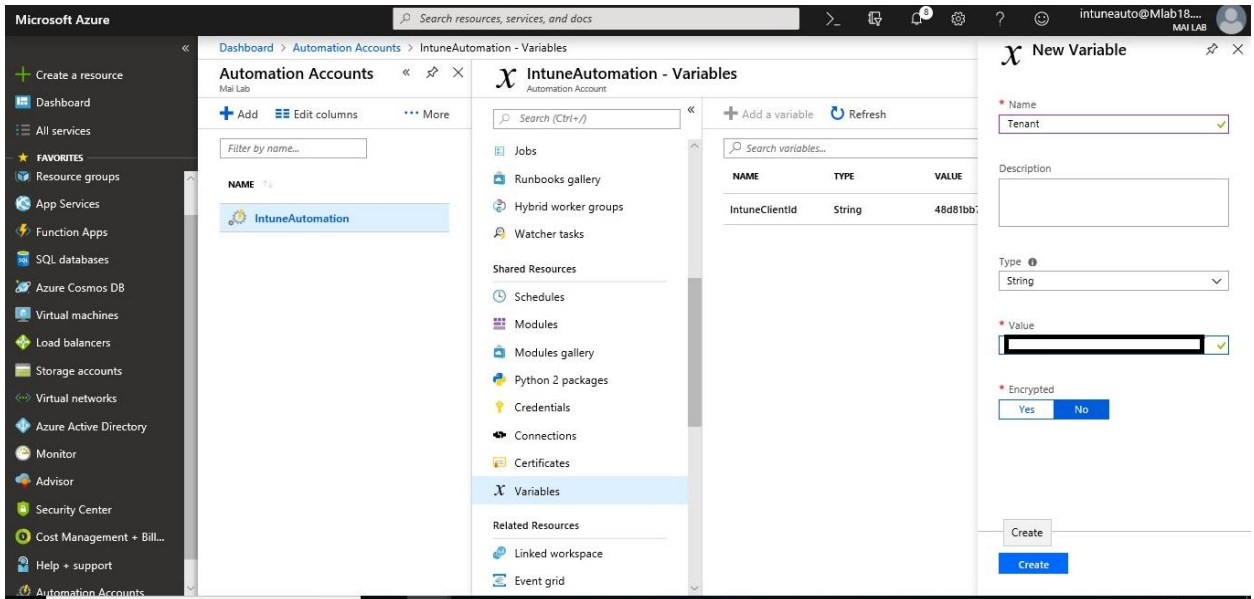


5. Create New Variable for Tenant which point to Tenant ID.

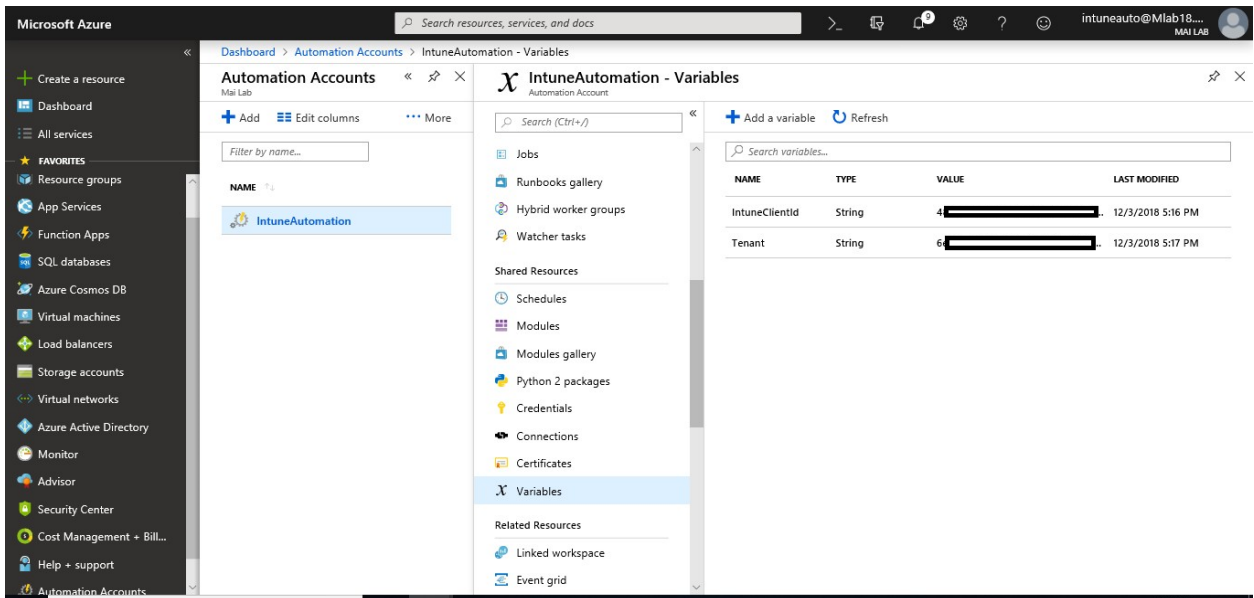


6. Complete the options on the **New Variable** blade and click **Create** save the new variable.

Microsoft Intune step by step on Azure portal



7. Now both variable for Tenant & Intune Client ID are created.

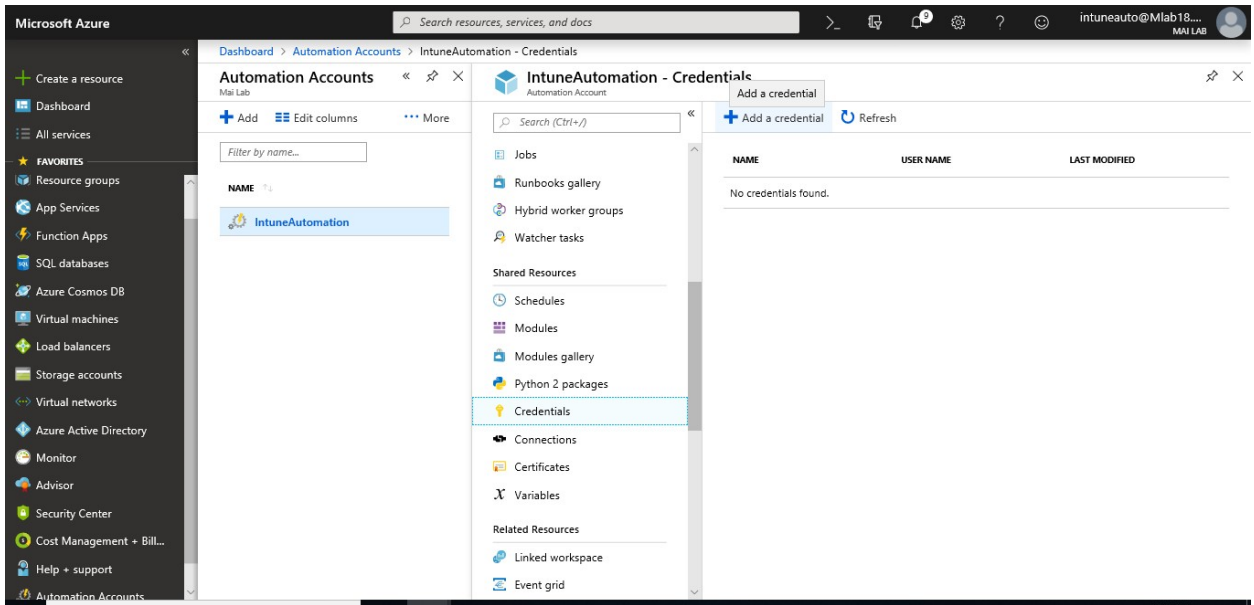


Step 7: Add credential Assets in Azure Automation

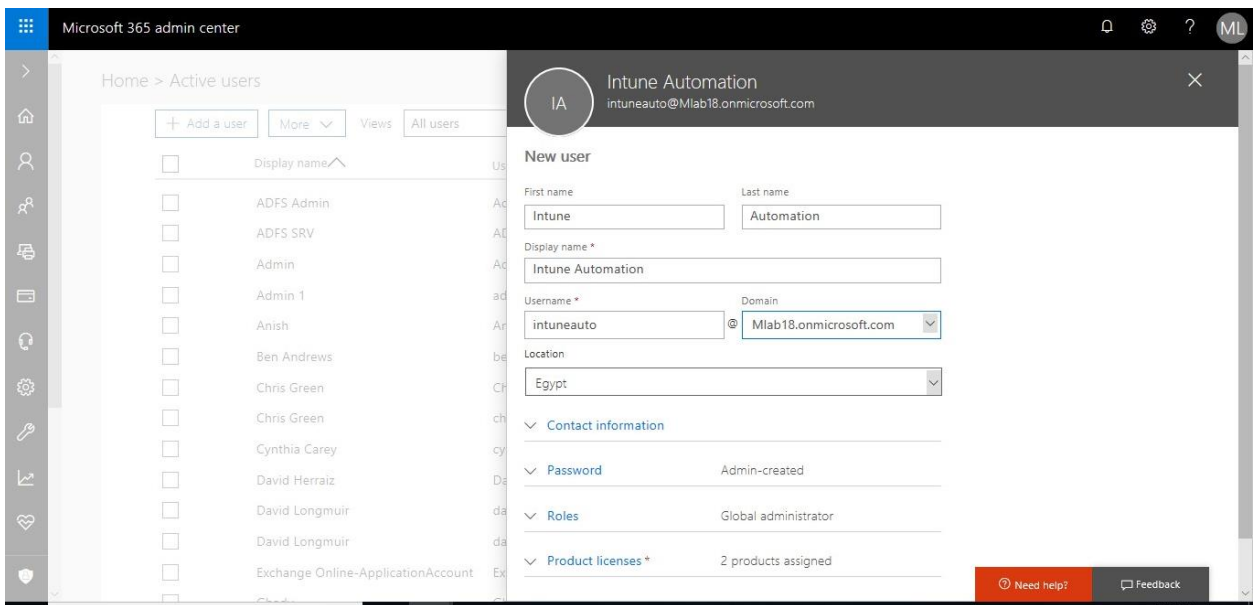
To create a new credential asset with the Azure portal, you need to follow below steps:

1. From your automation account, on the **Shared Resource** blade. Click the **Credentials** part to open the **Credentials** blade. Click **Add a credential** at the top of the blade.

Microsoft Intune step by step on Azure portal



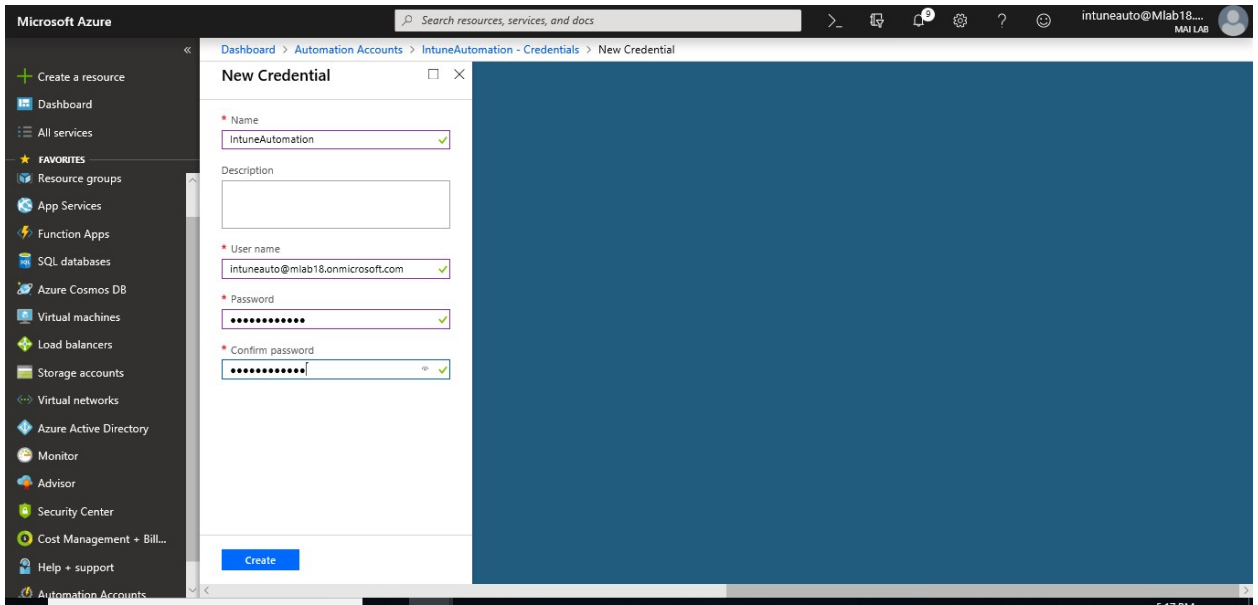
2. Type credential for global admin account that you created before for automation.



Note: you need to assign license for EMS to this automation account & get him global admin to be able to collect all Intune audit data.

3. Complete the form and click **Create** to save the new credential.

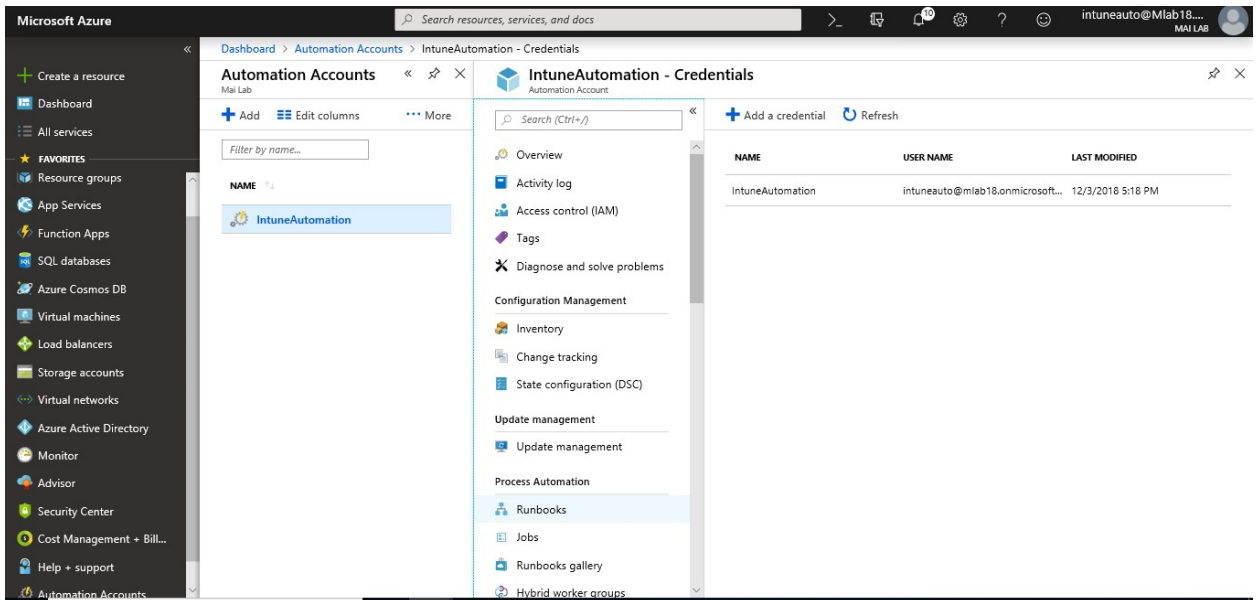
Microsoft Intune step by step on Azure portal



Step 8: Create & Publish PowerShell Runbook

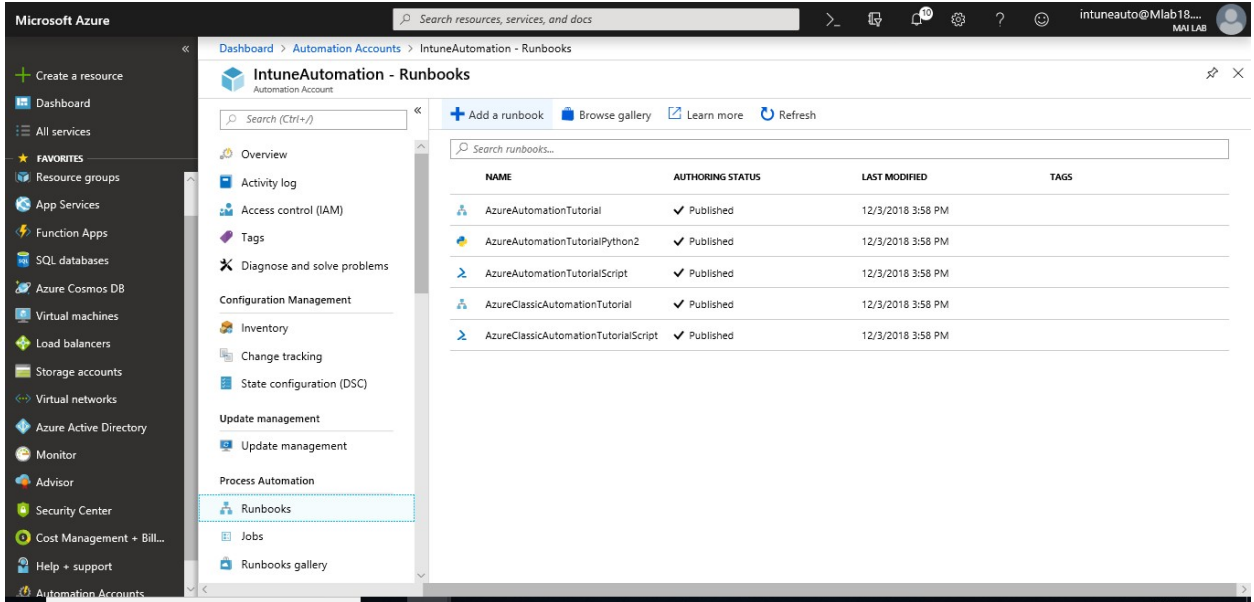
To create PowerShell Runbook, you need to follow below steps:

1. In the [Azure portal](#), open your Automation account.
2. Under **Process Automation**, select **Runbooks** to open the list of runbooks.

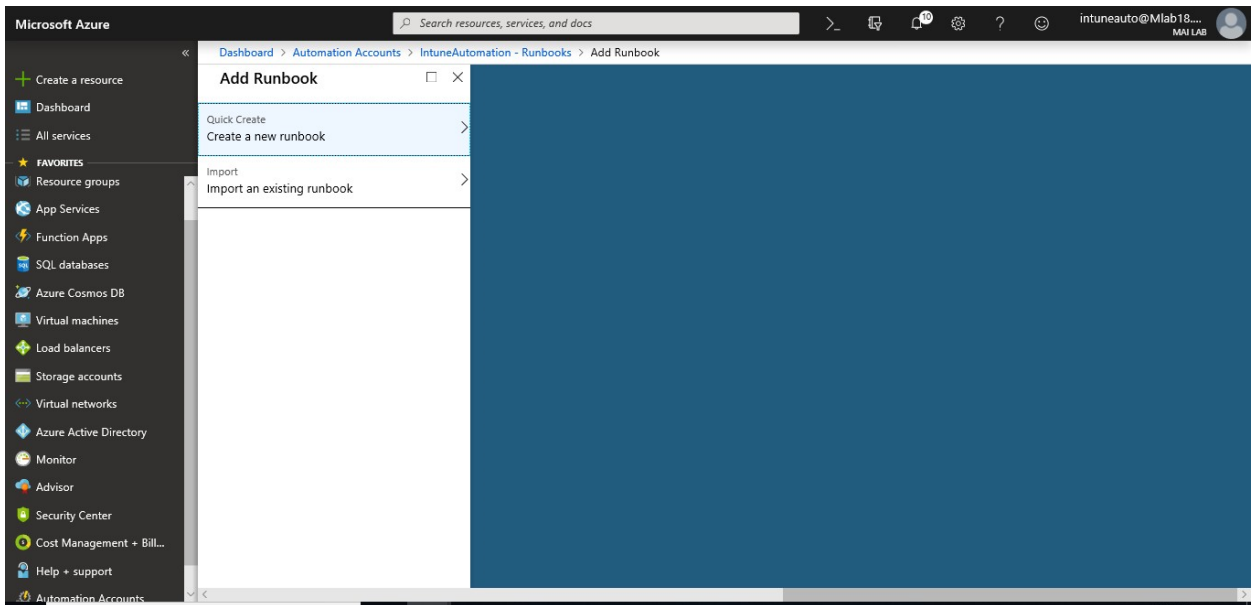


3. Click the **Add a runbook** button found at the top of the list.

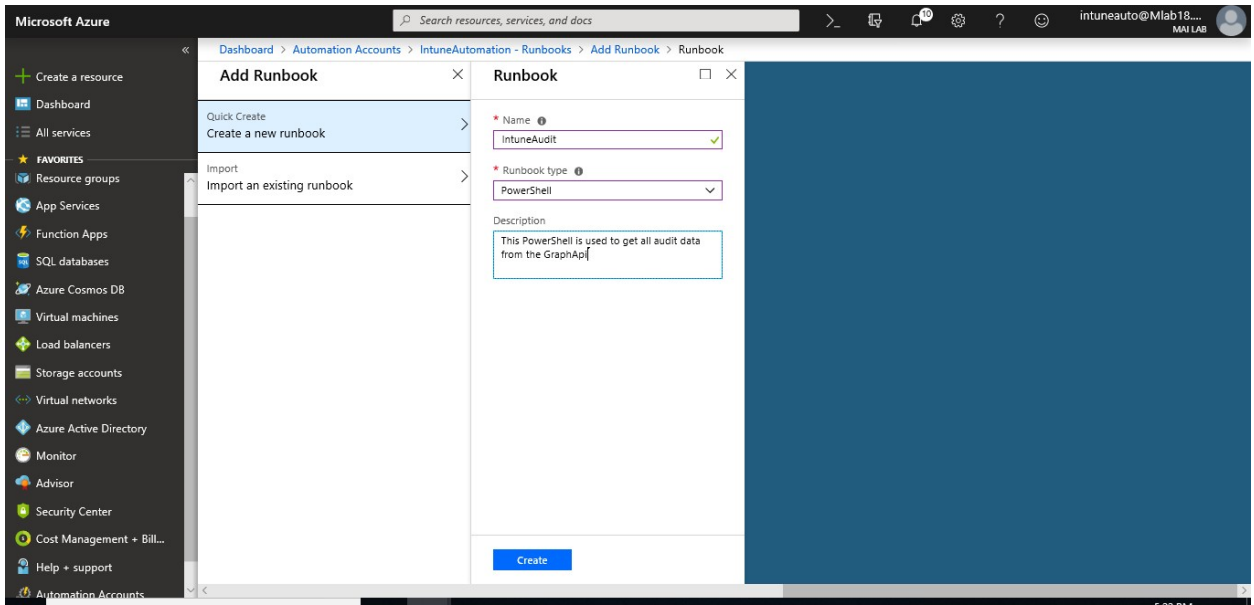
Microsoft Intune step by step on Azure portal



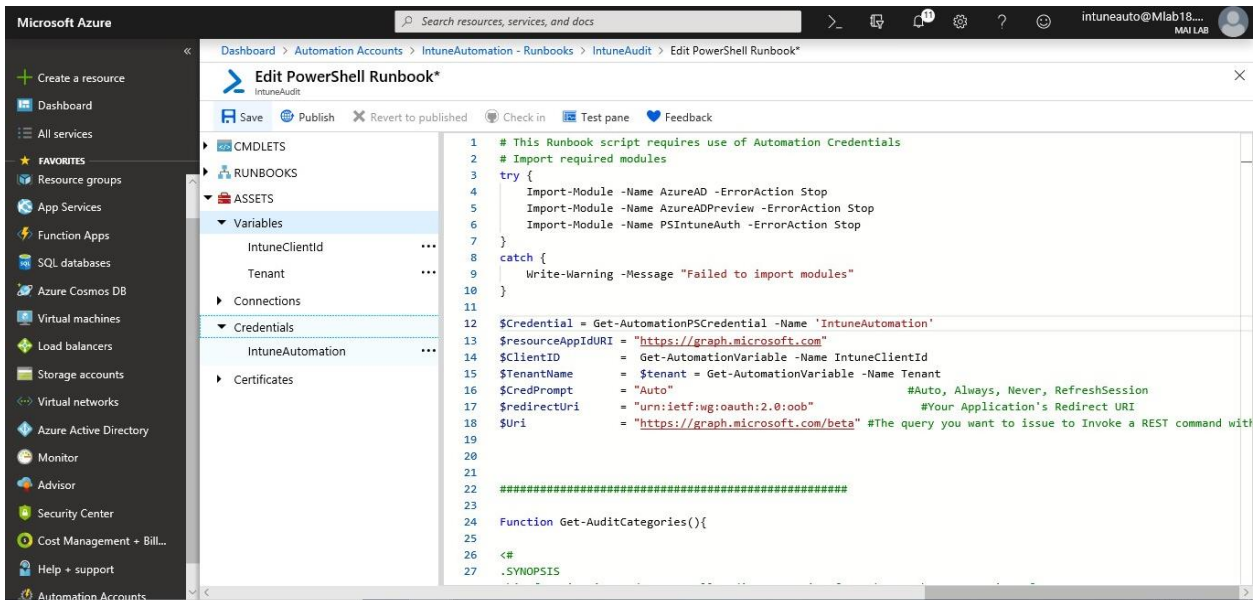
4. On the **Add Runbook** page, select **Quick Create**.



5. Enter "*Intune Audit*" for the runbook **Name** and select **PowerShell** for **Runbook type**. Click **Create**.



6. The runbook is created, and the **Edit PowerShell Runbook** page opens.
7. Type or copy and paste the following code into the edit pane. Ensure that variable & credential accounts on [Audit script type](#) as you created it before.



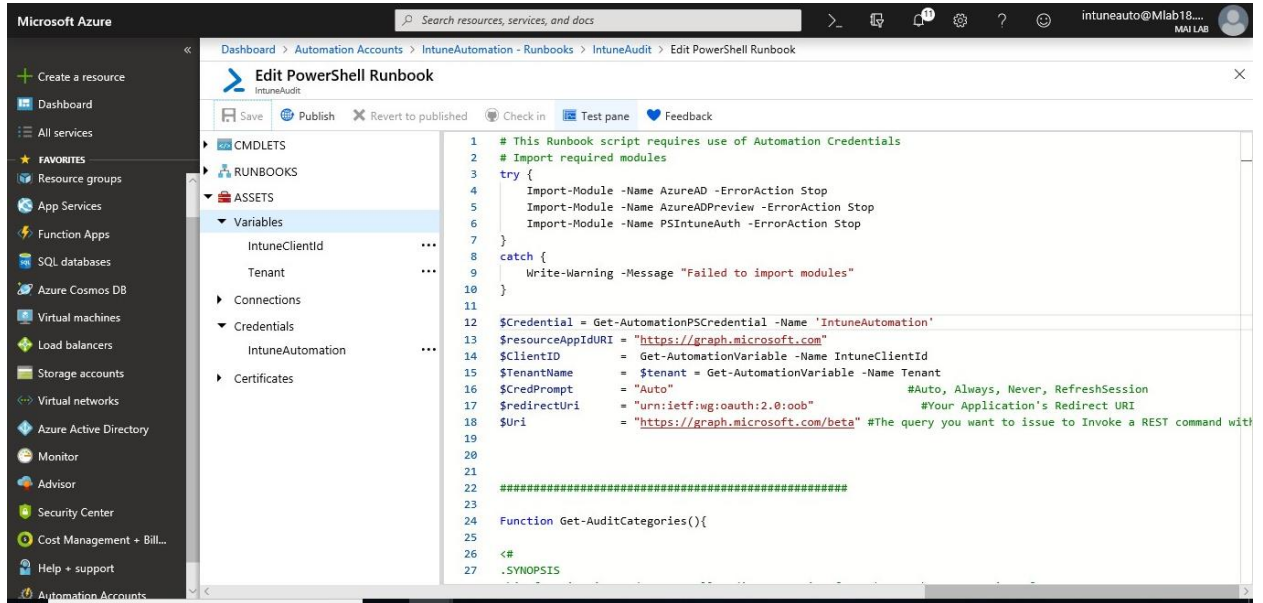
Note: Jan Ketil script is running audit for 1 day to get it 30 days as I did on my lab to have output, you need to change on section Function Audit Event on line else { \$days = 1 } to be 30 instead of 1.

8. Click **Save**, to save a draft copy of the runbook.

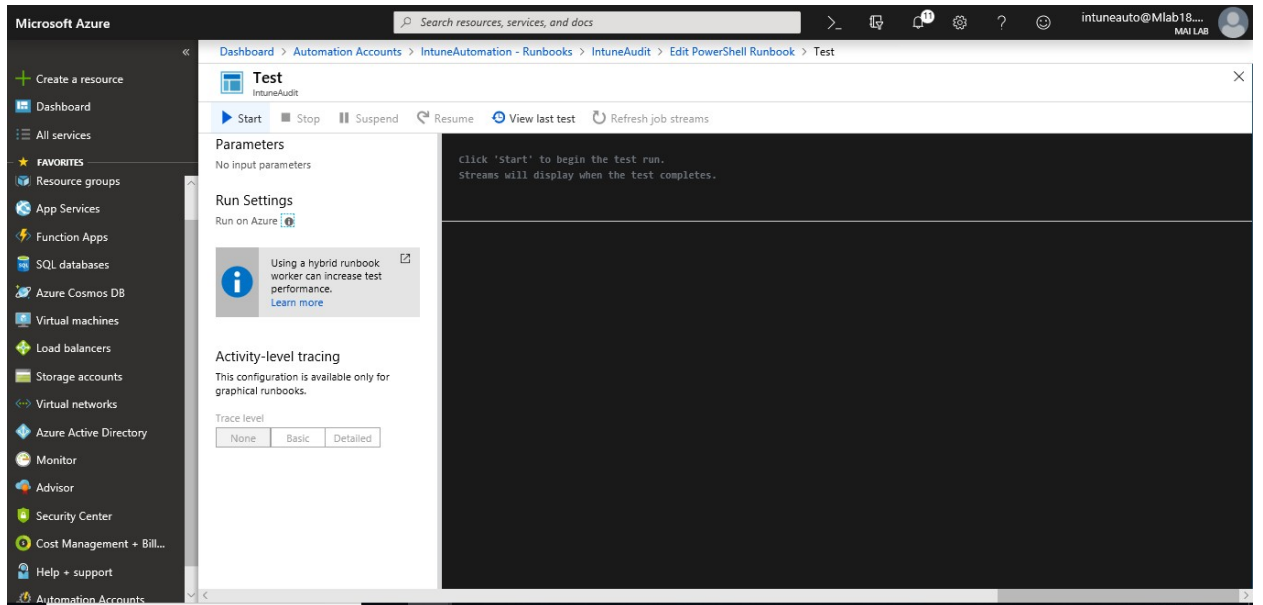
Once the runbook is created, you test the runbook to validate that it works.

Microsoft Intune step by step on Azure portal

1. Click **Test** pane to open the **Test** page.

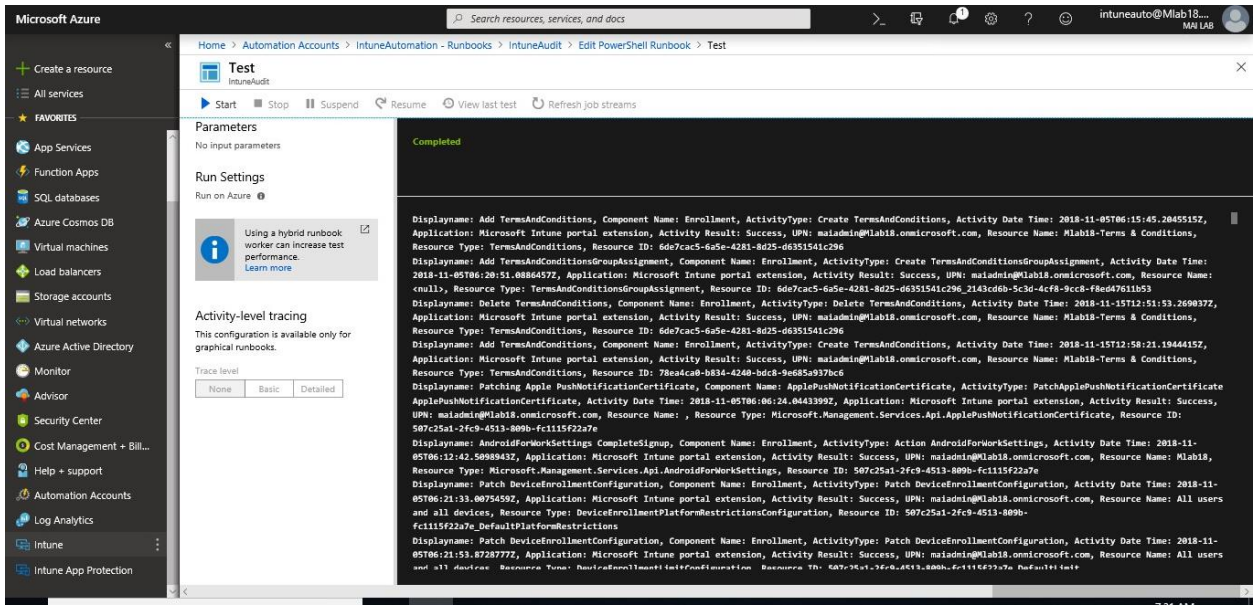


2. Enter a value for **Name** and click **Start**. The test job starts and the job status and output display.

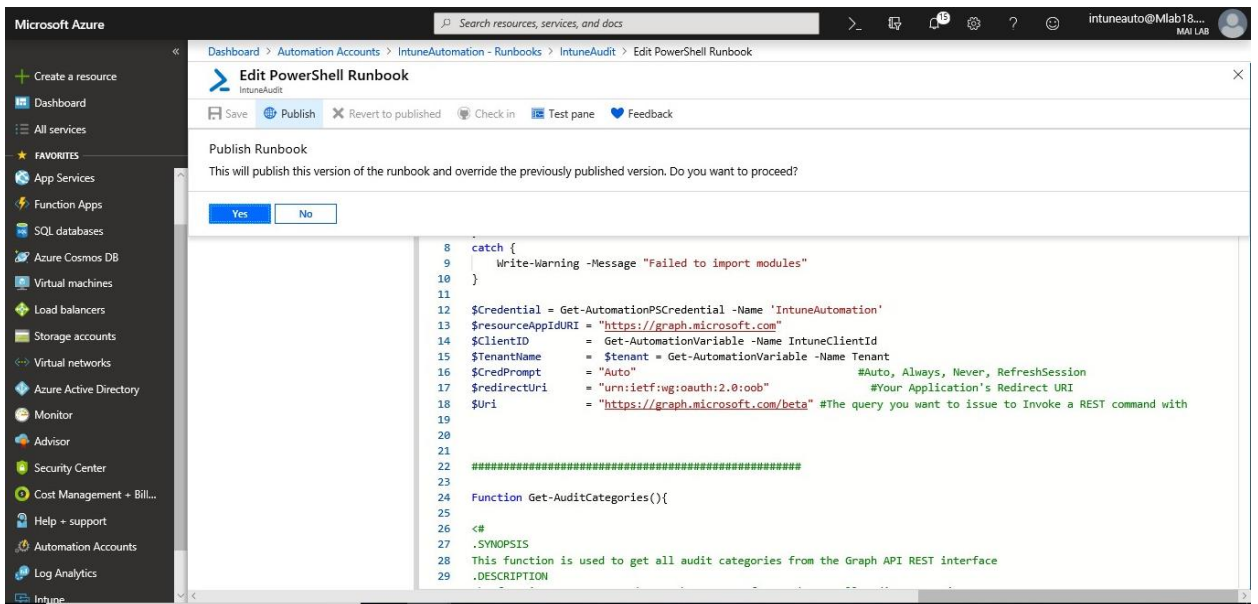


3. Once Test Job is completed. Close the **Test** page by clicking the **X** in the upper right corner. Select **OK** in the popup that appears.

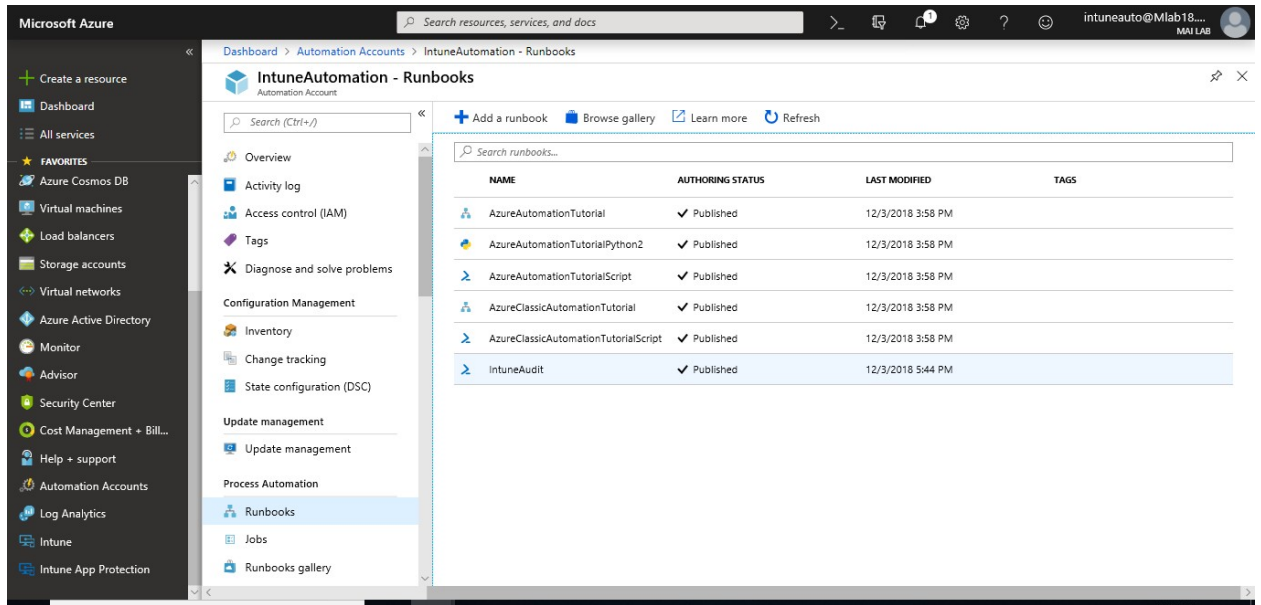
Microsoft Intune step by step on Azure portal



4. In the **Edit PowerShell Runbook** page, click **Publish** to publish the runbook as the official version of the runbook in the account.



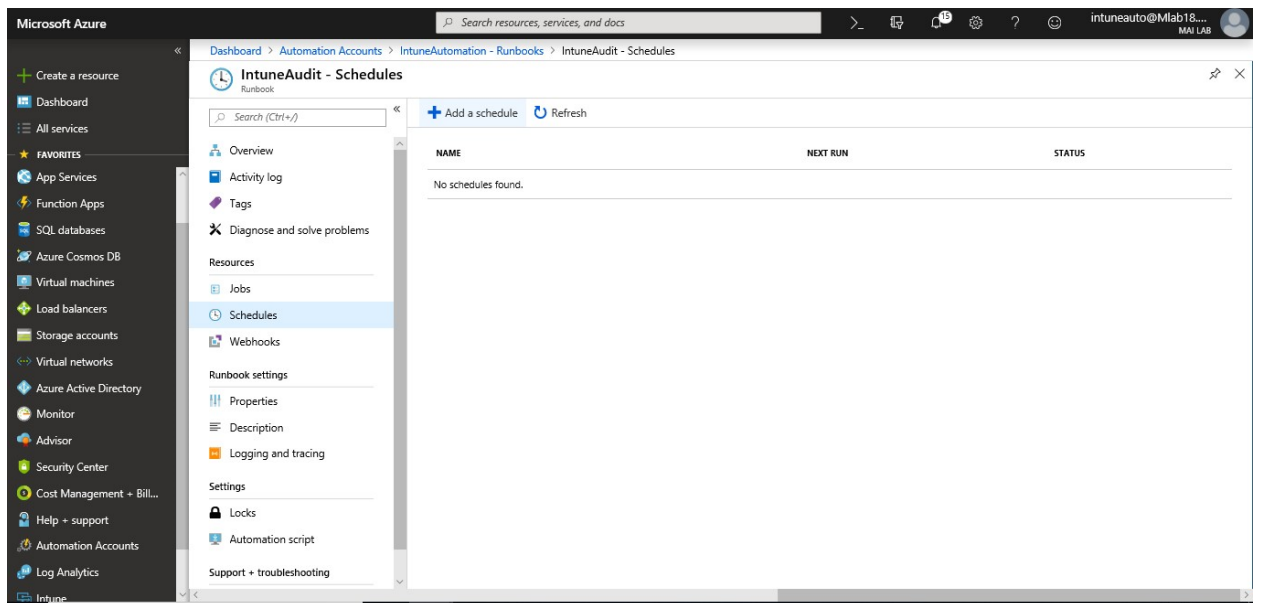
Microsoft Intune step by step on Azure portal



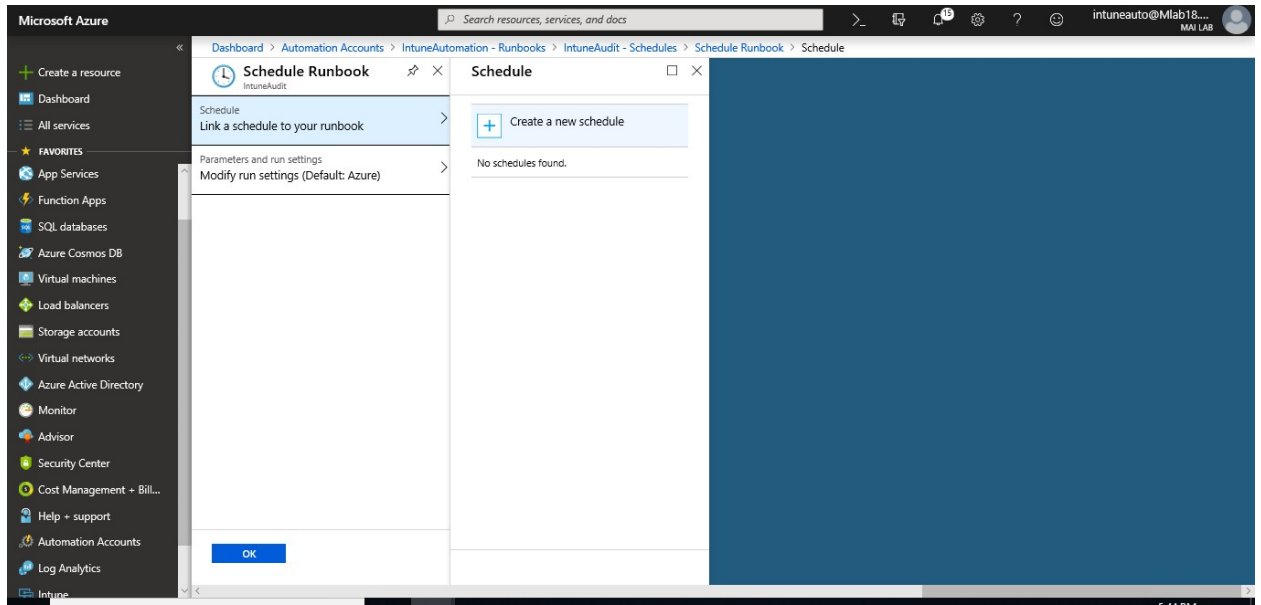
Step 9: Schedule PowerShell Runbook

To create a new schedule in the Azure portal, you need to follow below steps:

1. In the [Azure portal](#), from your automation account, select **Schedules** under the section **Shared Resources** on the left. Click **Add a schedule** at the top of the page.

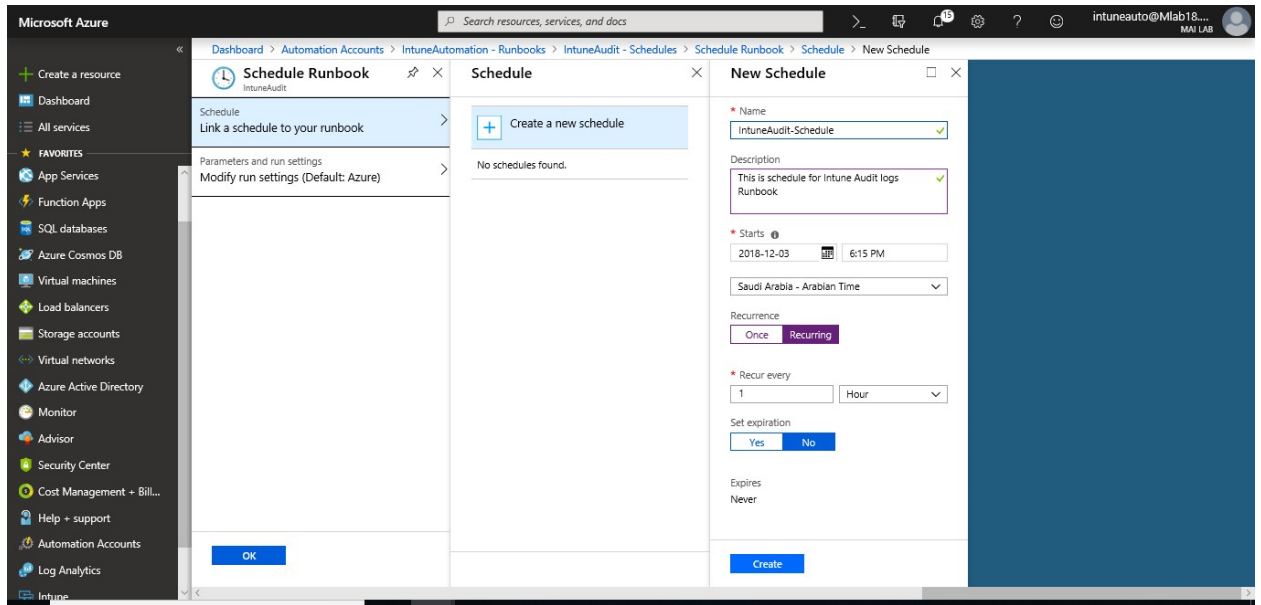


2. On the **New schedule** pane, type a **Name** and optionally a **Description** for the new schedule.

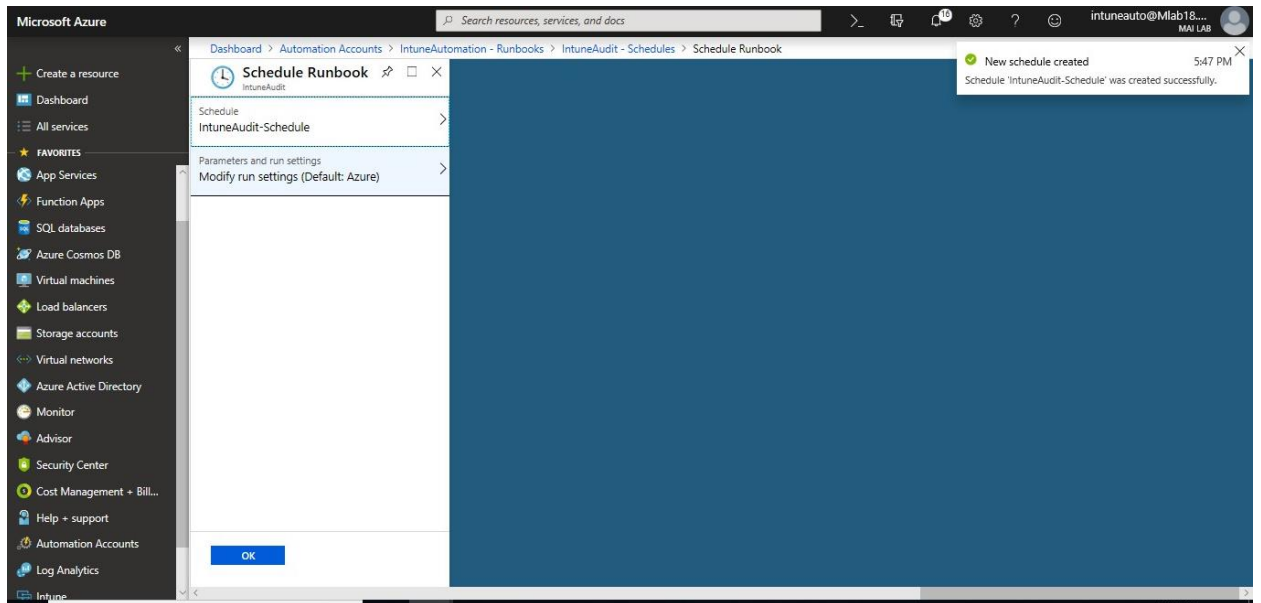


3. Select whether the schedule runs one time, or on a reoccurring schedule by selecting **Once** or **Recurring**. If you select **Once** specify a **Start time**, and then click **Create**. If you select **Recurring**, specify a **Start time** and for **Recur every**, select the frequency for how often you want the runbook to repeat - by **hour**, **day**, **week**, or by **month**. When done click **Create**
 - If you select **week**, you are provided a list of the days of the week to choose from. Select as many days as you want. The first run of your schedule will happen on the first day selected after the start time.
 - If you select **month**, you are given different options. For the **Monthly occurrences** option, select either **Month days** or **Week days**. If you choose **Month days** a calendar is shown that allows you to choose as many days as you want. If you choose a date such as the 31st that doesn't occur in the current month, the schedule will not run. If you want the schedule to run on the last day, choose **Yes** under **Run on last day of month**. If you choose **Week days**, the **Recur every** option is presented. Choose **First**, **Second**, **Third**, **Fourth**, or **Last**. Finally choose a day to repeat on.

Microsoft Intune step by step on Azure portal

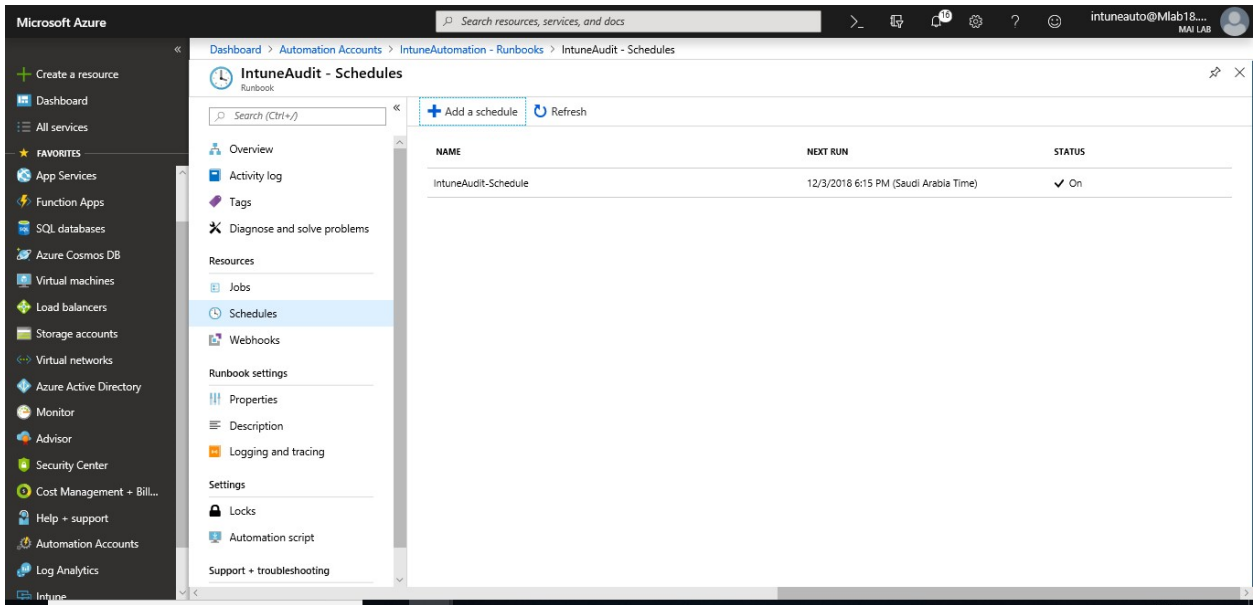


iv. Click **Ok**.



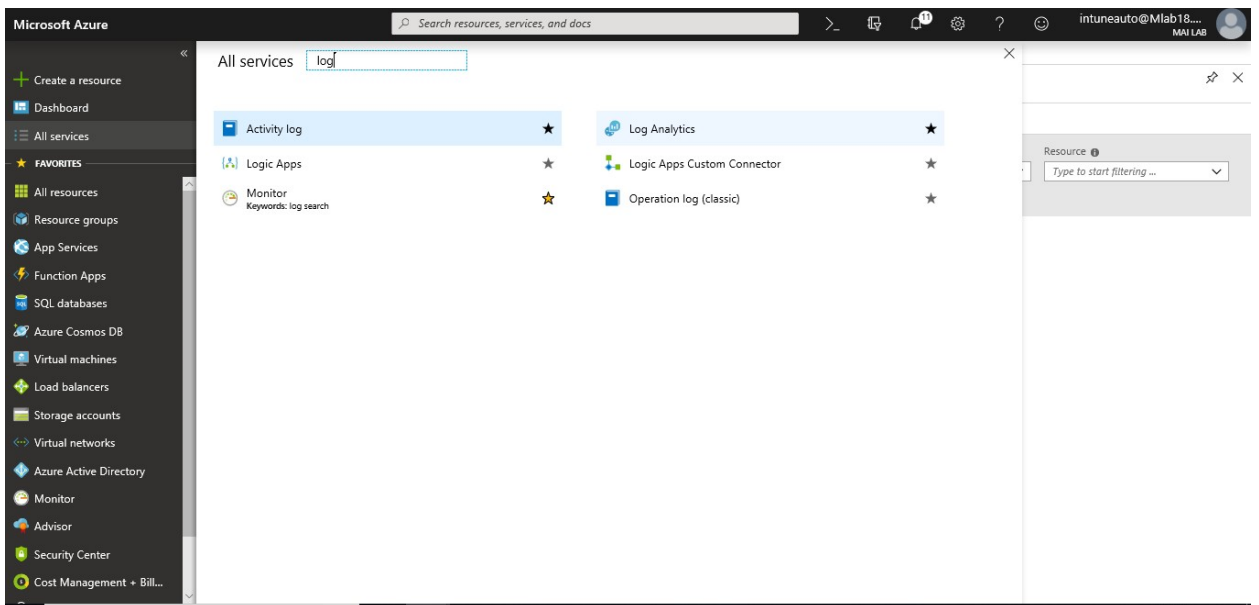
v. Now the schedule is created.

Microsoft Intune step by step on Azure portal



Step 10: Create OMS Workspace enabled for log analytics

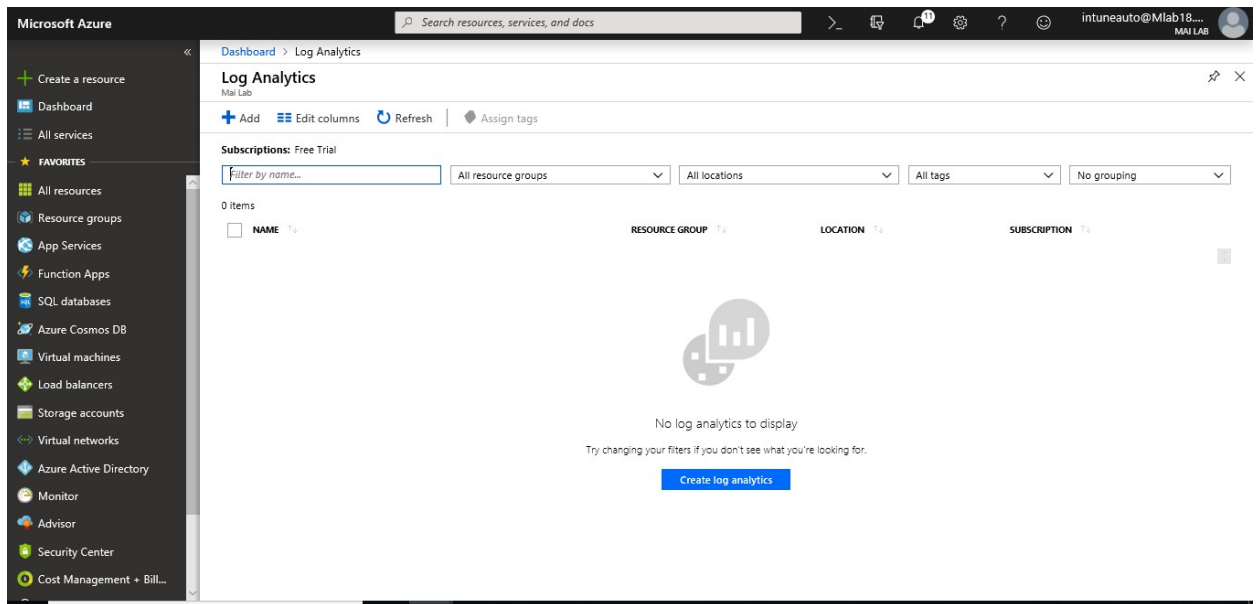
1. In the Azure portal, click **All services**. In the list of resources, type **Log Analytics**. As you begin typing, the list filters based on your input. Select **Log Analytics**.



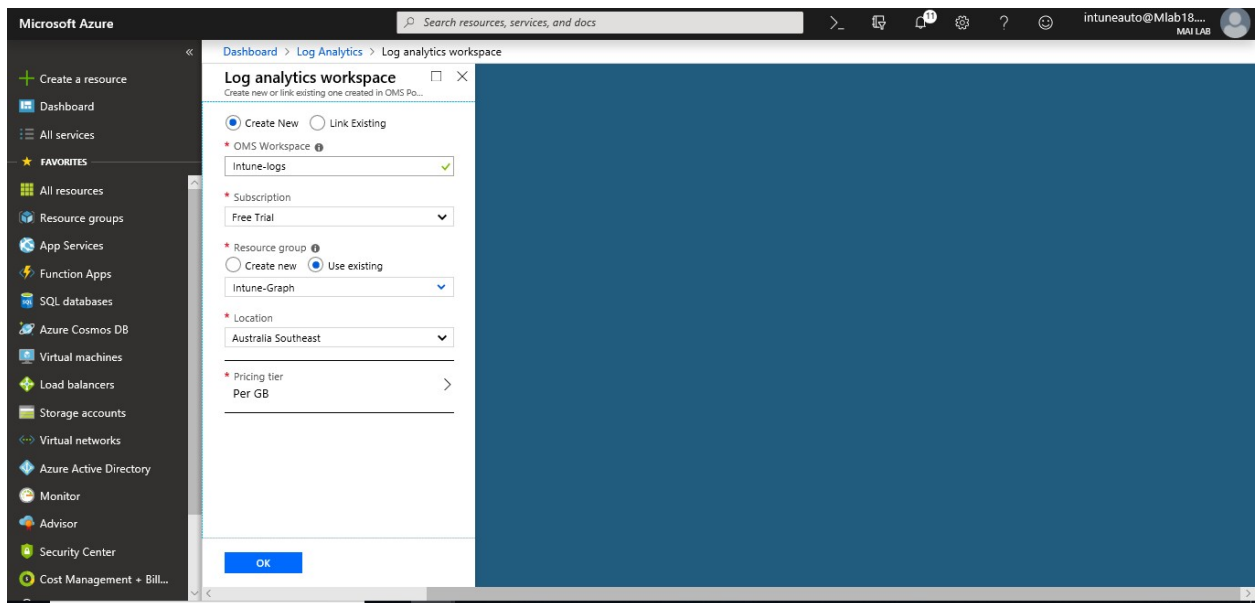
2. Click **Create**, and then select choices for the following items:
 - Provide a name for the new **Log Analytics Workspace**, such as *Intune-logs*.
 - Select a **Subscription** to link to by selecting from the drop-down list if the default selected is not appropriate.

