



**INTUNE**  
**Powershell**  
**Runbook: M365**  
**Business Edition**

## Guide Description

*The purpose of this guide is to provide a powershell runbook for implementing Intune. This guide is assuming you have the **M365 Business** License. It can apply to EMS licenses, but some features will not be covered such as Conditional Access and Windows Autopilot. After you run this powershell script you will have created:*

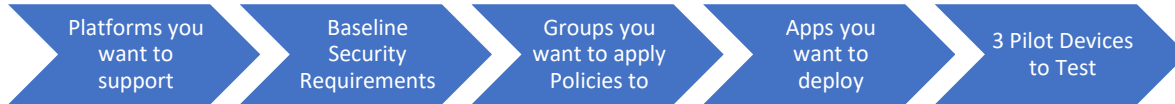
1. *A device compliance policy for:*
  - a. *iOS*
  - b. *Android*
  - c. *Windows*
2. *A device configuration policy for Windows Devices to have BitLocker*
3. *Terms and Conditions for when users enroll*
4. *Office 365 Business pushed out as a required App to window 10 devices and uninstall existing versions of proplus*
5. *Microsoft Authenticator pushed out as a required App for iOS and Android devices*

**\*\*Disclaimer\*\***

This guide is meant to provide best practices for policy creation and implementation of Intune. It is meant to be used as a template, but the policies defined will not be the same in all use cases. You must access to policies and configuration you will need for your customers environment and make changes as needed. As a best practice, test all configurations with a pilot group before moving to broad deployment across an entire organization

---

## Pre-Flight Checklist

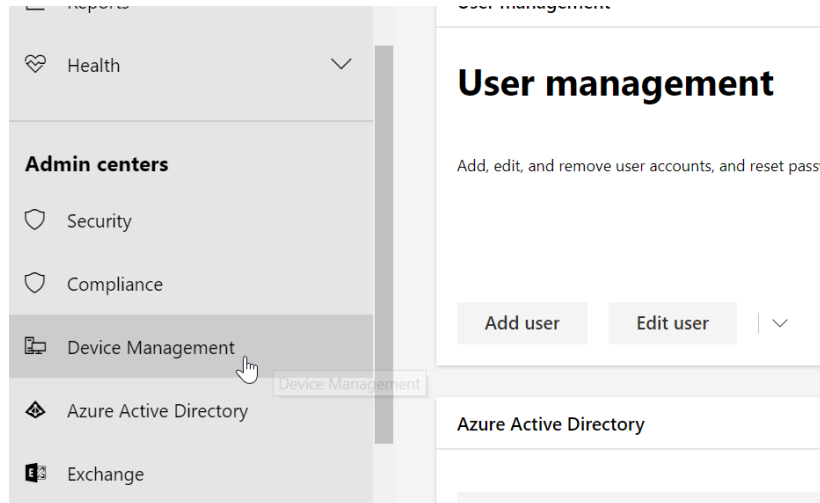


- a. Determine Platforms that you will support
  - i. IOS/Android
  - ii. MAC/Windows
- b. Have baseline security requirements compiled that you want to implement
  - i. Min/Max OS versions
  - ii. Password Requirements
  - iii. Encryption Enabled
- c. Determine if there will be separate groups for separate security policies
  - i. Ex1. I have one group I want to assign IOS policies to and I have another I want to assign Android policies to.
  - ii. Ex2. I have more granular security policies I want to apply to on group over another.
  - iii. I encourage you to create a test group for piloting everything you are looking to implement in your organization
- d. Access if there are any apps beyond 365 that you want users to have access to
- e. Choose 3 pilot devices you want to enroll into Intune