Microsoft Intune step by step on Azure portal

- For **Resource Group**, choose to use an existing resource group already setup or create a new one.
- Select an available **Location**.
- If you are creating a workspace in a new subscription created after April 2, 2018, it will automatically use the *Per GB* pricing plan and the option to select a pricing tier will not be available. If you are creating a workspace for an existing subscription created before April 2, or to subscription that was tied to an existing Enterprise Agreement (EA) enrollment, select your preferred pricing tier.

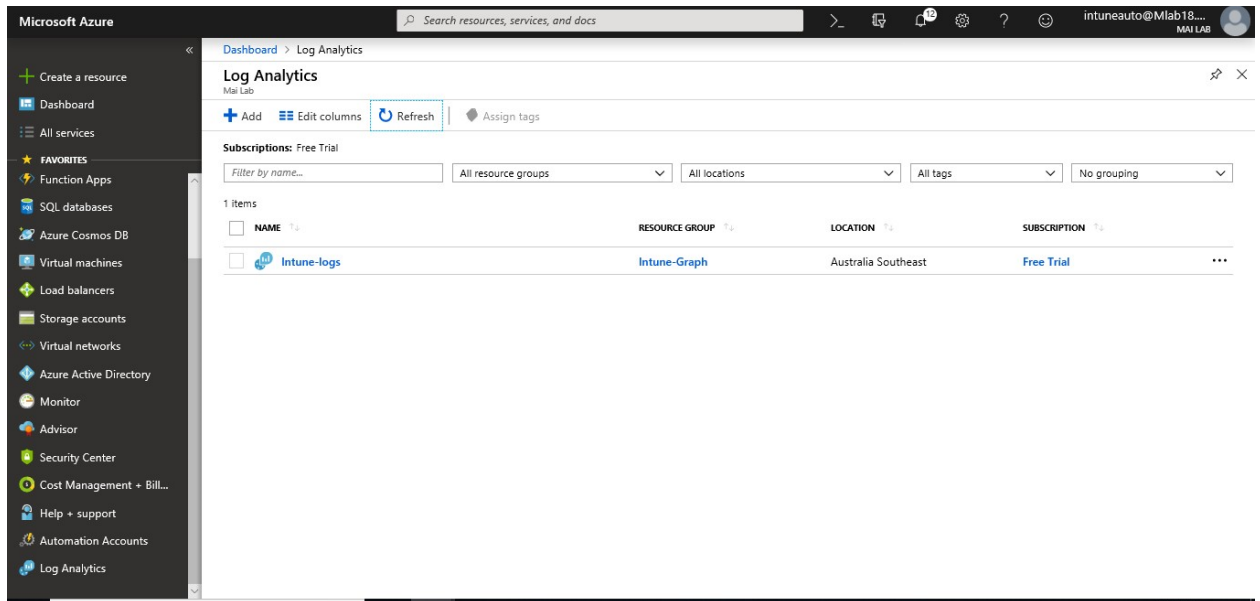


3. After providing the required information on the **Log Analytics Workspace** pane, click **OK**.



Microsoft Intune step by step on Azure portal

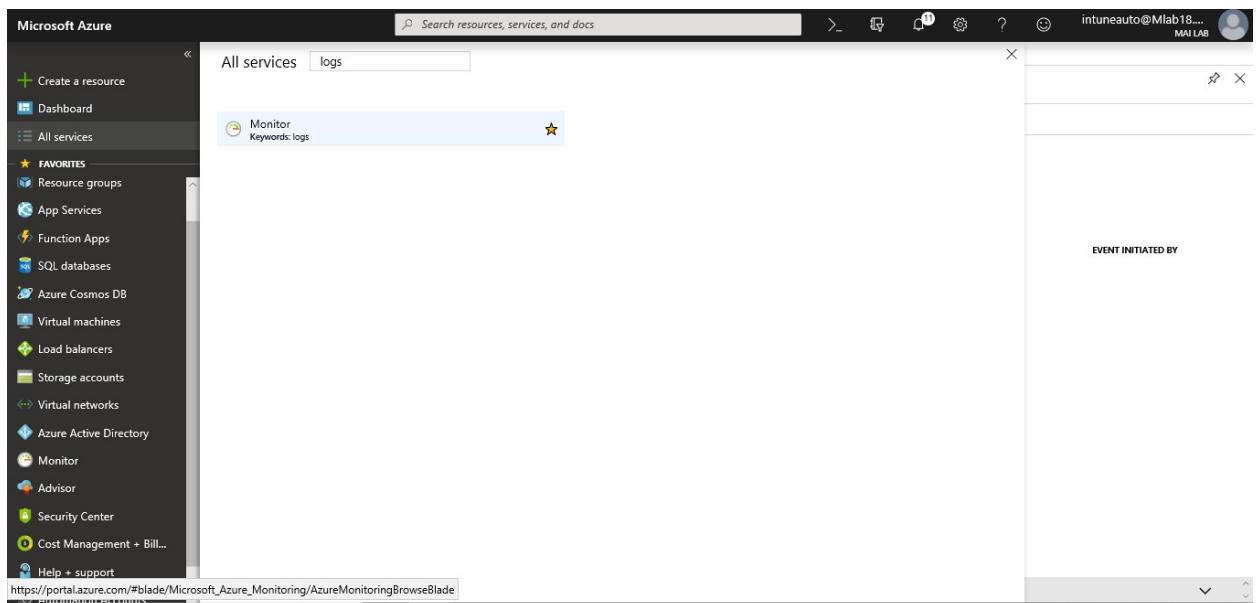
- vi. While the information is verified, and the workspace is created, you can track its progress under **Notifications** from the menu.



Step 11: Enable diagnostics on Azure Automation account

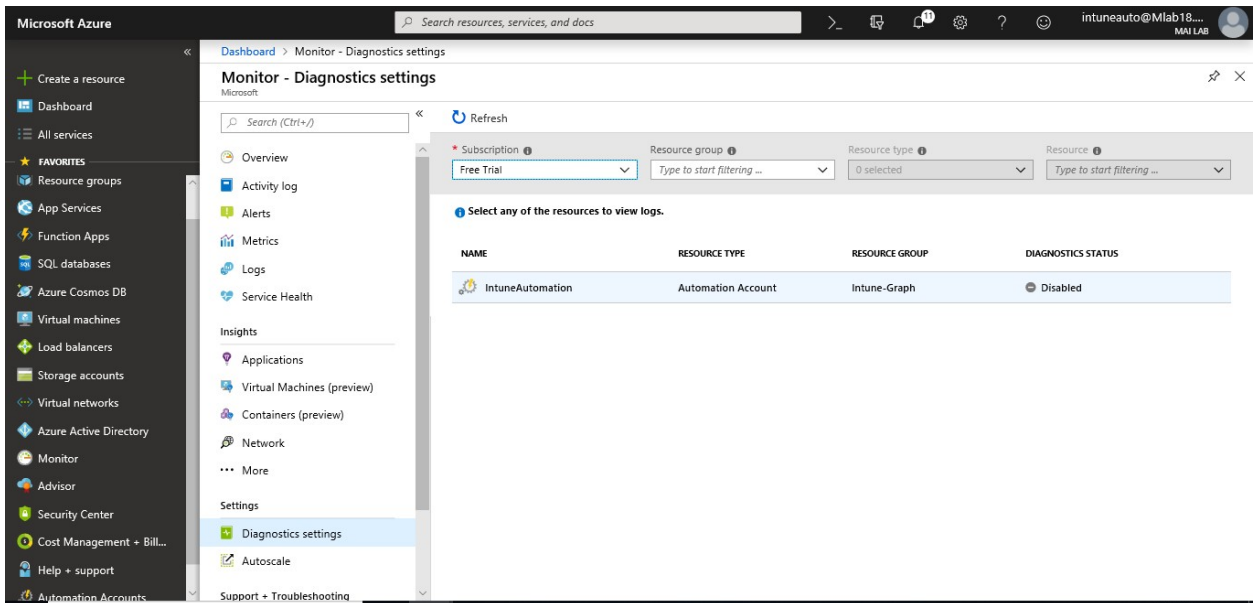
You can enable collection of resource diagnostic logs in the Azure portal after a resource has been created either by going to a specific resource or by navigating to Azure Monitor. To enable this via Azure Monitor:

1. In the [Azure portal](#), navigate to **All services > Monitor**.

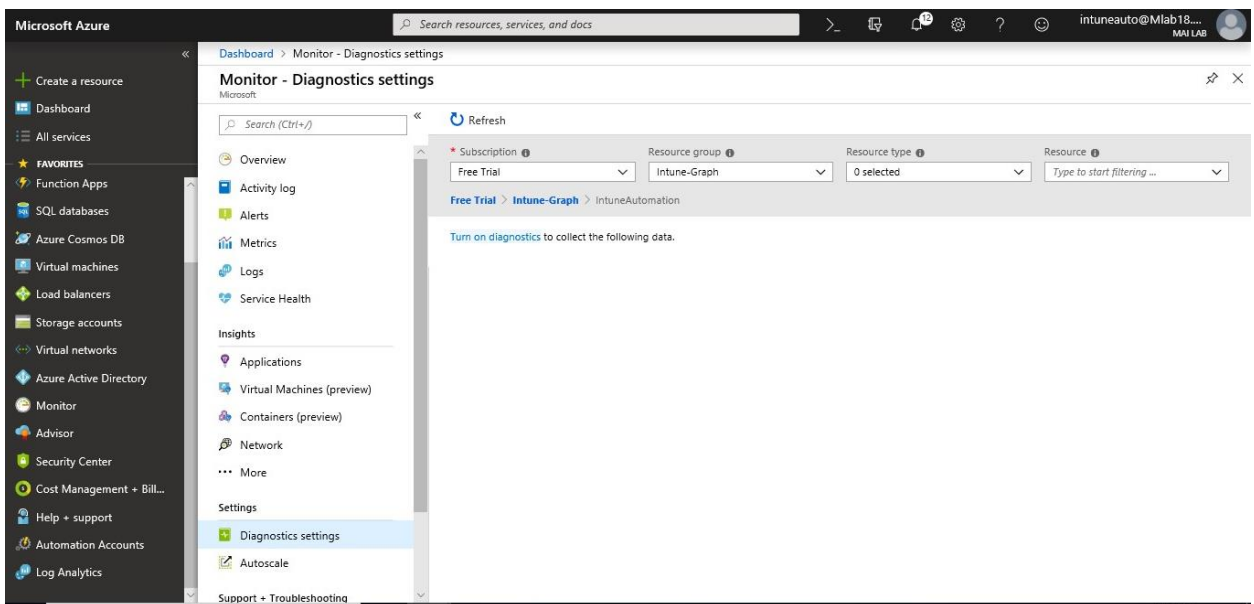


Microsoft Intune step by step on Azure portal

2. On **Monitor Blade**, Select **Diagnostic Settings** > you should find your account automation diagnostic is disabled by default.



3. If no settings exist on the resource you have selected, you are prompted to create a setting. Click "**Turn on diagnostics.**"

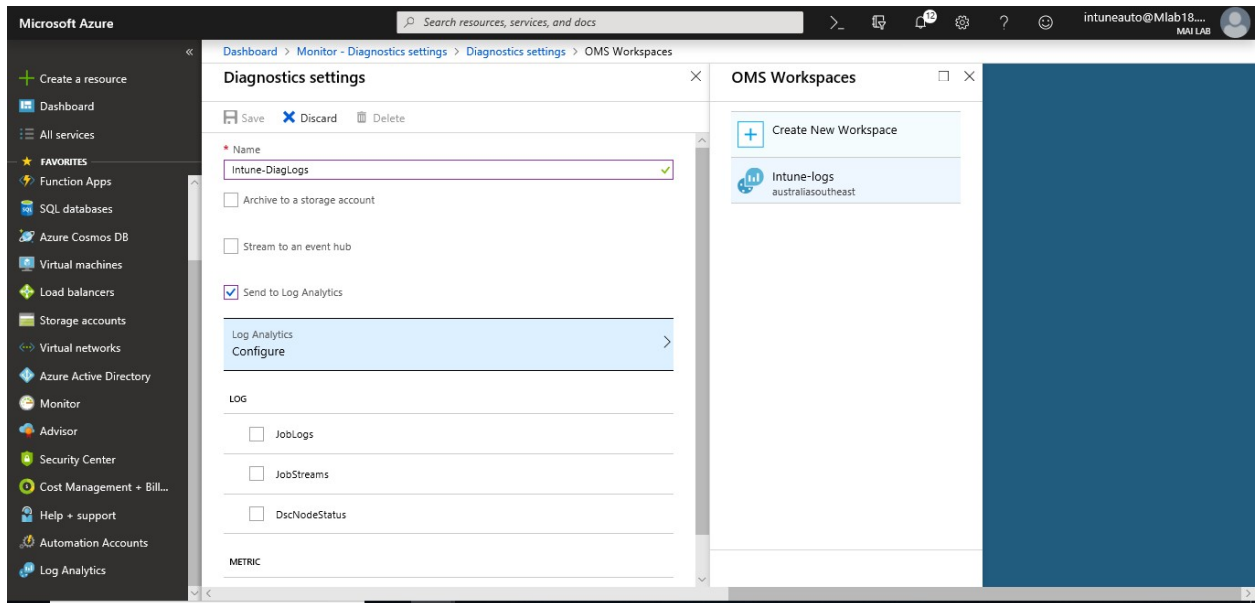


If there are existing settings on the resource, you will see a list of settings already configured on this resource. Click "**Add diagnostic setting.**"

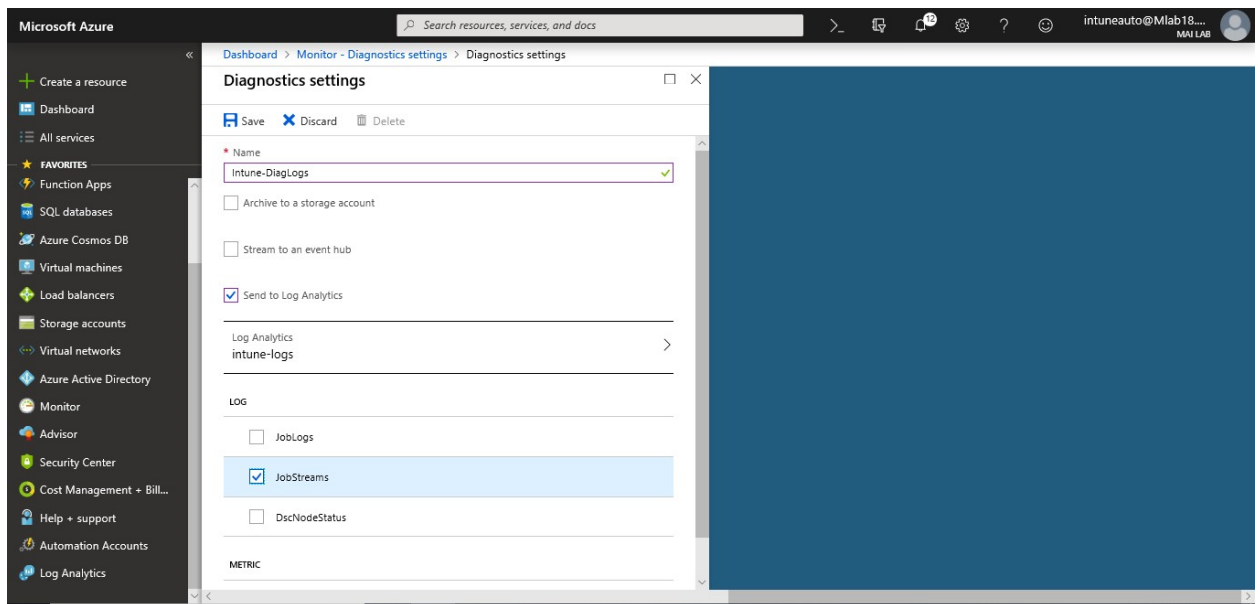
4. Give your setting a name, check the boxes for each destination to which you would like to send data, and configure which resource is used for each destination. Optionally, set a

Microsoft Intune step by step on Azure portal

number of days to retain these logs by using the **Retention (days)** sliders (only applicable to the storage account destination). A retention of zero days stores the logs indefinitely.

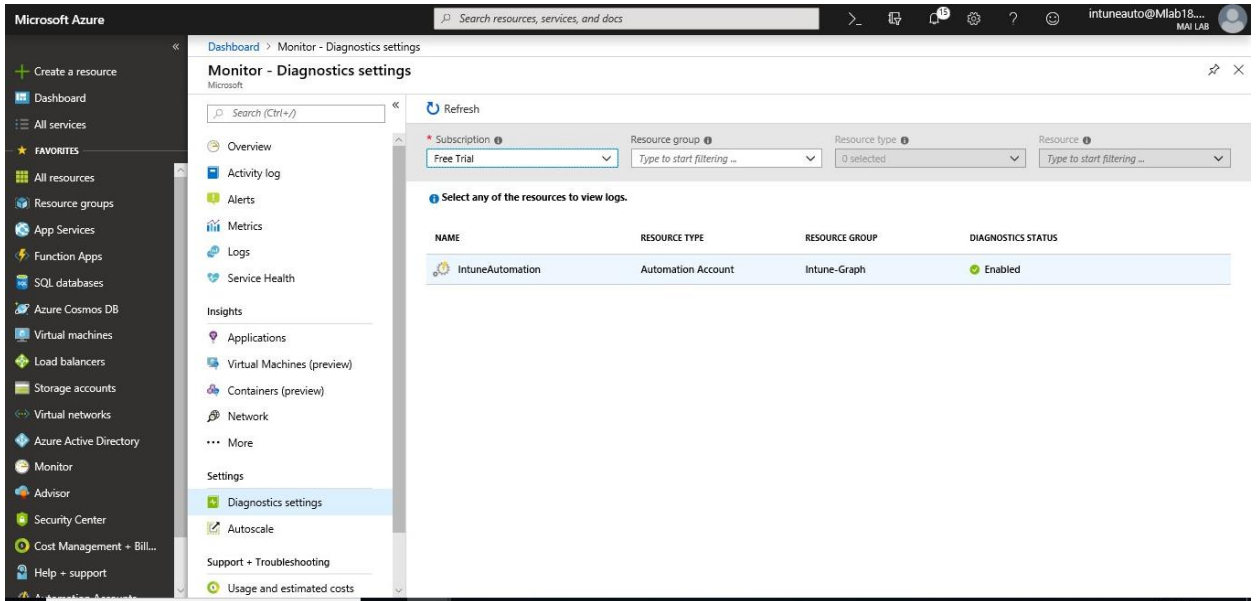
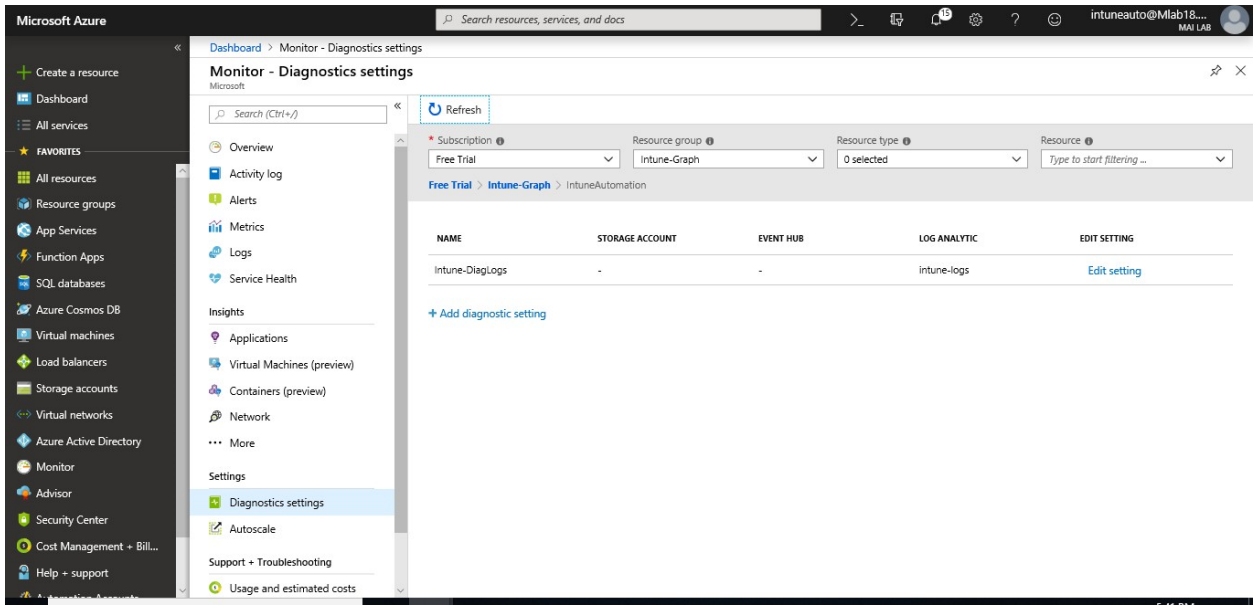


5. Click **Save**.



6. Now diagnostic settings option is created.

Microsoft Intune step by step on Azure portal

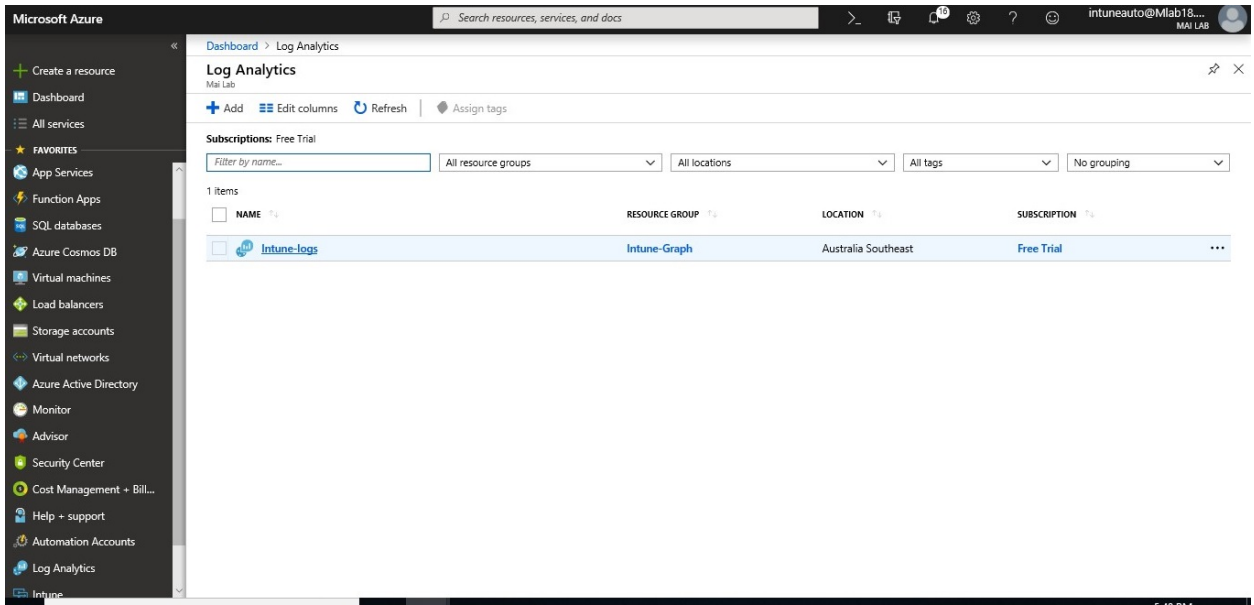


Step 12: Run Log analytics Query

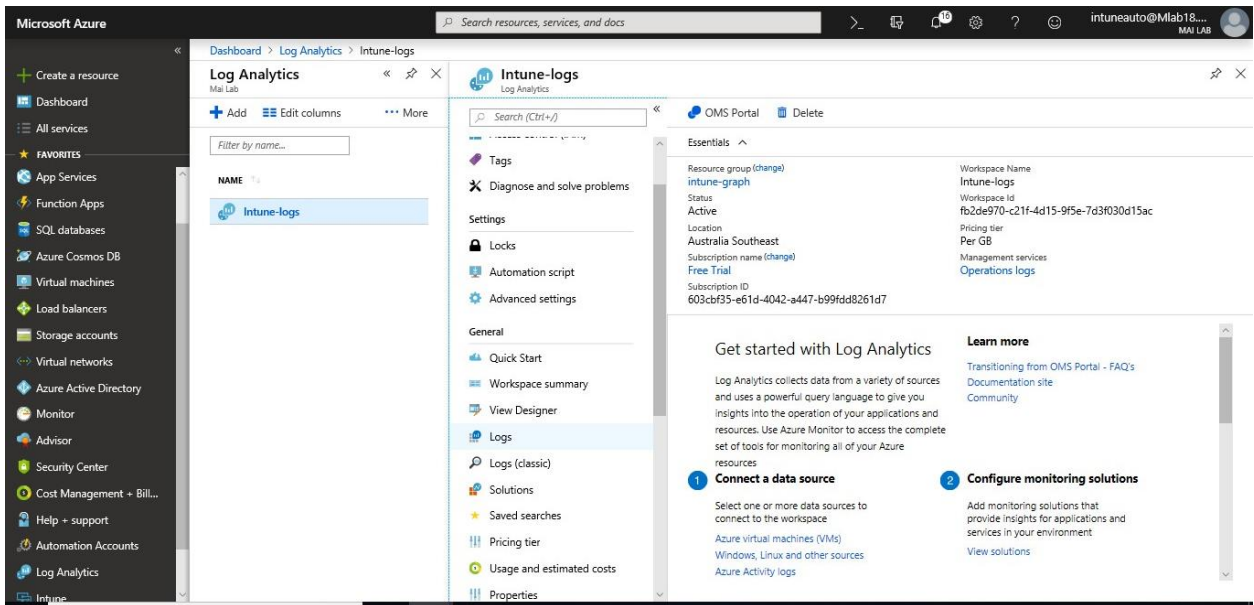
To run log analytics query, you can follow below steps:

1. Login to [Azure Portal](#). Click on **log Analytics**. Open Log analytic that you created before.

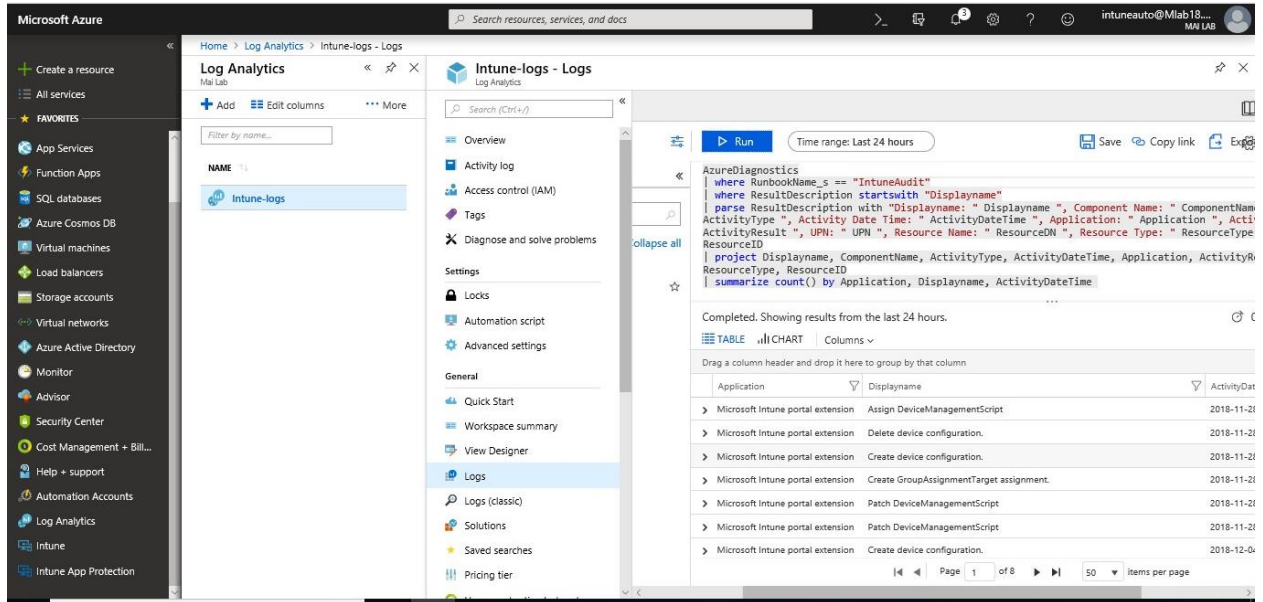
Microsoft Intune step by step on Azure portal



2. On your Log Analytics. Click on the **Log**.



3. Type the query that you want. Then click **Run**.



Note: You can type query to get all audit data for Intune as Jan Ketil did. If you want to get audit to specific component, you need only to type of the component e.g. *where ComponentName == "MobileApp"* before line */ summarize*.

AzureDiagnostics

```

/where RunbookName_s == "IntuneAudit"
/where ResultDescription startswith "Displayname"
/parse ResultDescription with "Displayname: " Displayname ", Component Name: "
ComponentName ", ActivityType: " ActivityType ", Activity Date Time: "
ActivityDateTime ", Application: " Application ", Activity Result: " ActivityResult ",
UPN: " UPN ", Resource Name: " ResourceDN ", Resource Type: " ResourceType ",
Resource ID: " ResourceID
/project Displayname, ComponentName, ActivityType, ActivityDateTime, Application,
ActivityResult, UPN, ResourceDN, ResourceType, ResourceID
/summarize count() by Application, Displayname, ActivityDateTime
    
```

4. Then click **Chart** > on stack column, click **Pie**. Then click on **Display Name**.

Microsoft Intune step by step on Azure portal

The screenshot shows the 'Intune-logs - Logs' page in the Azure portal. The query editor contains the following Kusto query:

```
AzureDiagnostics
| where RunbookName_s == "IntuneAudit"
| where ResultDescription startswith "Displayname"
| parse ResultDescription with "Displayname: " Displayname ", Component Name: " ComponentName ", ActivityType: " ActivityType ", Application: " Application ", ActivityResult: " ActivityResult ", UPN: " UPN ", Resource Name: " ResourceDN ", Resource Type: " ResourceType ", ResourceID
| project Displayname, ComponentName, ActivityType, ActivityDateTime, Application, ActivityResult, UPN, ResourceID
| summarize count() by Application, Displayname, ActivityDateTime
```

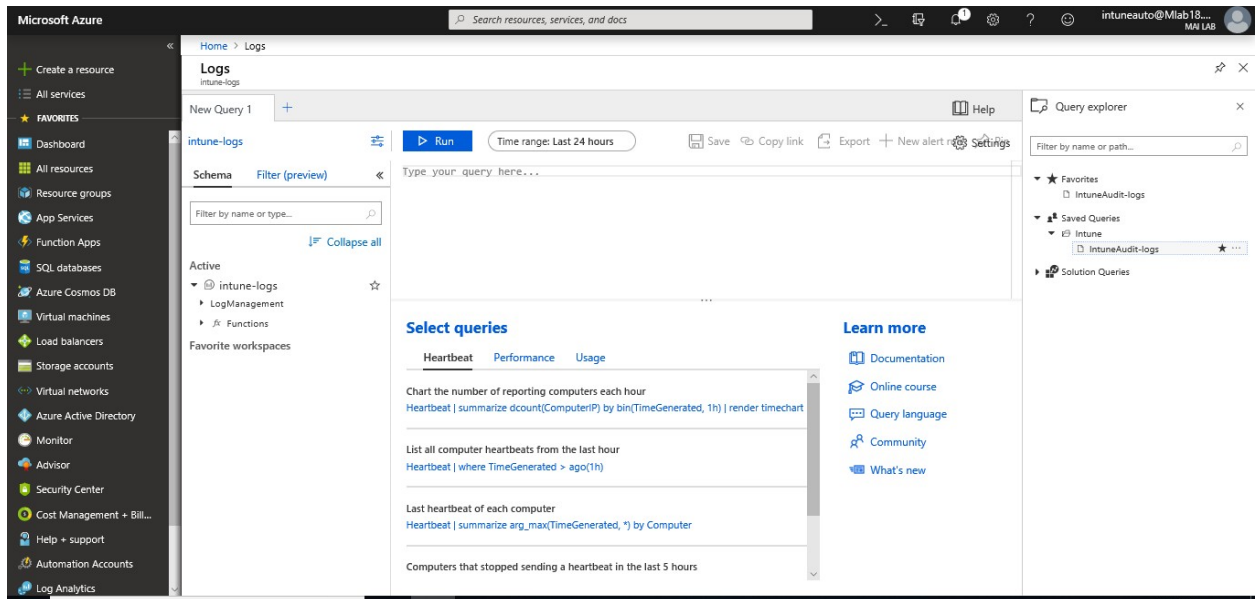
The results are displayed as a pie chart with various categories and their percentages, such as 'Update device config' (10.66%) and 'Create device category' (4.82%).

5. Then click **Save** to save this query and type name of category for this query.

The screenshot shows the 'Intune-logs - Logs' page in the Azure portal. The query editor contains the same Kusto query as in the previous screenshot. A 'Save' dialog box is open, showing the query name 'IntuneAudit-logs' and the category 'Intune'.

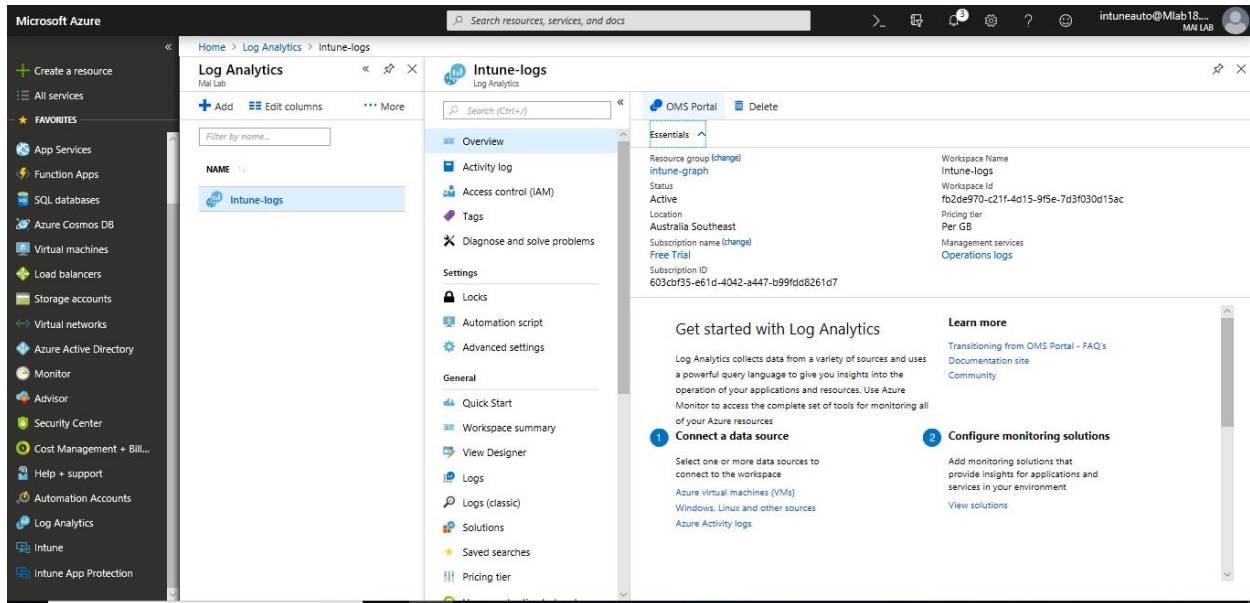
6. Then you should find saved query on **Query explorer**.

Microsoft Intune step by step on Azure portal



Step 13: Create views for query in Azure Log Analytics

You can create a new view in View Designer by selecting **View Designer** in the menu of your Log Analytics workspace.



View Designer has three panes:

- **Design:** Contains the custom view that you're creating or editing. Click **Donut**.
- **Controls:** Contains the tiles and parts that you add to the **Design** pane.
- **Properties:** Displays the properties of the tiles or selected parts.
 - Type title for Graph.

Microsoft Intune step by step on Azure portal

- On Query, type same query that you put it on logs but on summary select Type Activity only. **“/ summarize count() by ActivityType”**

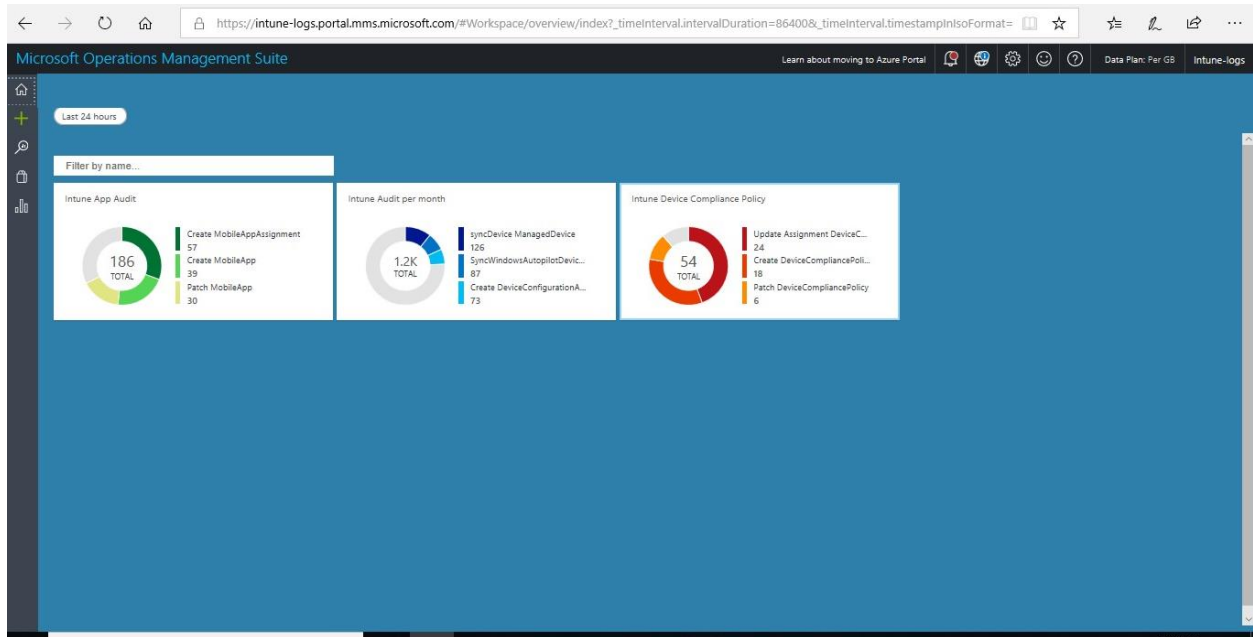
The screenshot shows the Microsoft Azure View Designer interface. The main view displays a donut chart titled "Intune Audit per month" with a total of 786. The chart is divided into three segments: "syncDevice Managed..." (84), "SyncWindowsAutopi..." (58), and "Create DeviceConfig..." (49). The Properties panel on the right shows the query: `:" Activity(Result | summarize count() by ActivityType`. The Properties panel also shows the center value as "Total" and the operation as "Sum".

Once you finished your view designer, click **Save**. Then you can add many view for each component as you want. e.g., for Mobile App & Device compliance Policy.

The screenshot shows the Microsoft Azure View Designer interface. The main view displays a donut chart titled "Intune App Audit" with a total of 186. The chart is divided into three segments: "Create MobileApp..." (57), "Create MobileApp" (39), and "Patch MobileApp" (30). The Properties panel on the right shows the query: `:" Activity(Result | summarize count() by ActivityType`. The Properties panel also shows the center value as "Total" and the operation as "Sum".

Now if you log in to OMS Portal, you should find all views that you created it.

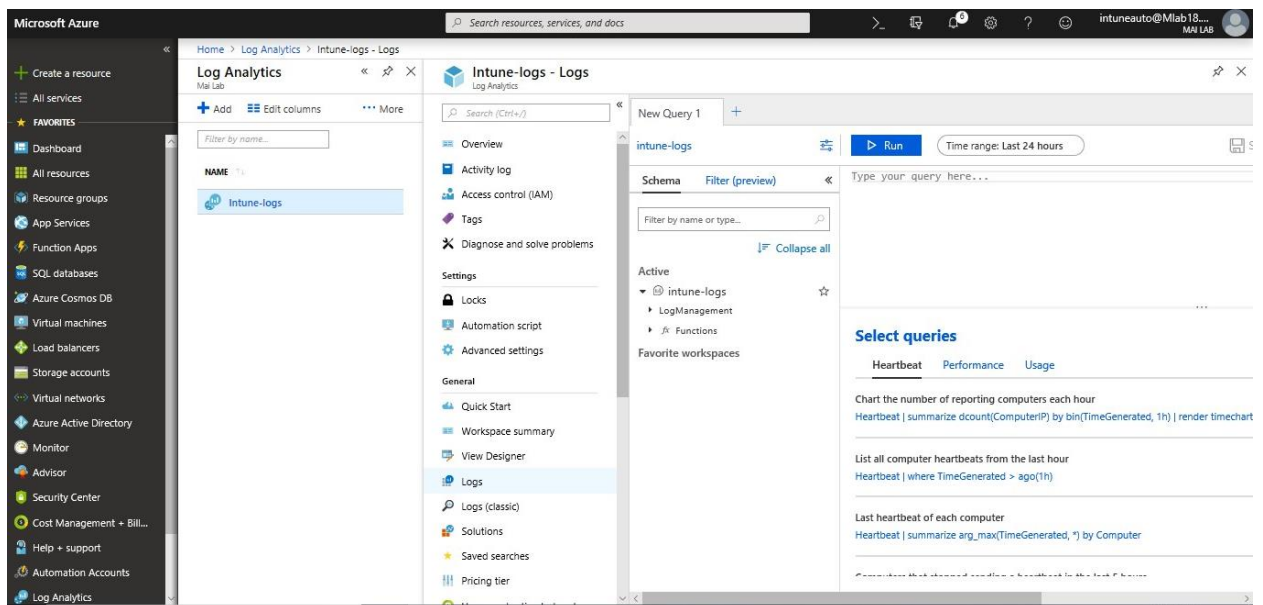
Microsoft Intune step by step on Azure portal



Step 14: Create alerts for query in Azure Log Analytics

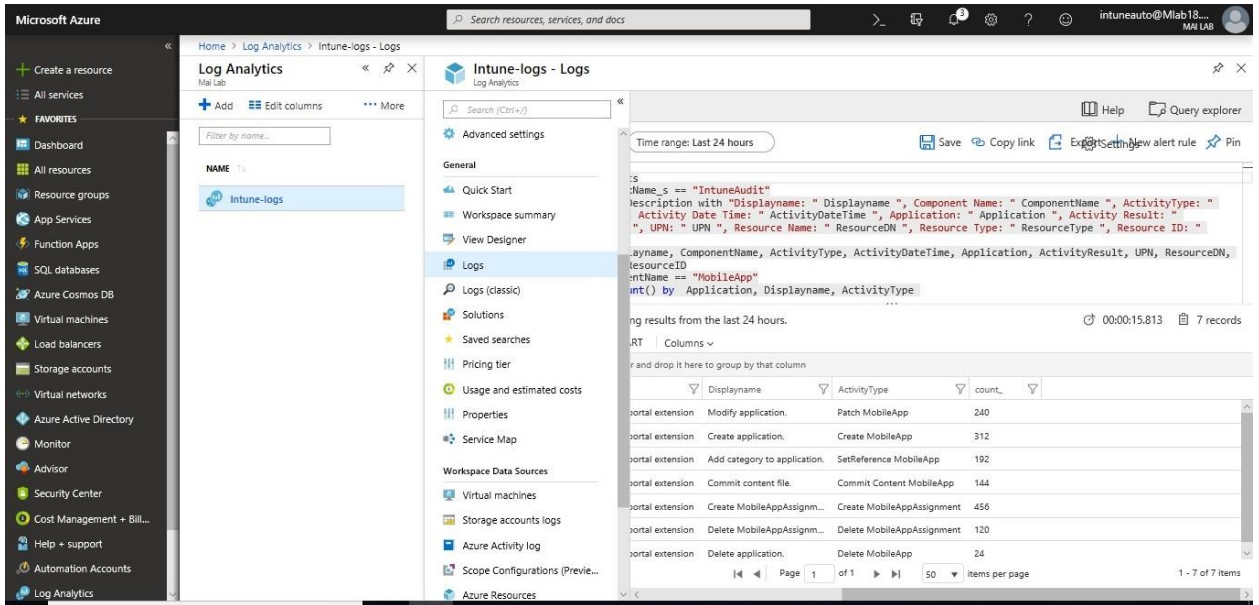
To create alert for log analytics query, you can follow below steps:

1. You can create a new Alert by selecting **Log** in the menu of your Log Analytics workspace.



2. Type the query that you want or point to saved query then Click **Run**. Then click **New Alert rule**.

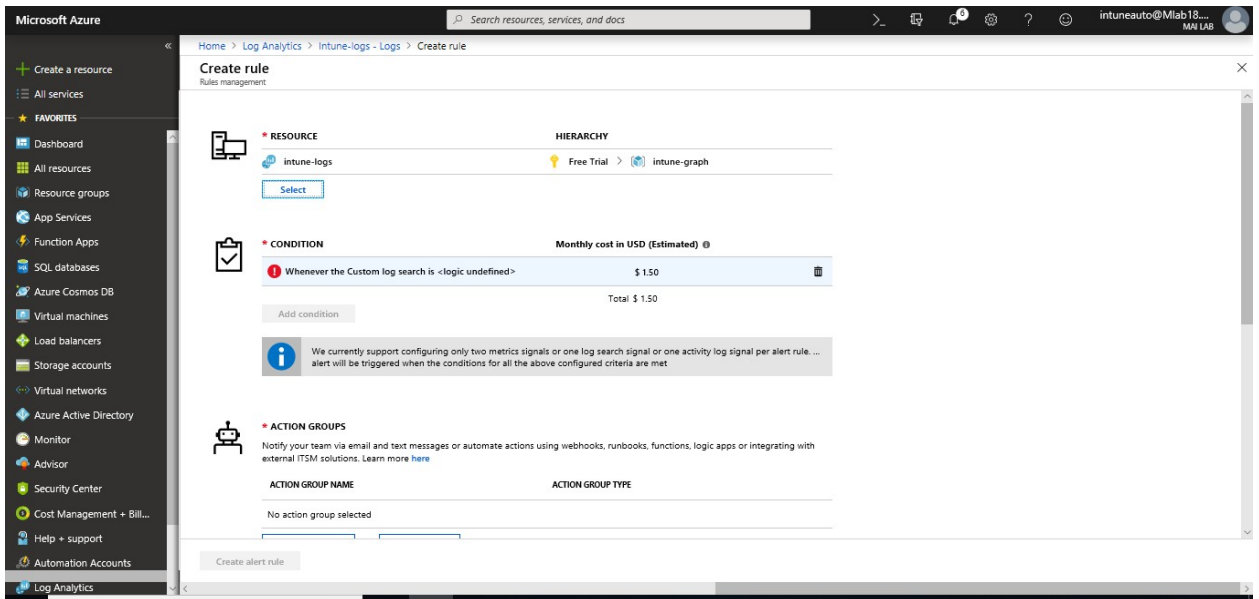
Microsoft Intune step by step on Azure portal



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains navigation options like 'Create a resource', 'All services', and 'FAVORITES'. The main content area is titled 'Intune-logs - Logs' and shows a list of logs. The logs are filtered by the last 24 hours. The table below shows the results:

Displayname	ActivityType	count
portal extension Modify application.	Patch MobileApp	240
portal extension Create application.	Create MobileApp	312
portal extension Add category to application.	SetReference MobileApp	192
portal extension Commit content file.	Commit Content MobileApp	144
portal extension Create MobileAppAssignm...	Create MobileAppAssignment	456
portal extension Delete MobileAppAssignm...	Delete MobileAppAssignment	120
portal extension Delete application.	Delete MobileApp	24

3. On Create Rule Page, select condition.



The screenshot shows the Microsoft Azure portal interface. The left sidebar contains navigation options like 'Create a resource', 'All services', and 'FAVORITES'. The main content area is titled 'Create rule' and shows the 'CONDITION' tab. The condition is 'Whenever the Custom log search is <logic undefined>' with a threshold of \$1.50. The page also shows the 'ACTION GROUPS' section.

4. On Condition tab, type your threshold that you want to alert after it.

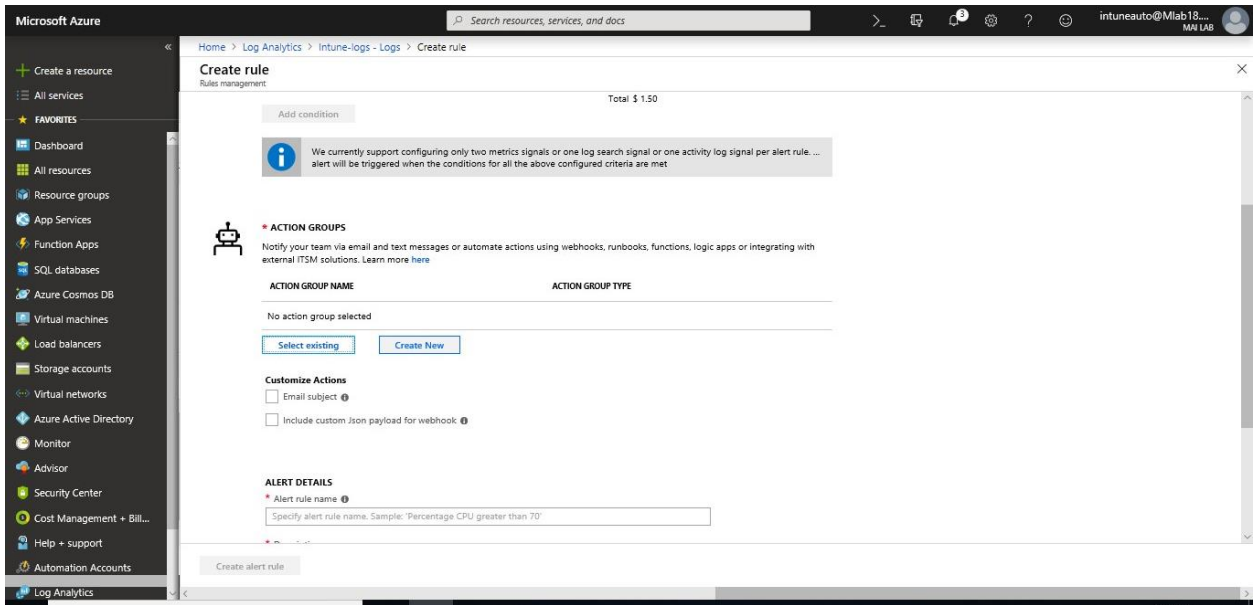
Microsoft Intune step by step on Azure portal

The screenshot shows the 'Create rule' configuration page in the Microsoft Azure portal. The left sidebar contains navigation options like 'Dashboard', 'All resources', and 'Log Analytics'. The main content area is titled 'Create rule' and includes sections for 'RESOURCE' (intune-logs), 'CONDITION' (Monthly cost in USD (Estimated) with a value of \$ 1.50), and 'ACTION GROUPS' (No action group selected). A 'Configure signal logic' panel is open on the right, displaying a search query and alert logic settings.

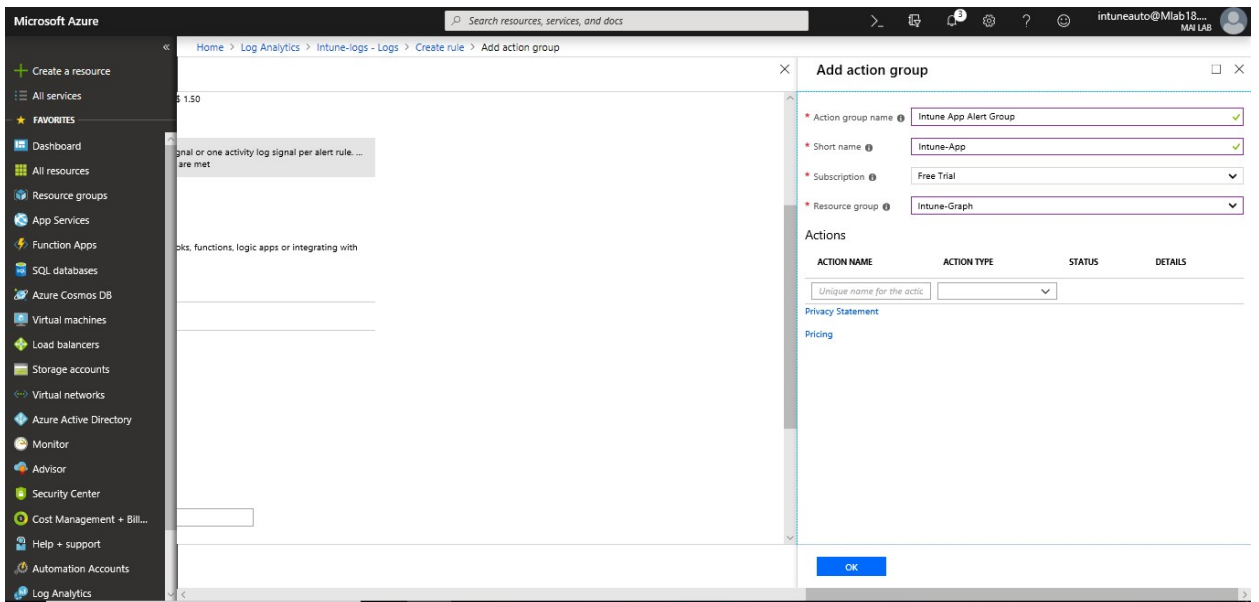
5. Then Click **Done** to create condition.

The screenshot shows the 'Create rule' configuration page in the Microsoft Azure portal. The 'CONDITION' section is now green, indicating it has been successfully created. The 'ACTION GROUPS' section is still empty. The 'Configure signal logic' panel is no longer visible.

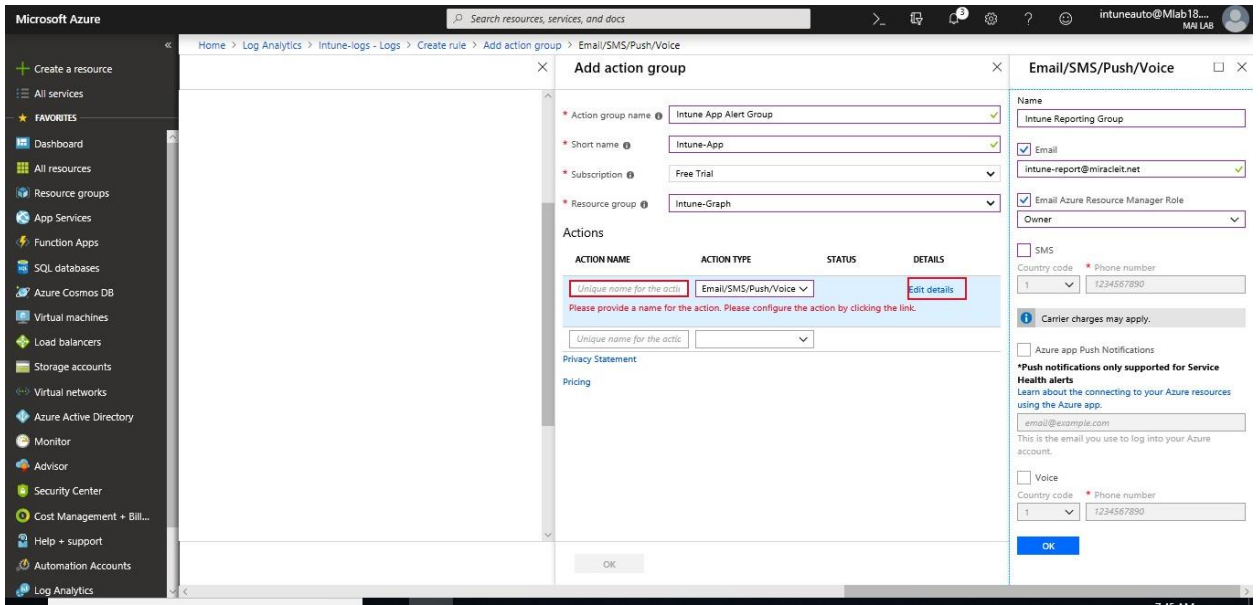
6. On **Action Groups**, if you already have action group select it or create new one.



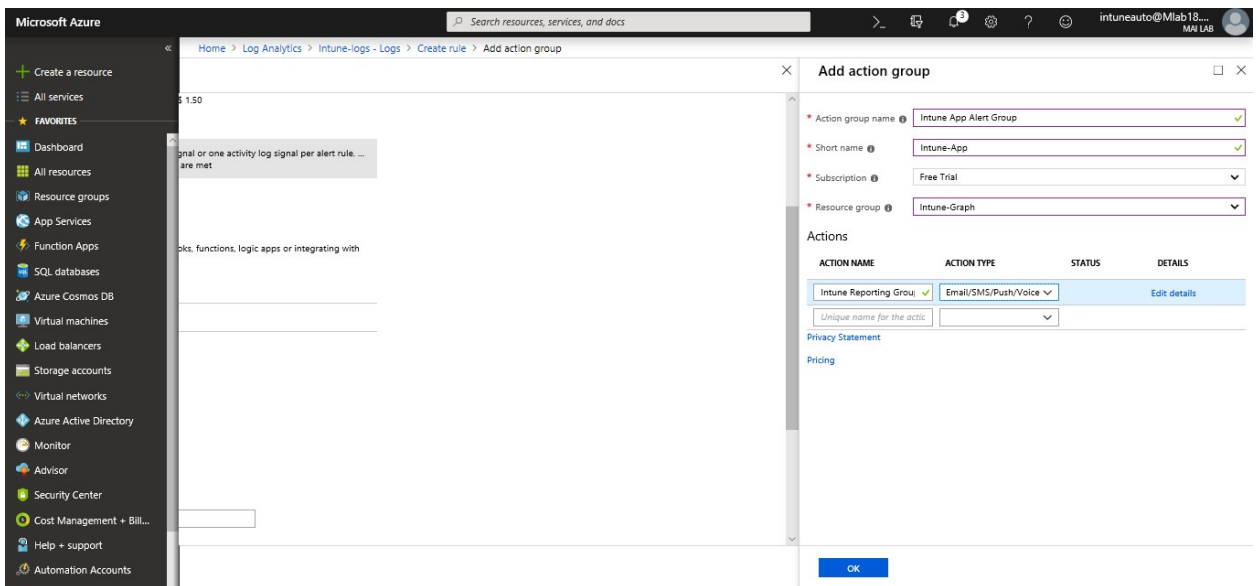
7. On Create New Action Group, type name of this group and select resource group then select **Action Type**.



8. Once you select action type: **Email/SMS/Push**, it will open new window to enter the following: Name of action & email address.



9. Once you finish click **Ok** to create action Group.



10. You can create **custom Email Subject** if you want, Check on **Email subject** and enter title.

11. Now moving onto the final step, provide a name of your alert in the **Alert rule name** field, such as **Audit on Application**. Specify a **Description** detailing specifics for the alert and select **Warning (Sev 1)** for the **Severity** value from the options provided.

12. To immediately activate the alert rule on creation, accept the default value for **Enable rule upon creation**.

Microsoft Intune step by step on Azure portal

Microsoft Azure

Home > Log Analytics > Intune-logs - Logs > Create rule

Create rule
Rules management

Intune App Alert Group 1 Email, 1 Email Azure Resource Manager Role

Select existing Create New

Customize Actions

- Email subject
- * Subject line: Intune App Alert ✓
- Include custom json payload for webhook

ALERT DETAILS

- * Alert rule name: Audit on Application ✓
- * Description: This alert to notify if there is any change happened on Intune Application. Create application or update or delete any application ✓
- * Severity: Warning(Sev 1) ▼

Enable rule upon creation: Yes No

Create alert rule

13. Then click **Create alert rule** to save the alert.

Microsoft Azure

Home > Log Analytics > Intune-logs - Logs > Create rule

Create rule
Rules management

Select existing Create New

Customize Actions

- Email subject
- * Subject line: Intune App Alert ✓
- Include custom json payload for webhook

ALERT DETAILS

- * Alert rule name: Audit on Application ✓
- * Description: This alert to notify if there is any change happened on Intune Application. Create application or update or delete any application ✓
- * Severity: Warning(Sev 1) ▼

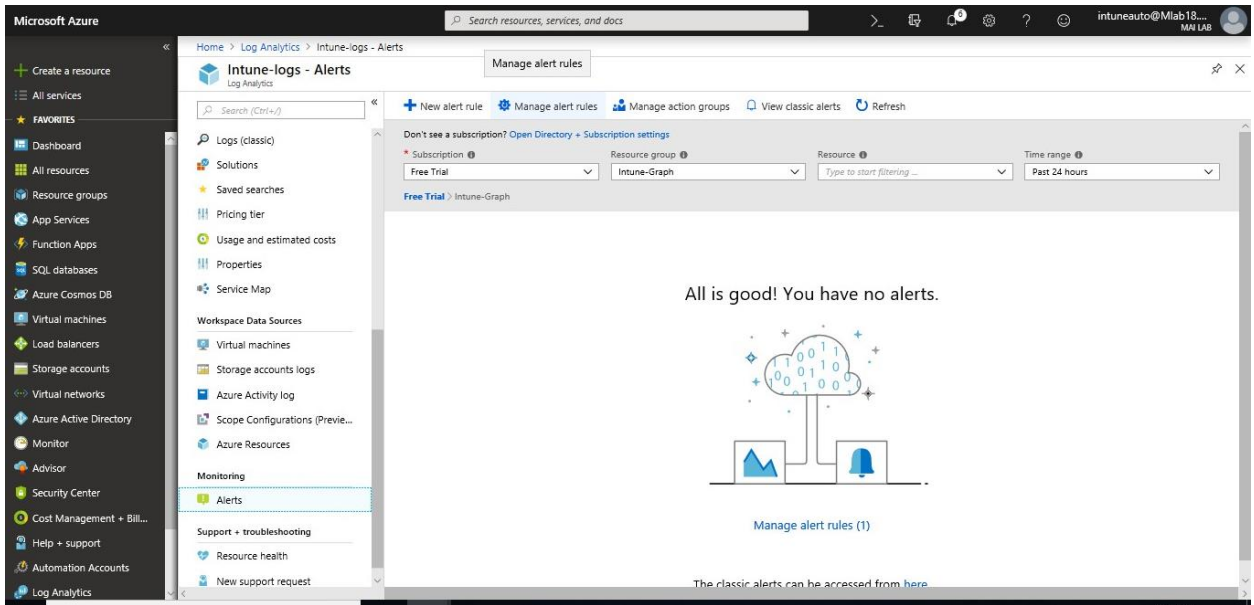
Enable rule upon creation: Yes No

Suppress Alerts

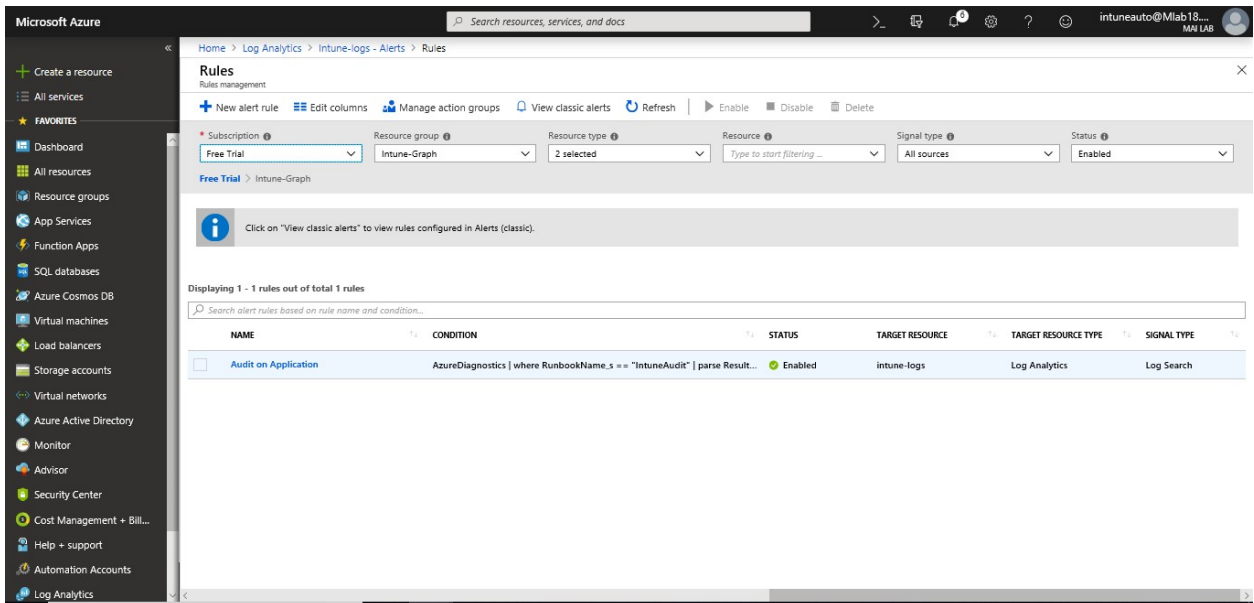
Create alert rule

14. To check created alert by selecting **Alerts** in the menu of your Log Analytics workspace.

Microsoft Intune step by step on Azure portal



15. Then Click **Manage alerts rules**, you should find the alert rule that you created.



16. Now anyone member for action group should receive alert according to created query.

Microsoft Intune step by step on Azure portal

The screenshot shows the Outlook interface with an email titled "Intune App Alert" from Microsoft Azure. The email content includes a notification about a triggered Azure Monitor alert and a table of alert details.

Intune App Alert

Microsoft Azure <azure-noreply@microsoft.com>
Today, 8:38 AM
Intune Reporting Group

To help protect your privacy, some content in this message has been blocked. To re-enable the blocked features, [click here](#).

To always show content from this sender, [click here](#).

Microsoft Azure

Your Azure Monitor alert was triggered

We are notifying you because there are 7 counts of "Audit on Application".

Essentials

Name	Audit on Application
Severity	1
Resource	Intune-logs
Search interval start time	December 6, 2018 5:12 UTC
Search interval duration	5 min

Chapter 11

Resource Access Profile with Microsoft Intune

Microsoft Intune **resource access profiles** work together to help your users gain access to the files and resources they need to do their work successfully, wherever they are.

Intune provides the following mobile device policies that help you to accomplish this goal:

Intune policy	What it does	Windows 8.1 and later	Windows 10 (desktop) and Windows 10 Mobile	iOS 8.0 or later	Android	Samsung KNOX	Android Enterprise (Android for work)
Certificate Profiles	Help secure access to company resources including wireless networks and VPN connections.	Yes	Yes	Yes	Yes	Yes	Yes
Wi-Fi Profiles	Deploy wireless network settings to your users. By deploying these settings, you minimize the end-user effort required to connect to the corporate network.	Yes (you can import a Windows Wi-Fi profile)	Yes	Yes	Yes	Yes	Yes
VPN Profiles	Deploy Virtual Private Network (VPN) settings to your users. By deploying these settings, you minimize the end-user effort required to connect to resources on the corporate network.	Yes	Yes	Yes	Yes	Yes	Yes
Email Profiles	Create, deploy and monitor Exchange ActiveSync email settings on devices in your organization.	No	Yes	Yes	No	Yes	Yes

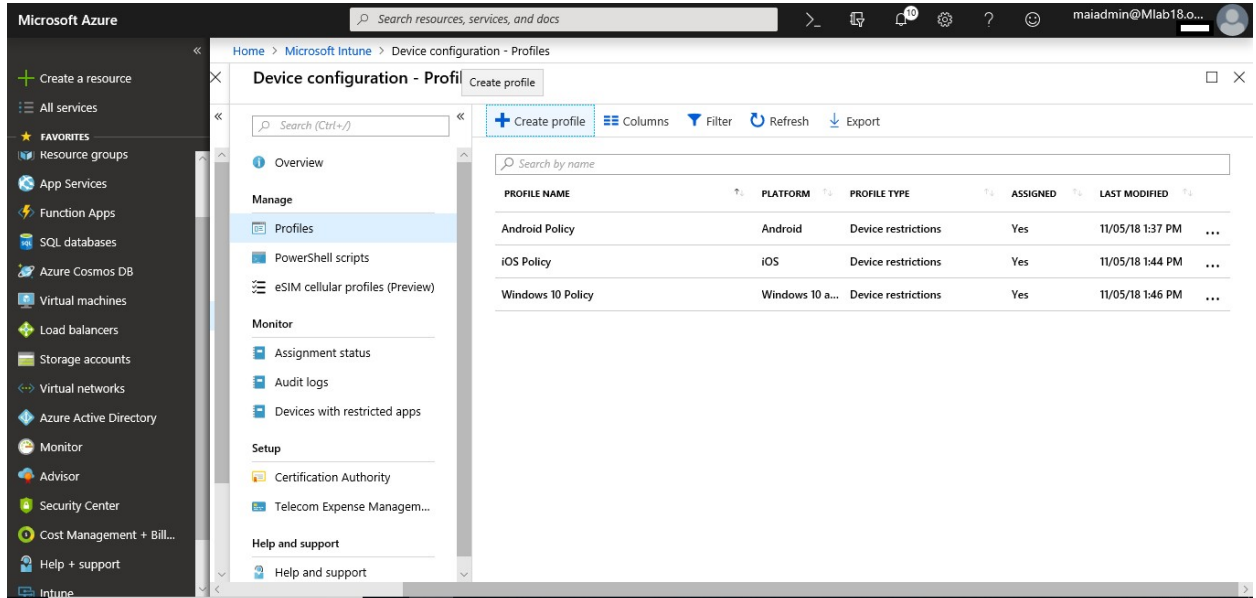
Enable access to corporate email using email profiles

Email profiles in Microsoft Intune help you create, deploy and monitor Exchange ActiveSync email settings on devices. This lets user's access corporate email on their corporate devices without any required setup on their part.

These steps will help you deploy an email profile for iOS devices.

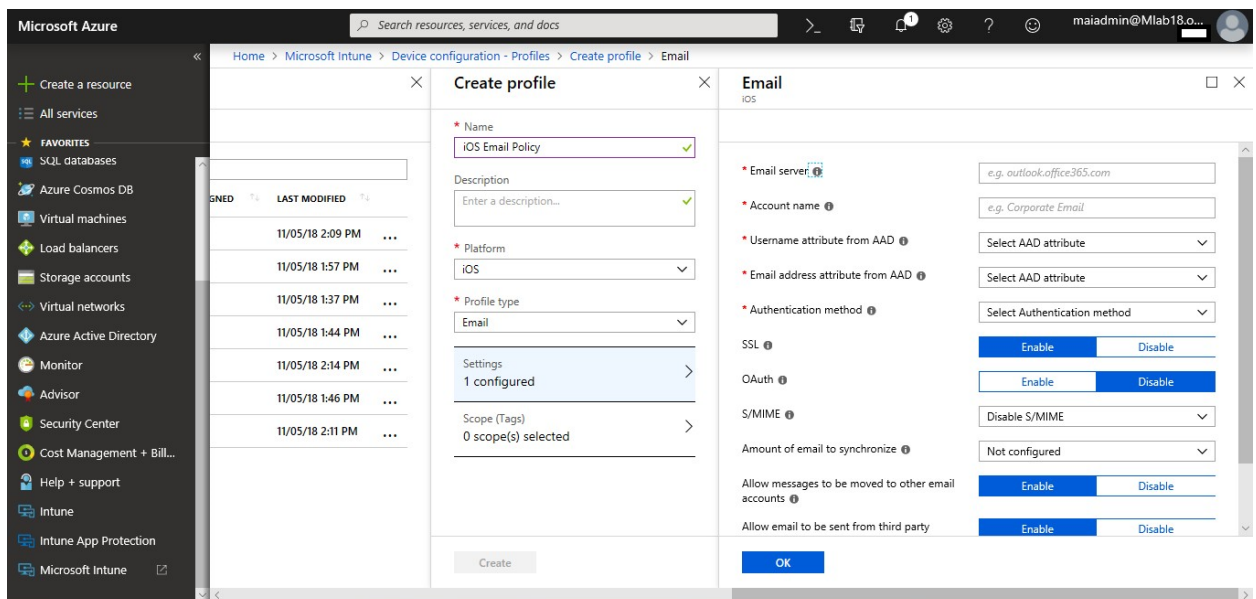
1. From the [Azure Portal](#), Select **All services** > **Intune**. Intune is located in the **Monitoring + Management** section.

2. In the **Intune** pane, click on **Device Configuration > Profiles**. Click on **create profile**.



3. Type a name for the policy “iOS Email Policy”. Enter the following profile information:

- For **Description**, enter description or leave it blank.
- For **Platform**, select **iOS**.
- For **Profile type**, select **Email**.



4. Select **Settings**, and enter the following settings (leave the defaults for other settings):

- **Email server**: enter **outlook.office365.com**. This setting specifies the Exchange location (URL) of the email server that the iOS mail app will use to connect to email.

Microsoft Intune step by step on Azure portal

- **Account name:** Enter **Company Email**.
- **Username attribute from AAD:** select **User Principal Name** to be used as the username for the profile.
- **Email address attribute from AAD:** select **User Principal Name**.
- **Authentication method:** select **Username and password**.

Microsoft Azure

Home > Microsoft Intune > Device configuration - Profiles > Create profile > Email

Create profile

Name: iOS Email Policy

Description: Enter a description...

Platform: iOS

Profile type: Email

Settings: 1 configured

Scope (Tags): 0 scope(s) selected

Email configuration:

- Email server: outlook.office365.com
- Account name: Mlab18 Email
- Username attribute from AAD: User Principal Name
- Email address attribute from AAD: User Principal Name
- Authentication method: Username and password
- SSL: Enable
- S/MIME: Disable S/MIME
- Amount of email to synchronize: Not configured
- Allow messages to be moved to other email accounts: Enable
- Allow email to be sent from third party applications: Enable

Create

5. Select **OK**.
6. Select **Create**. The new profile appears on the profiles list with the dashboard displayed.

Microsoft Azure

Home > Microsoft Intune > Device configuration - Profiles > Create profile

Create profile

Name: iOS Email Policy

Description: Enter a description...

Platform: iOS

Profile type: Email

Settings: 7 configured

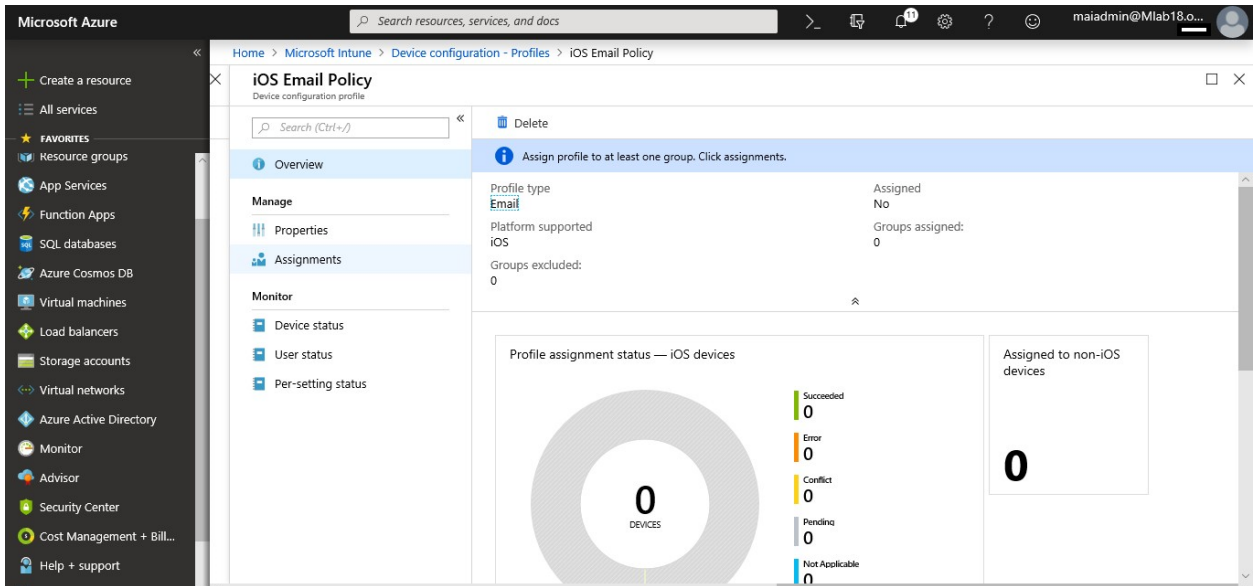
Scope (Tags): 0 scope(s) selected

Create

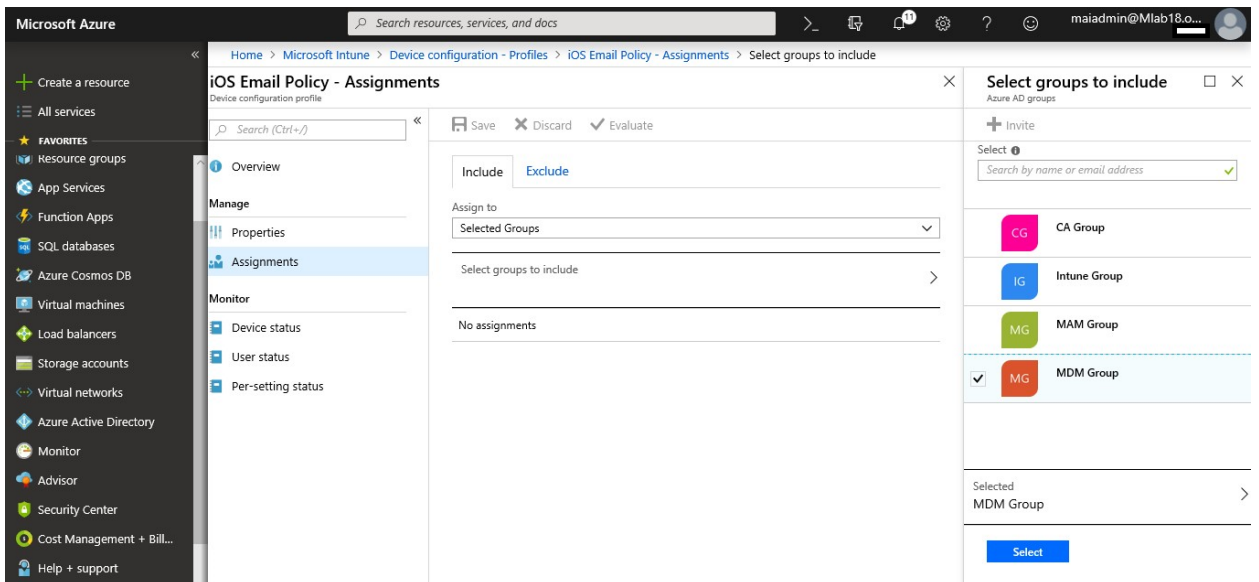
PROFILE NAME	PLATFORM	PROFILE TYPE	ASSIGNED	LAST MODIFIED
Android Policy	Android	Device restrictions	Yes	11/05/18 1:37 PM
iOS Policy	iOS	Device restrictions	Yes	11/05/18 1:44 PM
Windows 10 Policy	Windows 10 a...	Device restrictions	Yes	11/05/18 1:46 PM

7. Select **Assignments**.

Microsoft Intune step by step on Azure portal

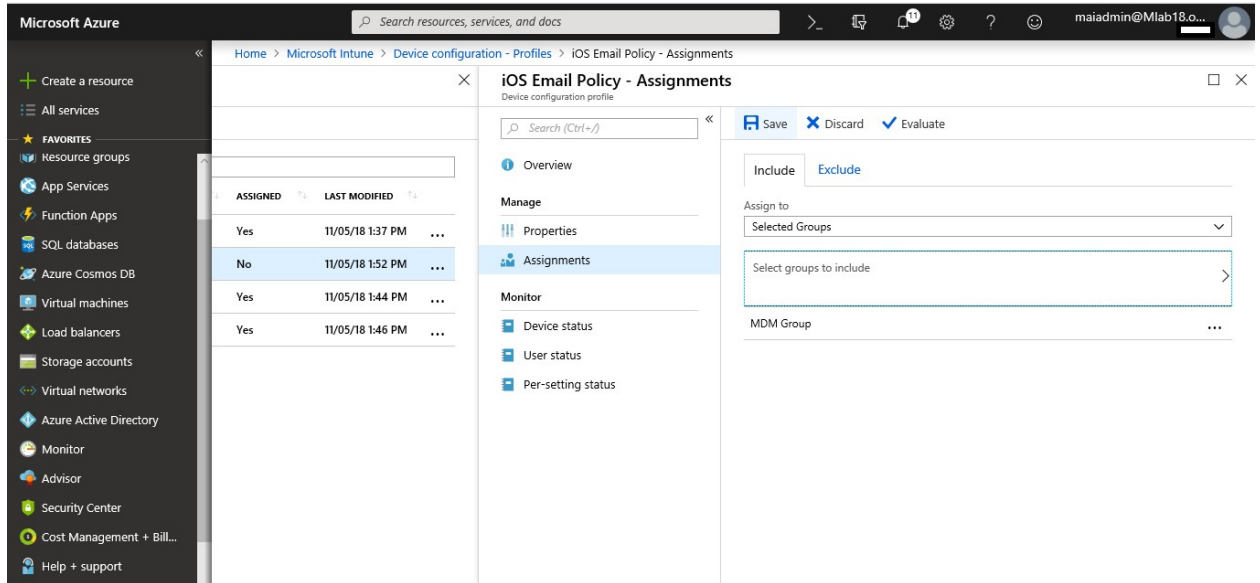


8. Select the **Include** tab, and then select **Group** that want to push email profile to them.



9. Select **Save**.

Microsoft Intune step by step on Azure portal



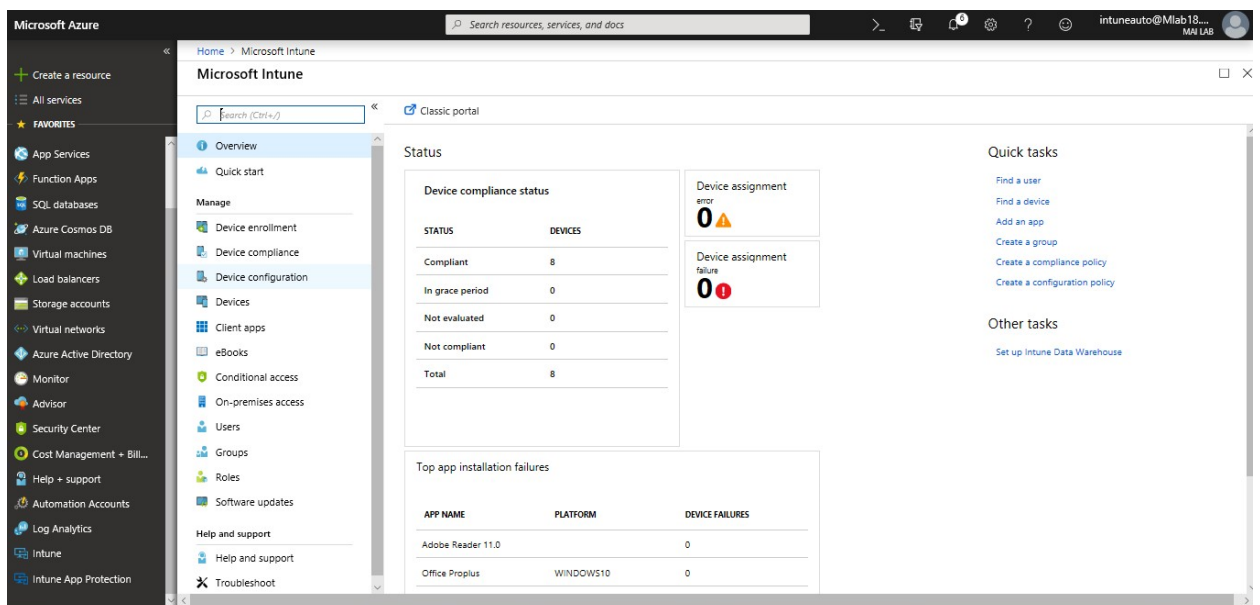
Help users connect to their work using VPN profiles

VPN profiles in Microsoft Intune help you Deploy Virtual Private Network (VPN) settings to your users. By deploying these settings, you minimize the end-user effort required to connect to resources on the corporate network.

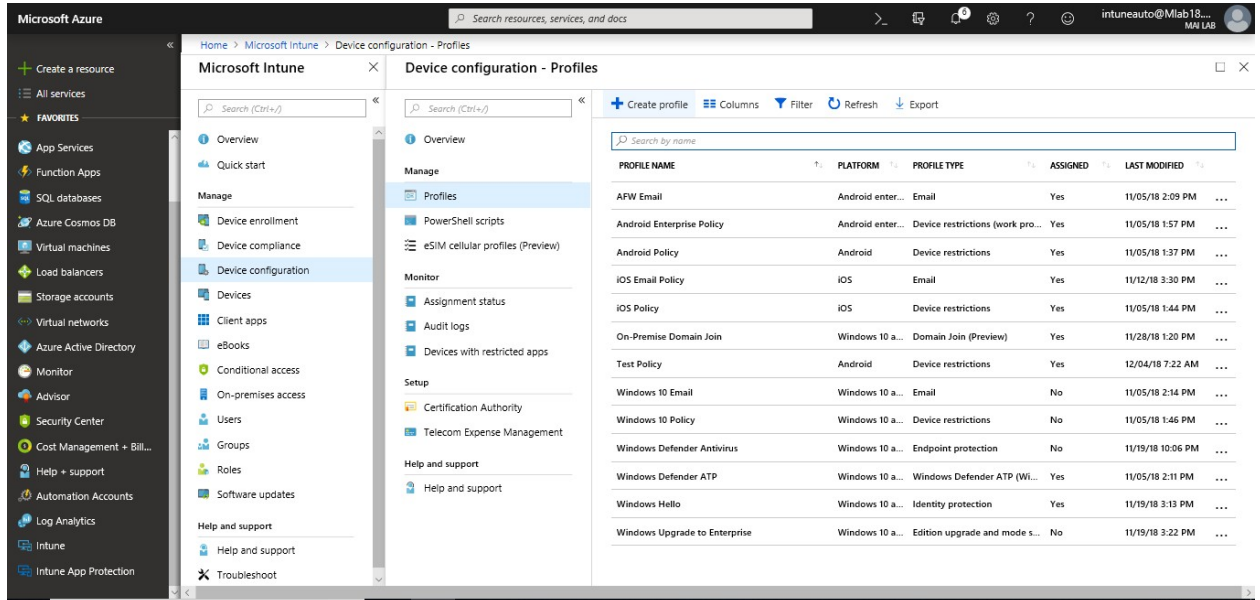
Configure VPN Profile for Windows 10 Devices

These steps will help you deploy an VPN profile for Windows 10 devices.

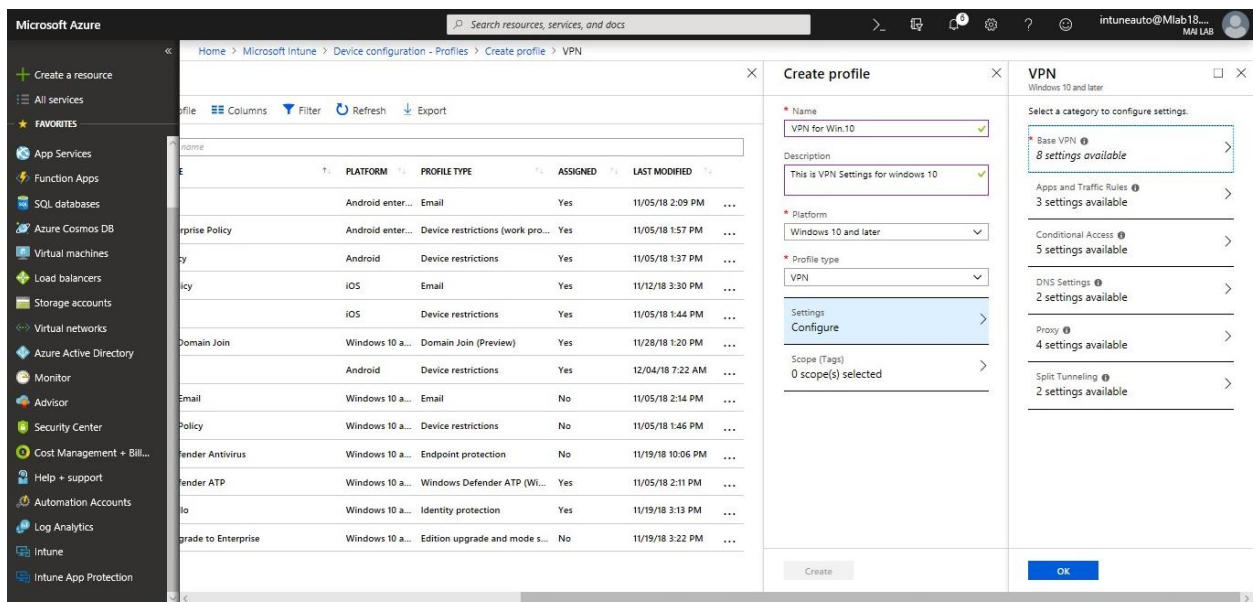
1. Sign in to the [Azure portal](#). Select **All services**, filter on **Intune**, and select **Microsoft Intune**.



2. Select **Device configuration** > **Profiles** > **Create profile**.

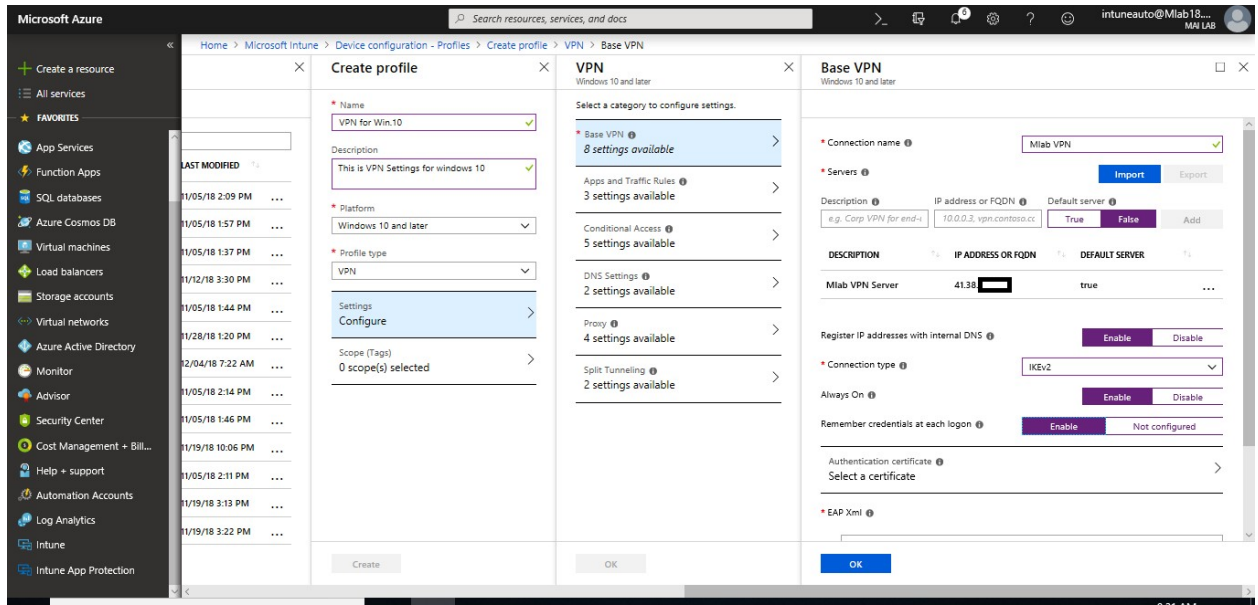


3. Enter a **Name** and **Description** for the VPN profile.
4. From the **Platform** drop-down list, select the device platform to which you want to apply VPN settings. Currently, you can choose one of the following platforms for VPN device settings: **Windows 10 and later**
5. From the **Profile type** drop-down list, choose **VPN**.



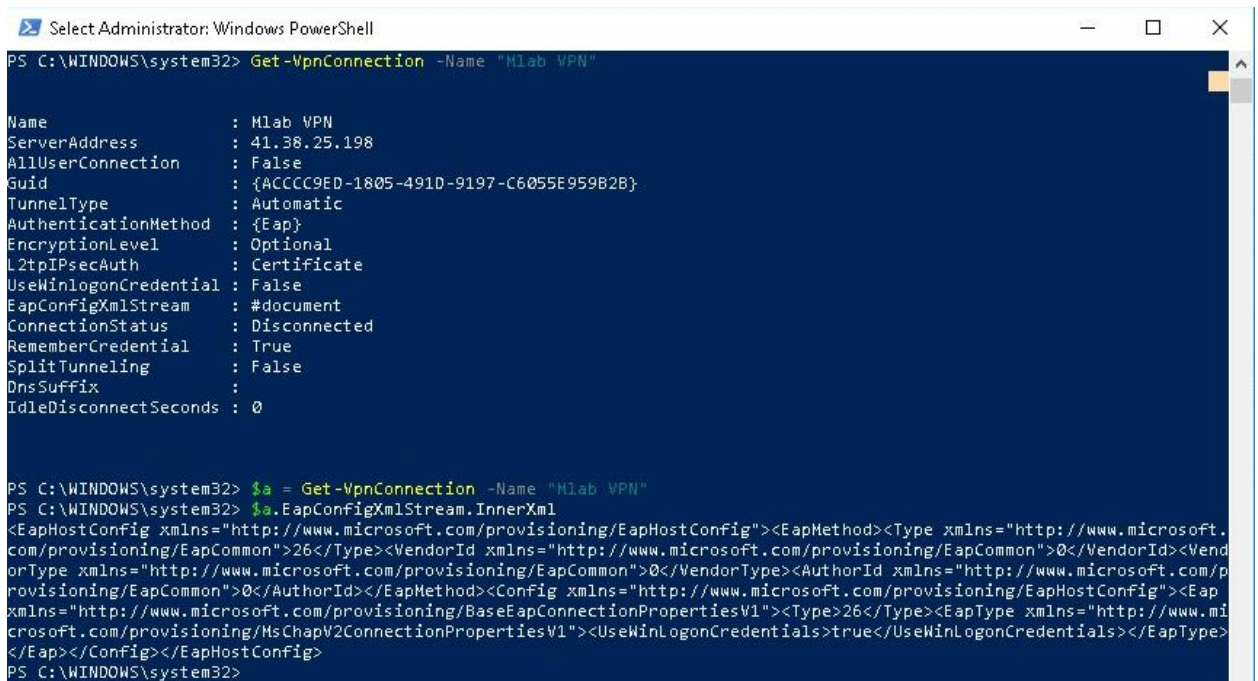
6. Depending on the platform you chose, the settings you can configure are different. Go to one of the following topics for detailed settings for each platform:

Base VPN settings	Description
Connection name	Enter a name for this connection. End users see this name when they browse their device for the list of available VPN connections.
Servers	<p>Add one or more VPN servers that devices connect to. When you add a server, you enter the following information:</p> <ol style="list-style-type: none"> i. Description: Enter a descriptive name for the server, such as Contoso VPN server ii. IP address or FQDN: Enter the IP address or fully qualified domain name of the VPN server that devices connect to, such as 192.168.1.1 or vpn.contoso.com iii. Default server: Enables this server as the default server that devices use to establish the connection. Set only one server as the default. iv. Import: Browse to a comma-separated file that includes a list of servers in the format: description, IP address or FQDN, Default server. Choose OK to import these servers into the Servers list. v. Export: Exports the list of servers to a comma-separated-values (csv) file
Register IP addresses with internal DNS:	Select Enable to configure the Windows 10 VPN profile to dynamically register the IP addresses assigned to the VPN interface with the internal DNS. Select Disable to not dynamically register the IP addresses.
Connection type	<p>Select the VPN connection type from the following list of vendors:</p> <ol style="list-style-type: none"> i. Pulse Secure ii. F5 Edge Client iii. SonicWALL Mobile Connect iv. Check Point Capsule VPN v. Citrix vi. Palo Alto Networks GlobalProtect vii. Automatic viii. IKEv2 ix. L2TP x. PPTP
Always On: Enable	<p>To automatically connect to the VPN connection when the following events happen:</p> <ol style="list-style-type: none"> i. Users sign into their devices ii. The network on the device changes iii. The screen on the device turns back on after being turned off
Authentication method	Select how you want users to authenticate to the VPN server. Using certificates provides enhanced features, such as zero-touch experience, on-demand VPN, and per-app VPN.
Remember credentials at each logon	Choose to cache the authentication credentials.

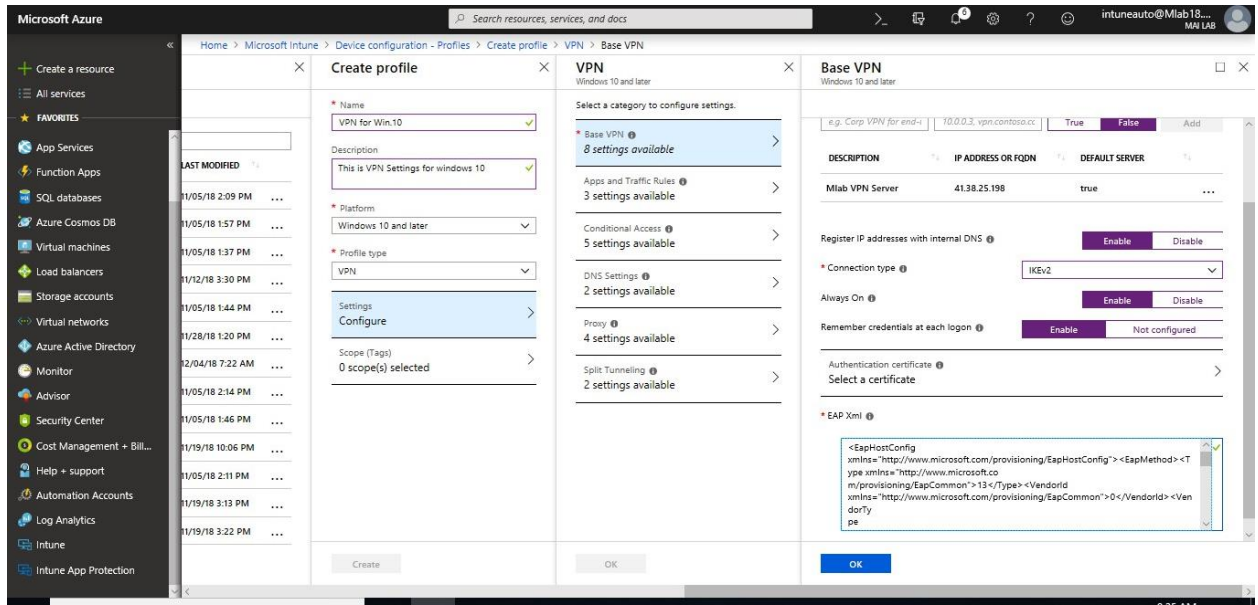


- Open PowerShell on any machine which already had VPN settings configure on it and use the following cmdlets to retrieve the EAP configuration XML.

```
Get-VpnConnection -Name "Mlab VPN"  
$a = Get-VpnConnection -Name "Mlab VPN"  
$a.EapConfigXmlStream.InnerXml
```



- EAP Xml:** Enter any EAP XML commands that configure the VPN connection

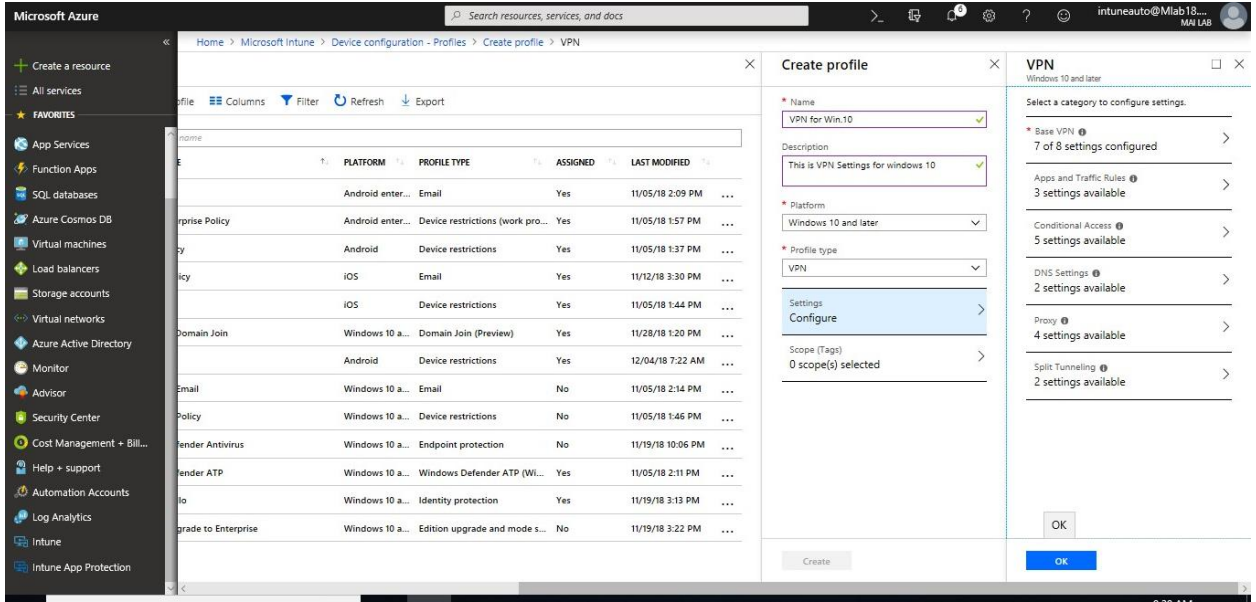


Apps and Traffic Rules	Description
Associate WIP or apps with this VPN	<p>Enable this setting if you only want some VPN apps to use the VPN connection. Your options:</p> <ol style="list-style-type: none"> Associate a WIP with this connection: Enter a WIP domain for this connection Associate apps with this connection: You can Restrict VPN connection to these apps, and then add Associated Apps. The apps you enter automatically use the VPN connection. The type of app determines the app identifier. For a universal app, enter the package family name. For a desktop app, enter the file path of the app.
Network traffic rules for this VPN connection	<p>Select which protocols, and which local & remote port and address ranges, are enabled for the VPN connection. If you don't create a network traffic rule, then all protocols, ports, and address ranges are enabled. After you create a rule, the VPN connection uses only the protocols, ports, and address ranges that you enter in that rule.</p>

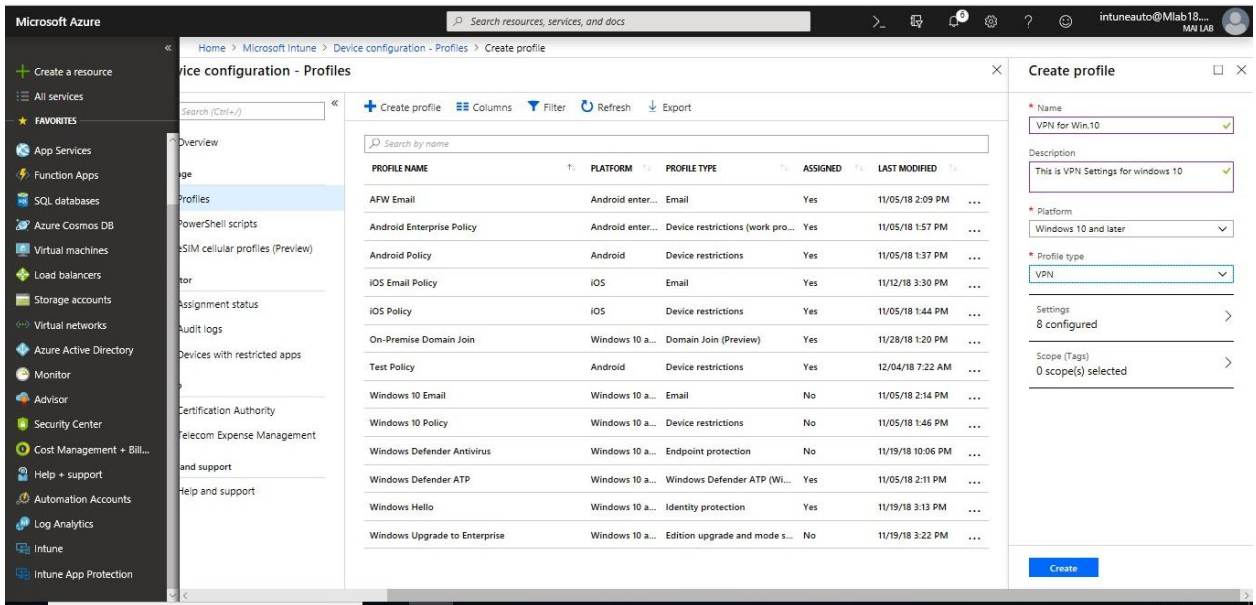
Note: We recommend that you secure all app lists created for per-app VPNs. If an unauthorized user changes this list, and you import it into the per-app VPN app list, then you potentially authorize VPN access to apps that shouldn't have access. One way you can secure app lists is using an access control list (ACL).

Conditional Access	Description
Conditional access for this VPN connection	<p>Enables device compliance flow from the client. When enabled, the VPN client communicates with Azure Active Directory (AD) to get a certificate to use for authentication. The VPN should be set up to use certificate authentication, and the VPN server must trust the server returned by Azure AD.</p>

Conditional Access	Description
Single sign-on (SSO) with alternate certificate	<p>For device compliance, use a certificate different from the VPN authentication certificate for Kerberos authentication. Enter the certificate with the following settings:</p> <ul style="list-style-type: none"> iii. Name: Name for extended key usage (EKU) iv. Object Identifier: Object identifier for EKU v. Issuer hash: Thumbprint for SSO certificate
DNS Settings	Description
DNS suffix search list	<p>In DNS suffixes, enter a DNS suffix, and Add. You can add multiple suffixes.</p> <ul style="list-style-type: none"> i. When using DNS suffixes, you can search for a network resource using its short name, instead of the fully qualified domain name (FQDN). When searching using the short name, the suffix is automatically determined by the DNS server. ii. DNS suffixes are resolved in the order listed, and the order can be changed. iii. To change the order, click the dots to the left of the DNS suffix, and then drag the suffix to the top
Domain and servers for this VPN connection	<p>Add domain and DNS server for the VPN to use. You can choose which DNS servers the VPN connection uses after the connection is established. For each server, enter:</p> <ul style="list-style-type: none"> i. Domain ii. DNS Server iii. Proxy
Proxy settings	Description
Automatic configuration script	Use a file to configure the proxy server. Enter the Proxy server URL , such as <code>http://proxy.contoso.com</code> , that includes the configuration file
Address	Enter the proxy server address, such as an IP address or <code>vpn.contoso.com</code>
Port number	Enter the TCP port number used by your proxy server
Bypass proxy for local addresses	If you don't want to use a proxy server for local addresses, then choose Enable . This setting applies if your VPN server requires a proxy server for the connection.
Split Tunneling	Description
Split tunneling	Enable or Disable to let devices decide which connection to use depending on the traffic. For example, a user in a hotel uses the VPN connection to access work files but uses the hotel's standard network for regular web browsing.
Split tunneling routes for this VPN connection	Add optional routes for third-party VPN providers. Enter a destination prefix, and a prefix size for each connection.

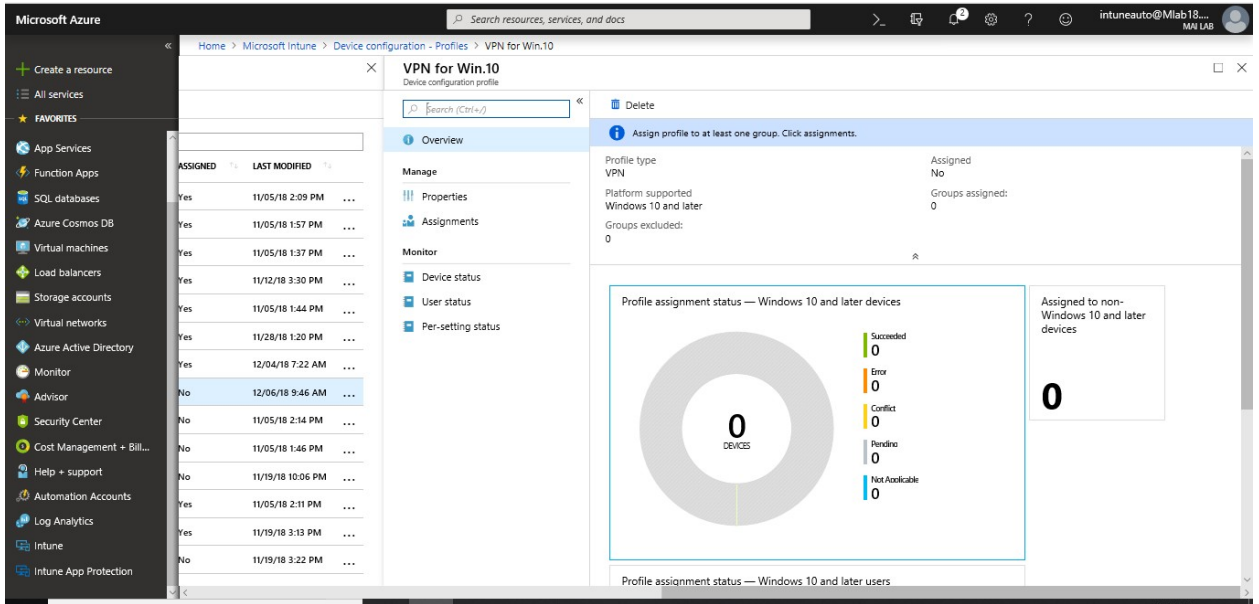


9. When you're done, **Create** your profile

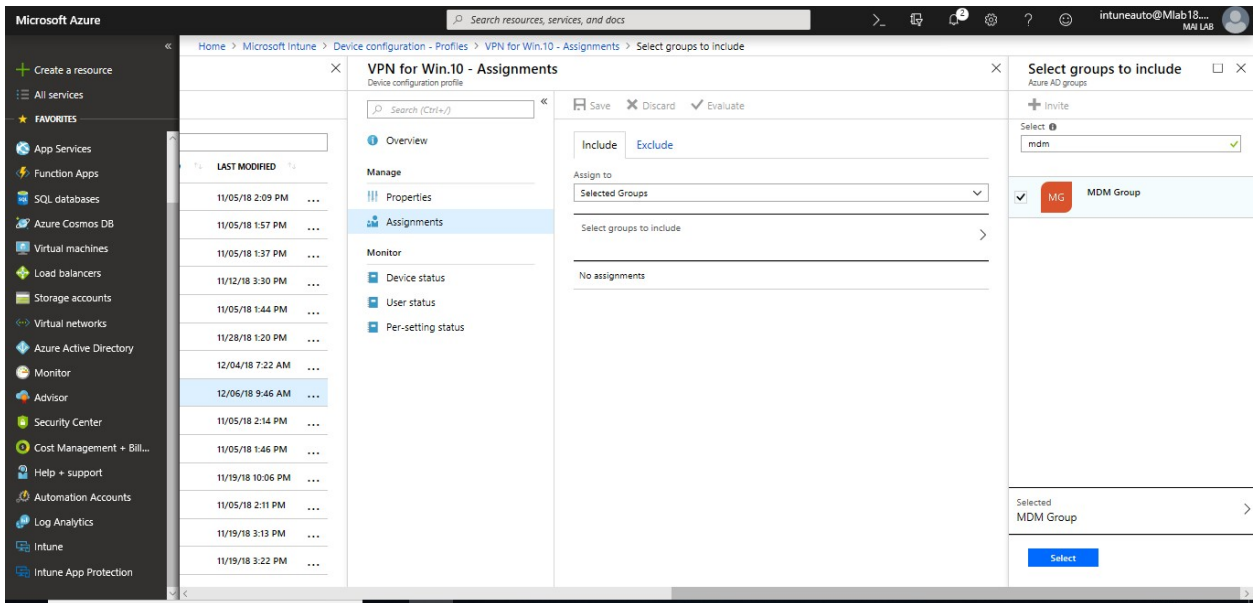


10. In the list of profiles, select the profile you want to assign, and then select **Assignments**.

Microsoft Intune step by step on Azure portal

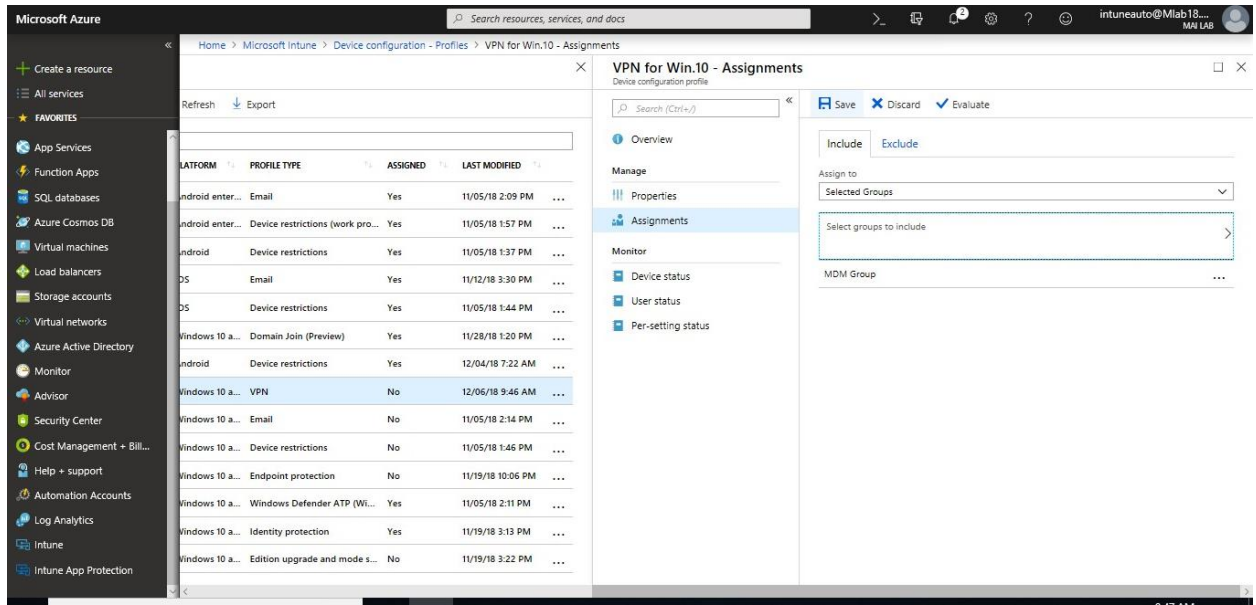


11. Choose to **Include** groups or **Exclude** groups, and then select groups.



12. When you are done, select **Save**.

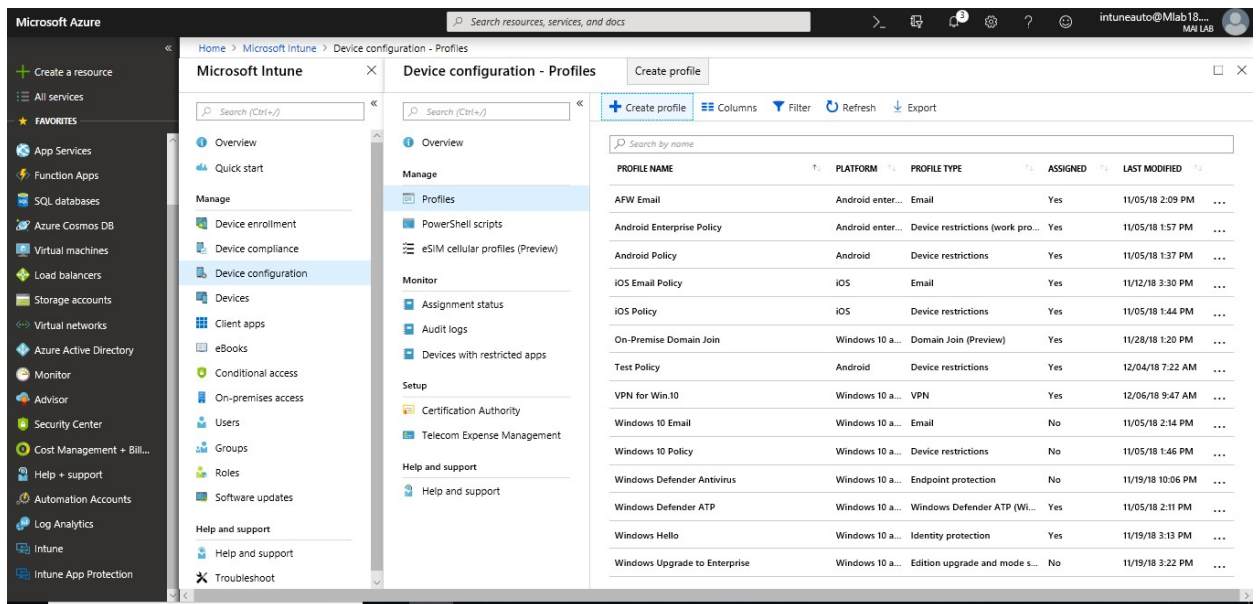
Microsoft Intune step by step on Azure portal



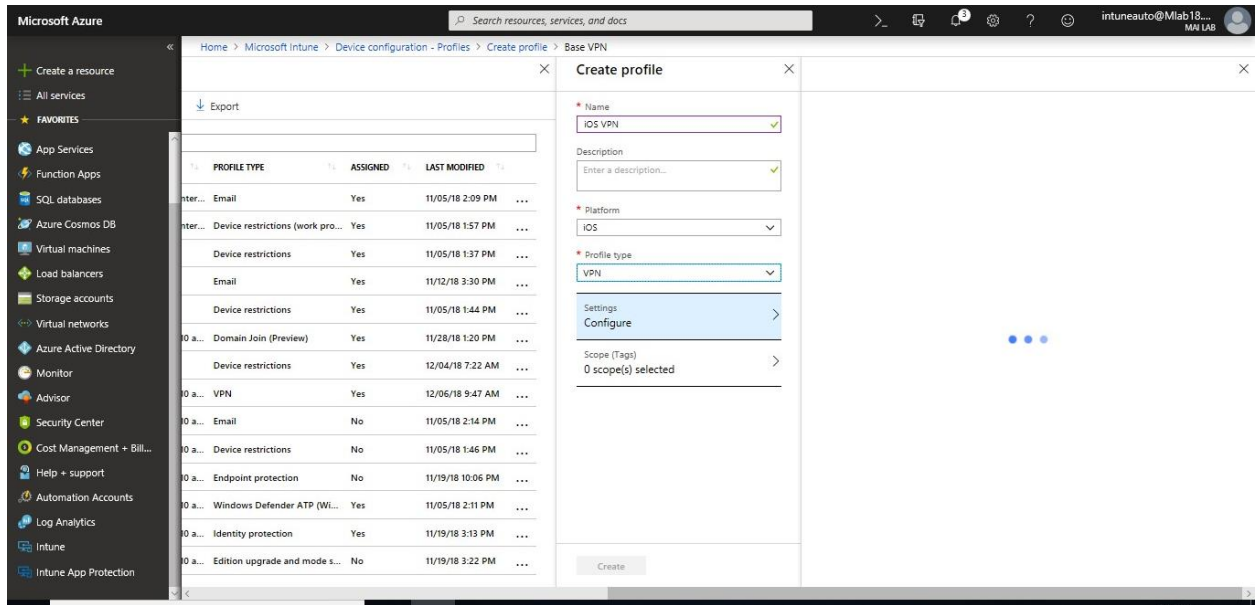
Configure VPN Profile for iOS Devices

These steps will help you deploy an VPN profile for iOS devices.

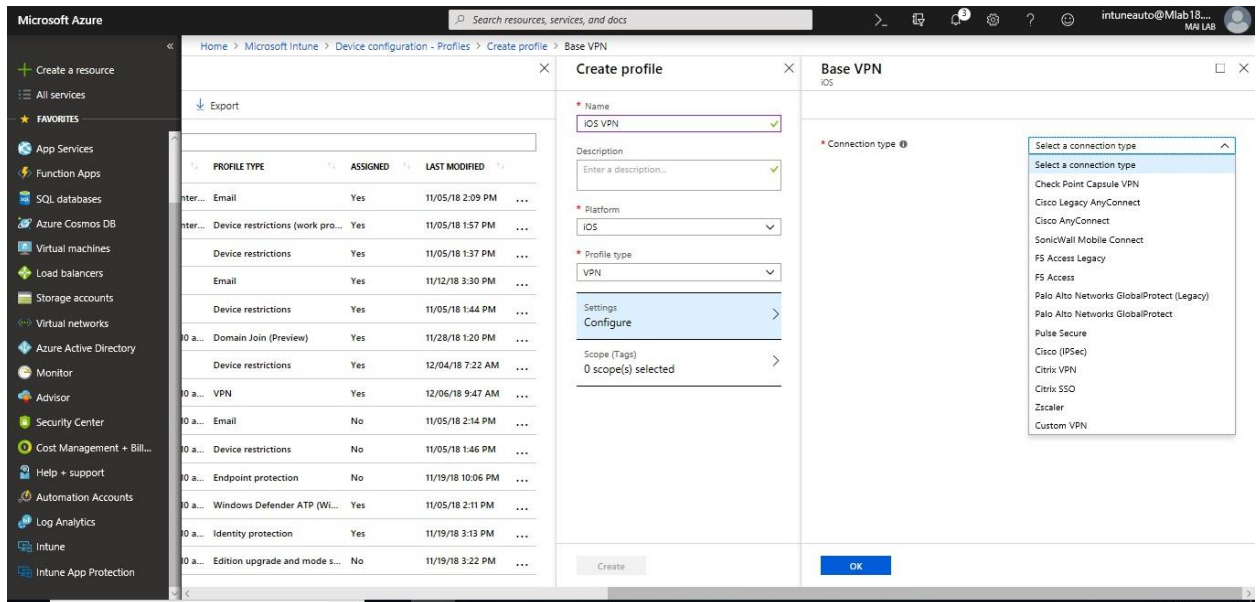
1. Sign in to the [Azure portal](#). Select **All services**, filter on **Intune**, and select **Microsoft Intune**. Select **Device configuration** > **Profiles** > **Create profile**.



2. Enter a **Name** and **Description** for the VPN profile.
3. From the **Platform** drop-down list, select the device platform to which you want to apply VPN settings. Currently, you can choose one of the following platforms for VPN device settings: **iOS**
4. From the **Profile type** drop-down list, choose **VPN**.



- Depending on the platform you chose, the settings you can configure are different. Go to one of the following topics for detailed settings for each platform: Select the VPN connection type from the following list of vendors:

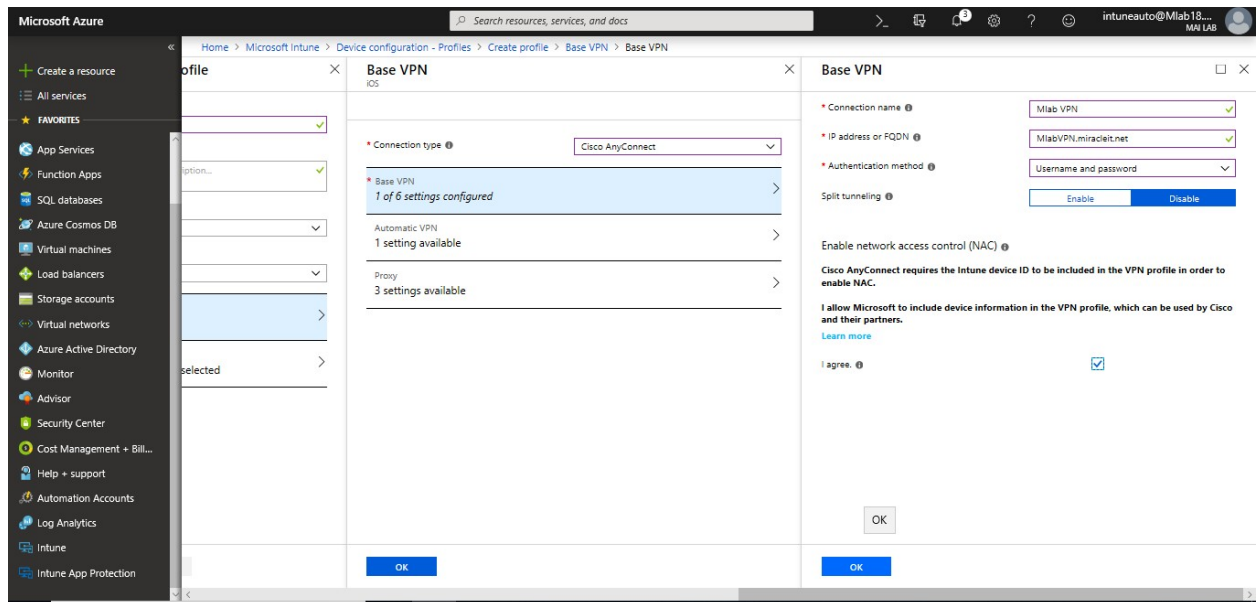


The settings shown in the following list are determined by the VPN connection type you choose.

Base VPN settings	Description
Connection name	End users see this name when they browse their device for a list of available VPN connections.

Base VPN settings	Description
IP address or FQDN	The IP address or fully qualified domain name (FQDN) of the VPN server that devices connect with. For example, enter 192.168.1.1 or vpn.contoso.com.
Authentication method	Choose how devices authenticate to the VPN server. <ul style="list-style-type: none"> ▪ Certificates: Under Authentication certificate, select an existing SCEP or PKCS certificate profile to authenticate the connection. ▪ Username and password: End users must enter a username and password to sign in to the VPN server.
Split tunneling	Enable or Disable to let devices decide which connection to use, depending on the traffic. For example, a user in a hotel uses the VPN connection to access work files but uses the hotel's standard network for regular web browsing.
Enable network access control (NAC) (Citrix SSO only)	When you choose I agree , the device ID is included in the VPN profile. This ID can be used for authentication to the VPN to allow or prevent network access.

Note: If username and password are used as the authentication method for Cisco IPsec VPN, they must deliver the Shared Secret through a custom Apple Configurator profile.



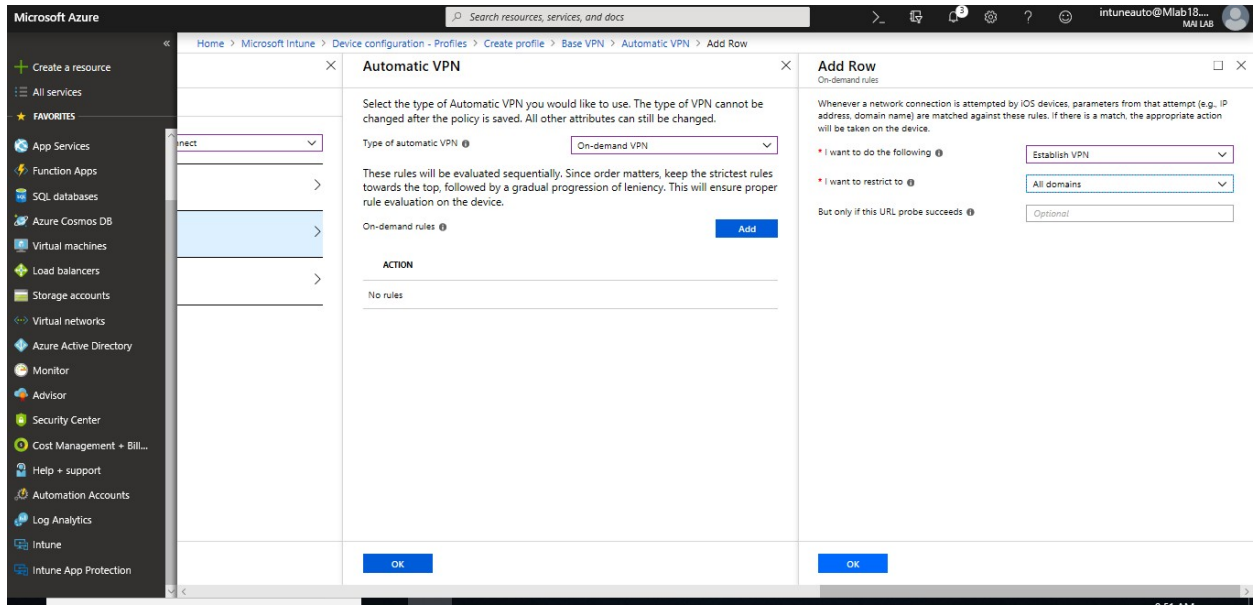
Note:

- When NAC is enabled, the VPN is disconnected every 24 hours.
- The device ID is part of the profile, but it can't be seen in Intune. This ID isn't stored by Microsoft anywhere, and isn't shared by Microsoft. Once this is supposed by VPN partners, the VPN client, such as Citrix SSO, can get the ID, and query Intune to confirm the device is enrolled and if the VPN profile is compliant or not compliant.

- c. To remove this setting, recreate the profile, and don't select **I agree**. Then, reassign the profile.

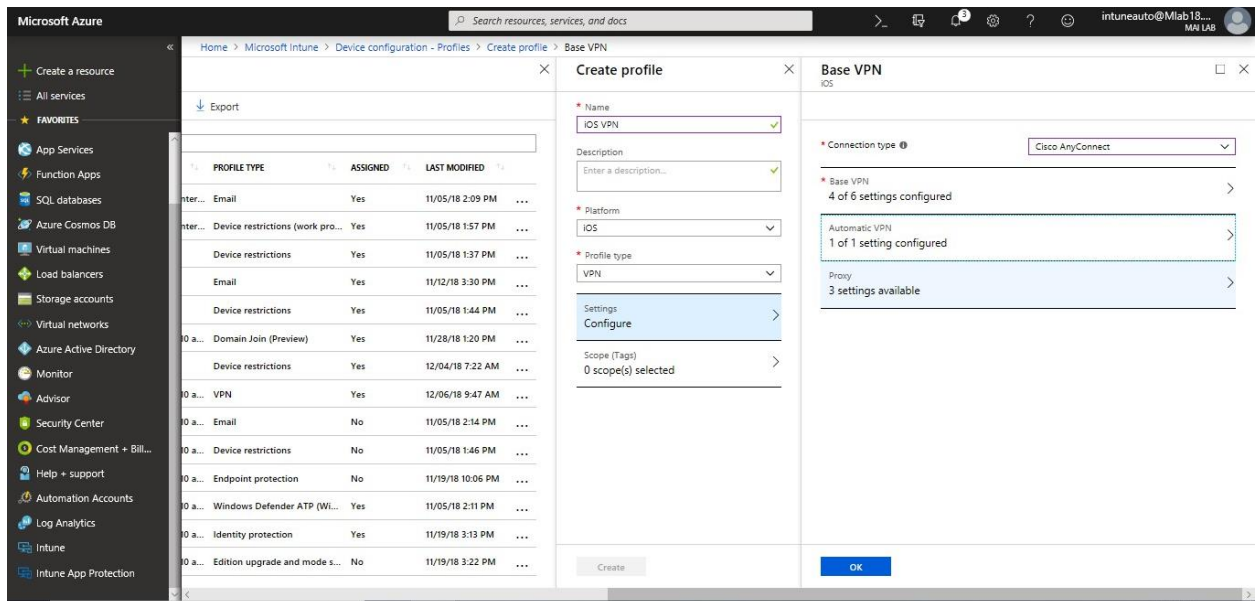
Automatic VPN settings	Description
Per-app VPN	<p>Enables per-app VPN. Allows the VPN connection to trigger automatically when certain apps are opened. Also associate the apps with this VPN profile.</p> <ul style="list-style-type: none"> ○ Provider Type: Only available for Pulse Secure and Custom VPN. ○ When using iOS per-app VPN profiles with Pulse Secure or a Custom VPN, choose app-layer tunneling (app-proxy) or packet-level tunneling (packet-tunnel). Set the ProviderType value to app-proxy for app-layer tunneling, or packet-tunnel for packet-layer tunneling. If you're not sure which value to use, check your VPN provider's documentation. ○ Safari URLs that will trigger this VPN: Add one or more web site URLs. When these URLs are visited using the Safari browser on the device, the VPN connection is automatically established.
On-demand VPN	<p>Configure conditional rules that control when the VPN connection is started. For example, create a condition where the VPN connection is only used when a device isn't connected to a company Wi-Fi network. Or, create a condition where, if a device can't access a DNS search domain you enter, then the VPN connection isn't initiated.</p> <ul style="list-style-type: none"> ○ SSIDs or DNS search domains: Select whether this condition uses wireless network SSIDs, or DNS search domains. Choose Add to configure one or more SSIDs or search domains. ○ URL string probe: Optional. Enter a URL that the rule uses as a test. If the device with this profile accesses this URL without redirection, then the VPN connection is initiated. And, the device connects to the target URL. The user doesn't see the URL string probe site. A URL string probe example is the address of an auditing Web server that checks device compliance before connecting the VPN. Another possibility is that the URL tests the ability of the VPN to connect to a site before connecting the device to the target URL through the VPN. ○ Domain action: Choose one of the following items: <ul style="list-style-type: none"> ▪ Connect if needed ▪ Never connect ○ Action: Choose one of the following items: <ul style="list-style-type: none"> ▪ Connect ▪ Evaluate connection ▪ Ignore ▪ Disconnect

Microsoft Intune step by step on Azure portal



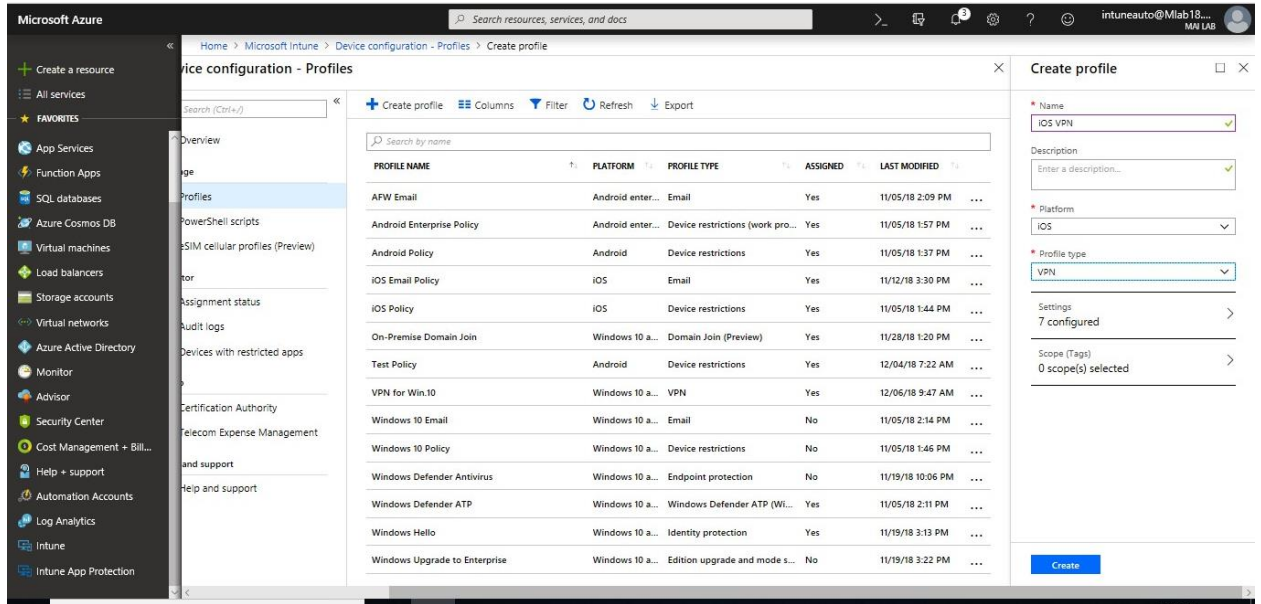
If you're using a proxy, configure the following settings. Proxy settings aren't available for Zscaler VPN connections.

Proxy settings	Description
Automatic configuration script	Use a file to configure the proxy server. Enter the Proxy server URL (for example http://proxy.contoso.com) that includes the configuration file.
Address	Enter the IP address of fully qualified host name of the proxy server.
Port number	Enter the port number associated with the proxy server

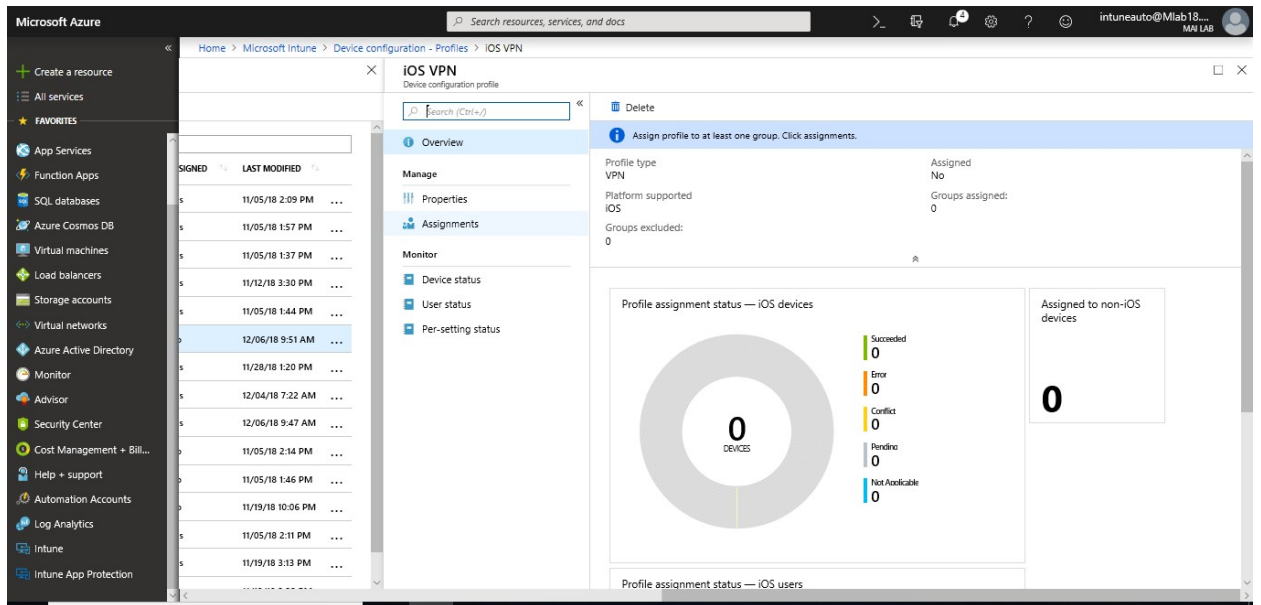


6. When you're done, **Create** your profile

Microsoft Intune step by step on Azure portal

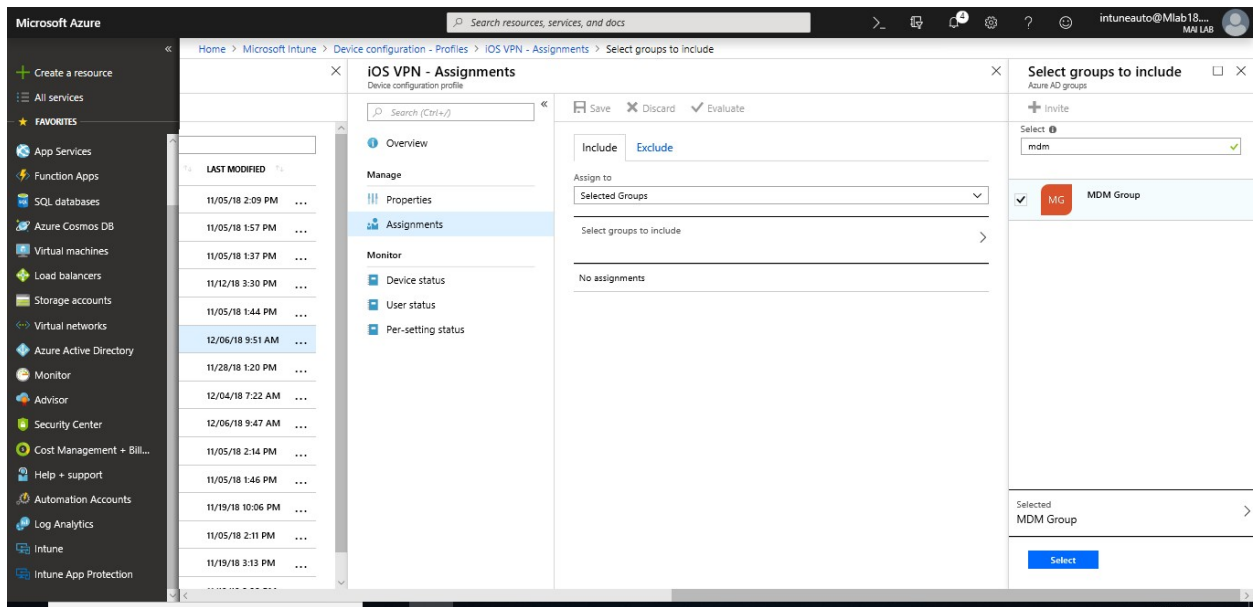


7. In the list of profiles, select the profile you want to assign, and then select **Assignments**.

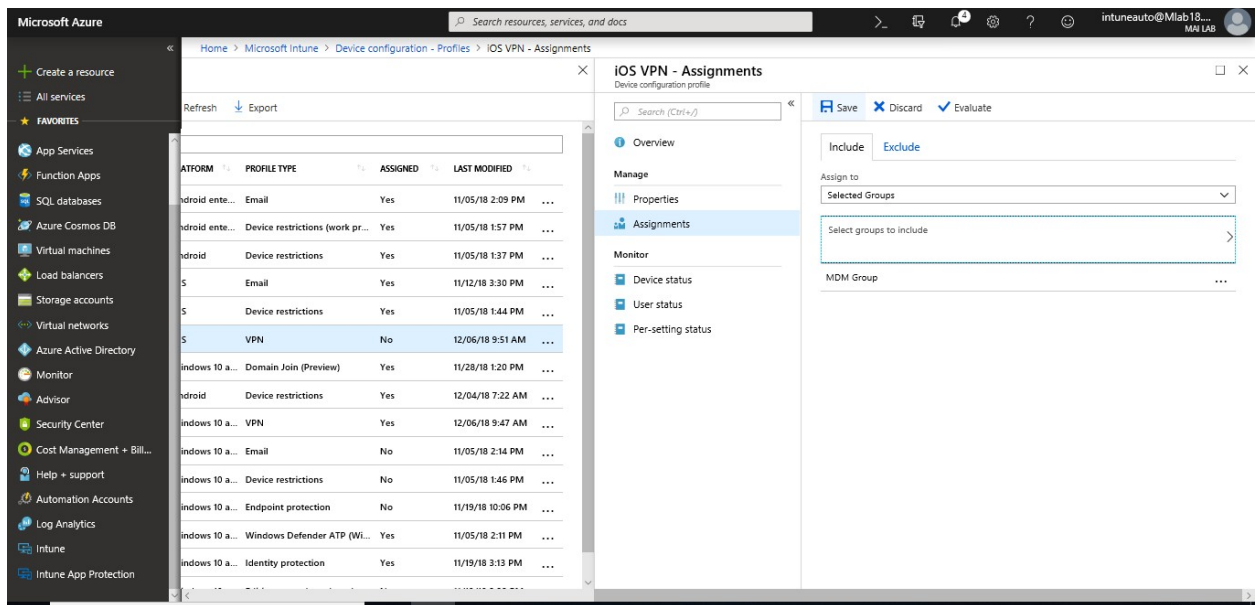


8. Choose to **Include** groups or **Exclude** groups, and then select groups.

Microsoft Intune step by step on Azure portal



9. When you are done, select **Save**.



Help users connect to company networks using Wi-Fi profiles

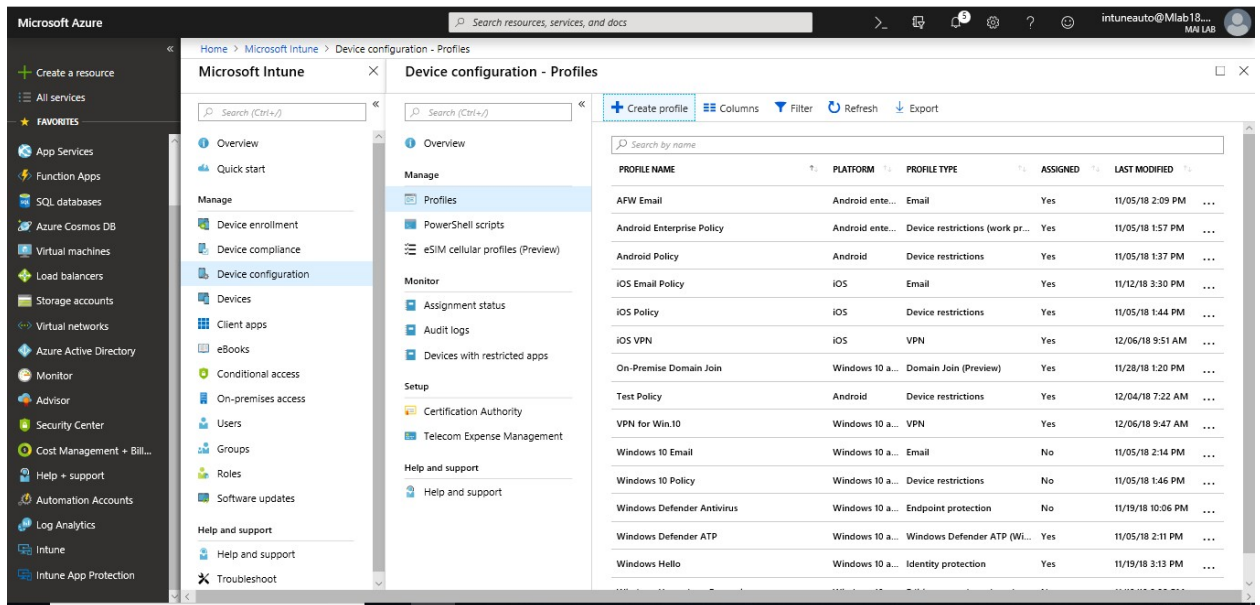
Wi-Fi profiles in Microsoft Intune help you Deploy wireless network settings to your users. By deploying these settings, you minimize the end-user effort required to connect to the corporate network.

Configure Wi-Fi Profile for Android Devices

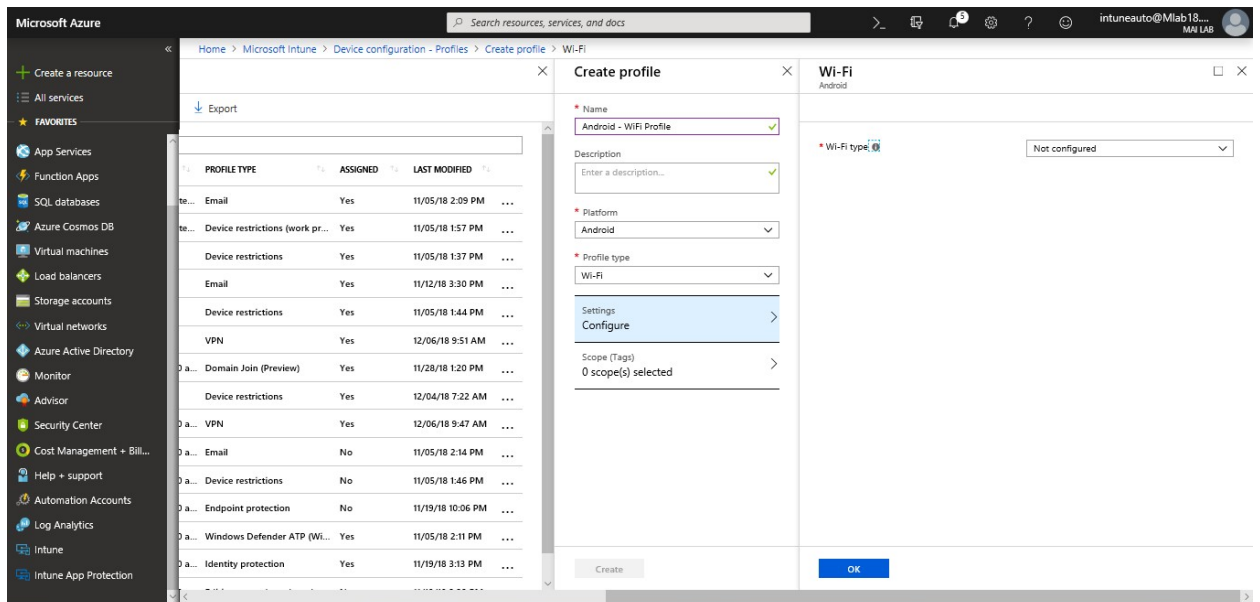
These steps will help you deploy a Wi-Fi profile for Android devices.

Microsoft Intune step by step on Azure portal

1. In the [Azure portal](#), select **All services** > filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device configuration** > **Profiles** > **Create profile**.



3. Enter a **Name** and **Description** for the Wi-Fi profile.
4. In the **Platform** drop-down list, select the device platform to apply the Wi-Fi settings.
Your options: **Android**
5. In **Profile Type**, choose **Wi-Fi**.



Note:

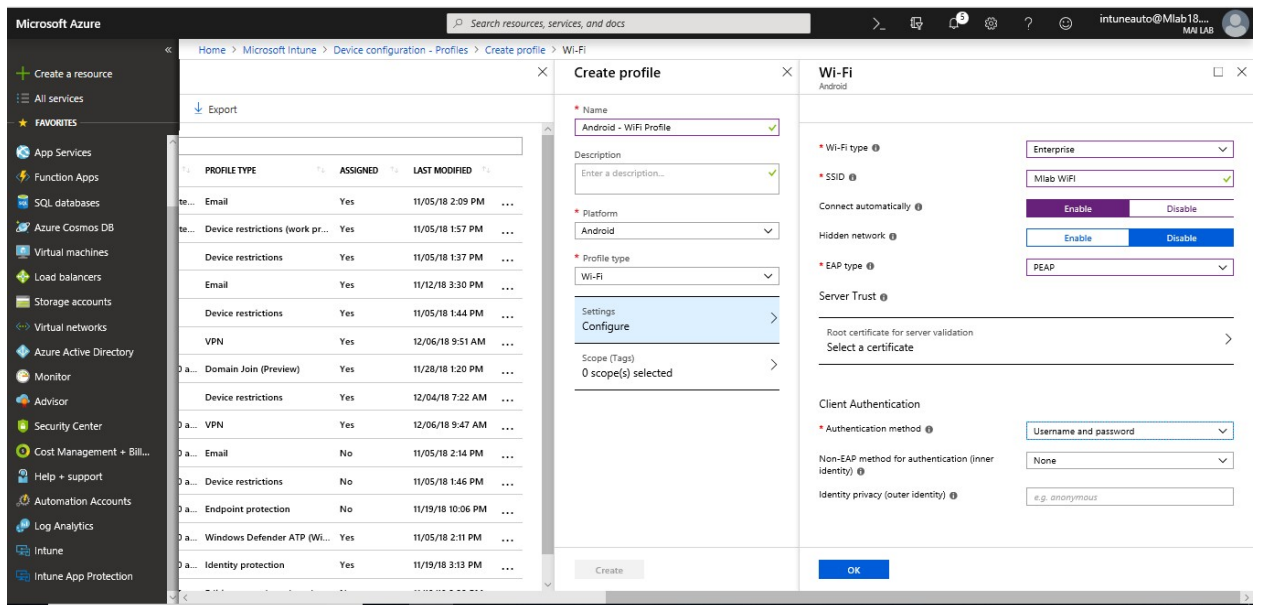
- For **Android Enterprise** devices running as a kiosk, you can choose **Device owner only** > **Wi-Fi**.

- For **Windows 8.1 and later**, you can choose **Wi-Fi import**. This option lets you import Wi-Fi settings as an XML file that you previously exported from a different device.
6. Most platforms have **Basic** and **Enterprise** settings. **Basic** includes features such as the network name and the SSID. **Enterprise** lets you supply more advanced information, such as the Extensible Authentication Protocol (EAP).

- **Wi-Fi type:** Choose **Enterprise**.
- **SSID:** Short for **service set identifier**. This setting is the real name of the wireless network that devices connect to.
- **Connect automatically:** Choose **Enable** to automatically connect to this network when the device is in range. Choose **Disable** to prevent devices from automatically connecting.
- **Hidden network:** Choose **Enable** to hide this network from the list of available networks on the device. The SSID isn't broadcasted. Choose **Disable** to show this network in the list of available networks on the device.
- **EAP type:** Choose the Extensible Authentication Protocol (EAP) type used to authenticate secured wireless connections. Your options:

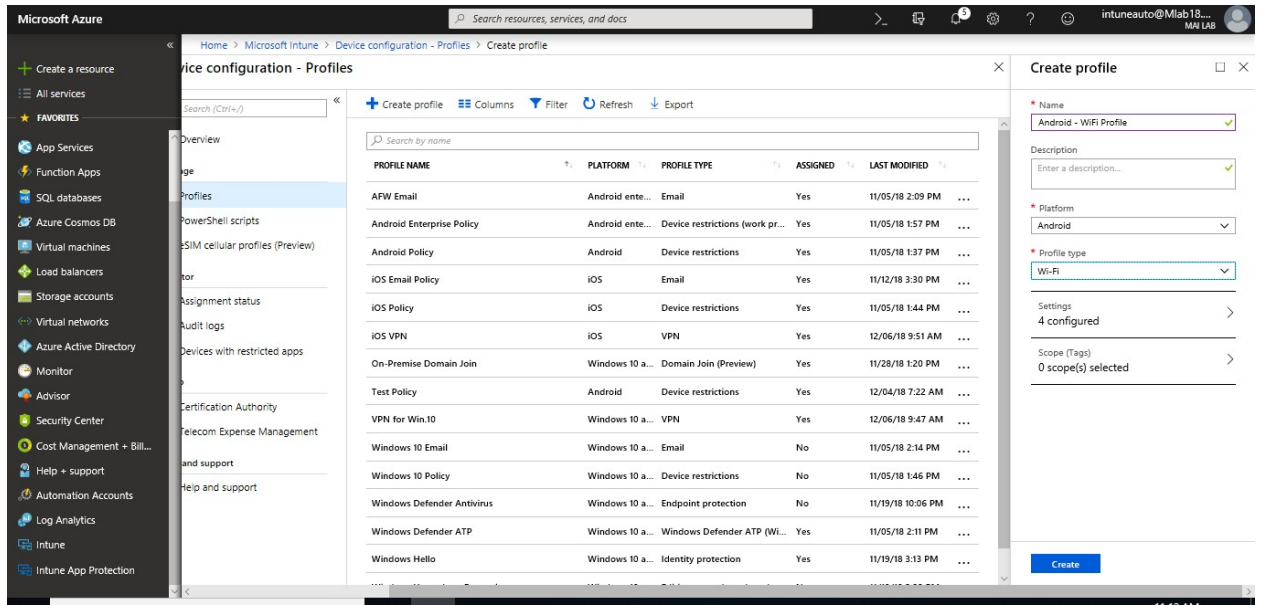
EAP Type	Description
EAP-TLS	<ul style="list-style-type: none"> ▪ Server Trust - Root certificate for server validation: Choose an existing trusted root certificate profile. This certificate is presented to the server when the client connects to the network and is used to authenticate the connection. Select OK to save your changes. ▪ Client Authentication - Client certificate for client authentication (Identity certificate): Choose the SCEP or PKCS client certificate profile that is also deployed to the device. This certificate is the identity presented by the device to the server to authenticate the connection. Select OK to save your changes.
EAP-TTLS	<ul style="list-style-type: none"> ▪ Server Trust - Root certificate for server validation: Choose an existing trusted root certificate profile. This certificate is presented to the server when the client connects to the network, and is used to authenticate the connection. Select OK to save your changes. ▪ Client Authentication - Choose an Authentication method. Your options: <ol style="list-style-type: none"> a. Username and Password: Prompt the user for a user name and password to authenticate the connection. Also enter: Non-EAP method (inner identity): Choose how you authenticate the connection. Be sure you choose the same protocol that's configured on your Wi-Fi network. Your options: Unencrypted password (PAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft CHAP (MS-CHAP), or Microsoft CHAP Version 2 (MS-CHAP v2) b. Certificates: Choose the SCEP or PKCS client certificate profile that is also deployed to the device. This certificate is the identity presented by the device to the server to authenticate the connection. Select OK to save your changes. c. Identity privacy (outer identity): Enter the text sent in the response to an EAP identity request. This text can be any value, such as anonymous. During authentication, this anonymous identity is initially sent, and then followed by the real identification sent in a secure tunnel.

EAP Type	Description
PEAP	<ul style="list-style-type: none"> ▪ Server Trust - Root certificate for server validation: Choose an existing trusted root certificate profile. This certificate is presented to the server when the client connects to the network and is used to authenticate the connection. Select OK to save your changes. ▪ Client Authentication - Choose an Authentication method. Your options: <ol style="list-style-type: none"> a. Username and Password: Prompt the user for a user name and password to authenticate the connection. Also enter: Non-EAP method for authentication (inner identity): Choose how you authenticate the connection. Be sure you choose the same protocol that's configured on your Wi-Fi network. Your options: None or Microsoft CHAP Version 2 (MS-CHAP v2) b. Certificates: Choose the SCEP or PKCS client certificate profile that is also deployed to the device. This certificate is the identity presented by the device to the server to authenticate the connection. Select OK to save your changes. c. Identity privacy (outer identity): Enter the text sent in the response to an EAP identity request. This text can be any value, such as anonymous. During authentication, this anonymous identity is initially sent, and then followed by the real identification sent in a secure tunnel.



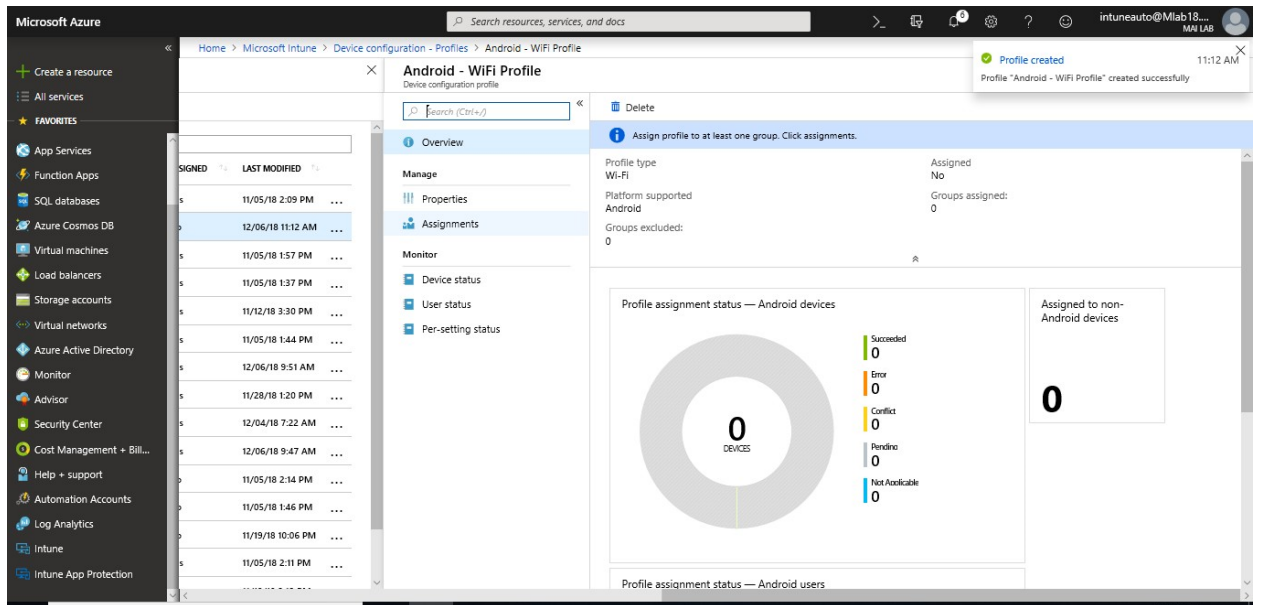
7. When finished adding your Wi-Fi settings, select **Create Profile > Create** to add the configuration profile. The profile is created and is shown in the profiles list (**Device configuration > Profiles**).

Microsoft Intune step by step on Azure portal



PROFILE NAME	PLATFORM	PROFILE TYPE	ASSIGNED	LAST MODIFIED
AFW Email	Android ente...	Email	Yes	11/05/18 2:09 PM
Android Enterprise Policy	Android ente...	Device restrictions (work pr...	Yes	11/05/18 1:57 PM
Android Policy	Android	Device restrictions	Yes	11/05/18 1:37 PM
iOS Email Policy	iOS	Email	Yes	11/12/18 3:30 PM
iOS Policy	iOS	Device restrictions	Yes	11/05/18 1:44 PM
iOS VPN	iOS	VPN	Yes	12/06/18 9:51 AM
On-Premise Domain Join	Windows 10 a...	Domain Join (Preview)	Yes	11/28/18 1:20 PM
Test Policy	Android	Device restrictions	Yes	12/04/18 7:22 AM
VPN for Win.10	Windows 10 a...	VPN	Yes	12/06/18 9:47 AM
Windows 10 Email	Windows 10 a...	Email	No	11/05/18 2:14 PM
Windows 10 Policy	Windows 10 a...	Device restrictions	No	11/05/18 1:46 PM
Windows Defender Antivirus	Windows 10 a...	Endpoint protection	No	11/19/18 10:06 PM
Windows Defender ATP	Windows 10 a...	Windows Defender ATP (Wi...	Yes	11/05/18 2:11 PM
Windows Hello	Windows 10 a...	Identity protection	Yes	11/19/18 3:13 PM

8. In the list of profiles, select the profile you want to assign, and then select **Assignments**.

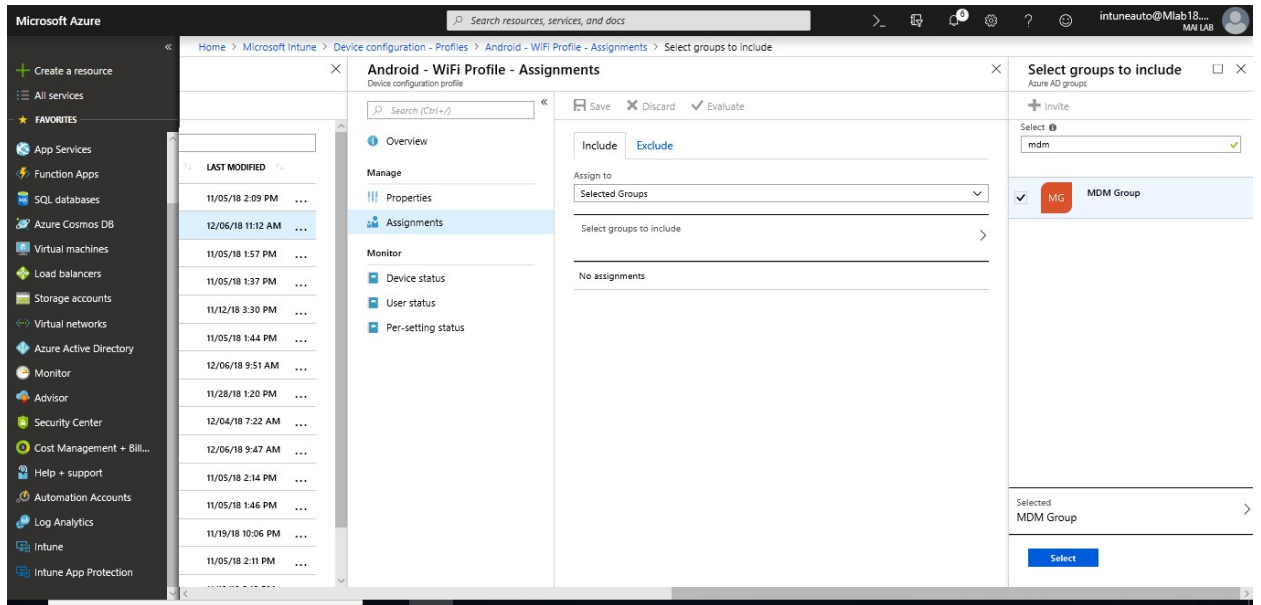


Profile assignment status — Android devices

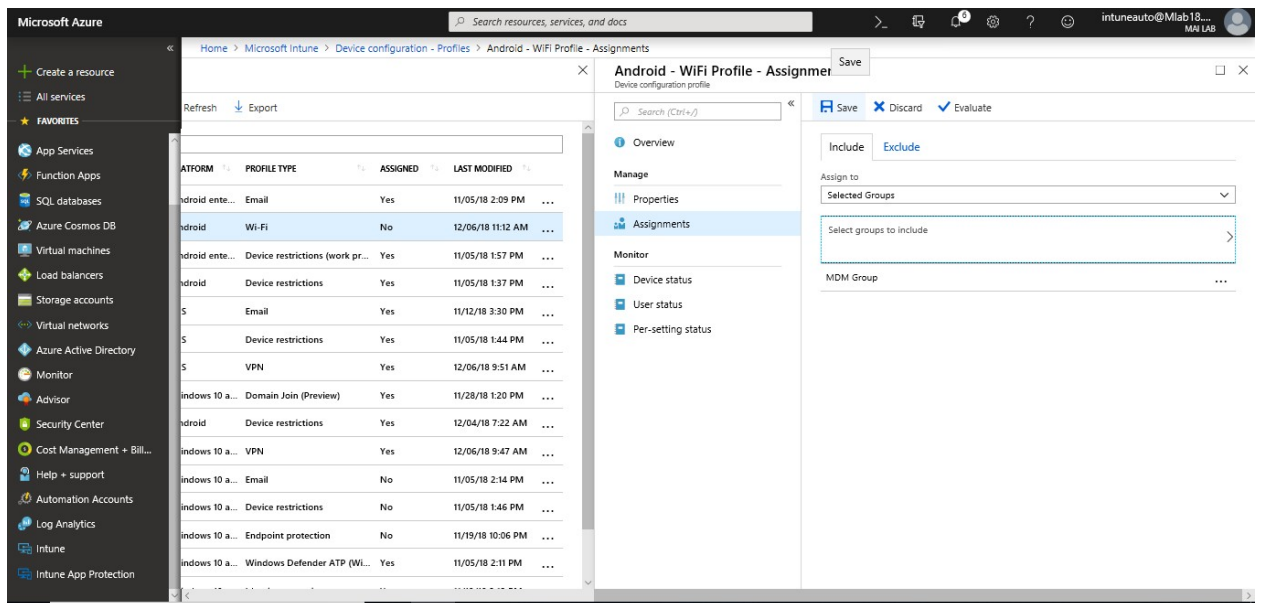
Succeeded	0
Error	0
Conflict	0
Pending	0
Not Assignable	0

Assigned to non-Android devices: 0

9. Choose to **Include** groups or **Exclude** groups, and then select groups.



10. When you are done, select **Save**.




Import Wi-Fi settings for Windows devices in Intune (Windows 8.1 or Later)

Use the Windows Wi-Fi Import Policy to import a set of Wi-Fi settings that you can then deploy to the required user or device groups. **For Windows 10 and later devices, you can also create a Wi-Fi profile directly in Intune.** Applies to:

- Windows 8.1 and later
- Windows 10 and later
- Windows 10 desktop or mobile
- Windows Holographic for Business

These steps will help you import Wi-Fi settings for Windows devices.

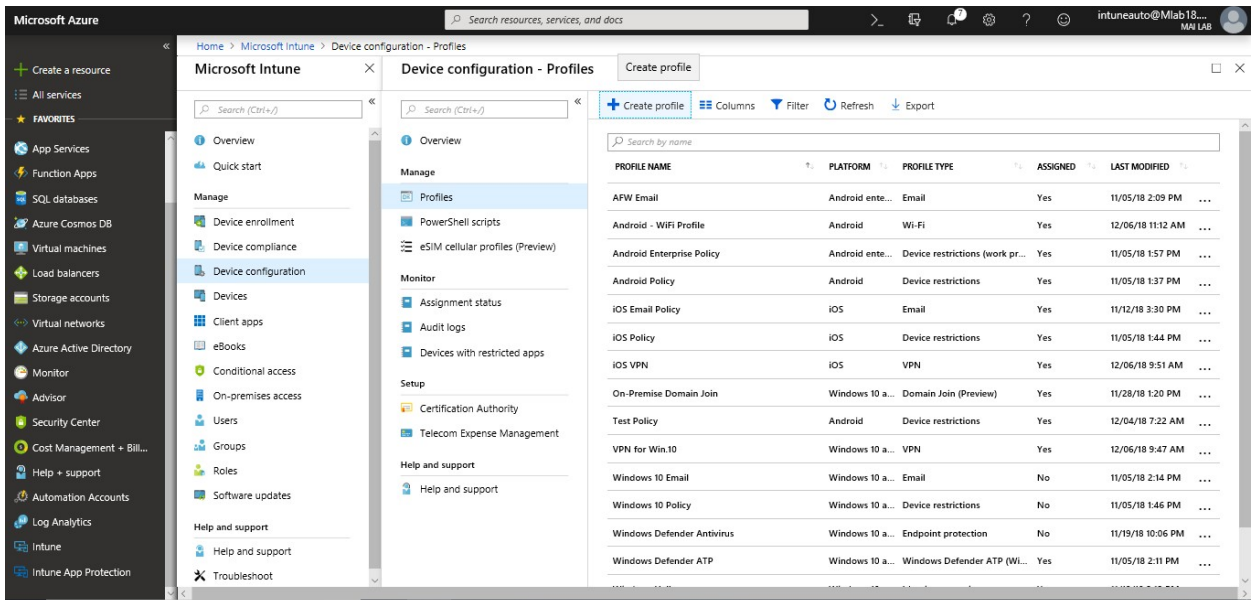
1. Open **Cmd** run as administrator and run “*netsh wlan export profile <name of wifi profile>*”



```
Select Administrator: Command Prompt
C:\windows\system32>netsh wlan export profile dlink_DWR-730
Interface profile "dlink_DWR-730" is saved in file ".\Wi-Fi-dlink_DWR-730.xml" successfully.
C:\windows\system32>
```

Note: if you run command as above, you will find xml saved on system 32 folder

2. In the [Azure portal](#), select **All services**, filter on **Intune**, and select **Microsoft Intune**.
3. Select **Device configuration > Profiles > Create profile**.

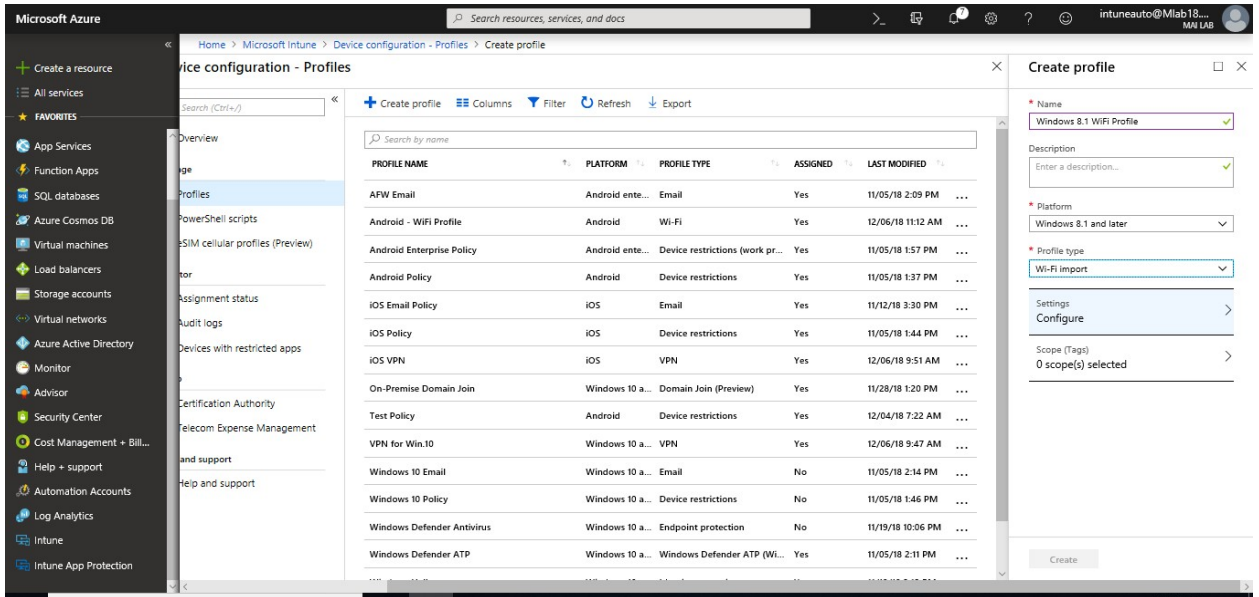


4. Enter a **Name** and **Description** for the device restriction profile.

Note:

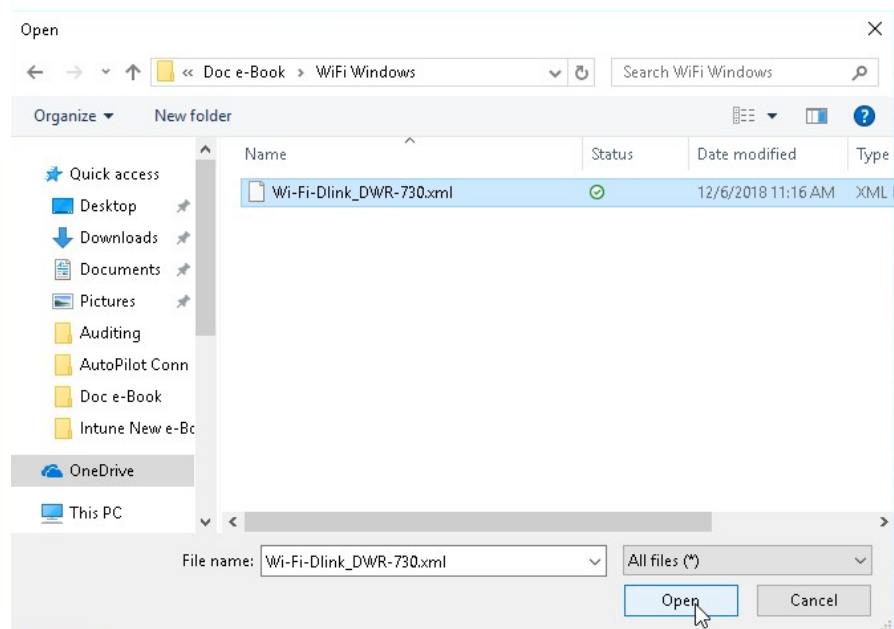
- The name **must** be the same as the name attribute in the Wi-Fi profile xml. Otherwise, it fails.
- If you are exporting a Wi-Fi profile that includes a pre-shared key, you **must** add key=clear to the command. For example, enter: netsh wlan export profile name="ProfileName" key=clear folder=c:\Wifi
- Using a pre-shared key with Windows 10 causes a remediation error to appear in Intune. When this happens, the Wi-Fi profile is properly assigned to the device, and the profile works as expected.
- If you export a Wi-Fi profile that includes a pre-shared key, be sure the file is protected. The key is in plain text, so it's your responsibility to protect the key.

5. In **Platform**, select **Windows 8.1 and later**.
6. In **Profile type**, select **Wi-Fi import**.



7. Configure the following settings:

- **Connection name:** Enter a name for the Wi-Fi connection. This name is displayed to end users when they browse available Wi-Fi networks.
- **Profile XML:** Select the browse button and choose the XML file that contains the Wi-Fi profile settings you want to import.
- **File contents:** Shows the XML code for the configuration profile you selected.



Microsoft Intune step by step on Azure portal

- When you're done, select **OK** > **Create** to save your changes. The profile is created and is shown in the profiles list.

The screenshot shows the 'Create profile' dialog in the Microsoft Azure portal. The dialog is titled 'Create profile' and is for a 'Wi-Fi' profile. The 'Name' field is 'Import WiFi Profile - Win. 8.1 or later'. The 'Platform' is 'Windows 8.1 and later'. The 'Profile type' is 'Wi-Fi import'. The 'Profile XML' field contains the following content:

```
<?xml version='1.0'?>
<WLANProfile xmlns='http://www.microsoft.com/networking/WLAN/profile/v1'?>
  <name>DUC_HO</name>
  <SSIDConfig>
    <SSID>
      <name>4E5435F8B4F</name>
      <name>DUC_HO</name>
    </SSID>
  </SSIDConfig>
  <connectionType>ESS</connectionType>
  <connectionMode>auto</connectionMode>
  <MSM>
    <security>
      <authEncryption>
        <authentication>WPA2</authentication>
        <encryption>AES</encryption>
        <useOneX>true</useOneX>
      </authEncryption>
      <PMKCacheMode>enabled</PMKCacheMode>
      <PMKCacheTTL>720</PMKCacheTTL>
    </security>
  </MSM>
</WLANProfile>
```

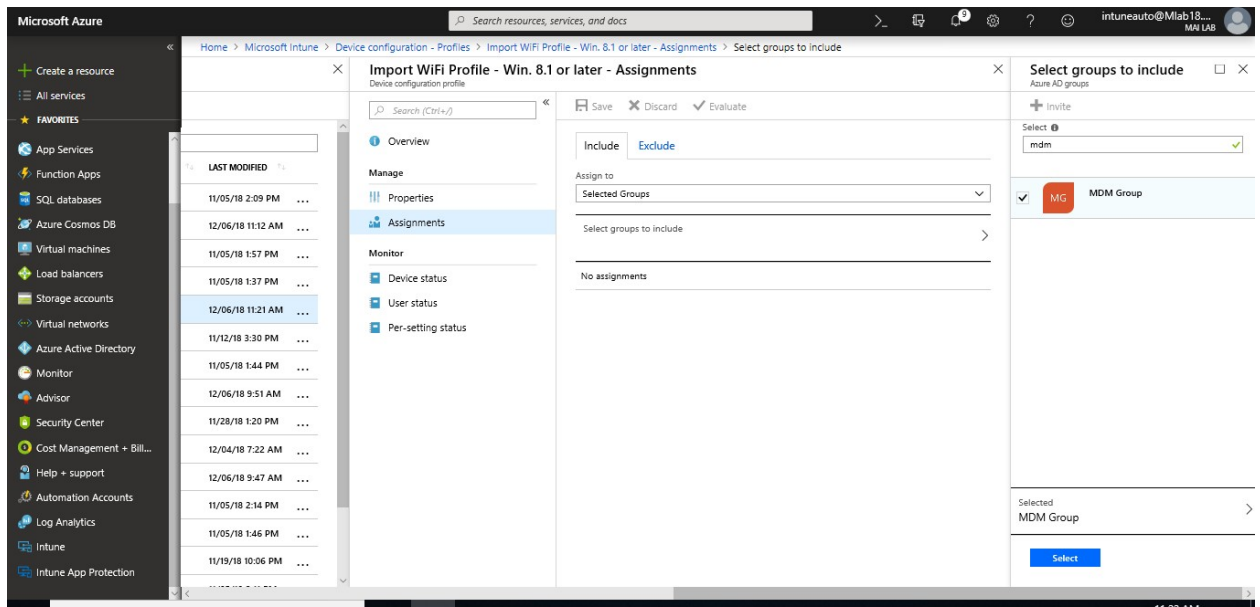
A notification at the top right of the portal indicates 'Upload Completed for Wi-Fi-Dlink_DWR-7... 11:21 AM' with a file size of 2.89 KB and 'Streaming upload'.

- In the list of profiles, select the profile you want to assign, and then select **Assignments**.

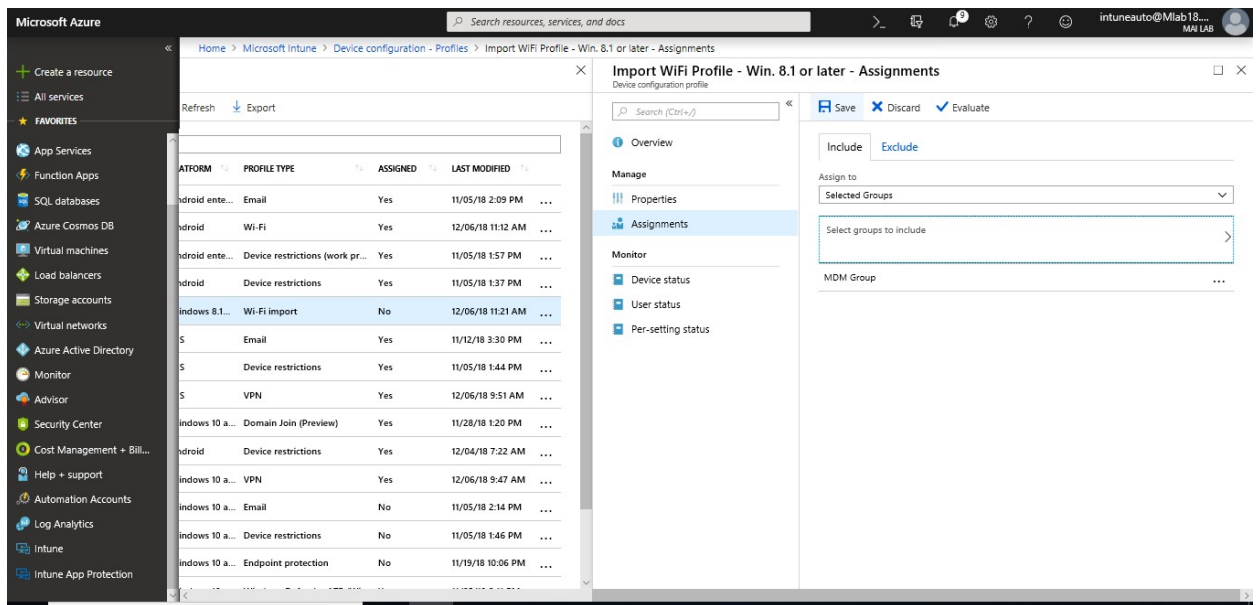
The screenshot shows the 'Import WiFi Profile - Win. 8.1 or later' profile page in the Microsoft Azure portal. The 'Assignments' tab is selected, showing a table with columns for Profile type, Platform supported, and Groups assigned. The 'Assignments' section shows a large circular gauge for 'Profile assignment status — Windows 8.1 and later devices' with 0 devices. A box on the right shows 'Assigned to non-Windows 8.1 and later devices' with 0 devices.

- Choose to **Include** groups or **Exclude** groups, and then select groups.

Microsoft Intune step by step on Azure portal



11. When you are done, select **Save**.



Enable access to company resources using Certificate profiles

Certificate profiles in Microsoft Intune help you to secure access to company resources including wireless networks and VPN connections.

Configure Prerequisites for Certificate Profile

Before you can configure certificate profiles you must complete the following tasks, which required the On-Premise Infrastructure as following:

- **Active Directory domain:** All servers listed in this section (except for the Web Application Proxy Server) must be joined to your Active Directory domain.
- **Certification Authority (CA):** Must be a Microsoft Enterprise Certification Authority (CA) that runs on an Enterprise edition of Windows Server 2008 R2 or later. A Standalone CA is not supported.
- **NDES Server:** On a Windows Server 2012 R2 or later, set up the Network Device Enrollment Service (NDES) server role. Intune doesn't support using NDES on a server that also runs the Enterprise CA. The NDES server must be joined to a domain within the same forest as the Enterprise CA.
- **Microsoft Intune Certificate Connector.**

Step 1 - Configure certificate templates on the certification authority

Step 2 - for SCEP profile only: Configure prerequisites on the NDES server

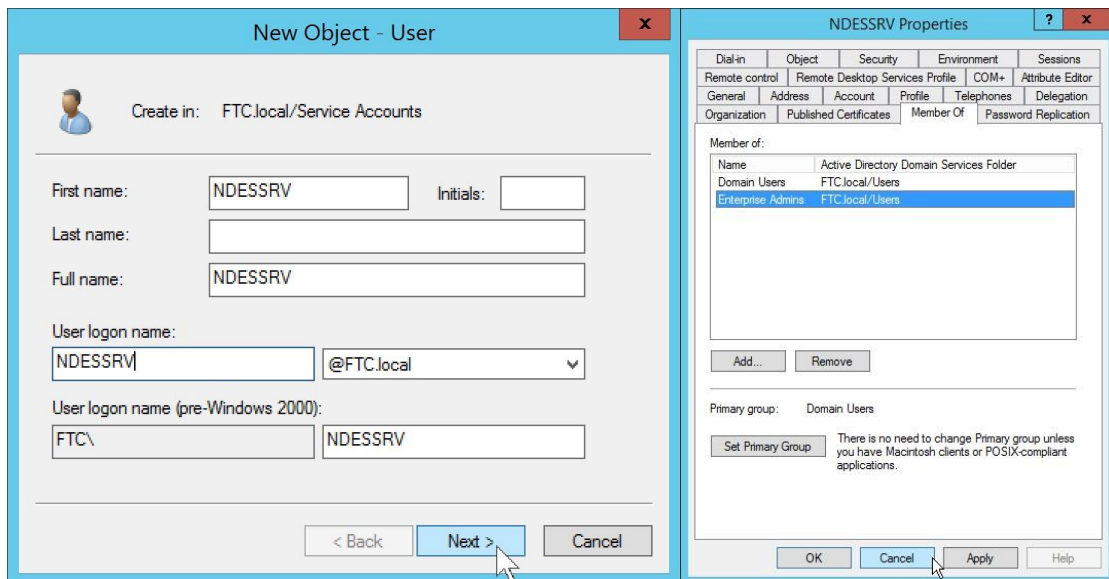
Step 3 - for SCEP profile only: Configure NDES for use with Intune

Step 4 - Enable, install, and configure the Intune Certificate Connector

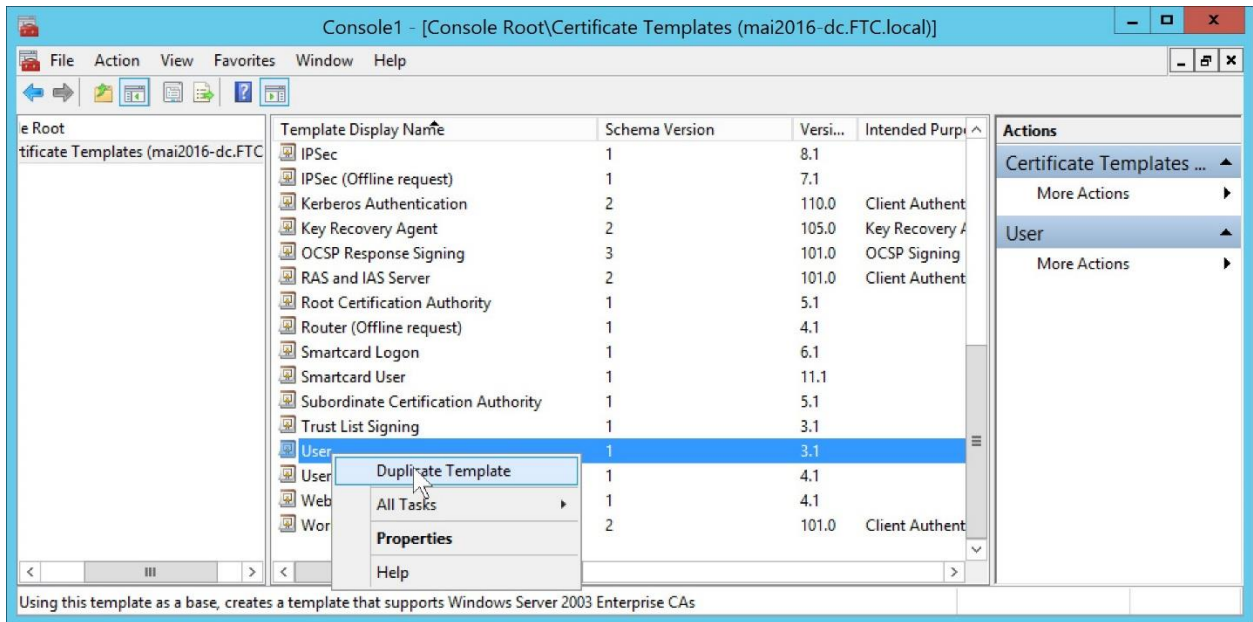
Step 1 - Configure certificate templates on the certification authority

To Configure certification authority, you need to follow below steps:

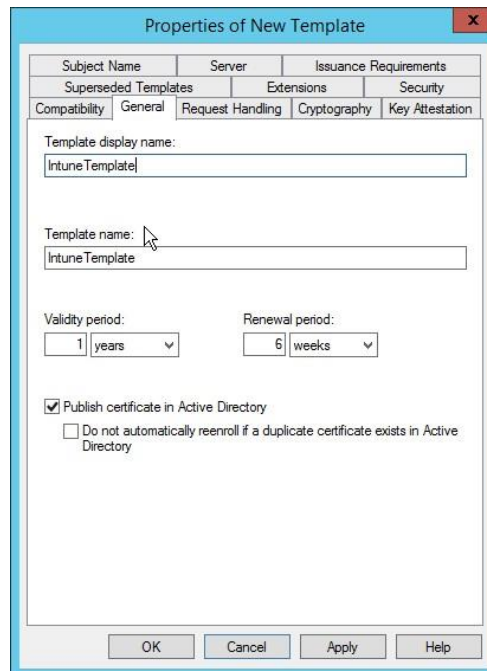
1. Create a domain user account to use as the **NDES service account**. You will specify this account when you configure templates on the issuing CA before you install and configure NDES.



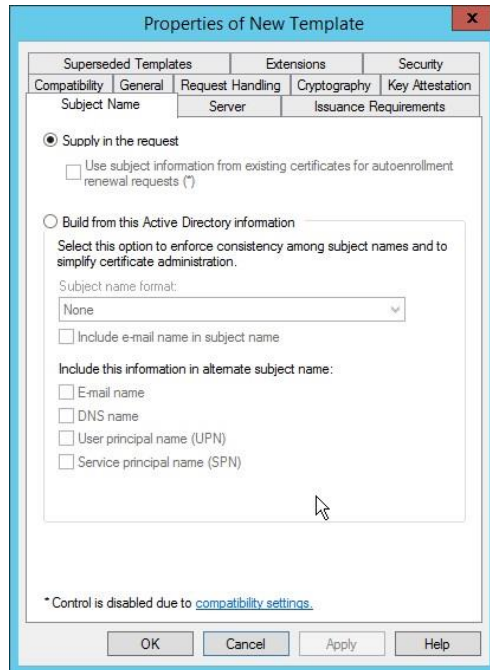
2. Create a new custom template or **copy an existing template** and then edit an existing template (like the User template), for use with NDES.



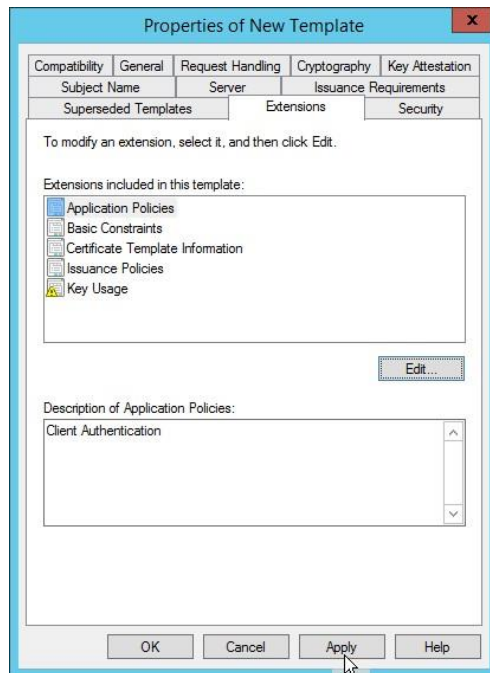
3. Specify a **friendly Template display name** for the template “IntuneTemplate”



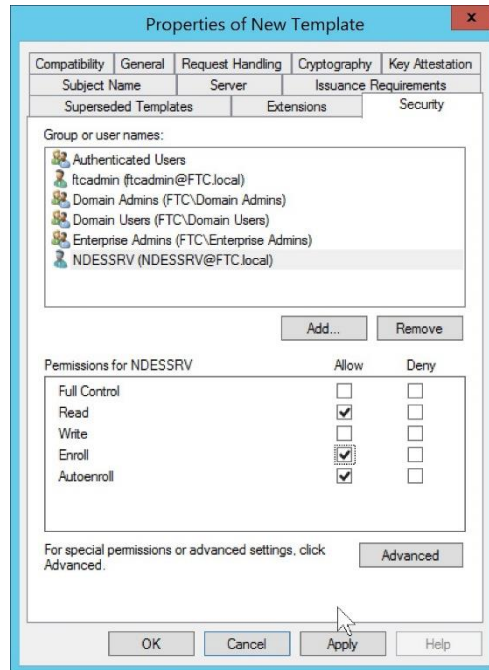
4. On the **Subject Name** tab, select **Supply in the request**. (Security is enforced by the Intune policy module for NDES).



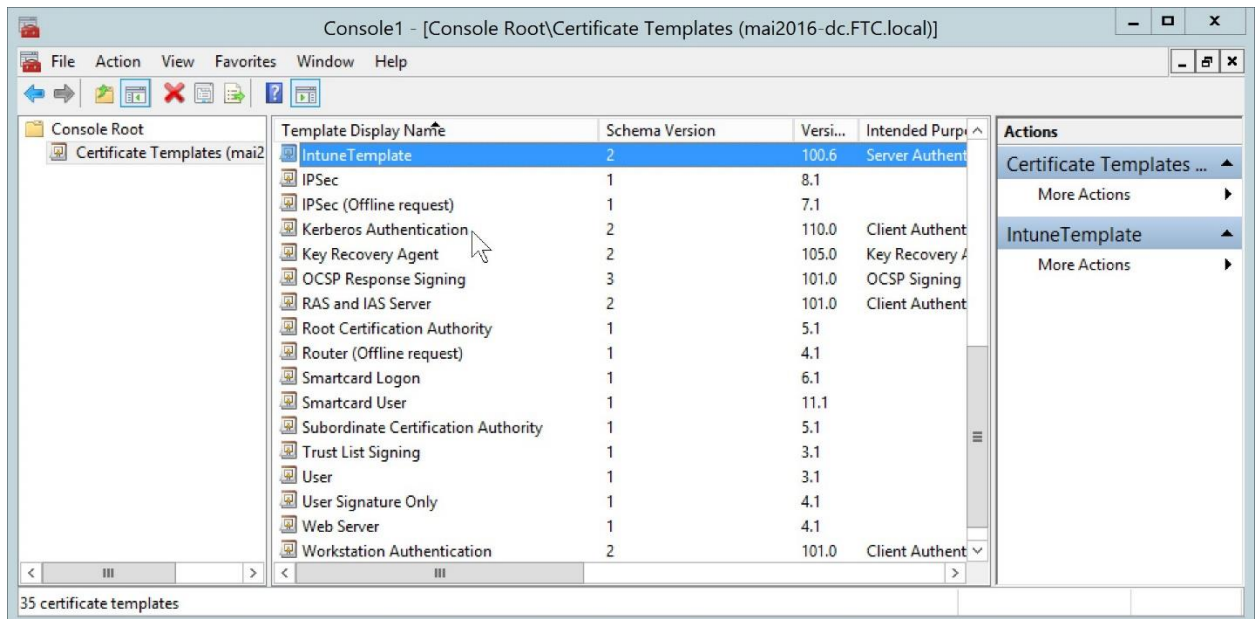
5. On the **Extensions** tab, ensure the **Description of Application Policies** includes **Client Authentication**.



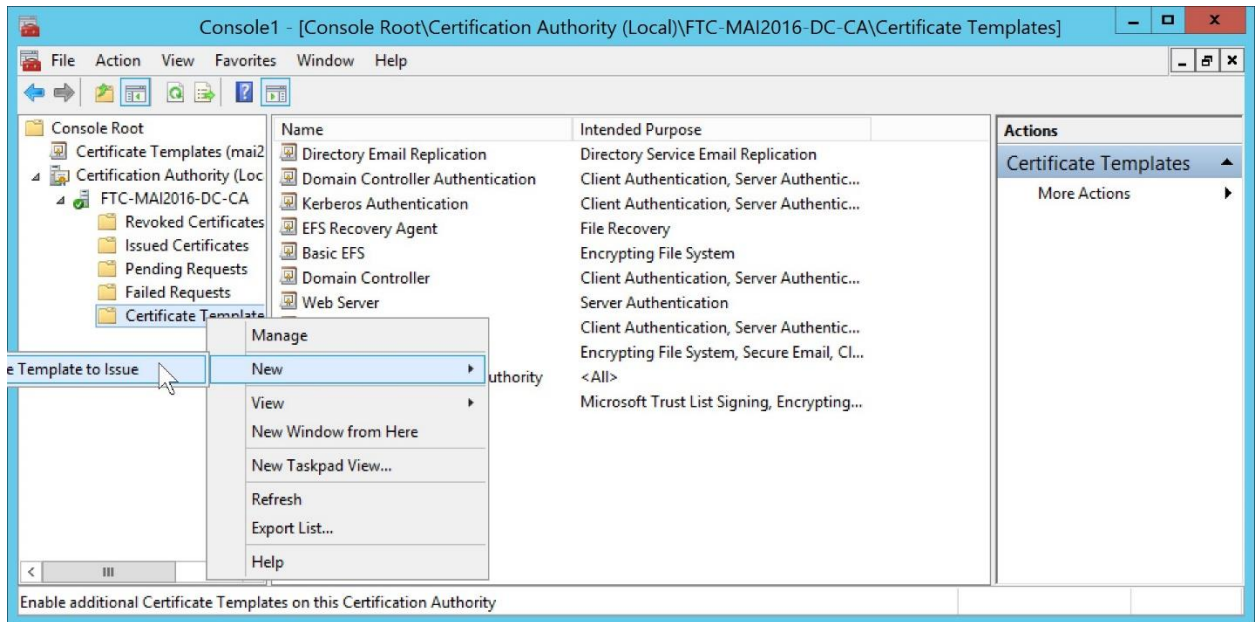
6. On the **Security** tab, add the **NDES service account**, and give it **Read and Enroll permissions** to the template.



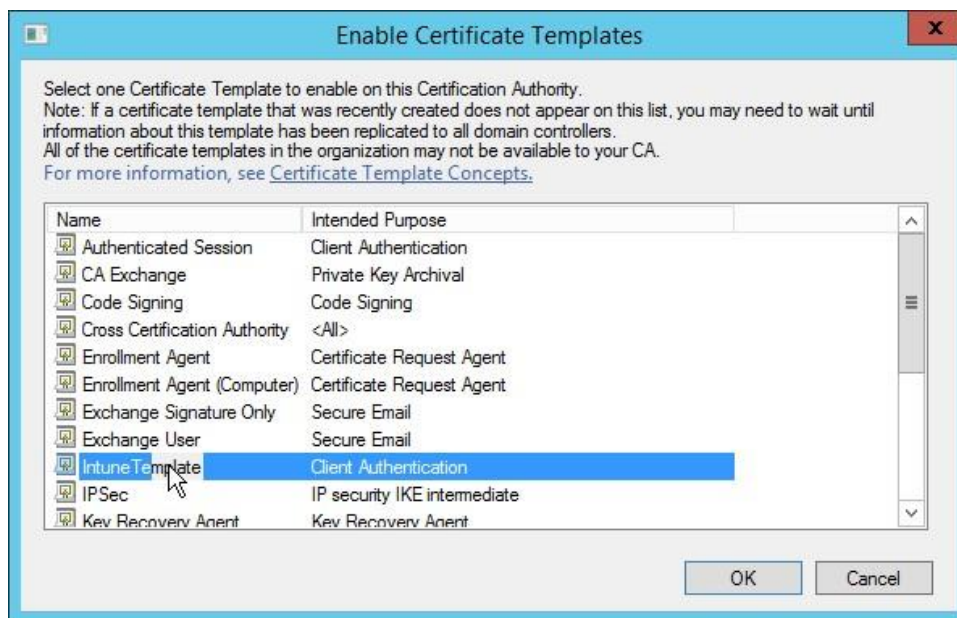
7. Click **Apply** > **OK**.



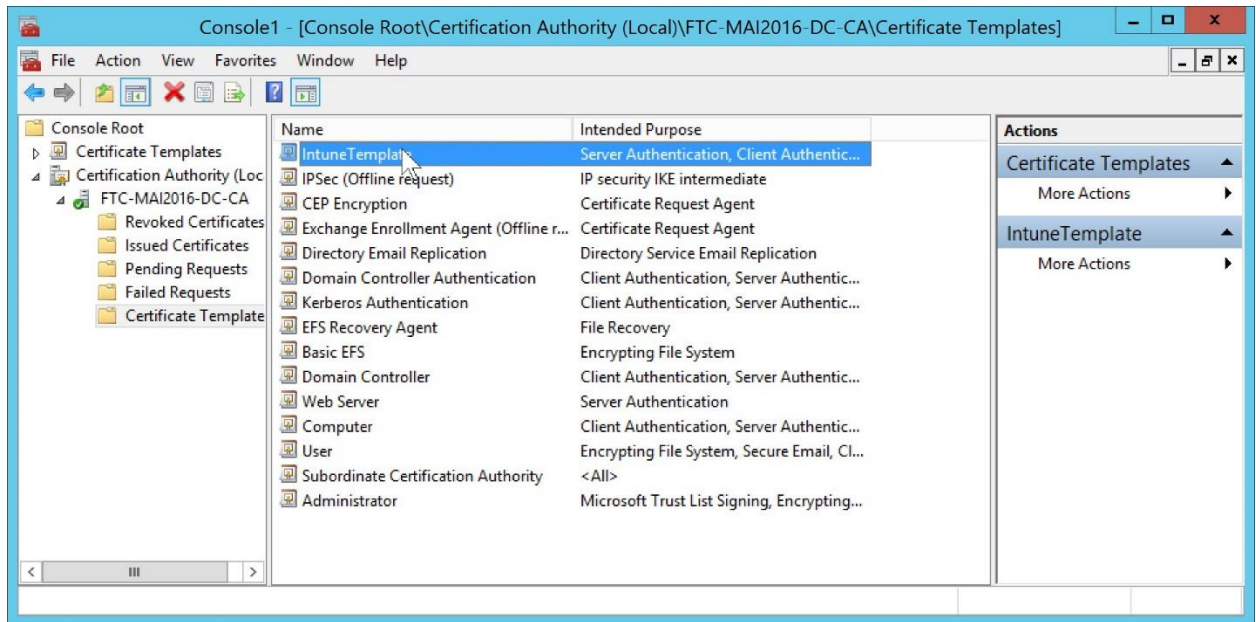
8. Select the **Certificate Templates** node, click **Action** > **New** > **Certificate Template to Issue**



9. Select the template you created in



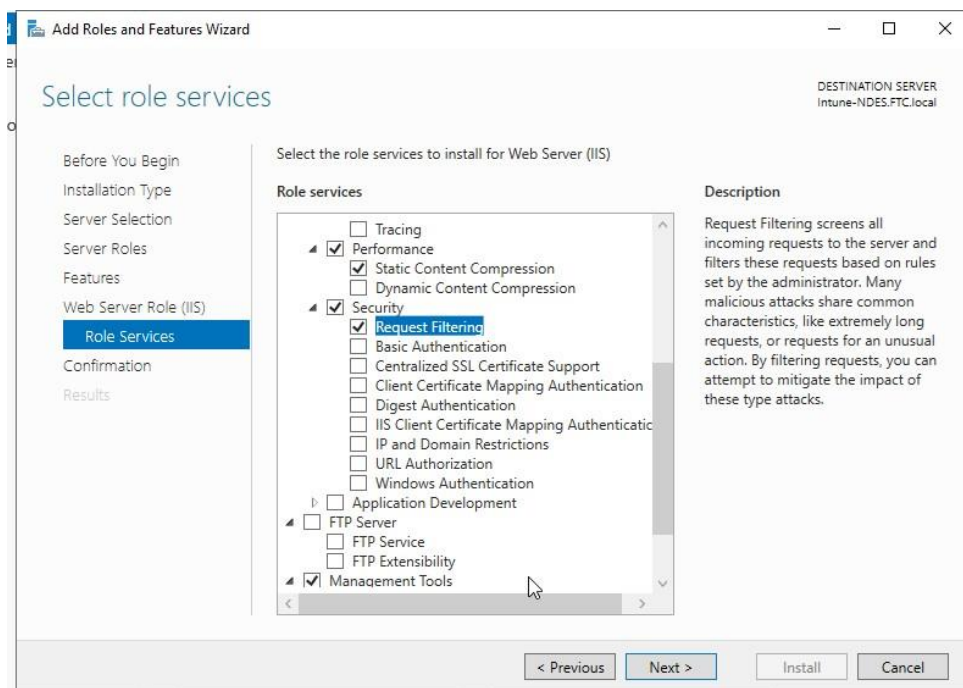
10. Validate that the template published by viewing it under the Certificate Templates folder.



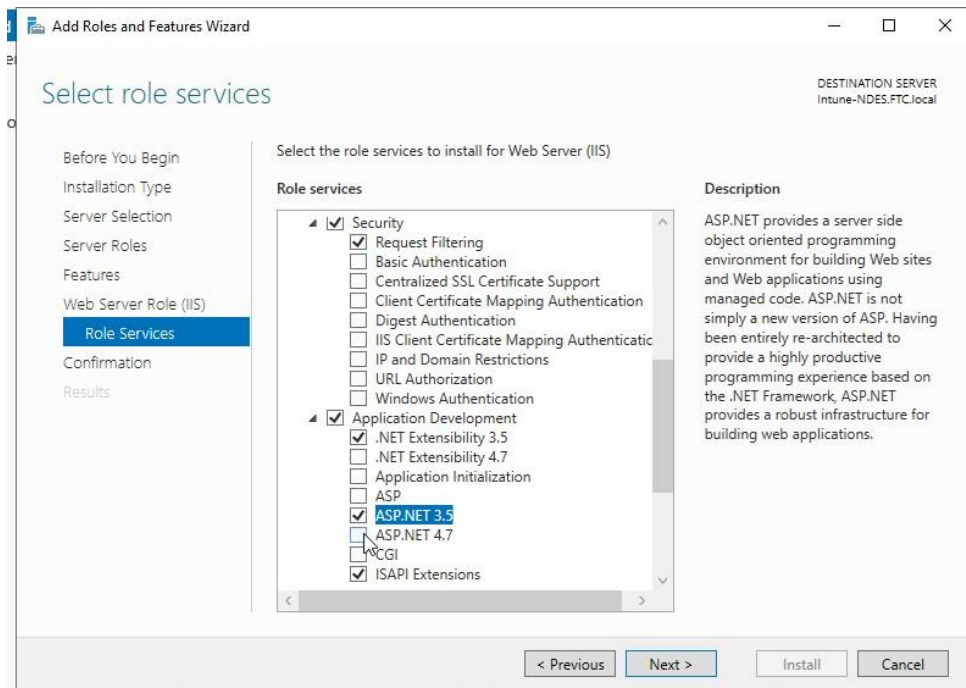
Step 2 - for SCEP profile only: Configure prerequisites on the NDES server

NDES Server should be on a Windows Server 2012 R2 or later, set up the Network Device Enrollment Service (NDES) server role. Intune doesn't support using NDES on a server that also runs the Enterprise CA. To configure prerequisites on the NDES sever, you need to follow below steps:

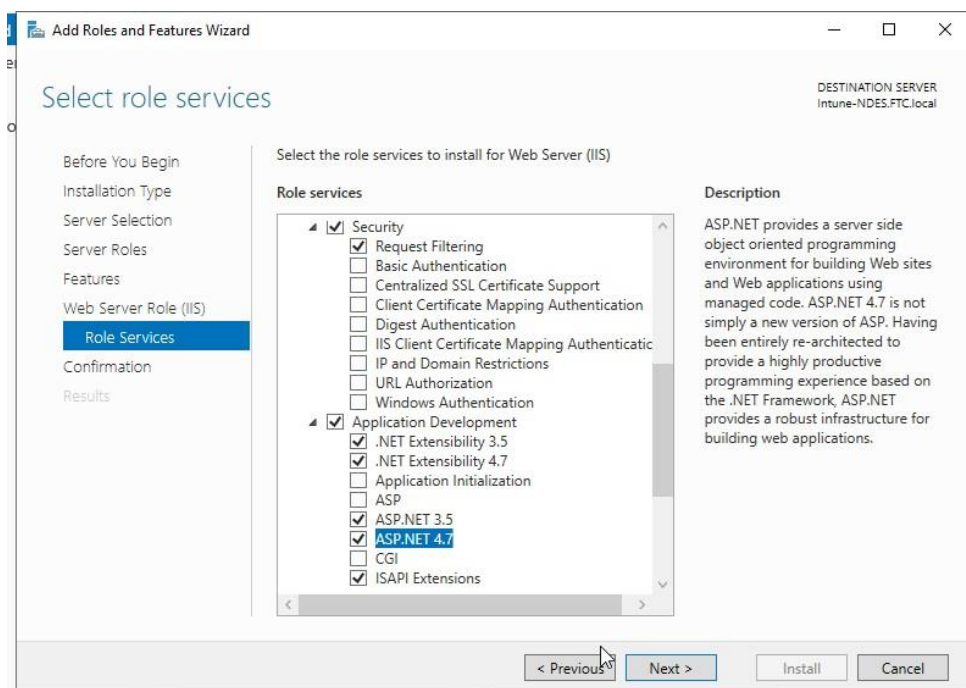
1. When NDES is added to the server, the wizard also installs IIS. Ensure IIS has the following configurations:
 - **Web Server > Security > Request Filtering**



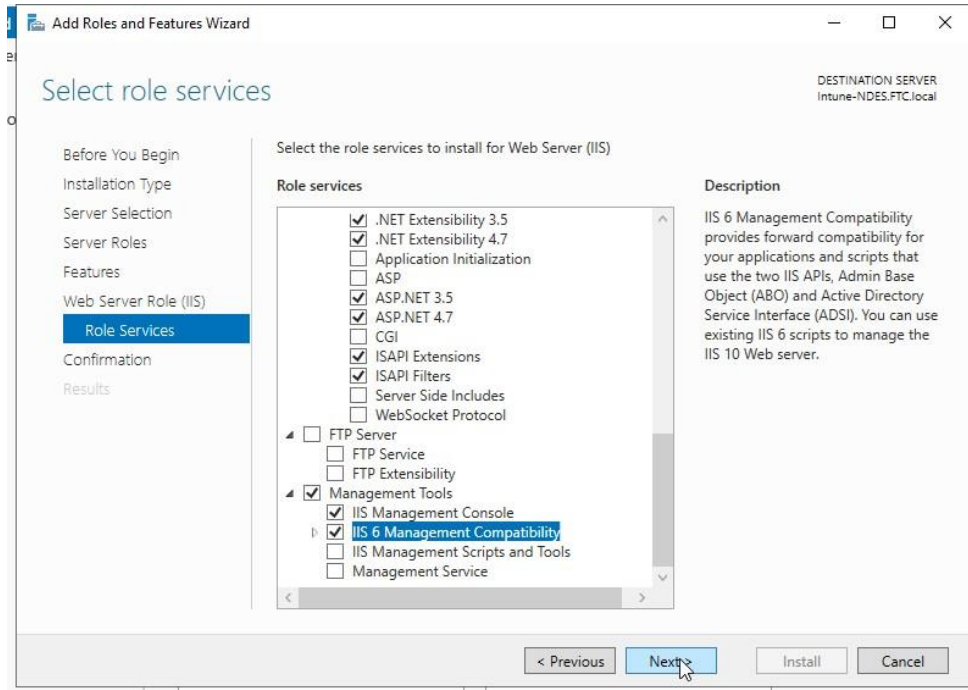
- **Web Server > Application Development > ASP.NET 3.5.** Installing ASP.NET 3.5 will install .NET Framework 3.5. When installing .NET Framework 3.5, install both the core **.NET Framework 3.5** feature and **HTTP Activation**.



- **Web Server > Application Development > ASP.NET 4.5.** Installing ASP.NET 4.5 will install .NET Framework 4.5. When installing .NET Framework 4.5, install the core **.NET Framework 4.5** feature, **ASP.NET 4.5**, and the **WCF Services > HTTP Activation** feature.

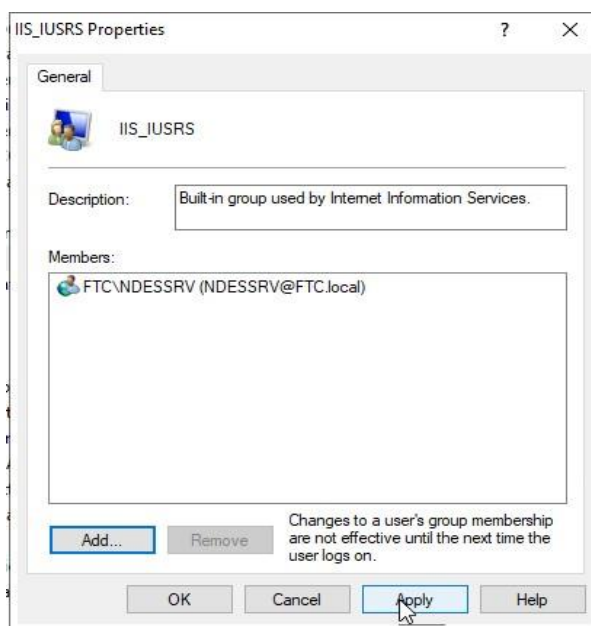


- **Management Tools > IIS 6 Management Compatibility > IIS 6 Metabase Compatibility**
- **Management Tools > IIS 6 Management Compatibility > IIS 6 WMI Compatibility**



Note: When you configure above features for Web role for first time, ensure that you point to Alternative resource D:\sources\sxs to install .net frame work 3.5 successfully from windows ISO image.

2. On the server, add the NDES service account as a member of the **IIS_IUSR** group.



- Run the following command to set the SPN of the NDES Service account: ***Setspn -s http/<DNS name of NDES Server> <Domain name>\<NDES Service account name>***

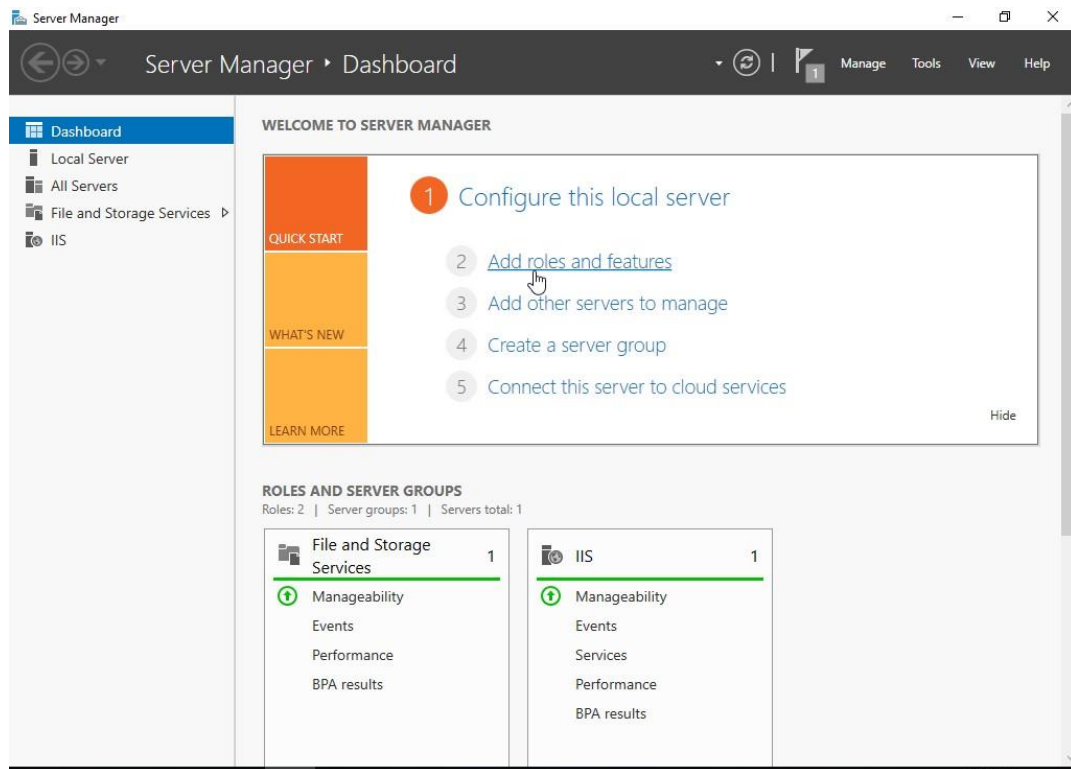
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ftcadmin>setspn -s http/intune-ndes.ftc.local FTC\NDESSRV
Checking domain DC=FTC,DC=local

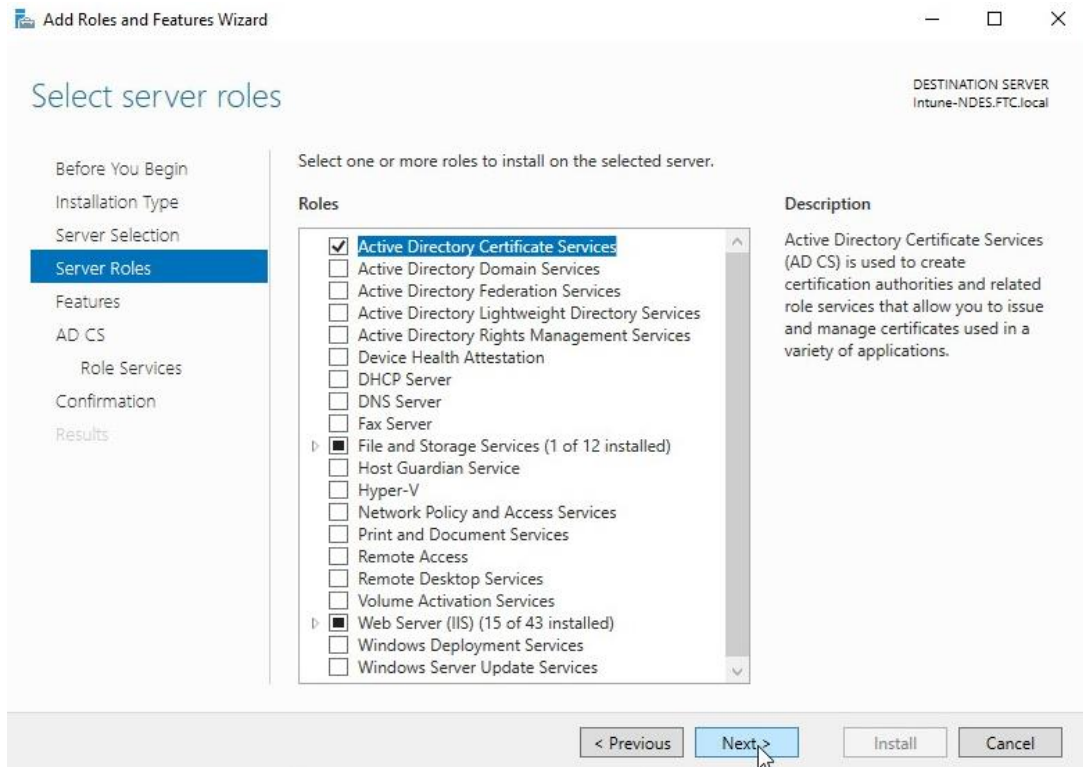
Registering ServicePrincipalNames for CN=NDESSRV,OU=Service Accounts,DC=FTC,DC=local
http/intune-ndes.ftc.local
Updated object

C:\Users\ftcadmin>
```

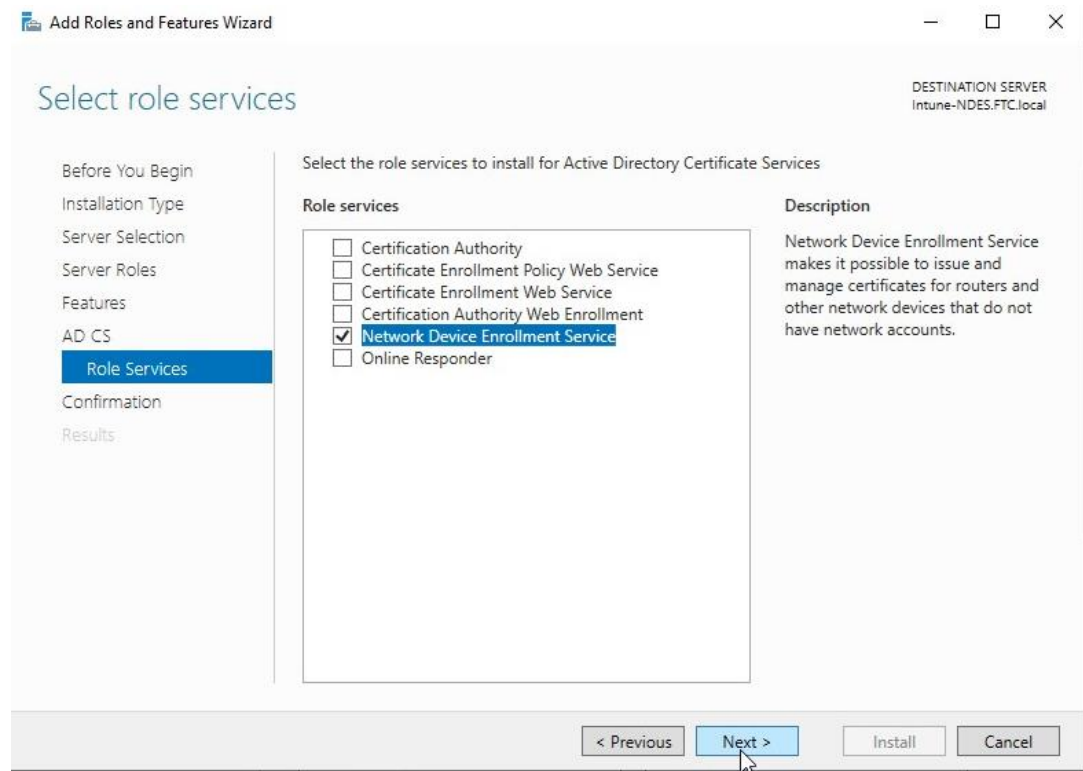
- On the server that will hosts **NDES**, you must log on as an **Enterprise Administrator**, and then use the **Add Roles and Features Wizard** to install NDES



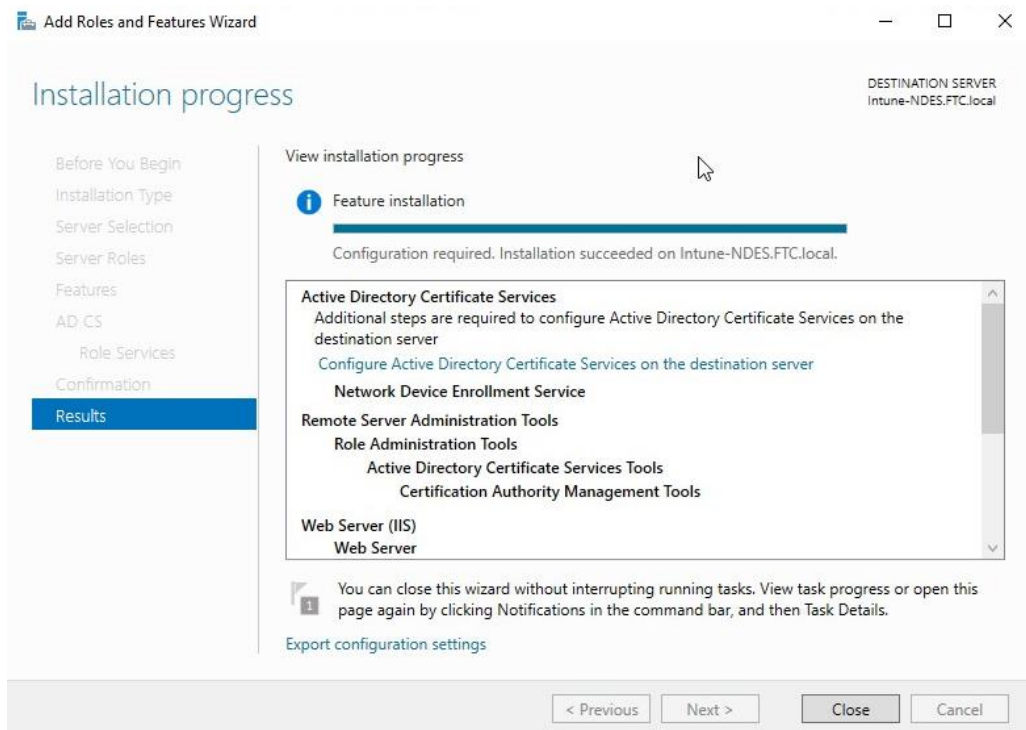
- In the Wizard, select **Active Directory Certificate Services** to gain access to the AD CS Role Services.



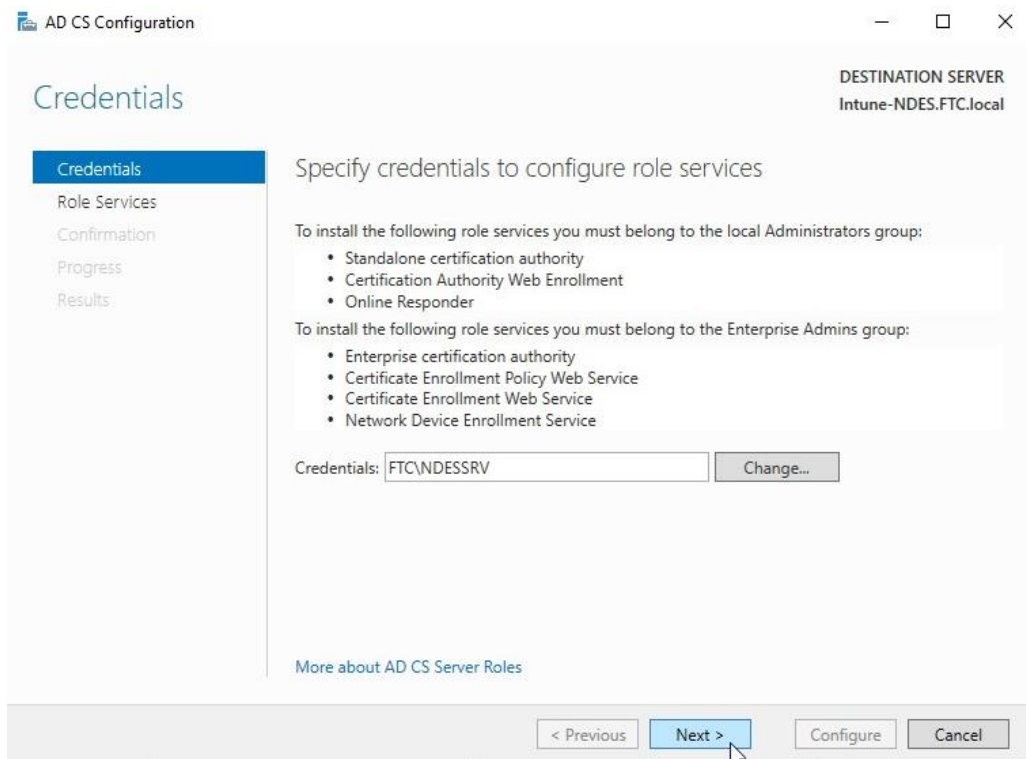
6. Select the **Network Device Enrollment Service**, uncheck Certification Authority, and then complete the wizard.



7. On the **Installation progress** page of the wizard, do not click Close. Instead, click the link for **Configure Active Directory Certificate Services on the destination server**.



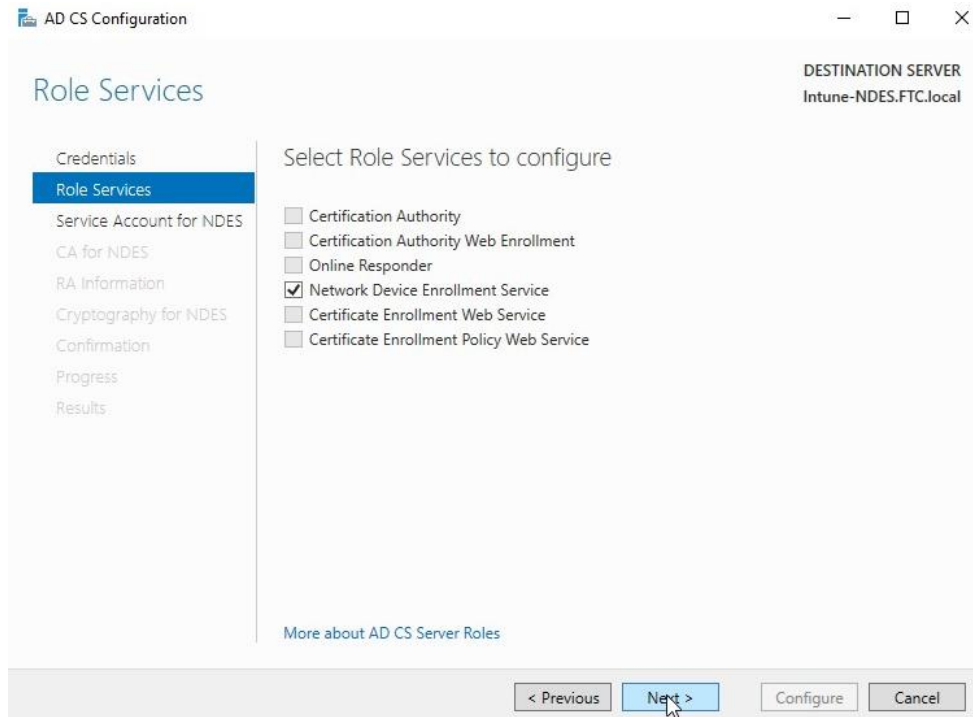
8. **NDES Configuration** windows will open



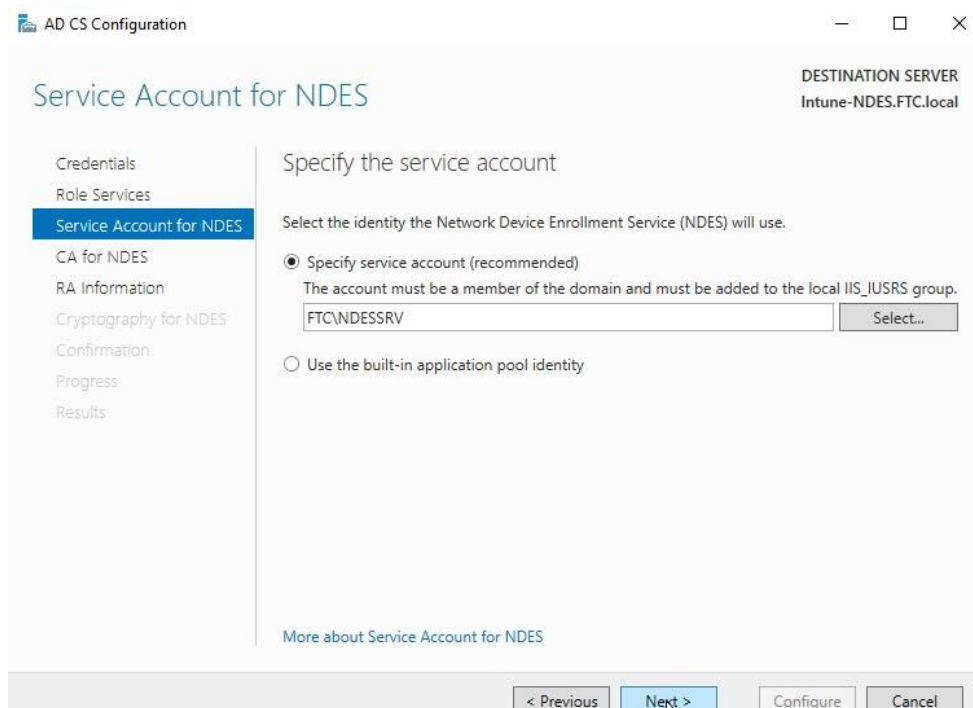
Step 3 - for SCEP profile only: Configure NDES for use with Intune

To configure NDES, you need to follow below steps:

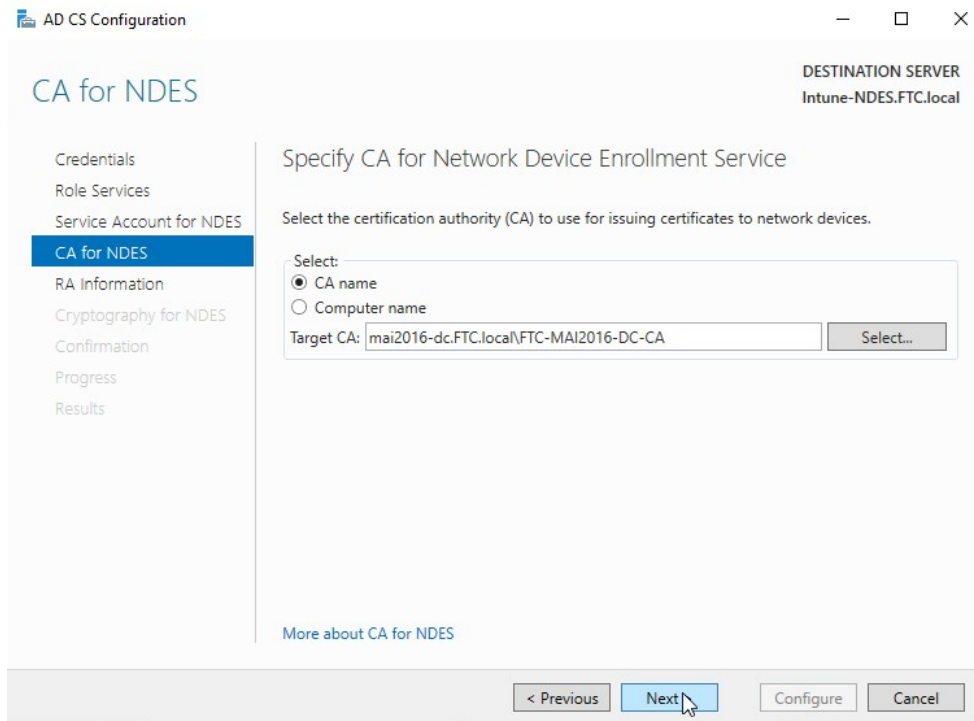
1. On the **Role Services** Page, select the **Network Device Enrollment Service**.



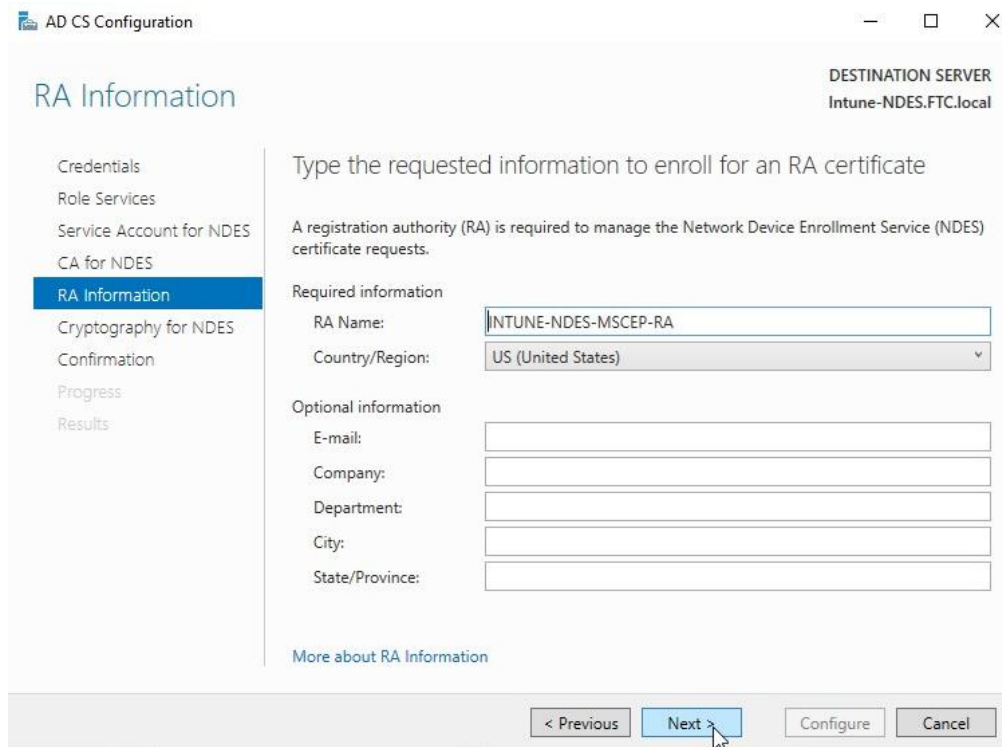
2. On the **Service Account for NDES** page, specify the **NDES Service Account**



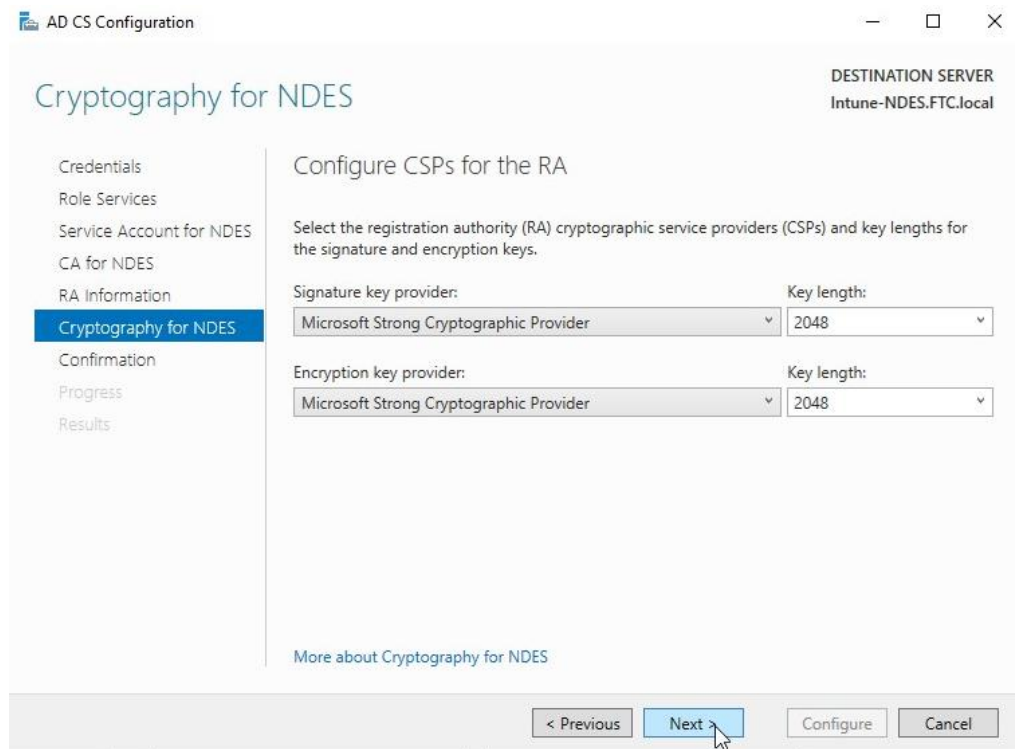
3. On the **CA for NDES** page, click **Select**, and then select the issuing **CA where you configured the certificate template**.



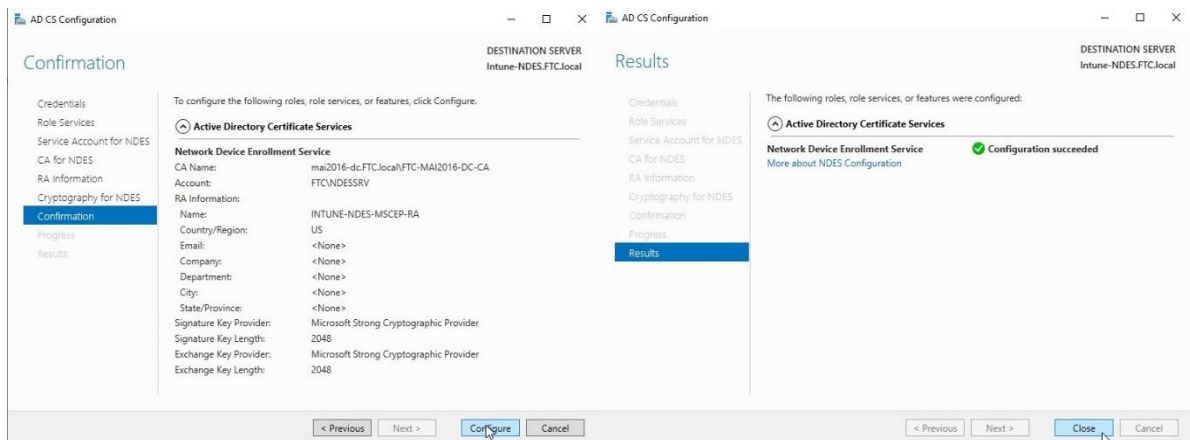
4. On **RA Information**, Click **Next**



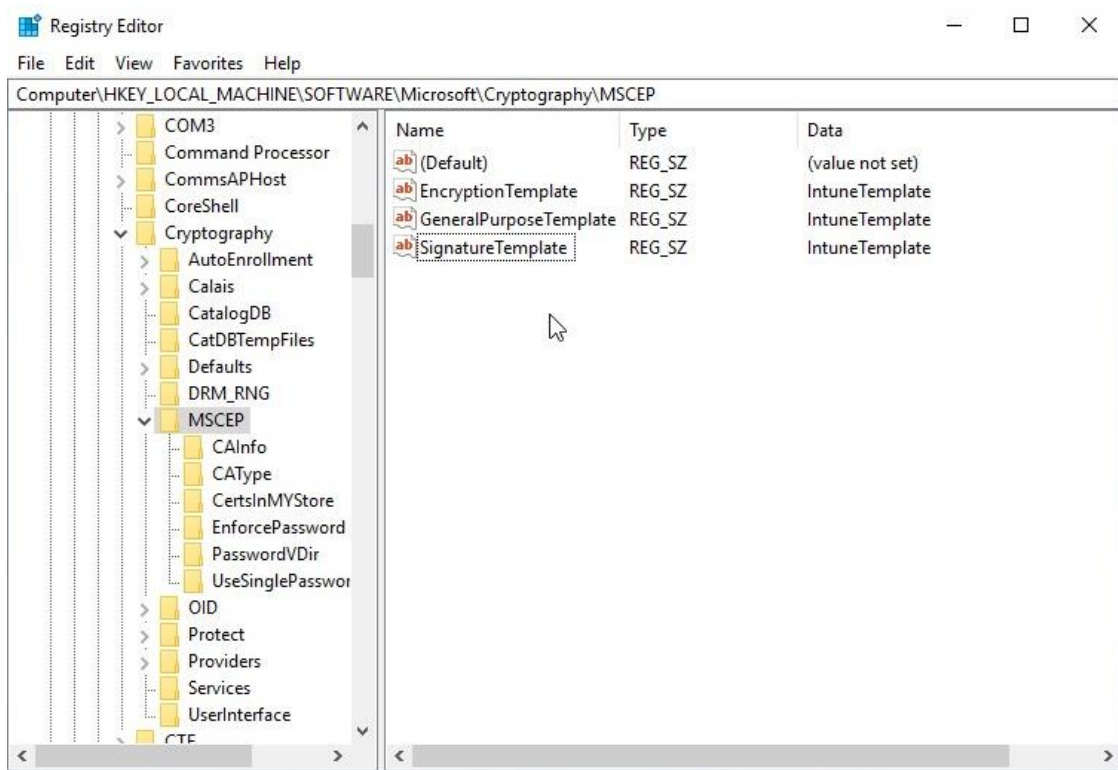
5. On the **Cryptography for NDES** page, set the key length to meet your company requirements.



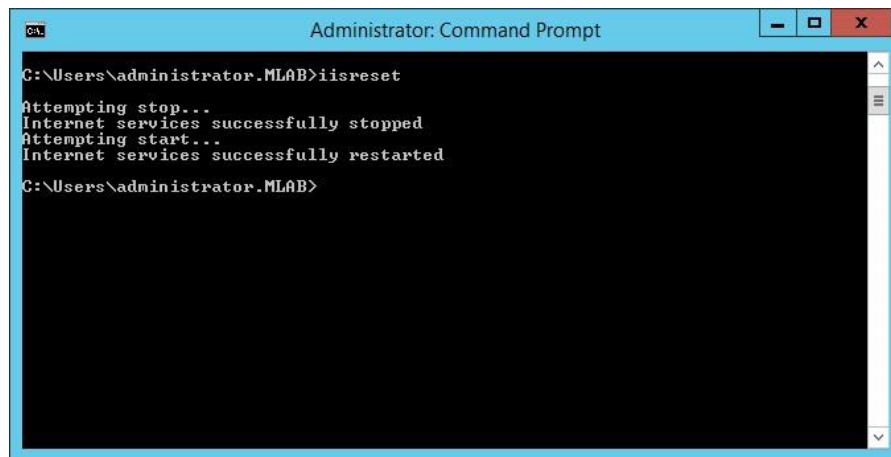
6. On the **Confirmation** page, click **Configure** to complete the wizard.



7. After the wizard completes, edit the following registry key on the **NDES Server**: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP**, edit on 3 Templates and type your template name **“IntuneTemplate”**

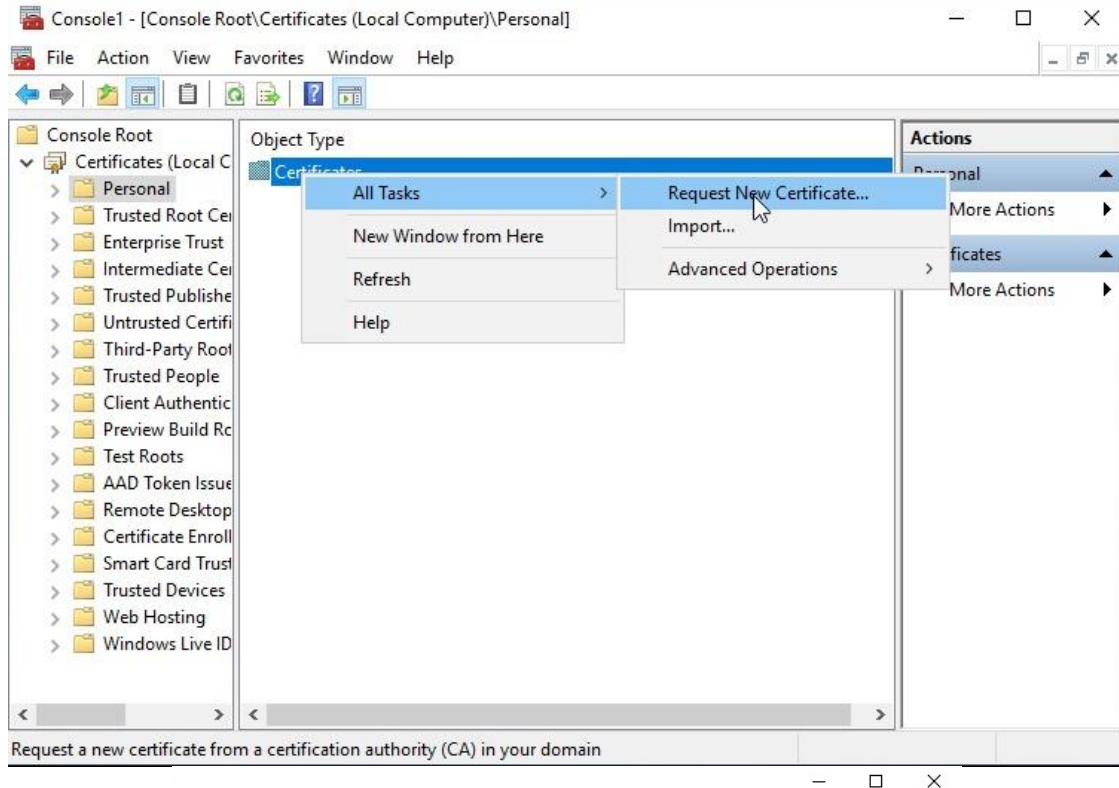


8. After editing the registry, run `iisreset` on the server to force the server to pick up recent configuration changes.



To Install and bind certificates on the NDES Server

1. On your **NDES Server**, request and install a **server authentication certificate** from your internal CA or public CA. You will then bind this SSL certificate in IIS.



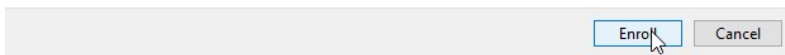
Certificate Enrollment

Request Certificates

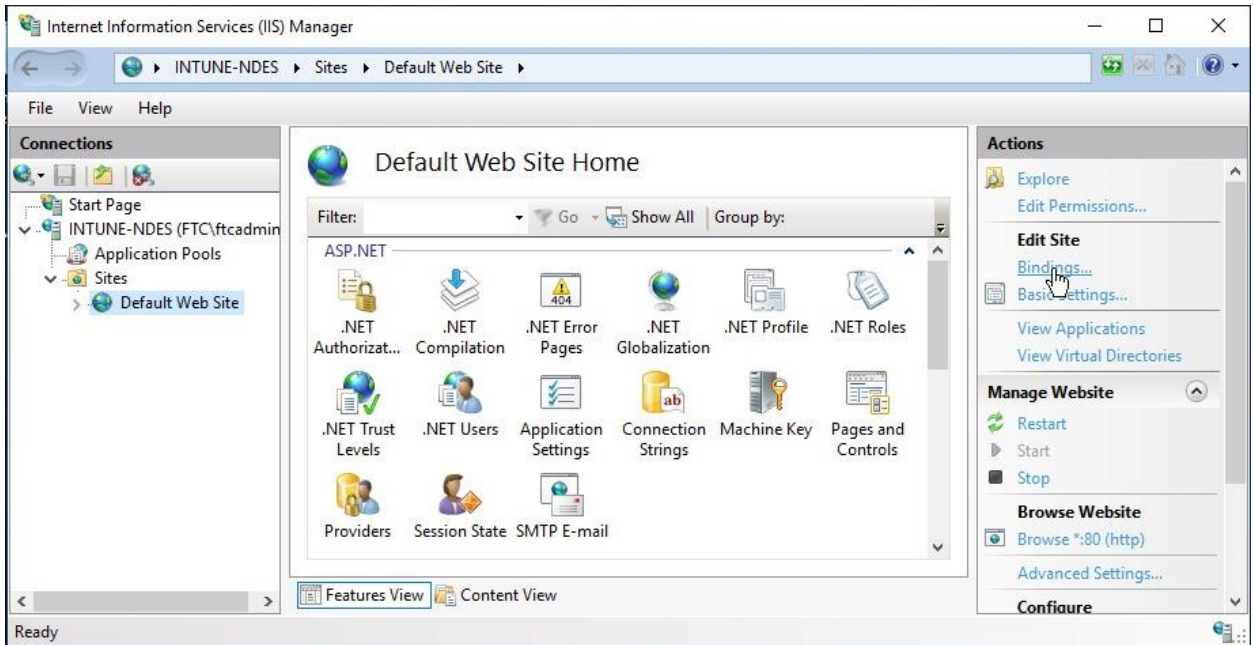
You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy		
<input checked="" type="checkbox"/> Computer	STATUS: Available	Details ▾
<input type="checkbox"/> ConfigMgr Client Certificate	STATUS: Available	Details ▾
<input type="checkbox"/> IntuneHybridTemplate	STATUS: Available	Details ▾
<input type="checkbox"/> IntuneTemplate	STATUS: Available	Details ▾

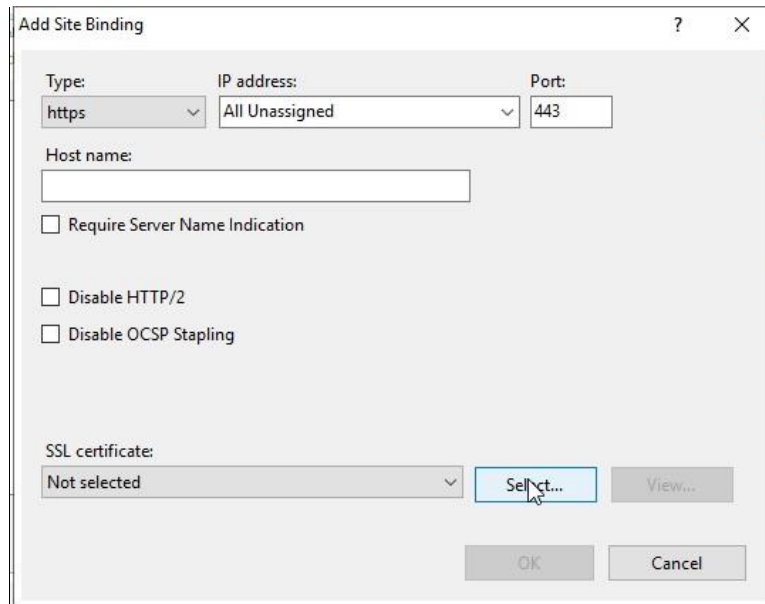
Show all templates



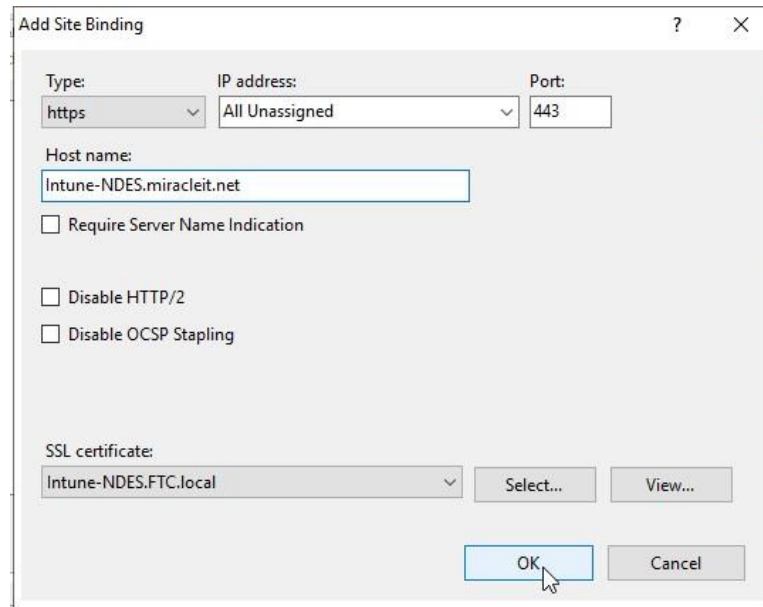
2. After you obtain the server authentication certificate, open **IIS Manager**, select the **Default Web Site** in the Connections pane, and then click **Bindings** in the Actions pane.



3. Click **Add**, set Type to **https**, and then ensure the port is **443**. (Only port 443 is supported for standalone Intune).

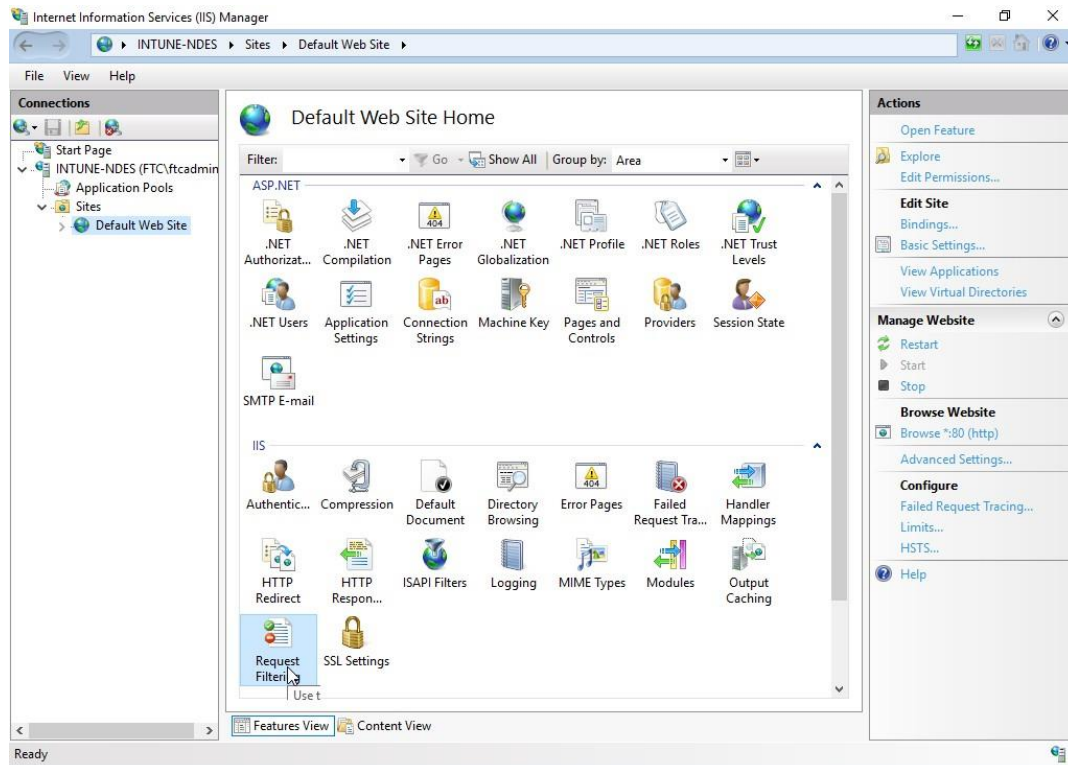


4. For **SSL certificate**, specify the **server authentication certificate**.

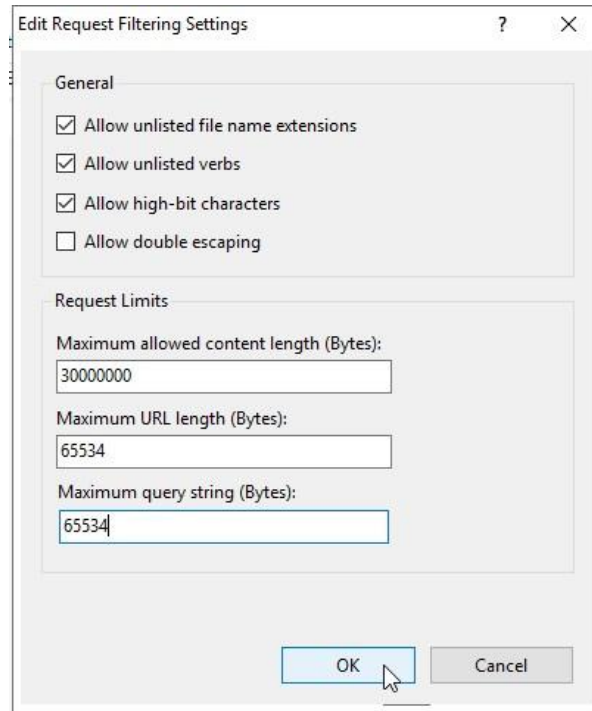


To configure IIS Request Filtering

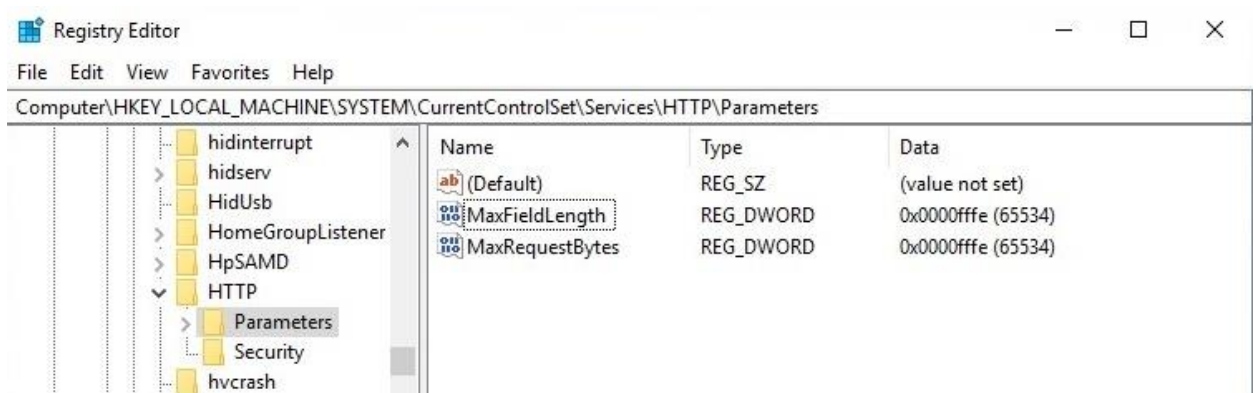
1. On the **NDES Server** open **IIS Manager**, select the **Default Web Site** in the Connections pane, and then open **Request Filtering**.



2. Click **Edit Feature Settings**, and then set the following:
 1. query string (Bytes) = 65534
 2. Maximum URL length (Bytes) = 65534



- Review the following registry key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters. Ensure the following values are set as DWORD entries:
 - Name: MaxFieldLength, with a decimal value of 65534
 - Name: MaxRequestBytes, with a decimal value of 65534



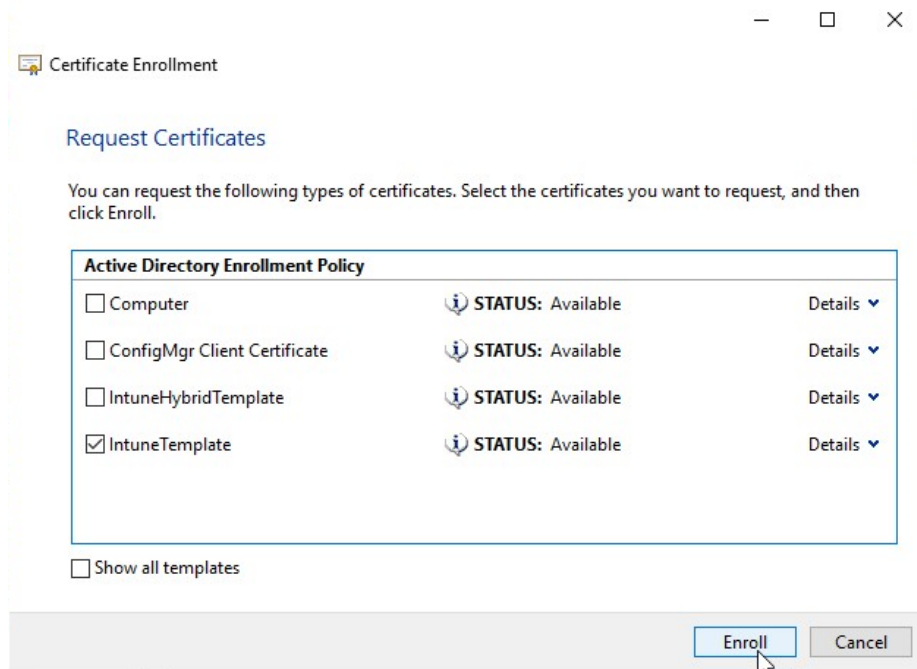
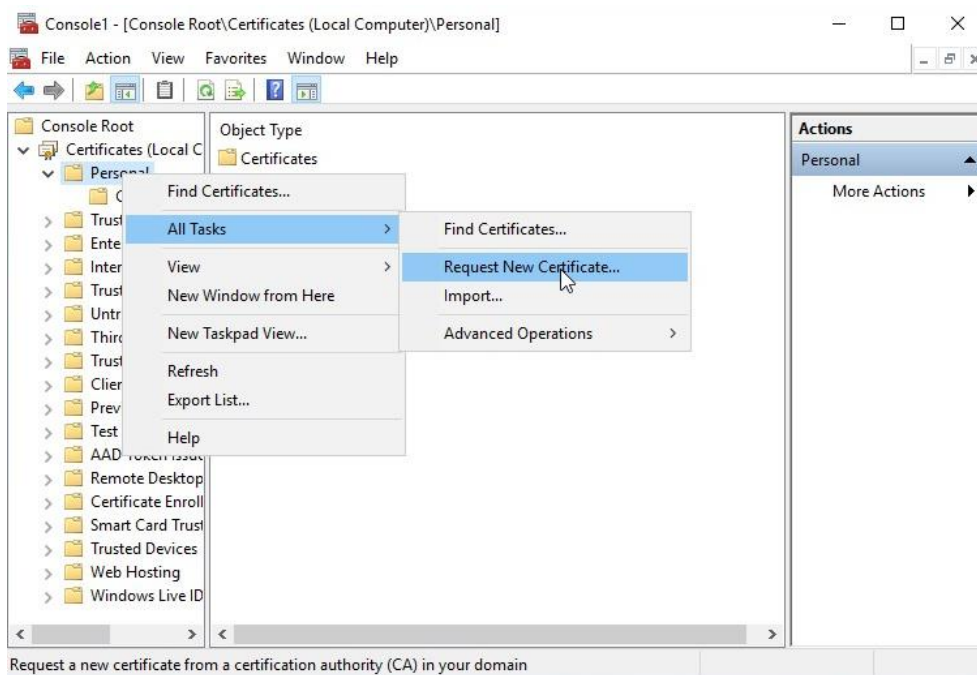
- Reboot the NDES server. The server is now ready to support the Certificate Connector.

Step 4 - Enable, install, and configure the Intune Certificate Connector

The Microsoft Intune Certificate Connector **must** be installed on a separate Windows server. It can't be installed on the issuing Certificate Authority (CA). It **must** also be installed on the same server as the Network Device Enrollment Service (NDES) role.

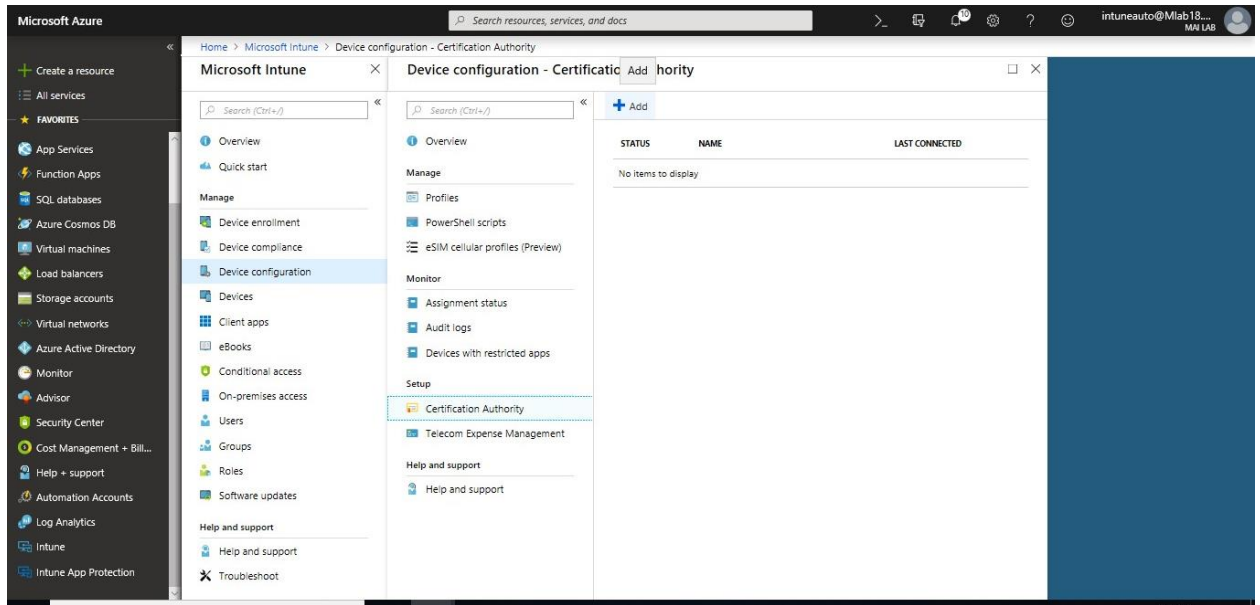
To download, install and configure the Certificate Connector

1. Click on Request certificate then Enroll Client Certificate “IntuneTemplate”

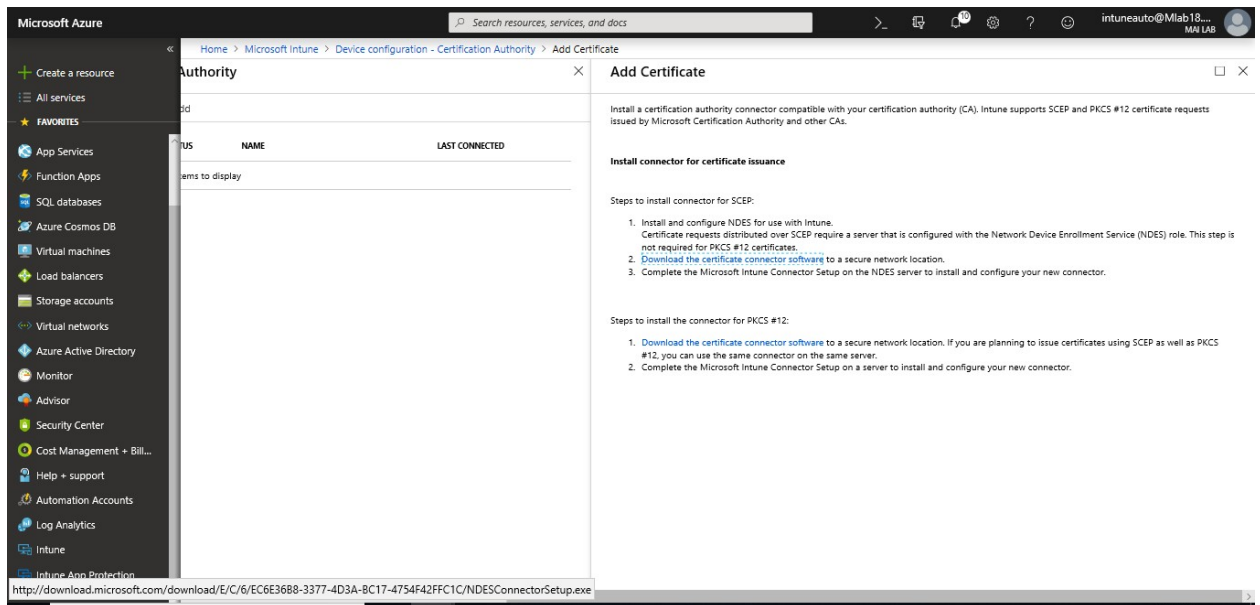


2. In the [Azure portal](#), select **All services**, filter on **Intune**, and select **Microsoft Intune**.
3. Select **Device configuration** > **Certification Authority** > **Add**

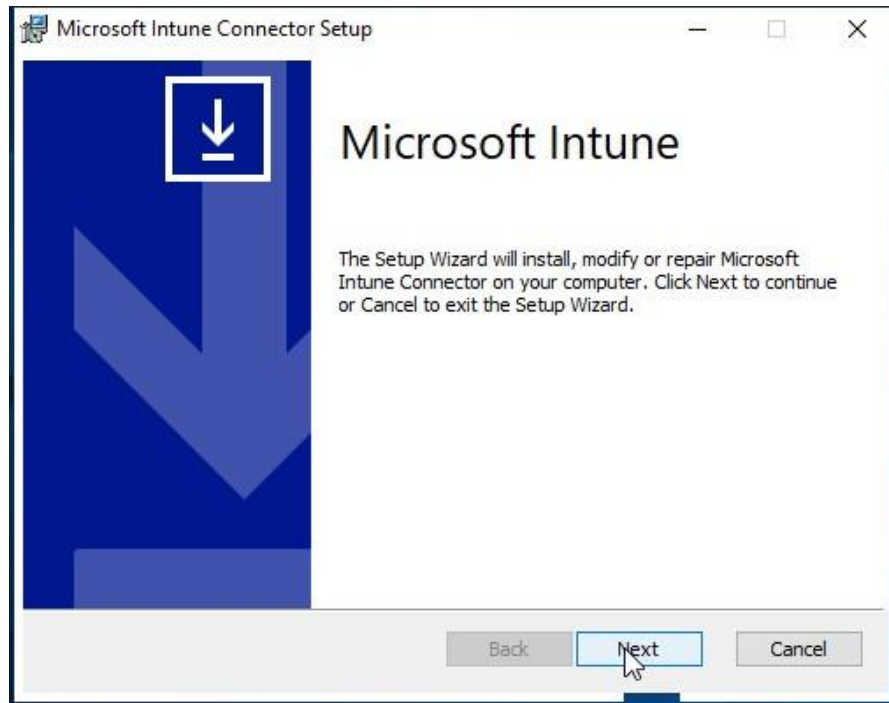
Microsoft Intune step by step on Azure portal



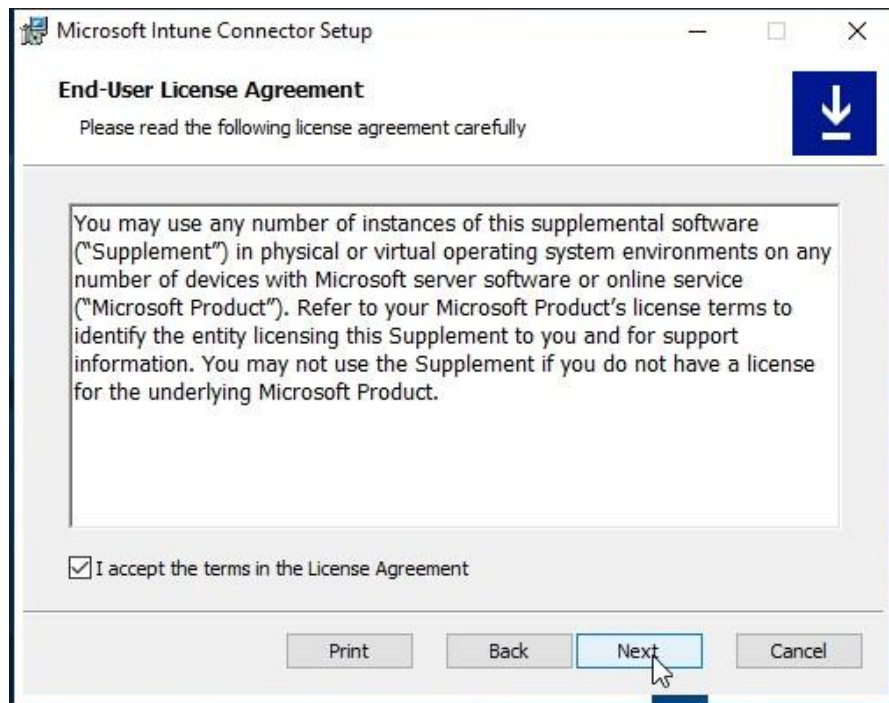
4. Download and save the connector file. Save it to a location accessible from the server where you're going to install the connector.



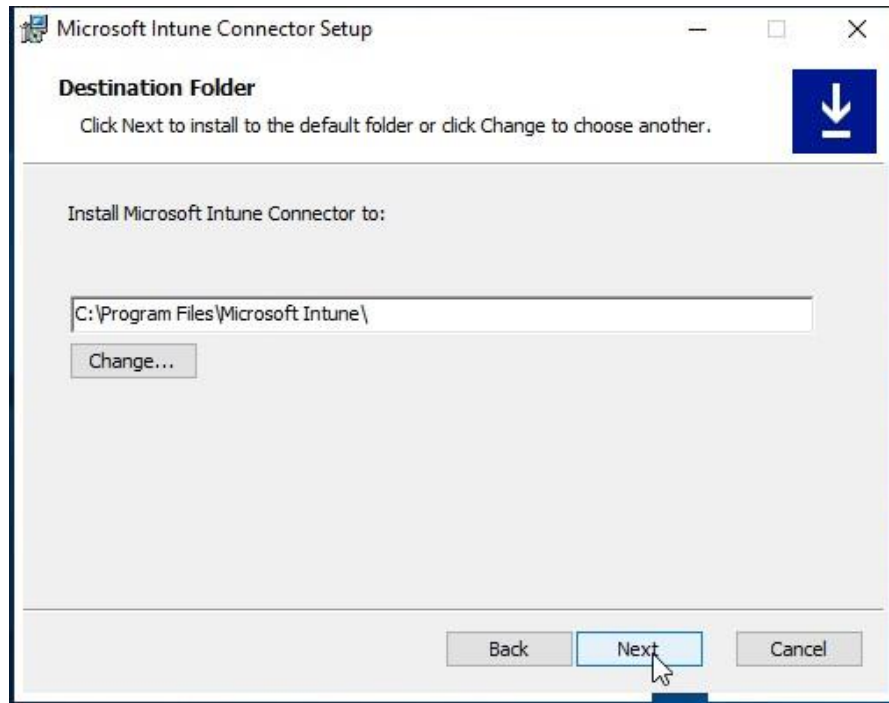
5. After the download completes, run the downloaded installer (ndesconnectorsetup.exe)
6. On Welcome Page, Click **Next**



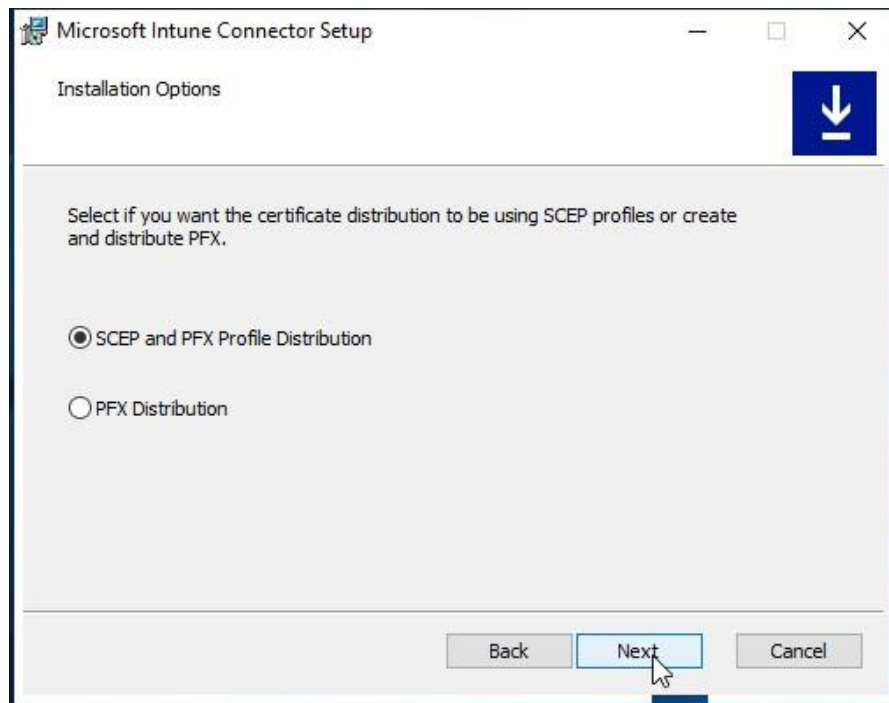
7. Check **I accept the terms in the License Agreement**, Click **Next**.



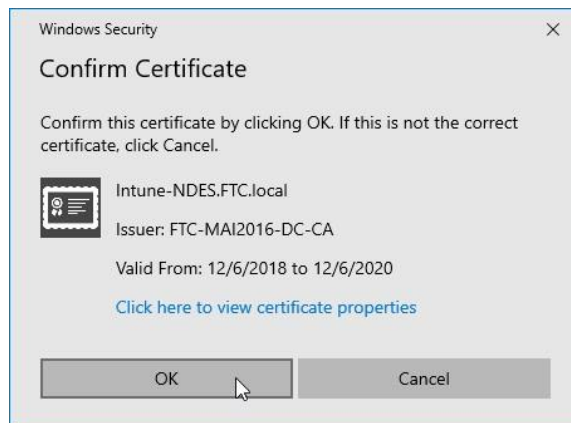
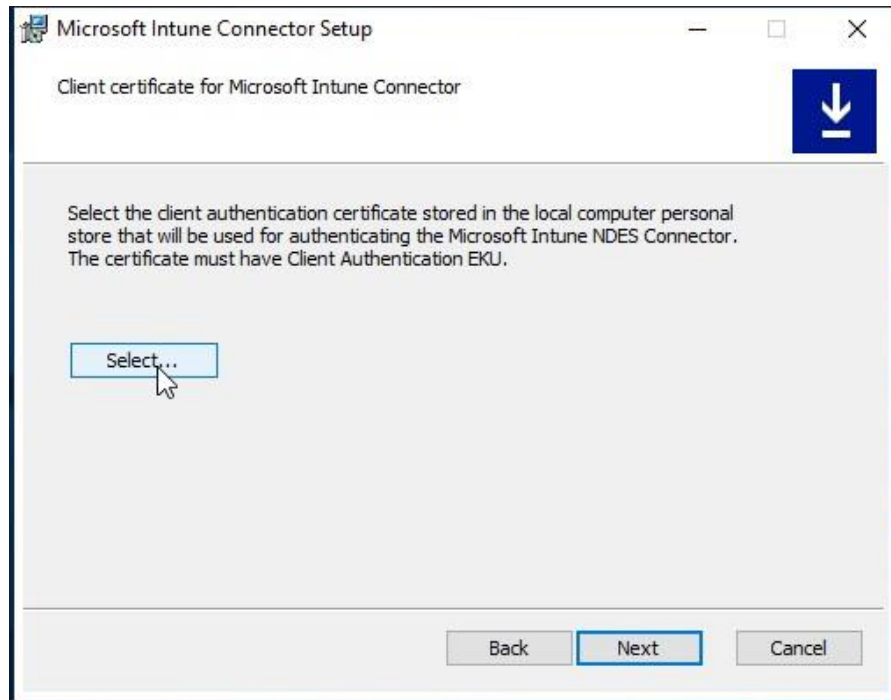
8. On **Destination Folder** Page, Click **Next**.



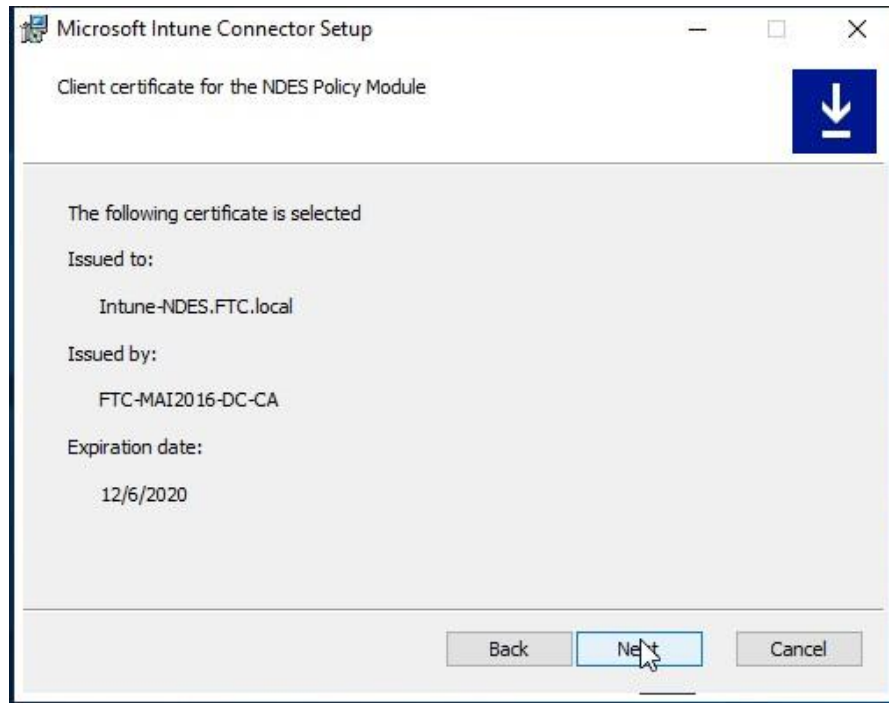
9. Select **SCEP and PFX Destination**, Click **Next**.



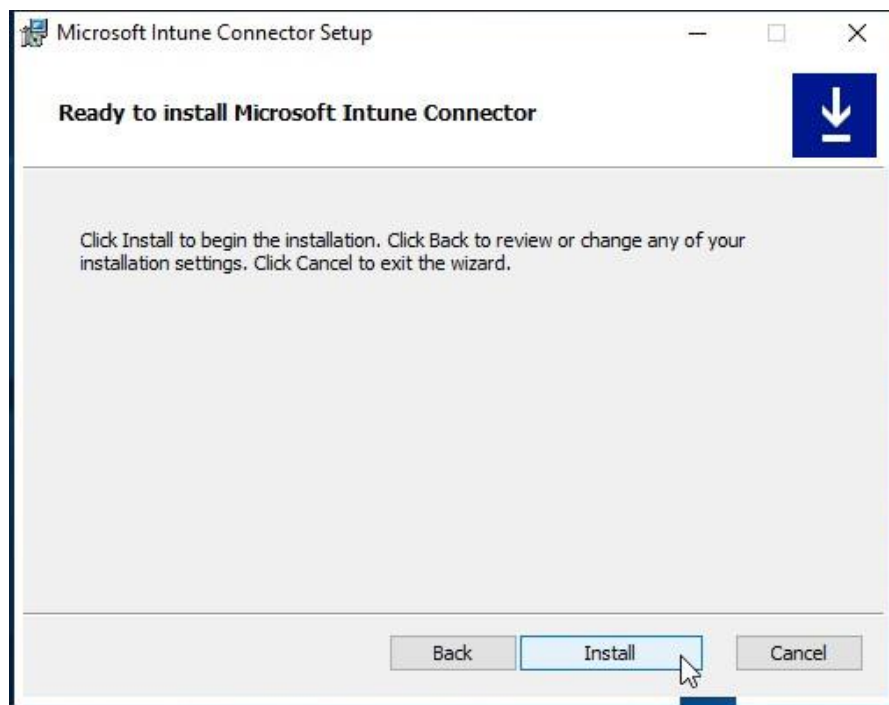
10. Click **Select** and select Intune Certificate then click **Ok**.



11. Ensure the Following Certificate is selected, Click **Next**

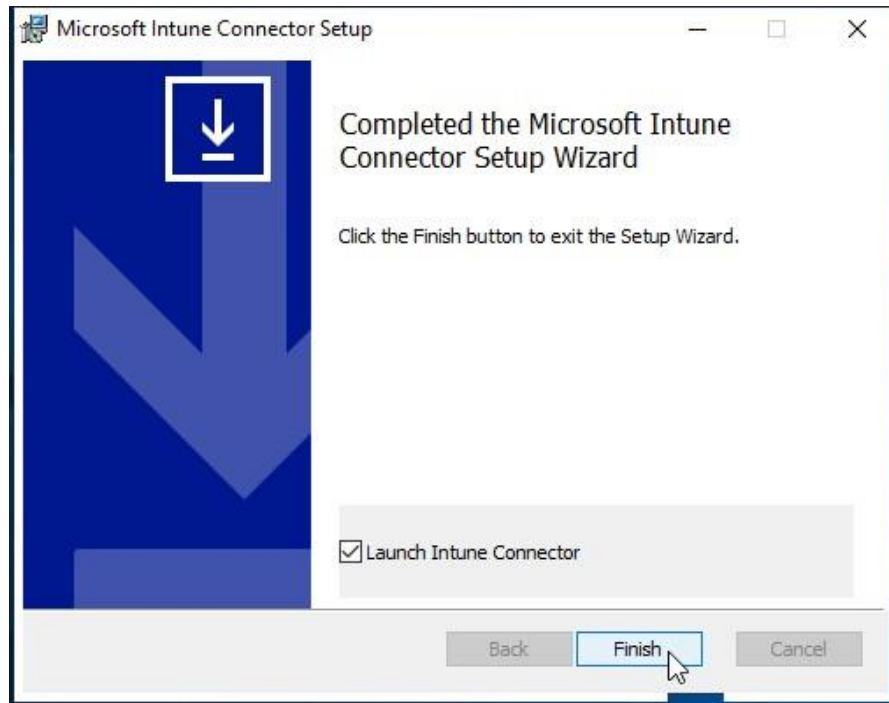


12. On **Ready to install Microsoft Intune connector** Page, Click **Install**.

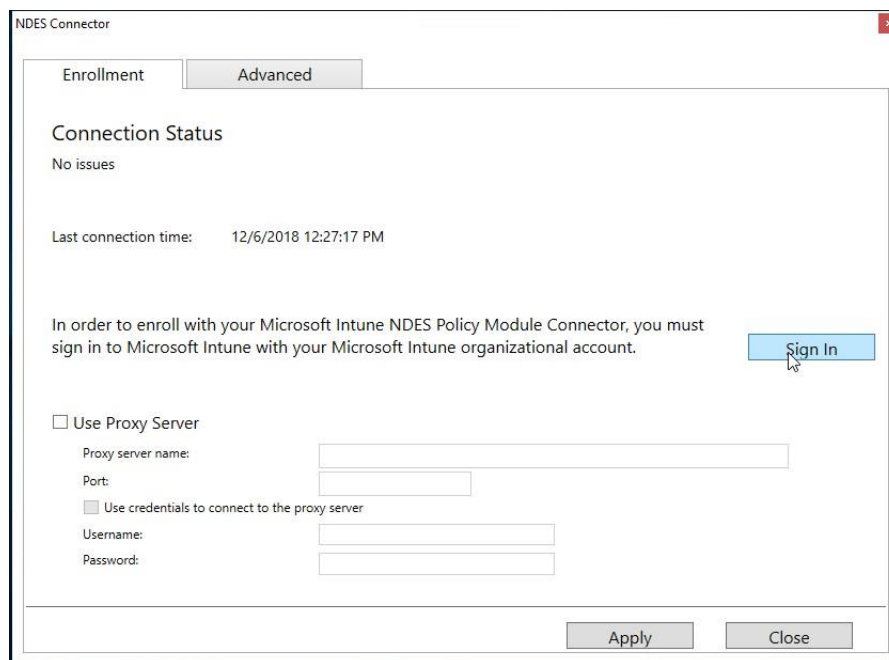


Note: Internet Explorer Enhanced Security Configuration must be disabled on the NDES server hosting the Intune Certificate Connector.

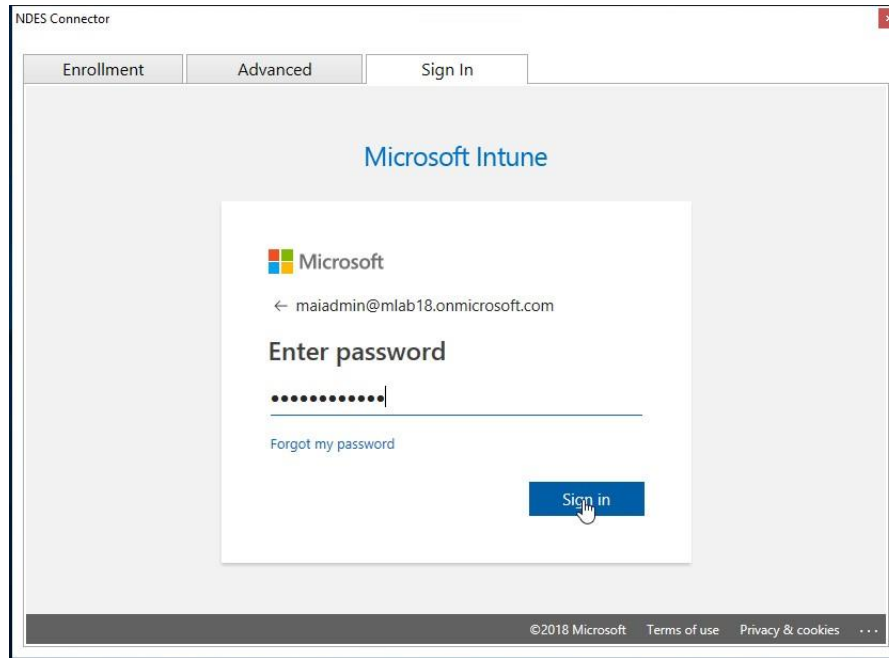
13. Select **Launch Intune connector** and click **finish**



14. Click **sign-in**



15. On **Sign in** Tab, enter your Intune service administrator credentials, or credentials for a tenant administrator with the global administration permission.



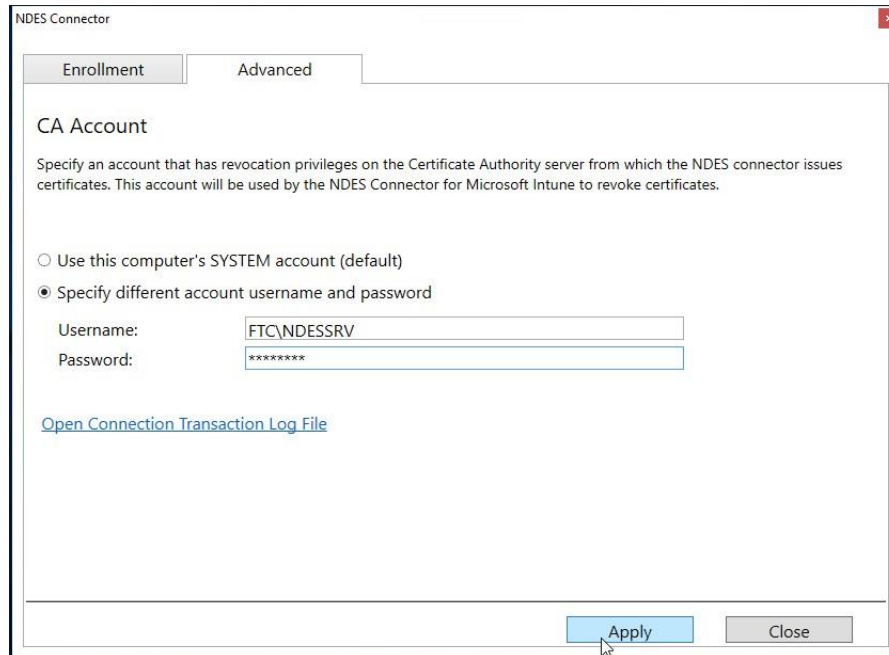
Note: The user account must be assigned a valid Intune license. If the user account does not have a valid Intune license, then NDESConnectorUI.exe fails.

16. Successfully **Enrolled**, Click **Ok**

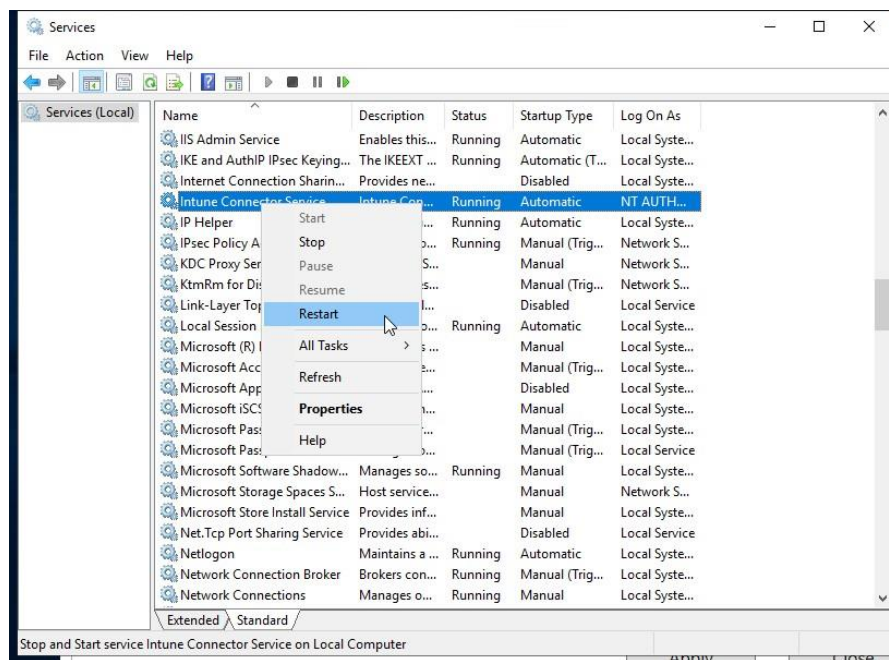


17. Select the **Advanced** tab, and then enter credentials for an account that has the **Issue and Manage Certificates** permission on your issuing Certificate Authority. **Apply** your changes. You can now close the Certificate Connector UI.

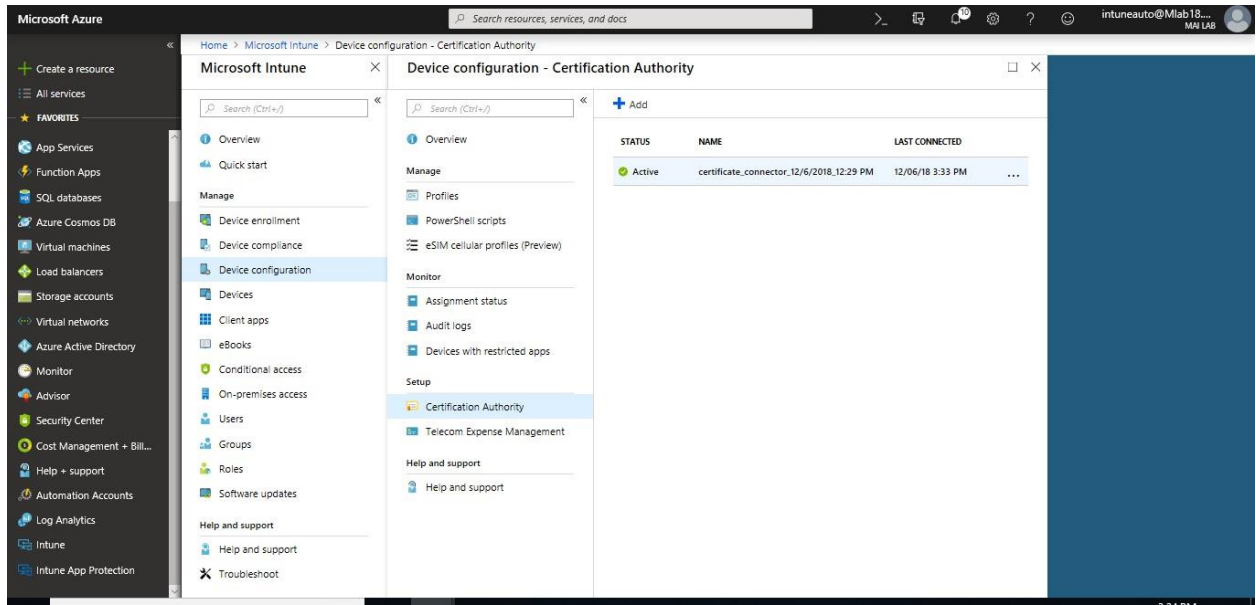
Microsoft Intune step by step on Azure portal



18. Open **run** and type **services.msc**, and then press **Enter**, right-click the **Intune Connector Service**, and then click **Restart**.



19. When you login to Azure Portal, you should find that the Intune Certificate Connector is created and active.



20. validate that the service is running, open a browser and enter the following URL, which should return a 403 error: http://<FQDN_of_your_NDES_server>/certsrv/mscep/mscep.dll. You are now ready to configure certificate profiles.

Note: TLS 1.2 support is included with the NDES Certificate connector. So, if the server with NDES Certificate connector installed supports TLS 1.2, then TLS 1.2 is used. If the server doesn't support TLS 1.2, then TLS 1.1 is used. Currently, TLS 1.1 is used for authentication between the devices and server.

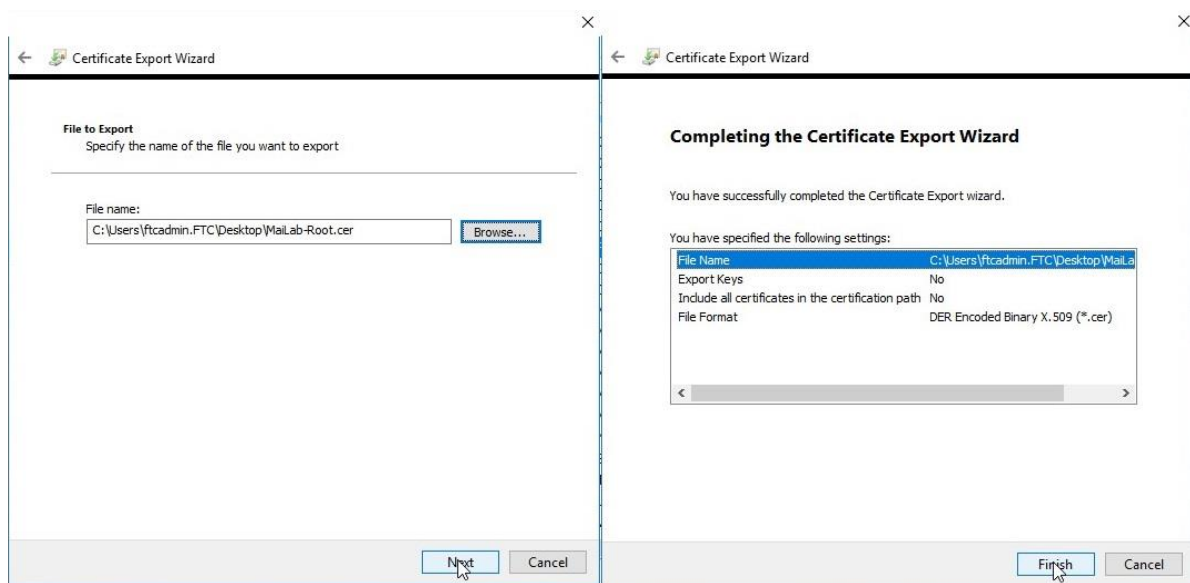
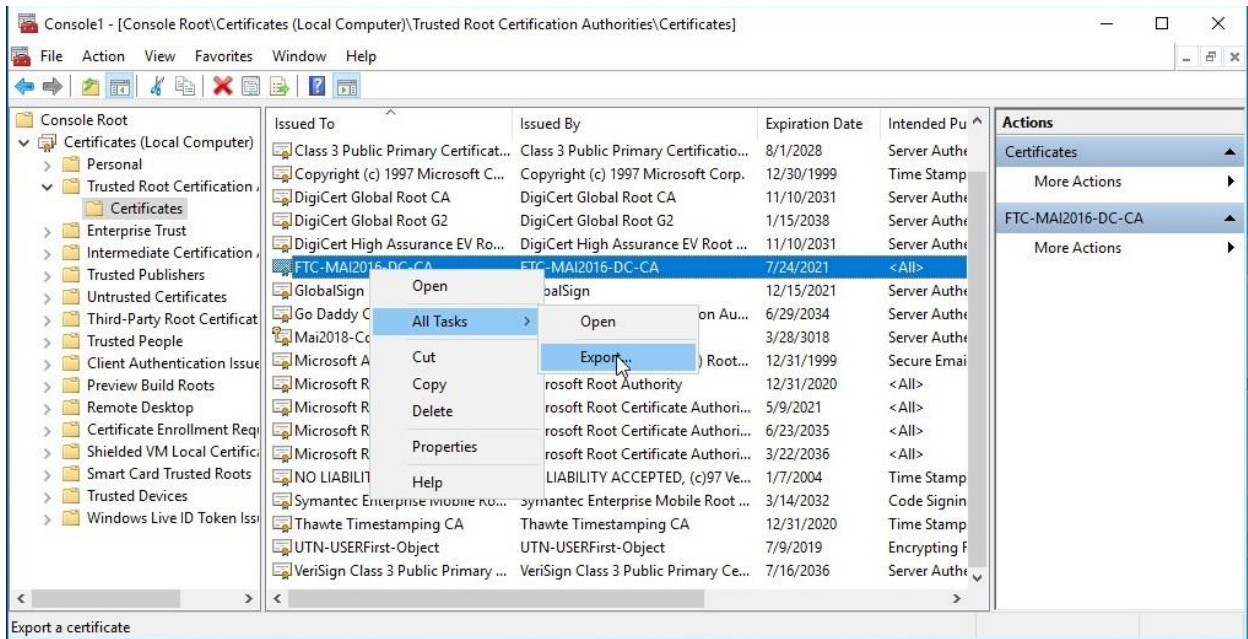
Configuring Certificate Profiles

After your infrastructure and certificates are configured, you can configure certificate profiles:

- Step 1 - Export the Trusted Root CA certificate
- Step 2 - Create Trusted CA certificate profiles
- Step 3 - Create SCEP certificate profiles
- Step 4 - Create PFX certificate profiles

Step 1 - Export the Trusted Root CA certificate

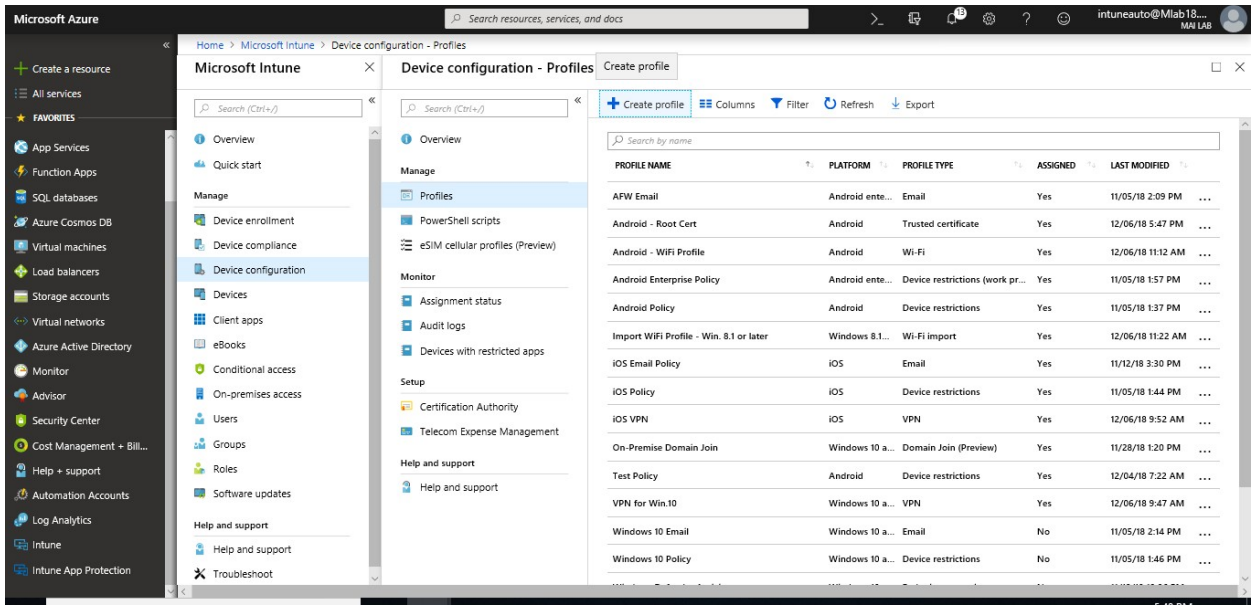
1. Export Root Certificate as a **.cer** file from the issuing CA



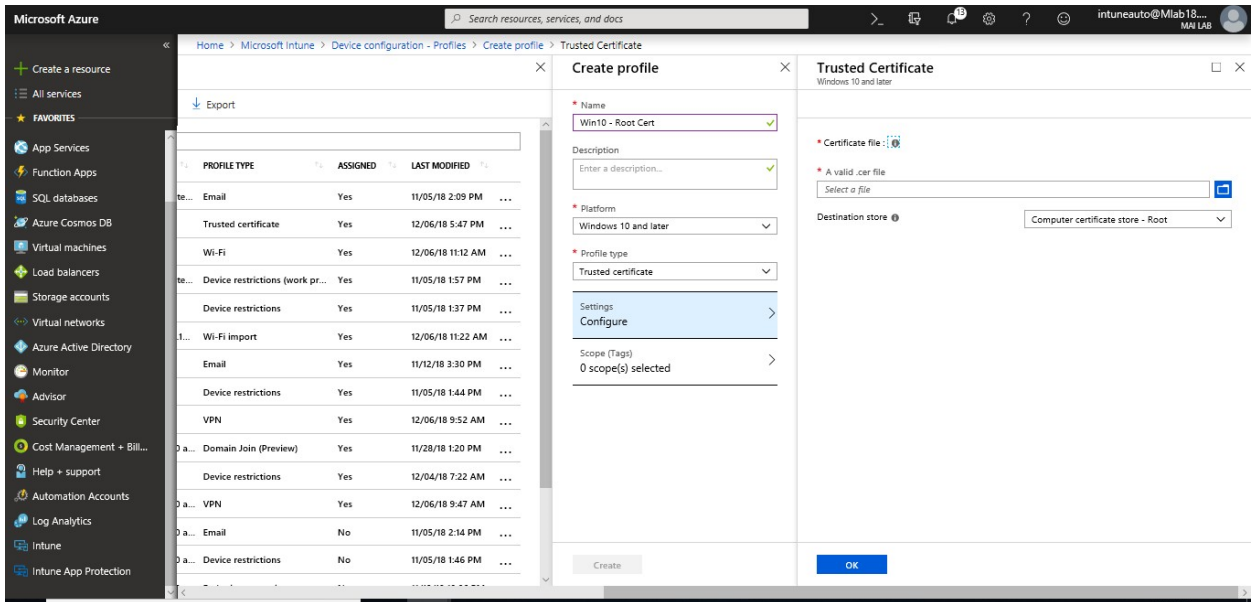
Step 2 - Create Trusted CA certificate profiles

Create a trusted certificate profile before you can create a SCEP or PKCS certificate profile. A trusted certificate profile and a SCEP or PKCS profile are needed for each device platform. The steps to create trusted certificates are similar for each device platform. To create Trusted CA certificate profile, you need to follow below steps:

1. Sign in to the [Azure portal](#). Select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device configuration** > **Manage** > **Profiles** > **Create profile**.



3. Enter a **Name** and **Description** for the trusted certificate profile.
4. From the **Platform** drop-down list, select the device platform for this trusted certificate.
Your options: **Windows 10 and later**
5. From the **Profile type** drop-down list, choose **Trusted certificate**.

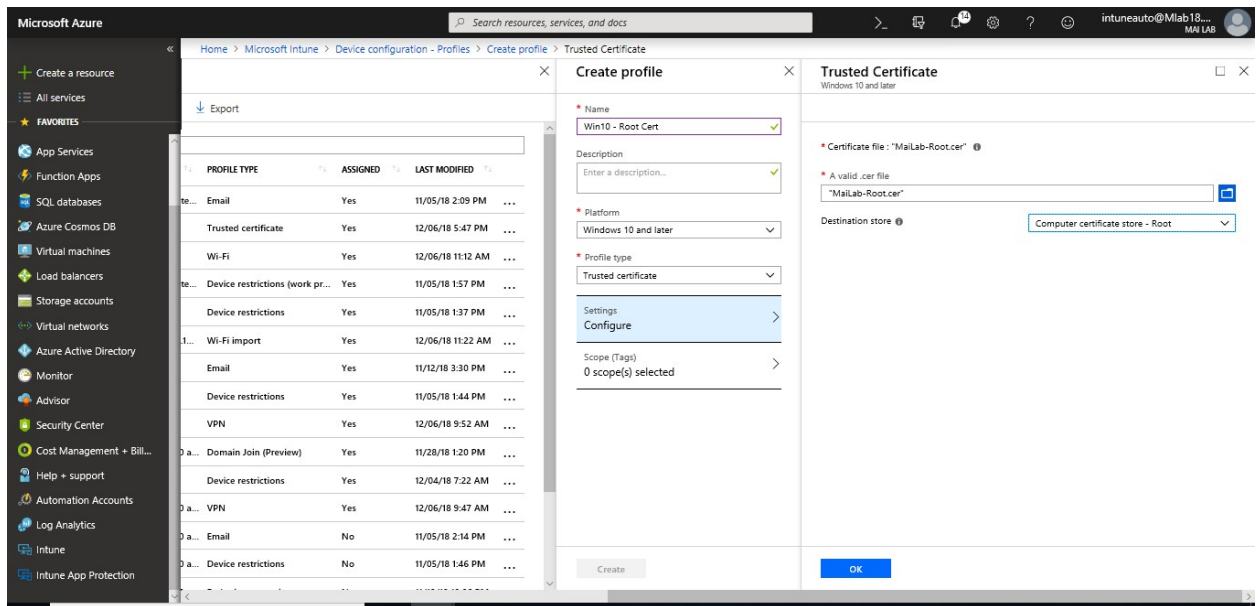


Note: The Trusted CA can be created to **Android, Android Enterprise, iOS, macOS, Windows Phone 8.1, Windows 8.1 and later.**

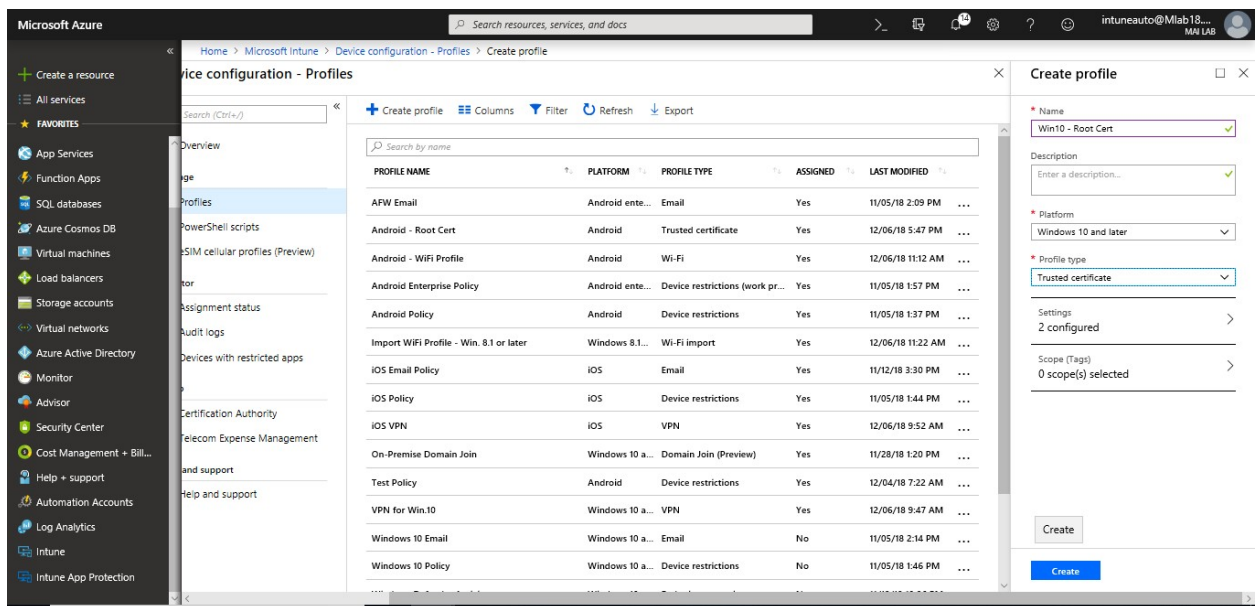
6. Browse to the certificate you saved in task 1, then select **OK**.
7. For Windows 8.1 and Windows 10 devices only, select the **Destination Store** for the trusted certificate from:

Microsoft Intune step by step on Azure portal

- Computer certificate store - Root
- Computer certificate store - Intermediate
- User certificate store – Intermediate

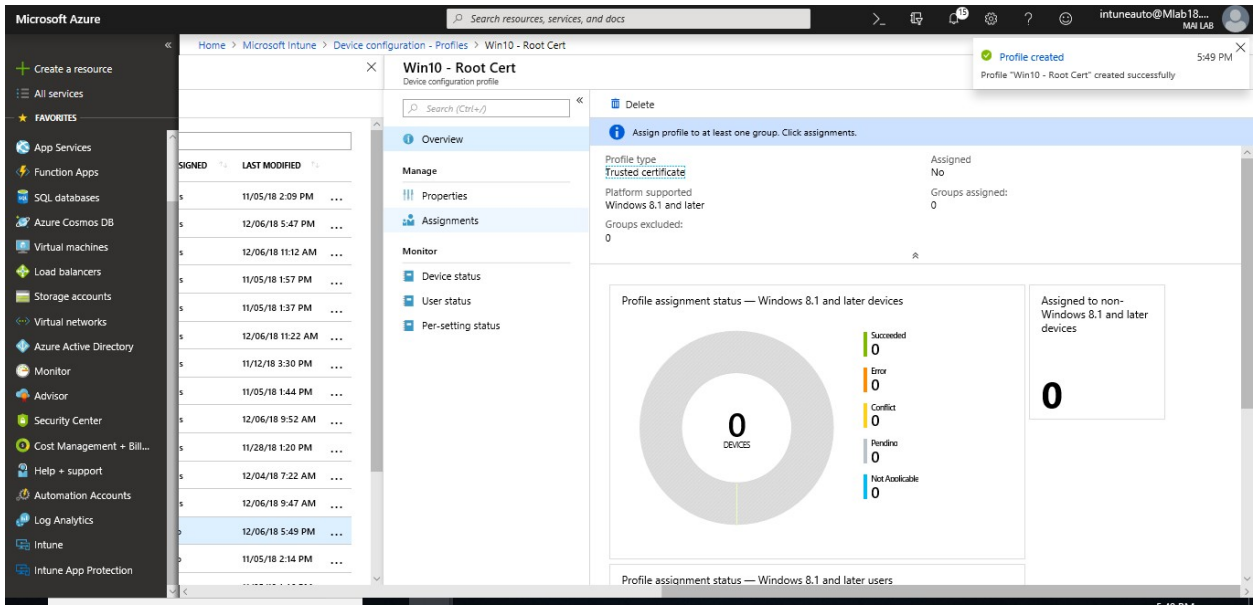


8. When you're done, choose **OK**, go back to the **Create profile** pane, and select **Create**.

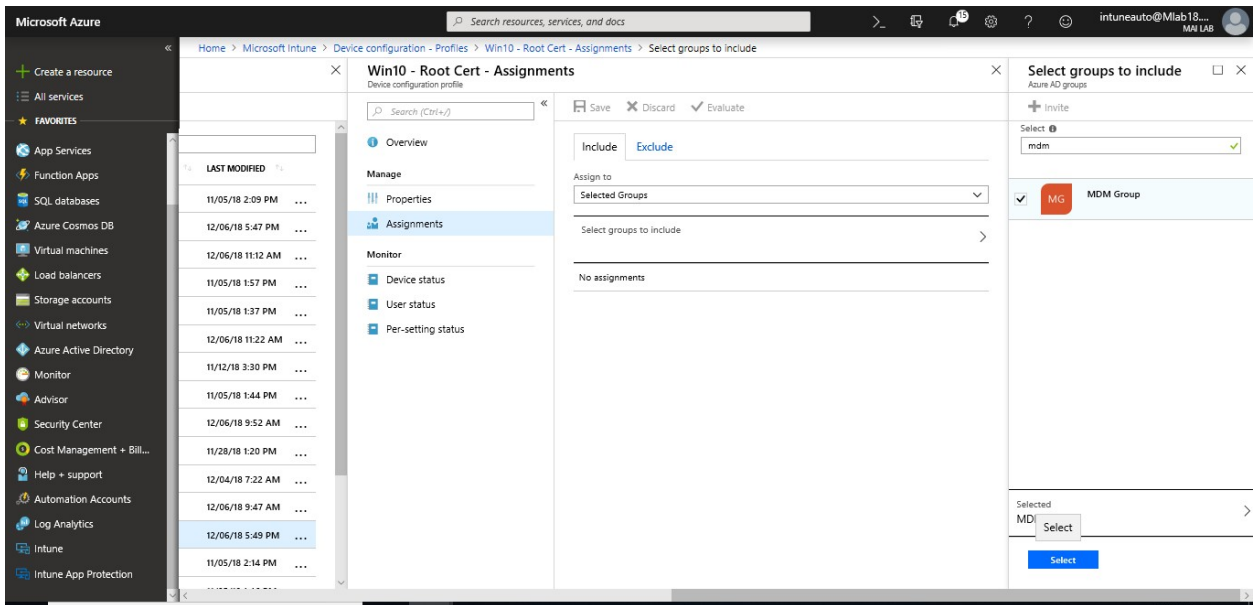


9. In the list of profiles, select the profile you want to assign, and then select **Assignments**.

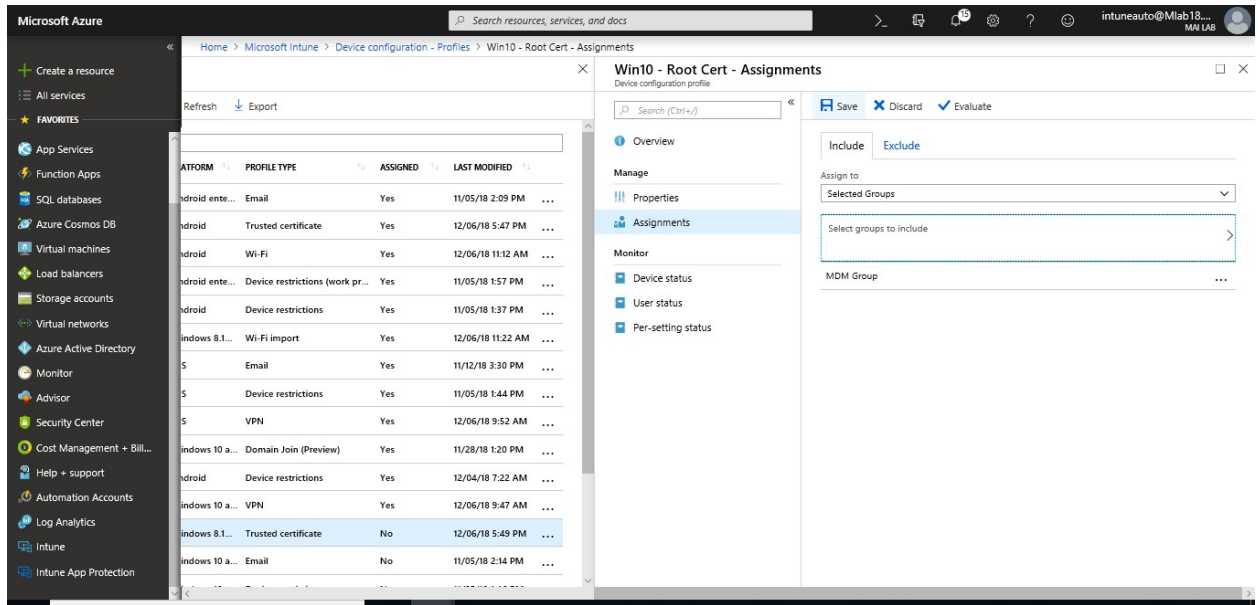
Microsoft Intune step by step on Azure portal



10. Choose to **Include** groups or **Exclude** groups, and then select groups.



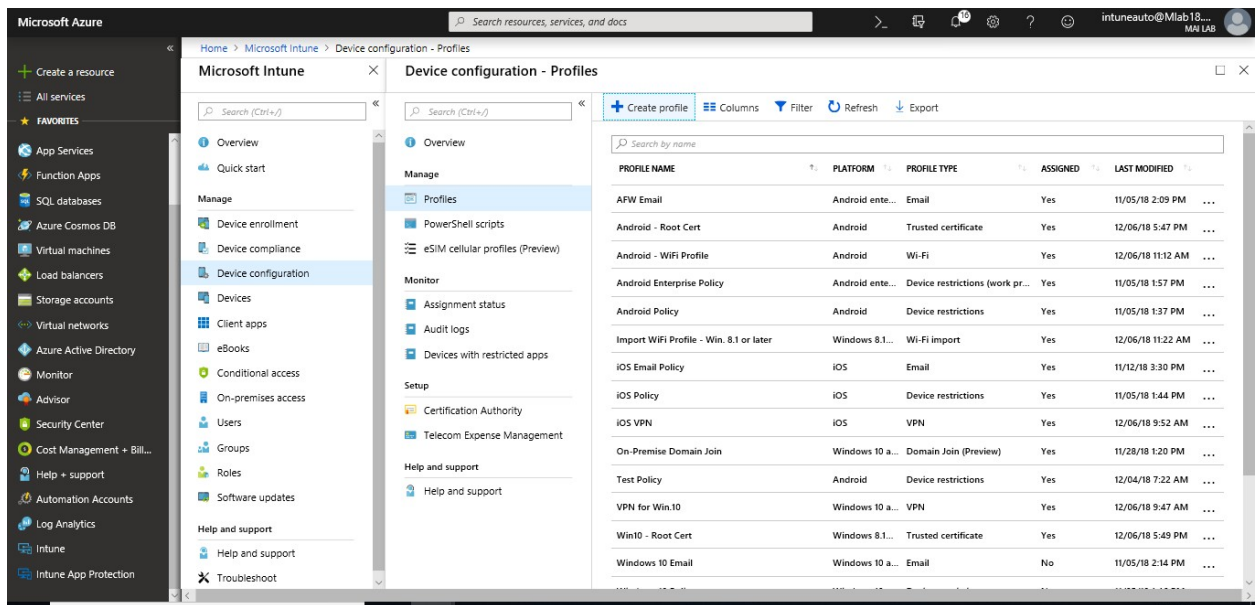
11. When you are done, select **Save**.



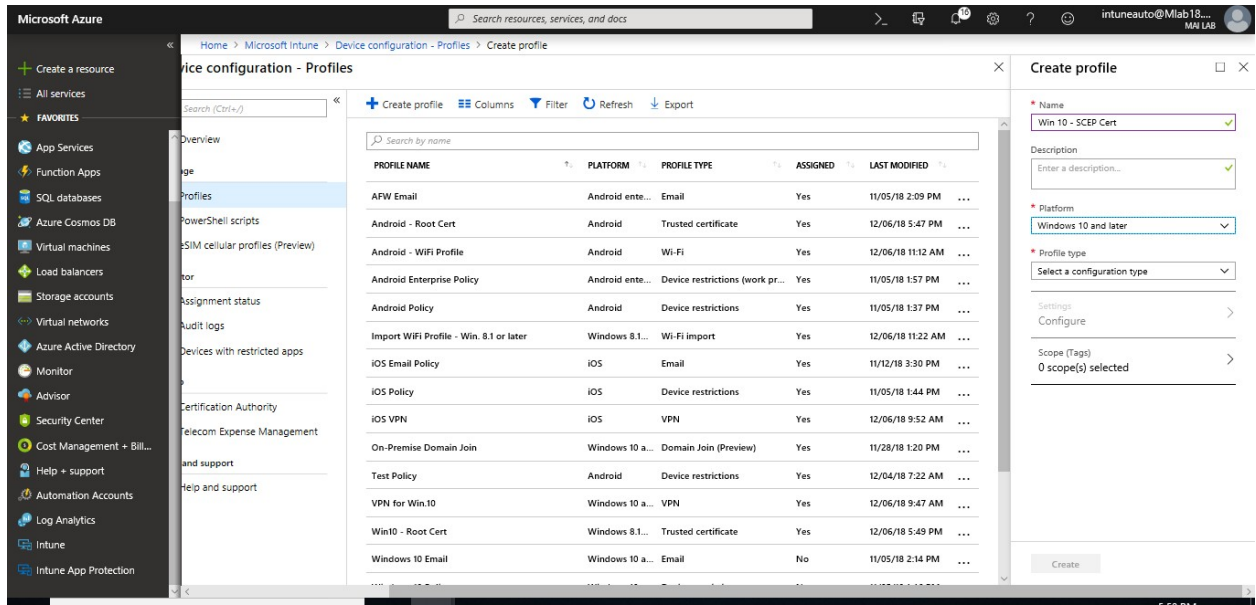
Step 3 - Create SCEP certificate profiles

To create a SCEP certificate profile, you need to follow below steps:

1. In the [Azure portal](#), select **All services**, filter on **Intune**, and select **Microsoft Intune**.
2. Select **Device configuration > Profiles > Create profile**.



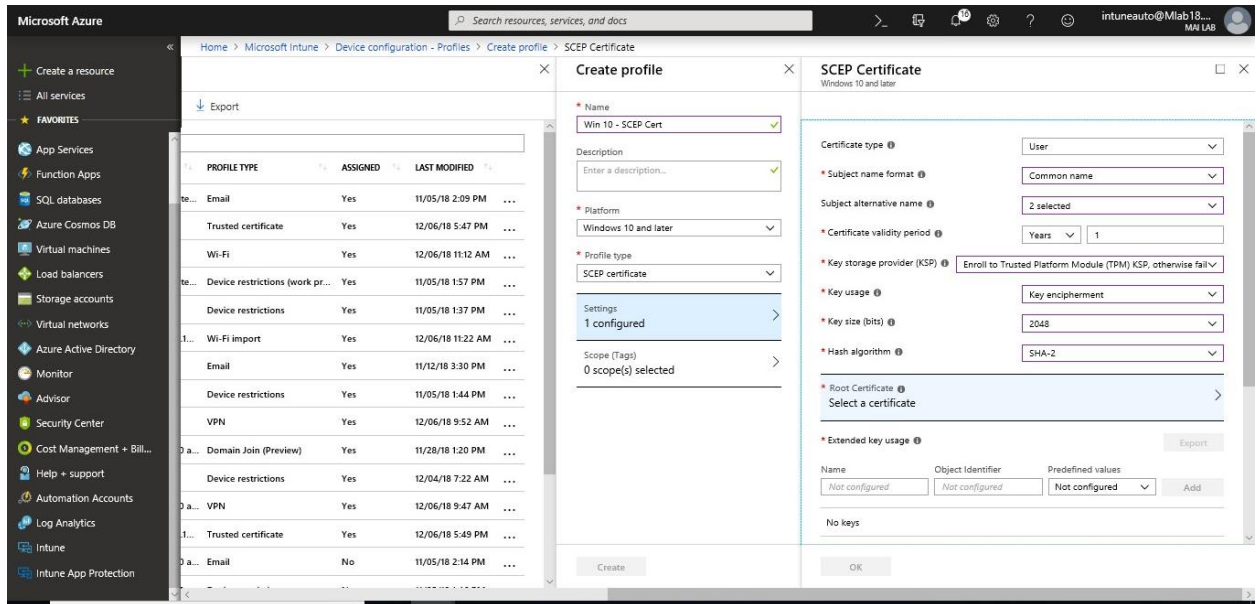
3. Enter a **Name** and **Description** for the SCEP certificate profile.
4. From the **Platform** drop-down list, select the device platform for this SCEP certificate. Currently, you can select one of the following platforms for device restriction settings:
Windows 10 and later
5. From the **Profile type** drop-down list, select **SCEP certificate**.



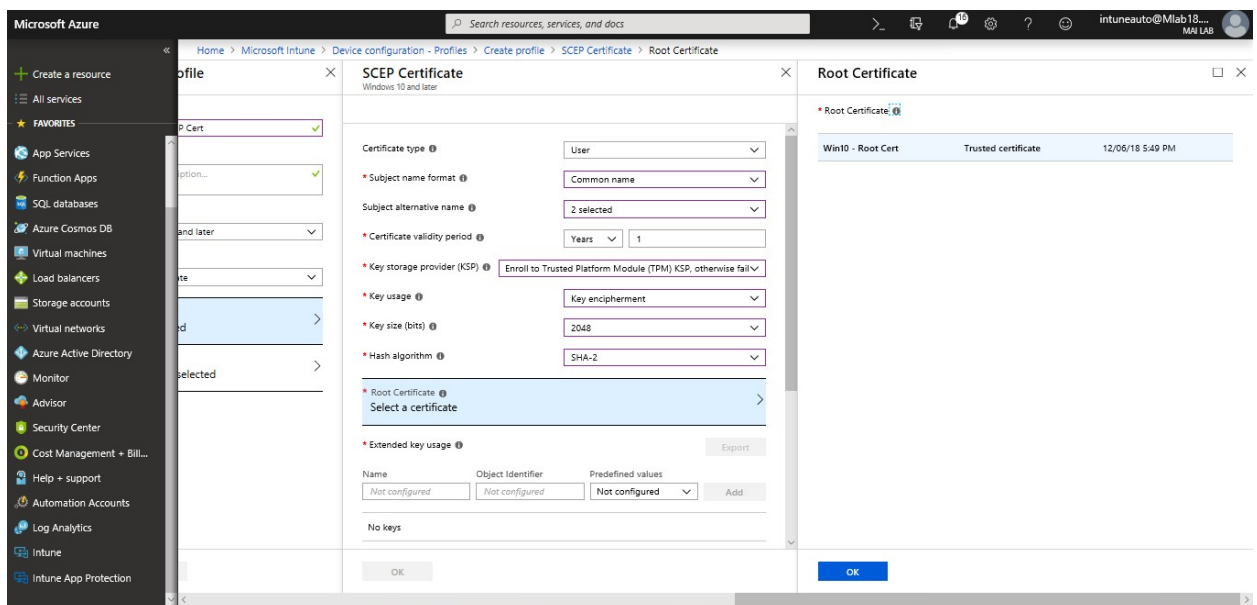
Note: The Trusted CA can be created to **Android, Android Enterprise, iOS, macOS, Windows Phone 8.1, Windows 8.1 and later.**

6. Enter the following settings:
 - a. **Certificate type:** Choose **User** for user certificates. Choose **Device** for user-less devices, such as kiosks. **Device** certificates are available for the following platforms:
 - i. iOS
 - ii. Windows 8.1 and later
 - iii. Windows 10 and later
 - iv. Android Enterprise
 - b. **Subject name format:** Select how Intune automatically creates the subject name in the certificate request. The options change if you choose a **User** certificate type or **Device** certificate type.
 - c. **Subject alternative name:** Enter how Intune automatically creates the values for the subject alternative name (SAN) in the certificate request. The options change if you choose a **User** certificate type or **Device** certificate type.
 - d. **Key storage provider (KSP)** (Windows Phone 8.1, Windows 8.1, Windows 10): Enter where the key to the certificate is stored. Choose from one of the following values:
 - i. Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software KSP
 - ii. Enroll to Trusted Platform Module (TPM) KSP, otherwise fail
 - iii. Enroll to Passport, otherwise fail (Windows 10 and later)
 - iv. Enroll to Software KSP
 - e. **Key usage:** Enter the key usage options for the certificate. Your options:
 - i. **Key encipherment:** Allow key exchange only when the key is encrypted

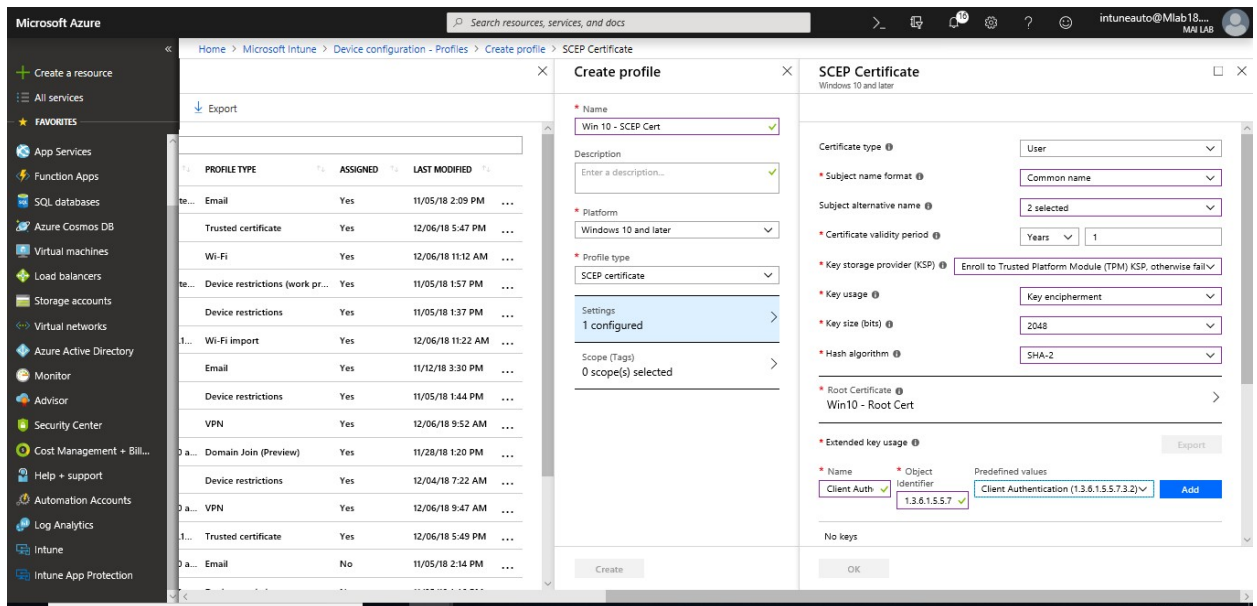
- ii. **Digital signature:** Allow key exchange only when a digital signature helps protect the key
- f. **Key size (bits):** Select the number of bits contained in the key
- g. **Hash algorithm** (Android, Windows Phone 8.1, Windows 8.1, Windows 10):
Select one of the available hash algorithm types to use with this certificate. Select the strongest level of security that the connecting devices support.



- h. **Root Certificate:** Choose a root CA certificate profile you previously configured and assigned to the user and/or device. This CA certificate must be the root certificate for the CA that issues the certificate that you are configuring in this certificate profile. Be sure to assign this trusted root certificate profile to the same group assigned in the SCEP certificate profile.

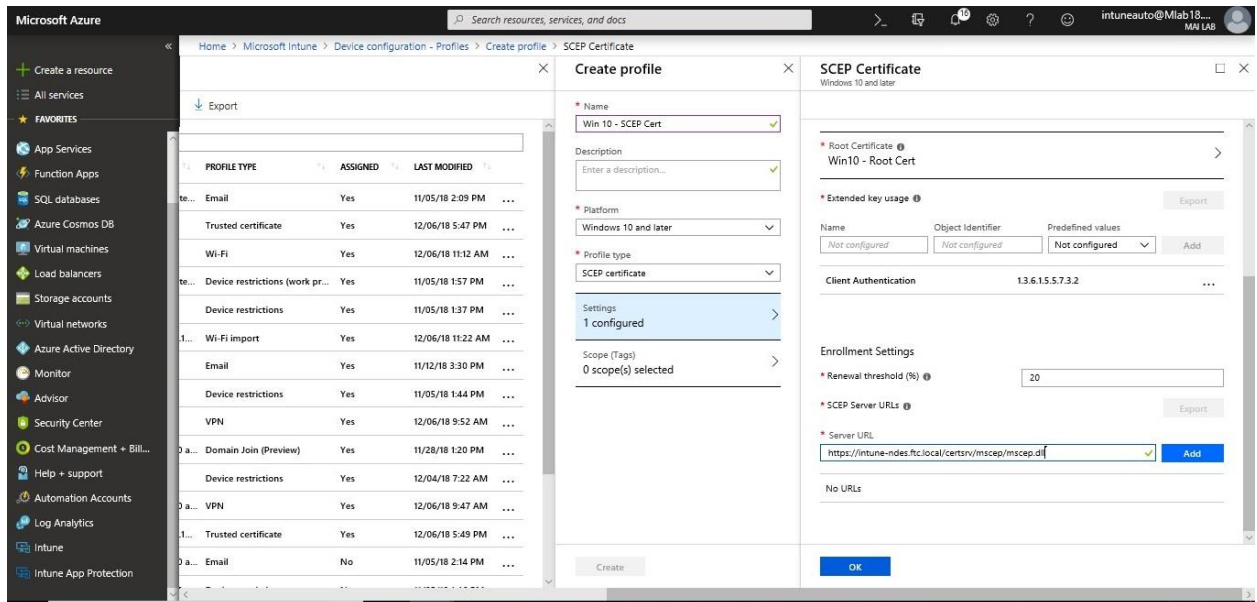


- i. **Extended key usage:** Add values for the certificate's intended purpose. In most cases, the certificate requires **Client Authentication** so that the user or device can authenticate to a server. However, you can add any other key usages as required.



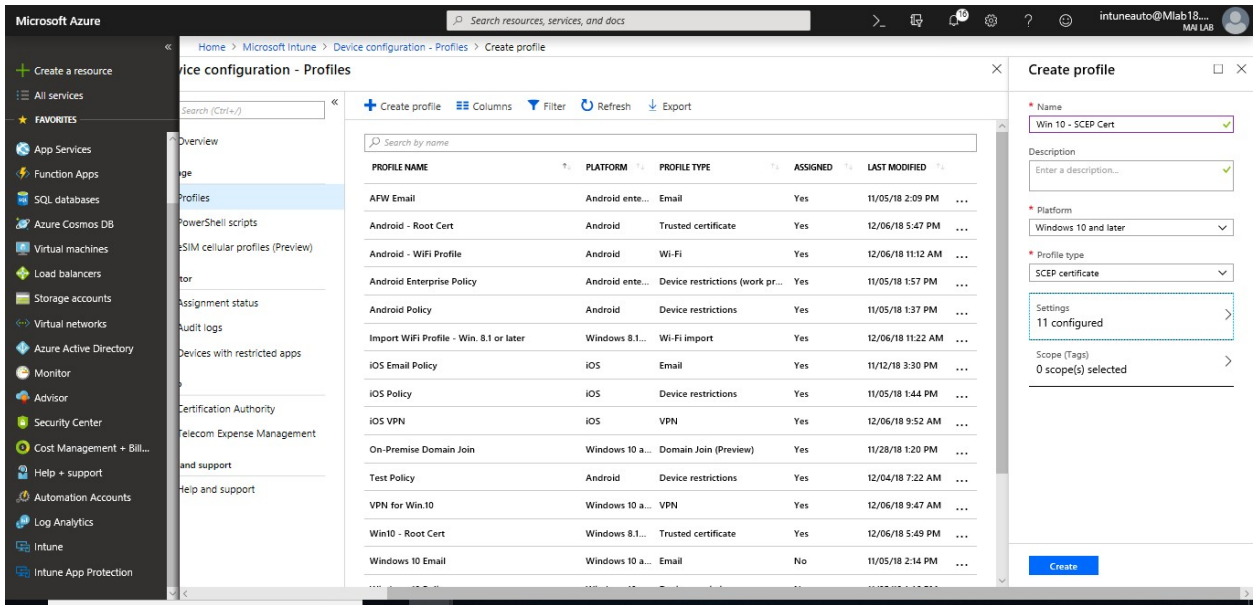
j. **Enrollment Settings**

- i. **Renewal threshold (%):** Enter the percentage of the certificate lifetime that remains before the device requests renewal of the certificate.
- ii. **SCEP Server URLs:** Enter one or more URLs for the NDES Servers that issue certificates via SCEP. For example, enter something similar to <https://ndes.contoso.com/certsrv/mscep/mscep.dll>.

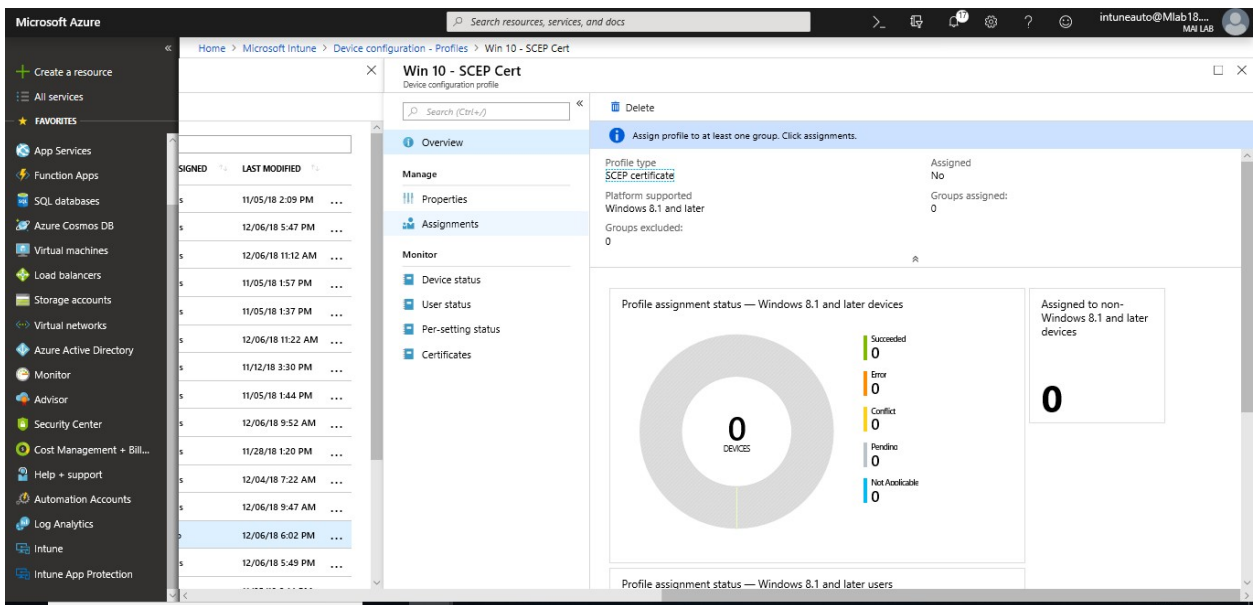


7. Select **OK** and **Create** your profile.

Microsoft Intune step by step on Azure portal

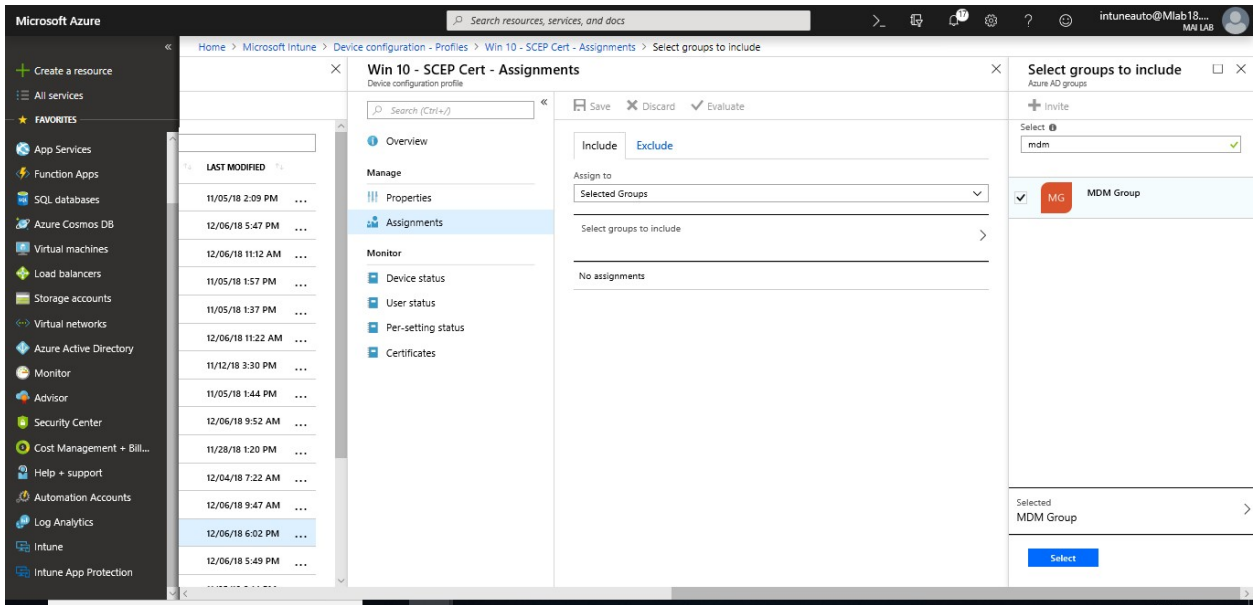


8. In the list of profiles, select the profile you want to assign, and then select **Assignments**.

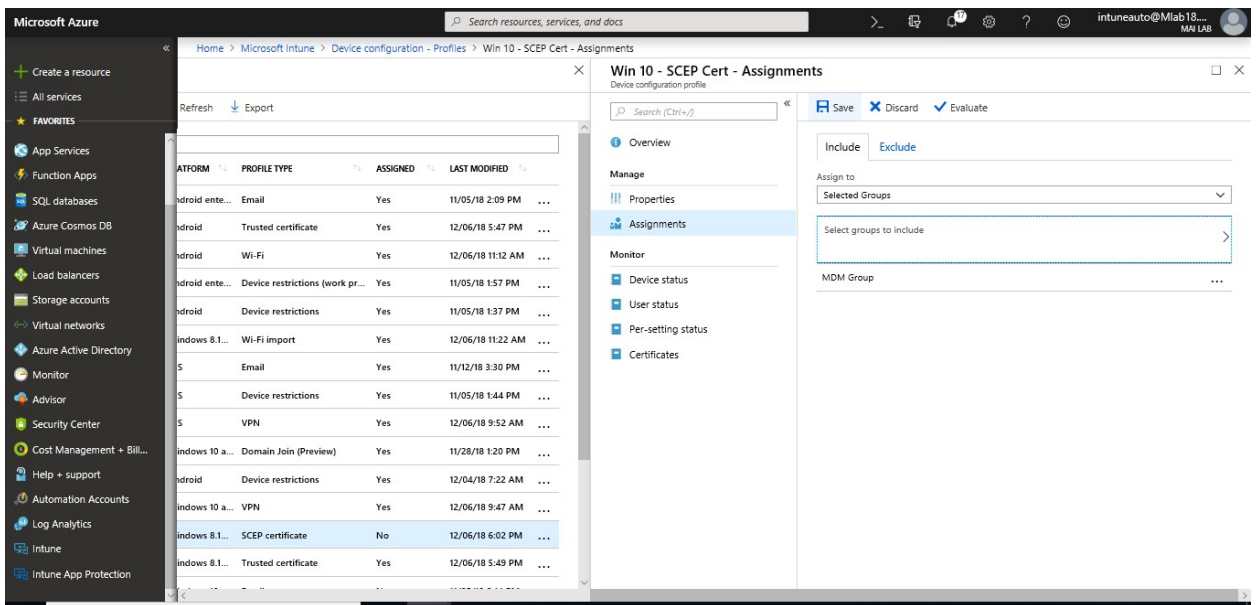


9. Choose to **Include** groups or **Exclude** groups, and then select groups.

Microsoft Intune step by step on Azure portal



10. When you are done, select **Save**.

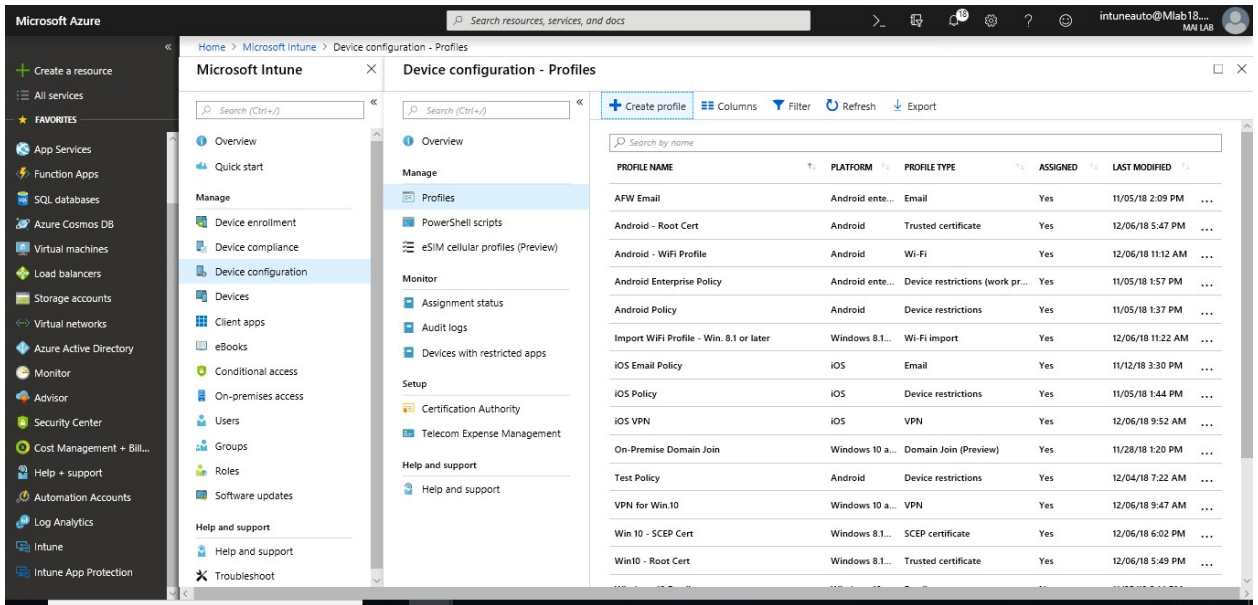


Step 4 - Create PKCS certificate profiles

PKCS Certificate don't need NDES server. It needs Intune Certificate connector & ADCS with an Enterprise Certification Authority (CA), not a Standalone CA. To create PKCS certificate profile, you need to follow below steps:

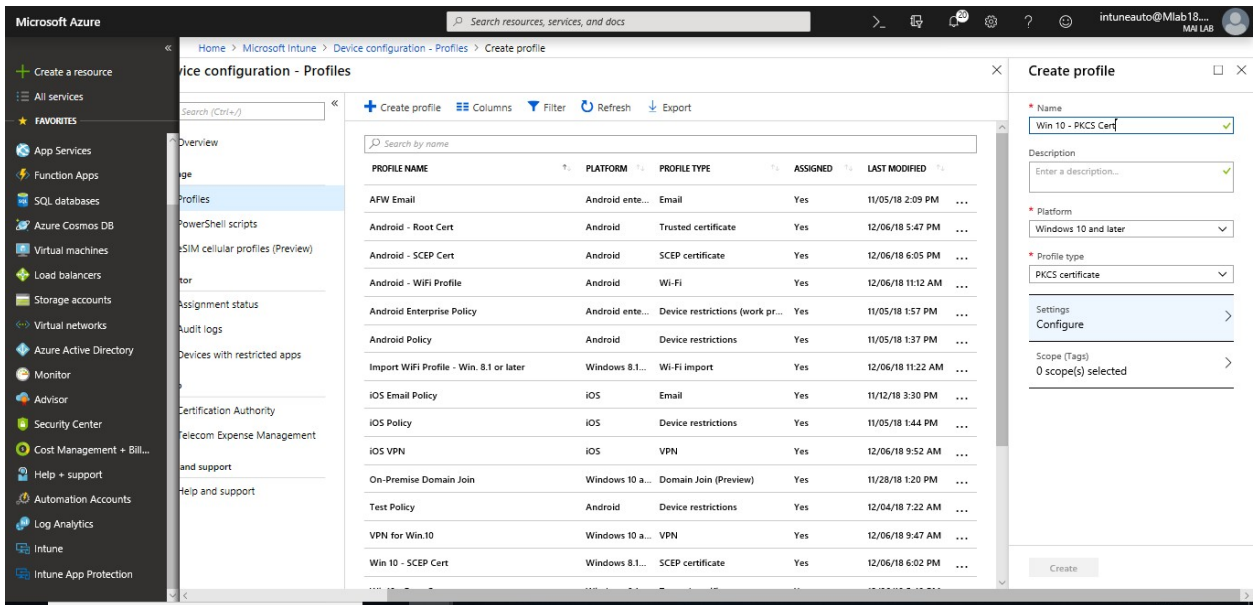
1. In the [Azure portal](#), go to **Intune > Device configuration > Profiles > Create profile**.

Microsoft Intune step by step on Azure portal



2. Enter the following properties:

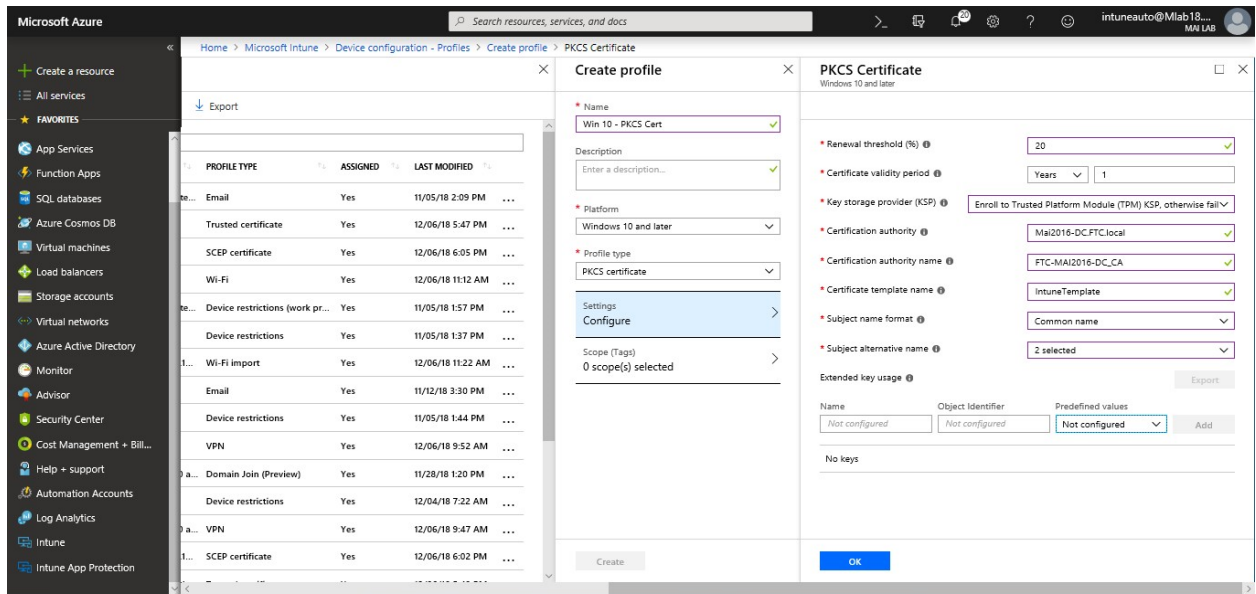
- **Name** for the profile
- Optionally set a description
- **Platform** to deploy the profile to
- Set **Profile type** to **PKCS certificate**



Note: The PKCS certificated can be created for **Android, Android Enterprise for work profile, iOS & windows 10 and later.**

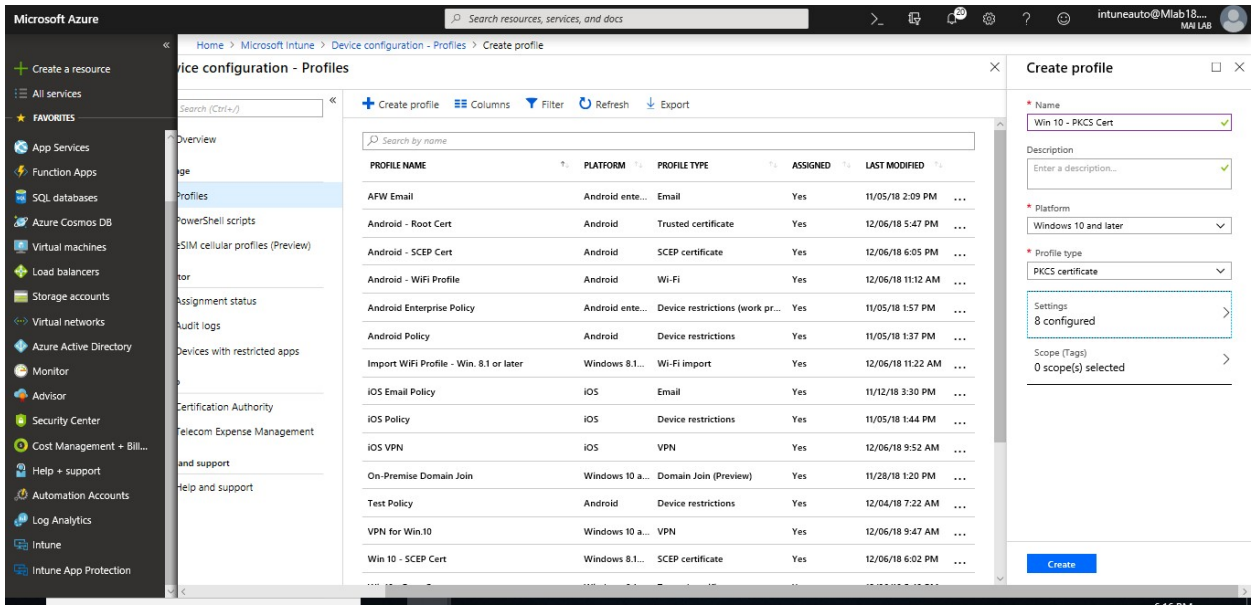
3. Go to **Settings**, and enter the following properties:

- **Renewal threshold (%):** Recommended is 20%.
- **Certificate validity period:** If you didn't change the certificate template, this option may be set to one year.
- **Key storage provider (KSP):** For Windows, select where to store the keys on the device.
- **Certification authority:** Displays the internal fully qualified domain name (FQDN) of your Enterprise CA.
- **Certification authority name:** Lists the name of your Enterprise CA, such as "Contoso Certification Authority".
- **Certificate template name:** The name of the template created earlier. Remember **Template name** by default is the same as **Template display name** with *no spaces*.
- **Subject name format:** Set this option to **Common name** unless otherwise required.
- **Subject alternative name:** Set this option to **User principal name (UPN)** unless otherwise required.



4. Select **OK > Create** to save your profile.

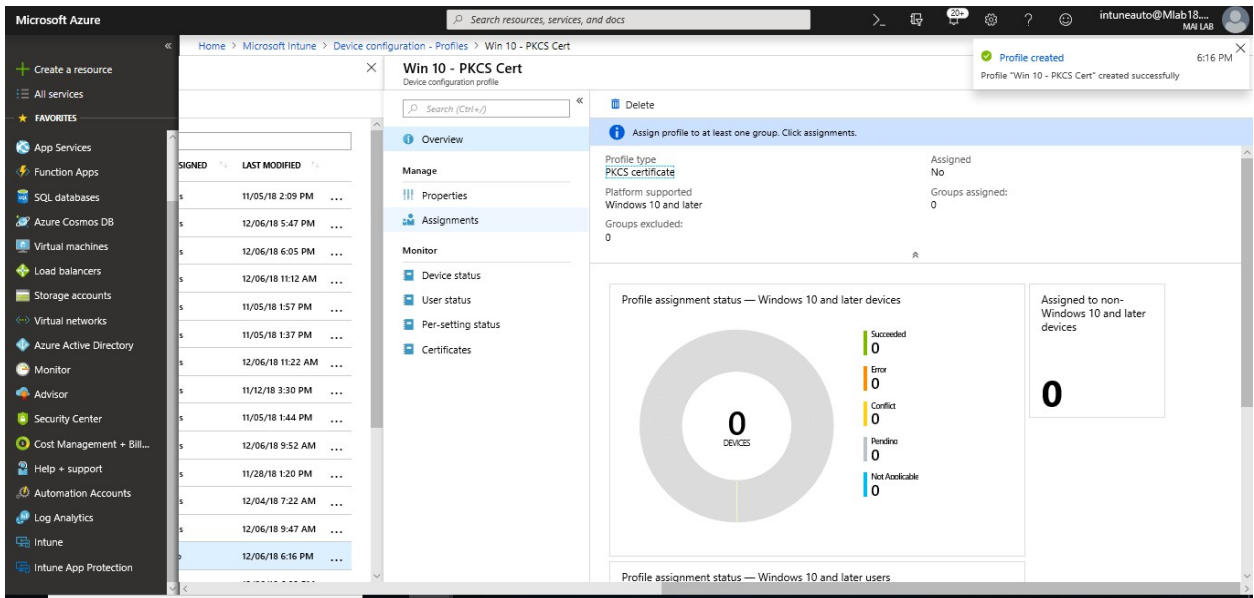
Microsoft Intune step by step on Azure portal



The screenshot shows the Microsoft Azure portal interface. The main content area displays a table of device configuration profiles. The 'Win 10 - PKCS Cert' profile is highlighted. The 'Create profile' dialog is open on the right, showing the profile name, description, platform, and profile type. The 'Assignments' tab is selected, showing a list of profiles and their details.

PROFILE NAME	PLATFORM	PROFILE TYPE	ASSIGNED	LAST MODIFIED
AFW Email	Android ente...	Email	Yes	11/05/18 2:09 PM
Android - Root Cert	Android	Trusted certificate	Yes	12/06/18 5:47 PM
Android - SCEP Cert	Android	SCEP certificate	Yes	12/06/18 6:05 PM
Android - WiFi Profile	Android	Wi-Fi	Yes	12/06/18 11:12 AM
Android Enterprise Policy	Android ente...	Device restrictions (work pr...	Yes	11/05/18 1:57 PM
Android Policy	Android	Device restrictions	Yes	11/05/18 1:37 PM
Import WiFi Profile - Win. 8.1 or later	Windows 8.1...	Wi-Fi import	Yes	12/06/18 11:22 AM
iOS Email Policy	iOS	Email	Yes	11/12/18 3:30 PM
iOS Policy	iOS	Device restrictions	Yes	11/05/18 1:44 PM
iOS VPN	iOS	VPN	Yes	12/06/18 9:52 AM
On-Premise Domain Join	Windows 10 a...	Domain Join (Preview)	Yes	11/28/18 1:20 PM
Test Policy	Android	Device restrictions	Yes	12/04/18 7:22 AM
VPN for Win10	Windows 10 a...	VPN	Yes	12/06/18 9:47 AM
Win 10 - SCEP Cert	Windows 8.1...	SCEP certificate	Yes	12/06/18 6:02 PM

5. In the list of profiles, select the profile you want to assign, and then select **Assignments**.



The screenshot shows the Microsoft Azure portal interface. The main content area displays the details for the 'Win 10 - PKCS Cert' profile. The 'Assignments' tab is selected, showing the profile type, platform supported, and groups assigned. A notification 'Profile created' is visible in the top right corner.

Profile type: PKCS certificate
Platform supported: Windows 10 and later
Groups assigned: 0
Groups excluded: 0

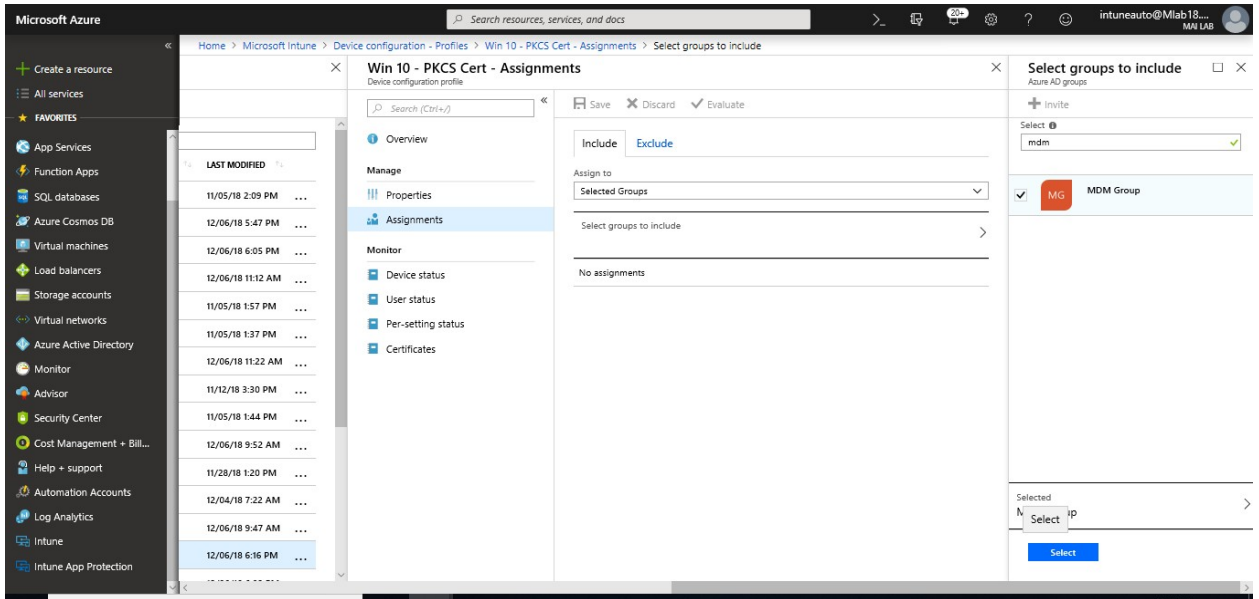
Profile assignment status — Windows 10 and later devices

Status	Count
Succeeded	0
Error	0
Conflict	0
Pending	0
Not Applicable	0

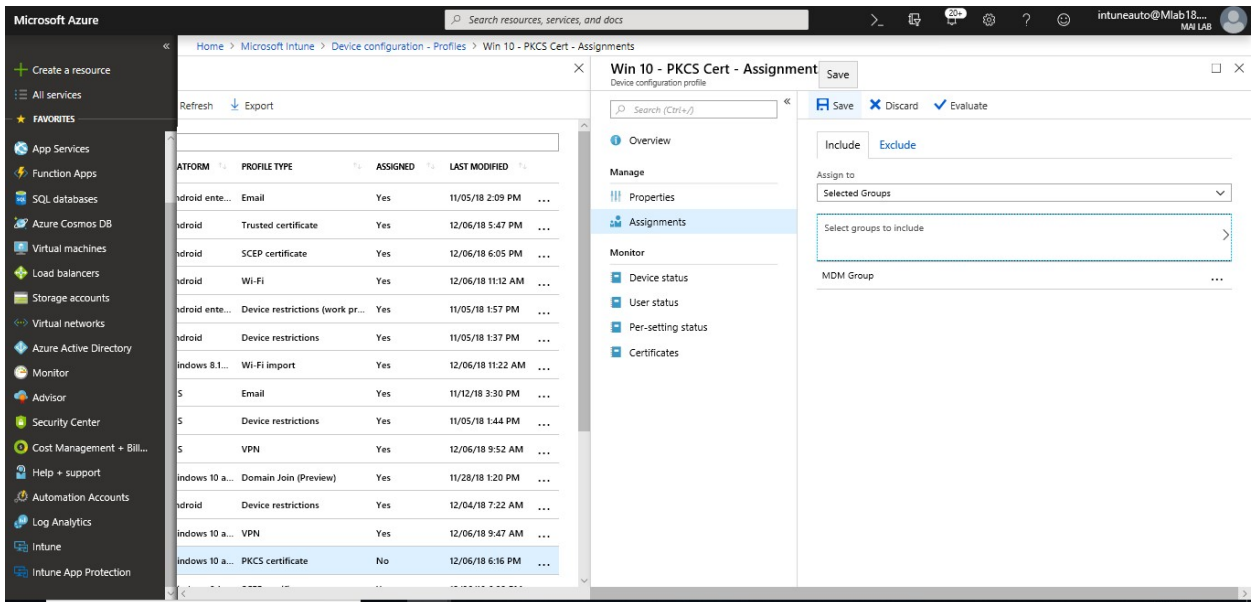
Assigned to non-Windows 10 and later devices: 0

6. Choose to **Include** groups or **Exclude** groups, and then select groups.

Microsoft Intune step by step on Azure portal



7. When you are done, select **Save**.

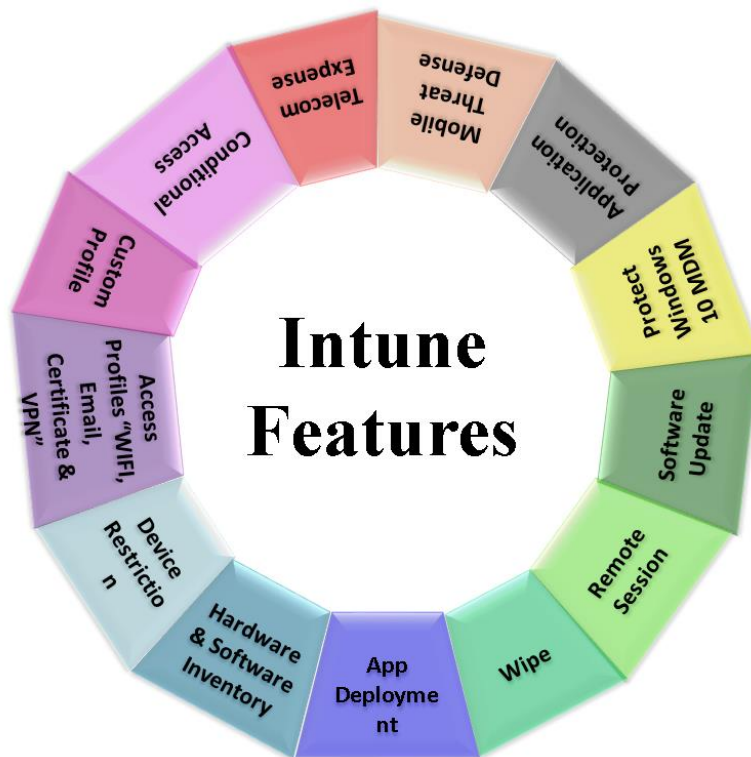


Chapter 12

Intune Scenarios & End User Actions

Intune Business Scenarios

Intune has many Features as we shown on previous chapters from Mobile Device Management, Mobile application Management & Windows 10 MDM.



Compare between Intune MDM & Intune MAM Without Enrollment

	Mobile Device Management (MDM)	Mobile Application Management Without Enrollment (MAM WE)
Purpose	<ul style="list-style-type: none"> Protecting the entire device Defining a security boundary at the device level 	<ul style="list-style-type: none"> Protecting only the corporate apps ad data Defining a security boundary at the app level
Need to enroll Mobile Device	Yes	No Note: For Android, you will need to install company portal without sign in & for iOS the Microsoft Authenticator app is required

	Mobile Device Management (MDM)	Mobile Application Management Without Enrollment (MAM WE)
Features	<ul style="list-style-type: none"> ▪ Hardware and Software inventory ▪ Application deployment ▪ Device-wide policies ▪ Full and selective wipe ▪ Access profiles (certificates, wireless network, email, virtual private network (VPN) profiles) ▪ Plus, all Features for MAM Policy 	<ul style="list-style-type: none"> ▪ App launch requirements (personal identification number (PIN), authentication, encryption) ▪ Restrict Cut/Copy/Paste ▪ Restrict Save/Save As location ▪ Identify corporate versus personal data ▪ Selective wipe of managed data ▪ Reporting for Protected App per User.
Use with other MDM Solution like Air watch or XenMobile	No, you need to unenroll mobile from another MDM Solution to be able to enrol with Intune.	Yes, because it only applies policy on Managed Application not on device.

Secure Corporate Data & Device

Business Scenario: Customers have many mobile devices within the corporate environment, but no efficient way to manage and secure those devices – devices may be corporately owned, or may be employee owned, but used for work purposes.

Solution: Apply MDM for Mobile Devices.

- Push applications.
- Enforce all Mobile devices to be compliance to access corporate data.
- Put restriction policy on Mobile devices.
- Push Access profiles (certificates, wireless network, email, virtual private network (VPN) profiles)
- Put restriction policy on managed application.
- Hardware and Software inventory.
- Full and selective wipe.

Business Results

- Improved productivity.
- Empowering users with best-in-class productivity across devices while providing IT security and control.
- Secure platform that meets rigorous compliance needs.

Secure Corporate Data on Employee’s personal device “Bring your Own Device”

Business Scenario: Customers have many mobile devices within the corporate environment, but no efficient way to manage and secure Corporate data – End User own his device.

Solution: Apply MAM WE for personal Mobile devices.

- Put restriction Policy to save only OneDrive & SPO.
- App launch requirements (personal identification number (PIN), authentication, encryption)
- Restrict Cut/Copy/Paste.
- Encrypt App Data.
- Put restriction on managed browser by using App configuration policy.
- Enforce end user to use managed app.
- Selective wipe of managed App (Corporate Data).

Business Results

- Keep users productive on all devices.
- Secure access to corporate applications.

Secure Windows PCs as MDM

Business Scenario: Customer want to deploy Office ProPlus 365 and doesn't have a clear view of their current PC update status and may not have an efficient way to deploy Office applications. Also, Customer has team who are using laptop from anywhere and want to secure access to corporate data from these devices and provide any assistance remotely if end user need.

Solution: Manage Windows 10 PCs using MDM

- Put restriction Policy to devices.
- Push .exe application & OPP.
- Push PowerShell Script.
- Manage Software update using Windows 10 update rings.
- Push Access profiles (certificates, wireless network, email, virtual private network (VPN) profiles).
- Enforce device to be compliance to access corporate data.
- Apply Windows Information Protection.
- Protect Windows 10 MDM using Windows defender, Identity Protection & windows security Baselines.
- Allow Remote access to PC.
- Wipe Device & remove data.

Note: In the case, customer is using **Configuration Manager**, he will need to configure **Co-management** to be able to manage device using Intune & SCCM at the same time and offload some workloads to Intune like resource access profiles or add feature like block non-compliance device from access corporate data.

Business Results

- Improve Productivity.
- Reduce IT effort.
- Secure Corporate Device & Data.

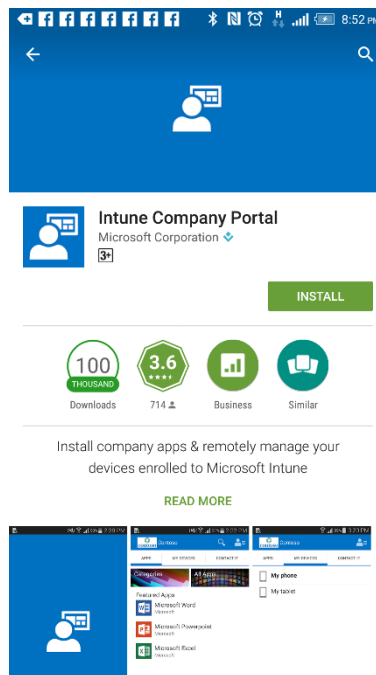
Enroll Mobile Devices Using Microsoft Intune

For Android

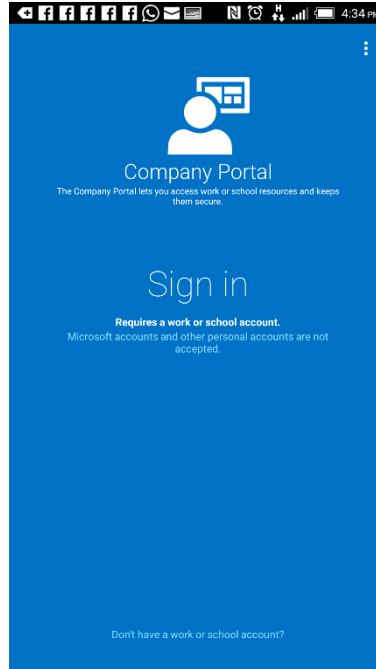
Android mobile devices allow users to enroll using the Company Portal app available from Google Play.

Enroll Android devices in Intune

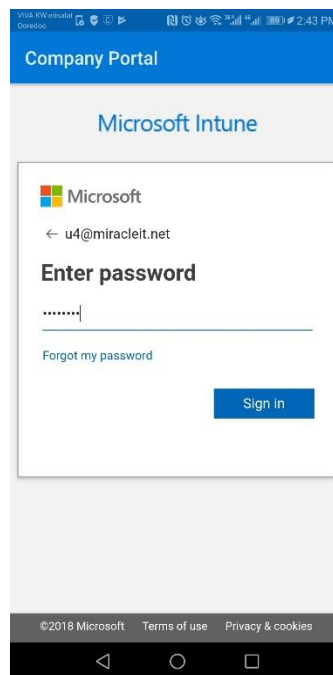
1. On your Android device, open the **Play Store** and search for Intune, open the **Intune Company Portal** app and click on **Install**, then accept the permissions



2. Open the Intune Company Portal app and click on **Sign in**



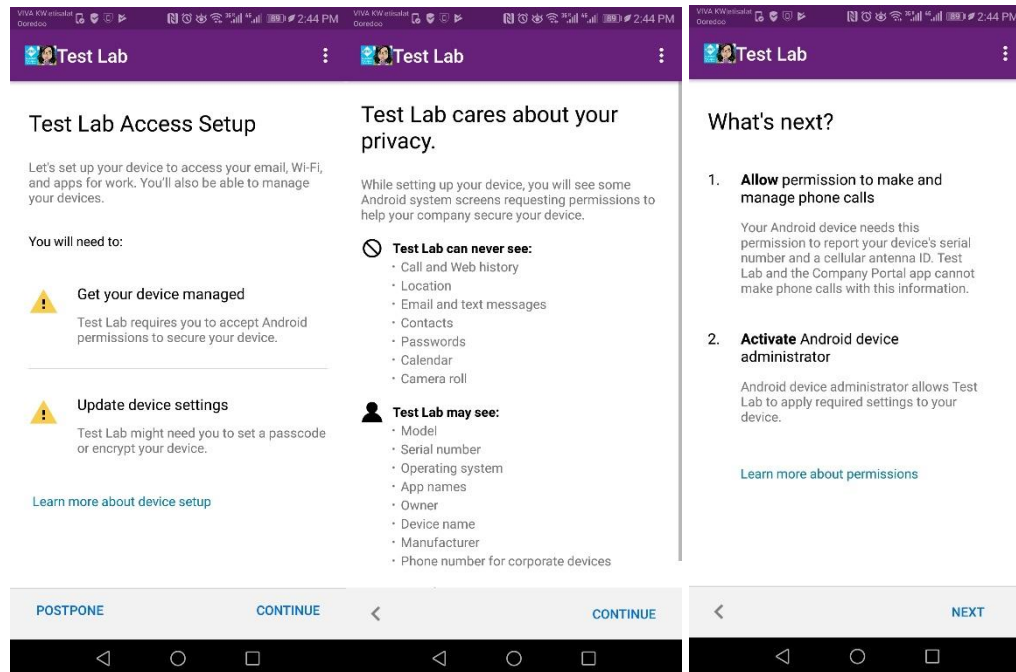
3. Type your user name and password



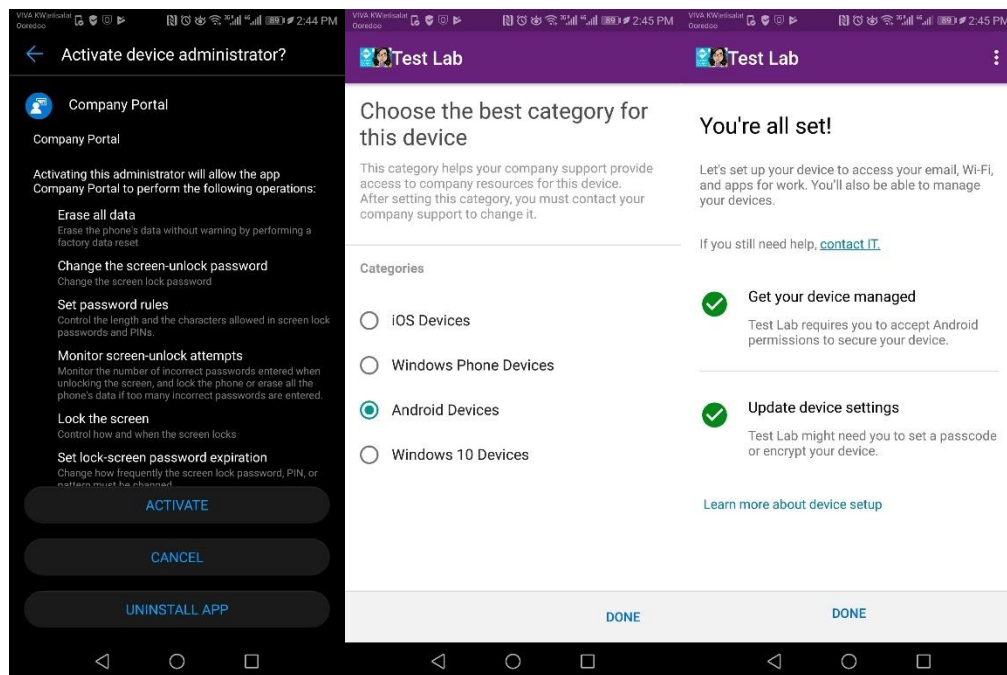
4. Click on **Sign in**, then click on **Continue** and then on **Next**.

Note: Depending on the policies defined in Intune, you will receive prompts to setup password and/or encrypt your device. Follow the prompts to make the device compliant.

Microsoft Intune step by step on Azure portal



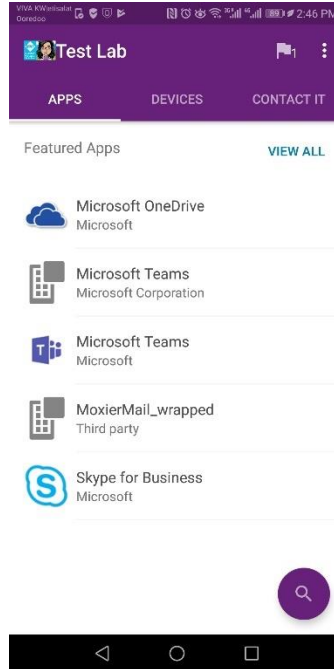
5. Click **Activate** & Then click **Done**.



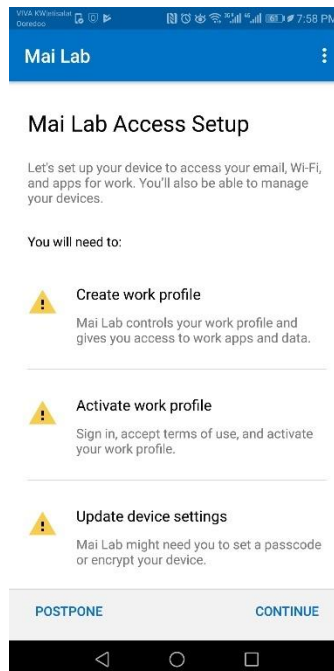
Note: If you already configure Device category, select device category to add device below it.

6. Now Mobile device is now Enrolled

Microsoft Intune step by step on Azure portal



Note: If you already add this user for enroll as Android Enterprise “Android for Work”, it will be same steps from end user for enrollment. Enroll Device as Android Enterprise will **encrypt** device during enrollment.

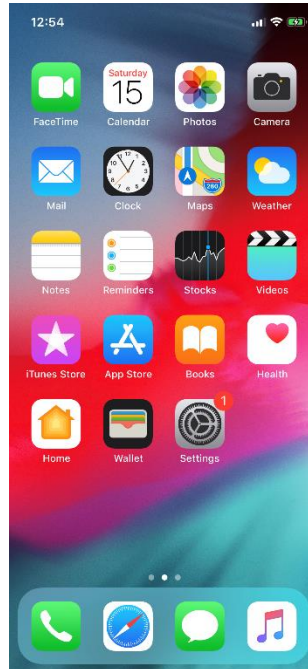


For iOS

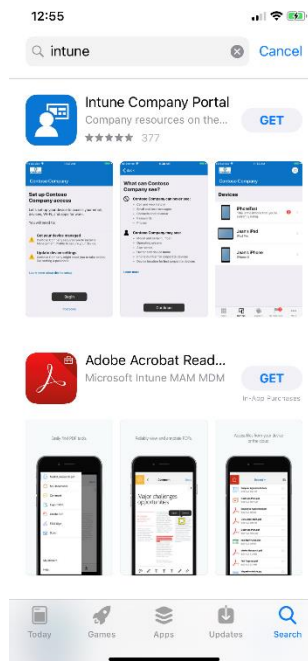
To enroll iOS Mobile Phone, you need to follow below steps

Microsoft Intune step by step on Azure portal

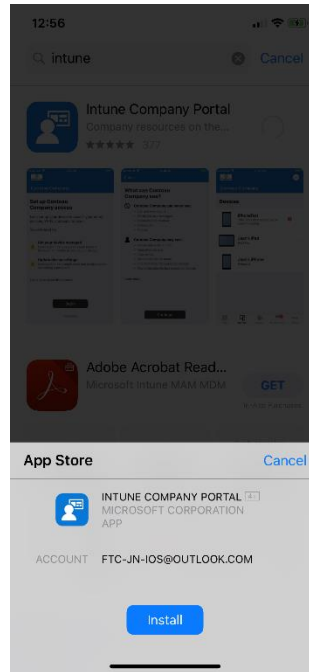
1. From the iOS device, open the **Apple Store app** and search for Intune



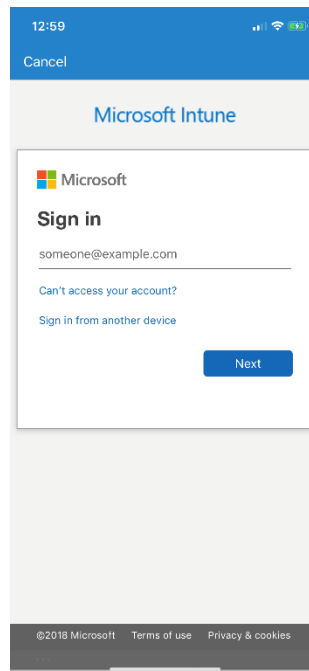
2. Open **Microsoft Intune Company Portal** app and click on **Get**



3. Click **Install**

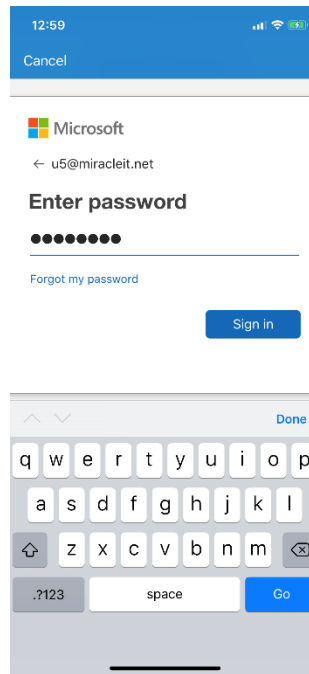


4. Open the app and type your user name and password

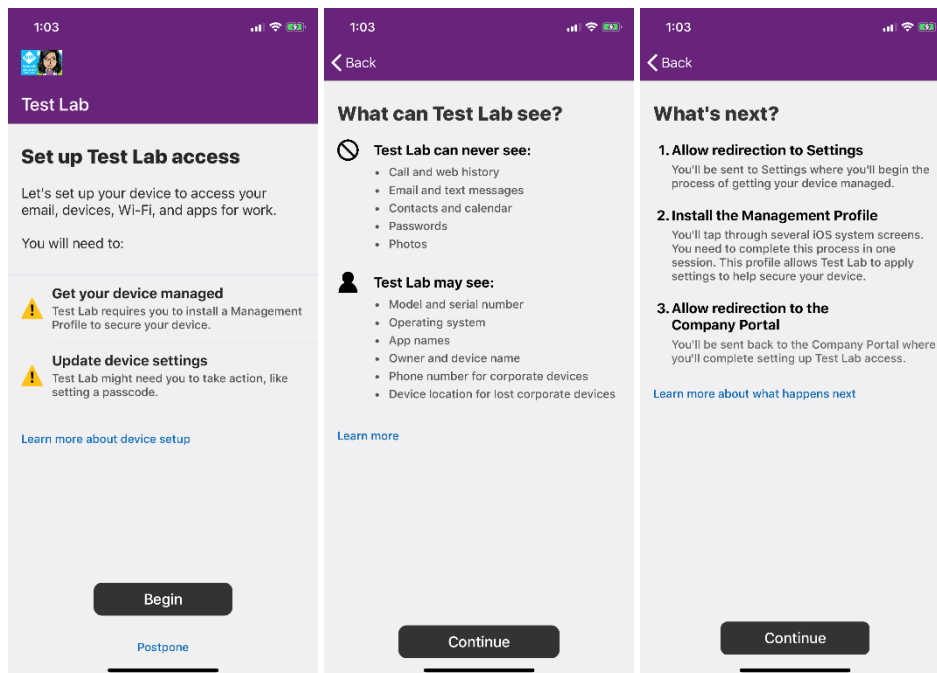


5. Click on **Sign in**

Microsoft Intune step by step on Azure portal

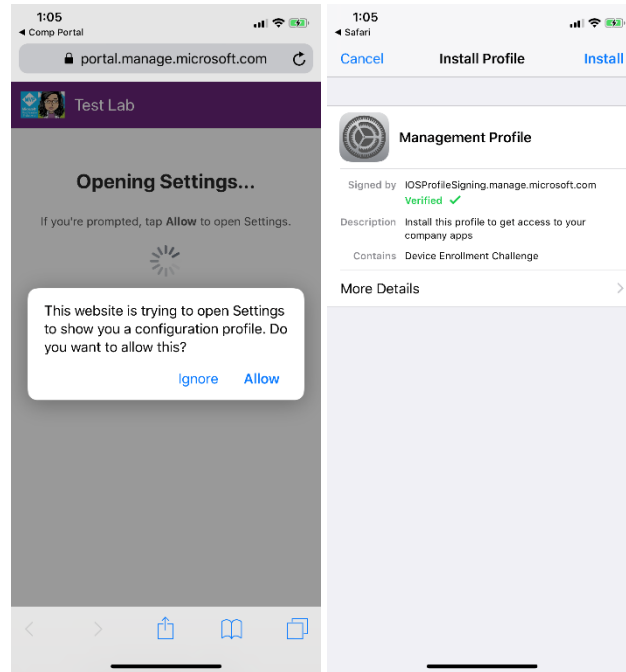


6. Wait for the process to complete
7. Read the rules and conditions Click on **Begin** > **Continue** > **Continue**

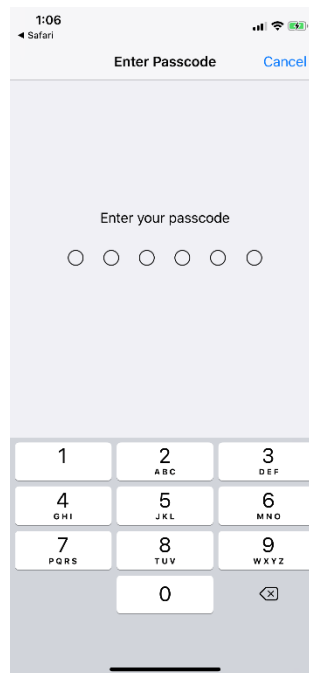


8. Click **Allow** Then Click on **Install**

Microsoft Intune step by step on Azure portal

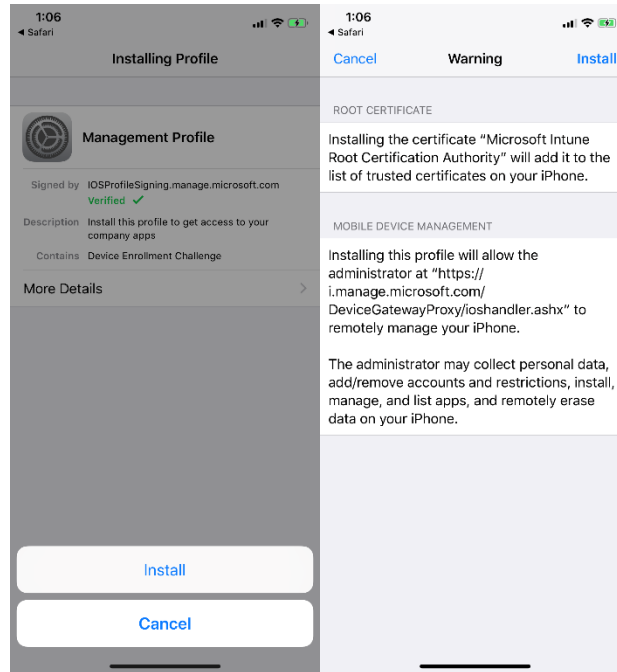


9. Enter Passcode

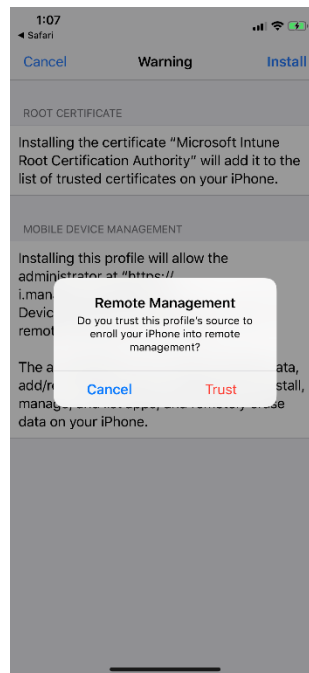


10. Click Install again

Microsoft Intune step by step on Azure portal

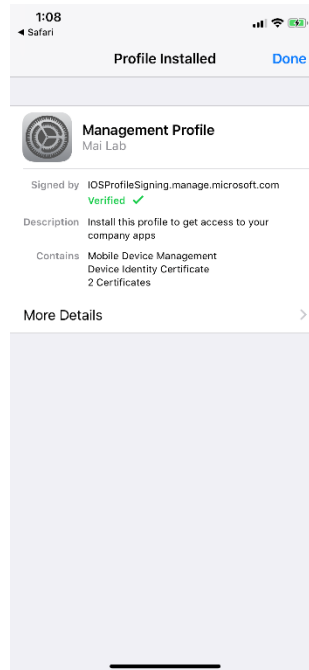


11. Click **Trust**

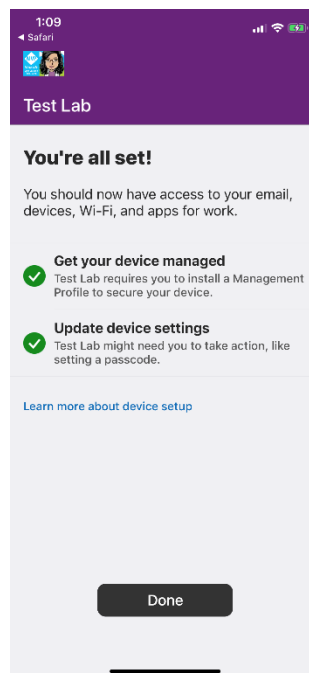


12. Click on Done

Microsoft Intune step by step on Azure portal



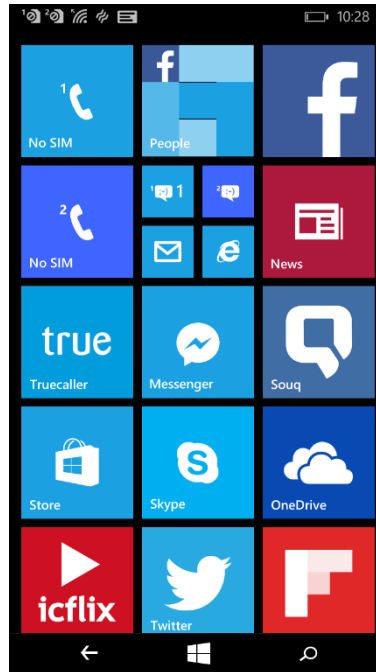
13. Click **Done**. Now Mobile device is enrolled.



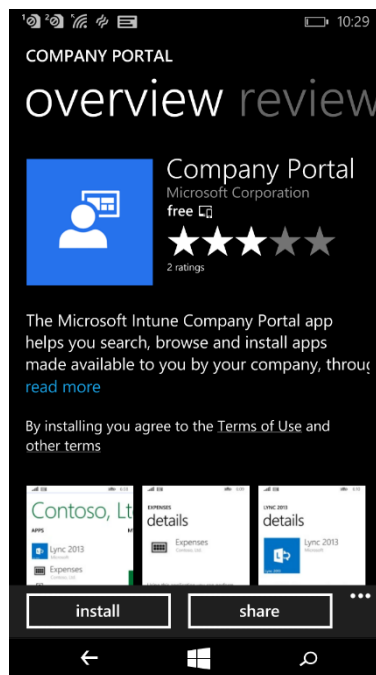
For Windows Phone

Follow these steps to enroll a Windows phone.

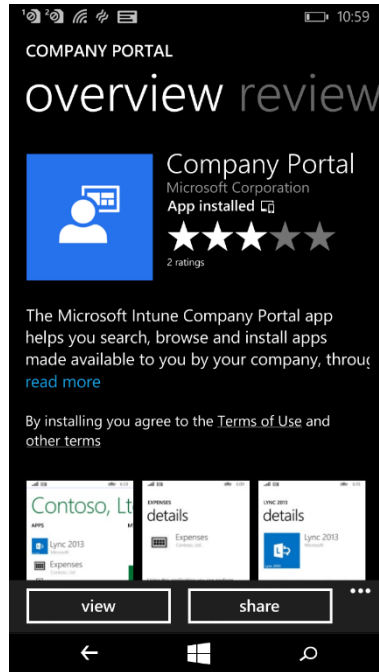
1. Click **Store** and search on Intune



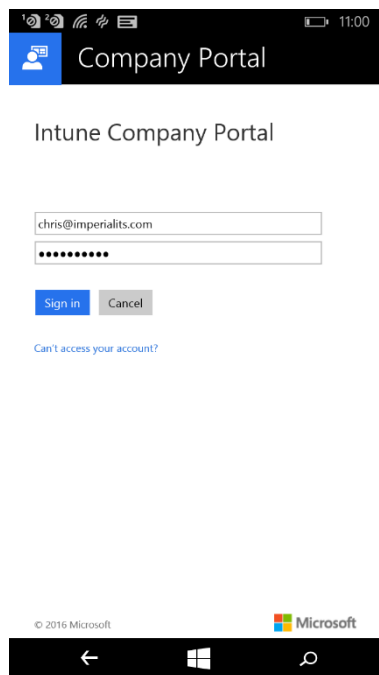
2. Click **Company Portal**



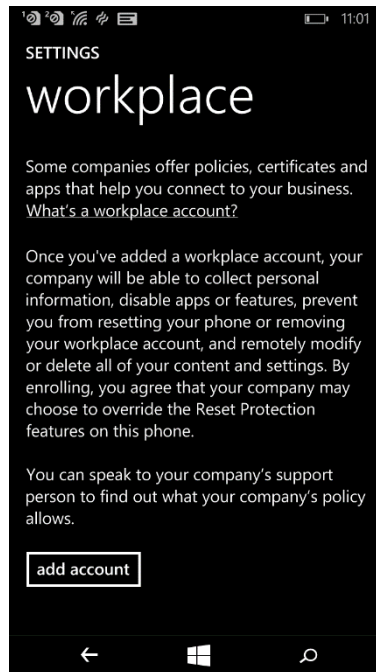
3. On Company Portal click **view**



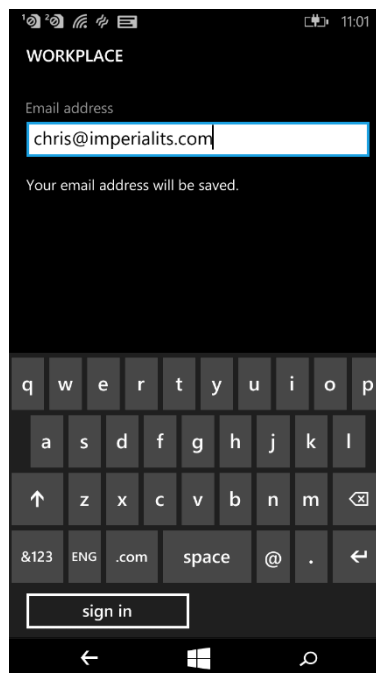
4. Type your Username and password then click sign in



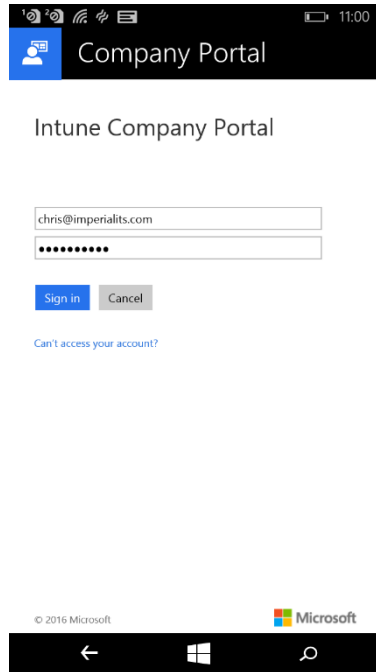
5. On the Windows phone, open **Settings** and click on **workplace**
6. Click on **add account**.



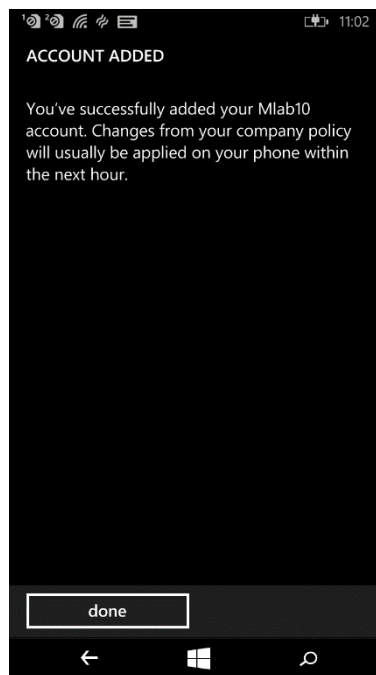
7. Type your user name and Click on **sign in**.



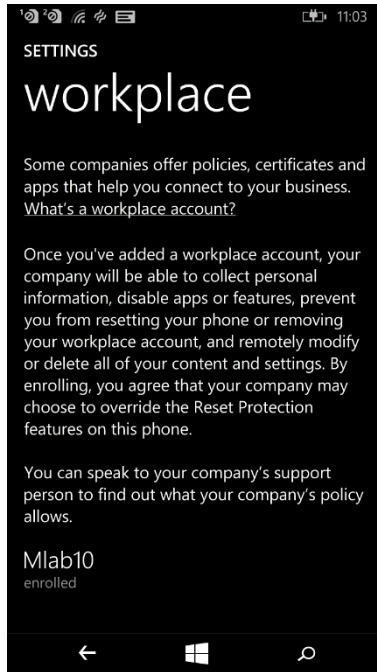
8. Type your Username and password then click **sign in**.



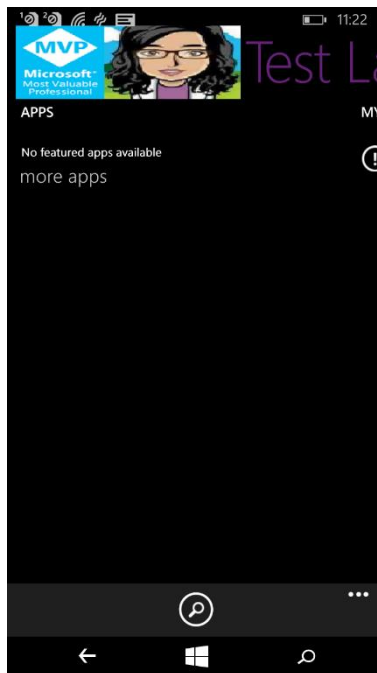
9. Account Added click **done**



10. Setting workplace is enrolled



11. Now Company portal is enrolled



APPENDIX

Firewall and Proxy Server Settings for MDM Devices

Those of you out there with firewalls may have run into issues with the Windows Intune clients having difficulty communicating with the service. The excerpt below provides detailed information on how to set up your firewall for a successful Intune Implementation.

If you want to use Intune to manage PCs that exist behind firewalls or proxy servers, you must configure the firewall or proxy server to allow Intune to communicate with the client computers.

Required Firewall Configuration

If the PCs exist behind a firewall, you must configure the firewall to allow communications with the Intune through the specified ports that are listed in the following tables.

Domain	Ports
portal.manage.microsoft.com	80 and 443
*.microsoftonline.com	80
m.manage.microsoft.com	80
www.microsoft.com	80
*.update.microsoft.com	80 and 443
download.microsoft.com	80 and 443
update.microsoft.com	80 and 443
*.manage.microsoft.com	80 and 443
*.spynet2.microsoft.com	443
manage.microsoft.com	80 and 443
wustat.microsoft.com	80 and 443
*.download.windowsupdate.com	80 and 443
*.windowsupdate.com	80 and 443
download.windowsupdate.com	80 and 443
ntservicepack.microsoft.com	80 and 443
windowsupdate.microsoft.com	80 and 443
enterpriseregistration.windows.net	80 and 443

Apple Device Network Information

Hostname	URL (IP address/subnet)	Protocol	Port	Device
Admin Console	gateway.push.apple.com (17.0.0.0/8)	TCP	2195	Apple iOS & macOS
Admin Console	feedback.push.apple.com(17.0.0.0/8)	TCP	2196	Apple iOS and macOS
Admin Console	Apple iTunesitunes.apple.com, *.mzstatic.com, *.phobos.apple.com, *.phobos.apple.com.edgesuite.net	HTTP	80	Apple iOS and macOS

Hostname	URL (IP address/subnet)	Protocol	Port	Device
PI Server	gateway.push.apple.com(17.0.0.0/8) feedback.push.apple.com(17.0.0.0/8)	TCP	2195, 2196	For Apple iOS and macOS cloud messaging.
Device Services	gateway.push.apple.com	TCP	2195	Apple
Device Services	feedback.push.apple.com	TCP	2196	Apple
Device Services	Apple iTunesitunes.apple.com *.mzstatic.com*.phobos.apple.com *.phobos.apple.com.edgesuite.net	HTTP	80	Apple
Devices (Internet/Wi-Fi)	#-courier.push.apple.com(17.0.0.0/8)	TCP	5223 and 443	Apple only. '#' is a random number from 0 to 200.
Devices (Internet/Wi-Fi)	phobos.apple.comocsp.apple.commax.itunes.a pple.com	HTTP/H TTPS	80 or 443	Apple only

Required Proxy Server Configuration

If the managed PCs exist behind proxy server, you must configure the proxy server as follows:

- Intune communicates with computers by using both the **HTTP and HTTPS** protocols. Confirm that the proxy server supports HTTP and HTTPS.
- Intune requires unauthenticated proxy server access to manage.microsoft.com for some tasks such as downloading software and updates.

You can modify proxy server settings on individual client computers, or you can use Group Policy to change settings for all client computers that exist behind a specified proxy server.

Authenticated proxy servers are not supported

Average Network Traffic

This table lists the approximate size and frequency of common content that travels across the network for each client.

Note: To ensure devices receive the updates and content from Intune, they must periodically connect to the Internet. The time required to receive updates or content can vary, but they should remain continuously connected to the Internet for at least one hour each day.

Content type	Approximate size	Frequency and details
Client enrollment package	15 MB	One time Additional downloads are possible when there are updates for this content type.
Daily client operations	6 MB	Daily The Intune client regularly communicates with the Intune service to check for updates and policies, and to report the client's status to the service.

Content type	Approximate size	Frequency and details
Endpoint Protection malware definition updates	Varies Typically 40 KB to 2 MB	Daily Up to three times a day.
Endpoint Protection engine update	5 MB	Monthly
Software updates	Varies The size depends on the updates you deploy.	Monthly Typically, software updates release on the second Tuesday of each month. A newly enrolled or deployed computer can use more network bandwidth while downloading the full set of previously released updates.
Software distribution	Varies The size depends on the software you deploy.	Varies Depends on when you deploy software.

Reduce Network Bandwidth Use

You can use **a proxy server to cache content requests** to reduce network bandwidth use for Intune clients.

A proxy server can cache content to reduce duplicate downloads and reduce network bandwidth from content from the Internet.

A caching proxy server that receives content requests from clients can retrieve that content and cache both web responses and downloads. The server uses cached data to answer subsequent requests from clients.

The following are typical settings to use for a proxy server that caches content for Intune clients.

Setting	Recommended value	Details
Cache size	5 GB to 30 GB	The value varies based on the number of client computers in your network and the configurations you use. To prevent files from being deleted too soon, adjust the size of the cache for your environment.
Individual cache file size	950 MB	This setting might not be available in all caching proxy servers.
Object types to cache	HTTP HTTPS BITS	Intune packages are CAB files retrieved by Background Intelligent Transfer Service (BITS) download over HTTP.

Note: When you plan to use Intune on Production, you will need to go through [planning guide](#) to put plan of configuring Intune on production & rollout service on phases after announce end user with the Intune for protect your corporate App. & Data.

Reference

TechNet Microsoft

- <https://www.microsoft.com/en-us/cloud-platform/microsoft-intune>
- <https://technet.microsoft.com/en-us/library/dn646960.aspx>
- <https://docs.microsoft.com/en-us/intune/index>
- <https://docs.microsoft.com/en-us/intune/planning-guide>
- <https://docs.microsoft.com/en-us/intune/setup-steps>

Other Articles

This eBook is part of a series of articles dedicated to Configuration and Troubleshooting System Center Family and Intune.

They are actually written and hosted on Mai Ali's Blog <http://expertslab.wordpress.com>

- How to Install Operation Manager 2012R2 using PowerShell
- Troubleshooting the Installation of the System Center Operations Manager Agent
- SQL Server cannot authenticate using Kerberos because the Service Principal Name (SPN) is missing, misplaced, or duplicated
- Removing Bulk Management Packs using PowerShell
- Enable Proxy Agent for all SCOM Agents
- Error Configure Portal web site during Install SCSM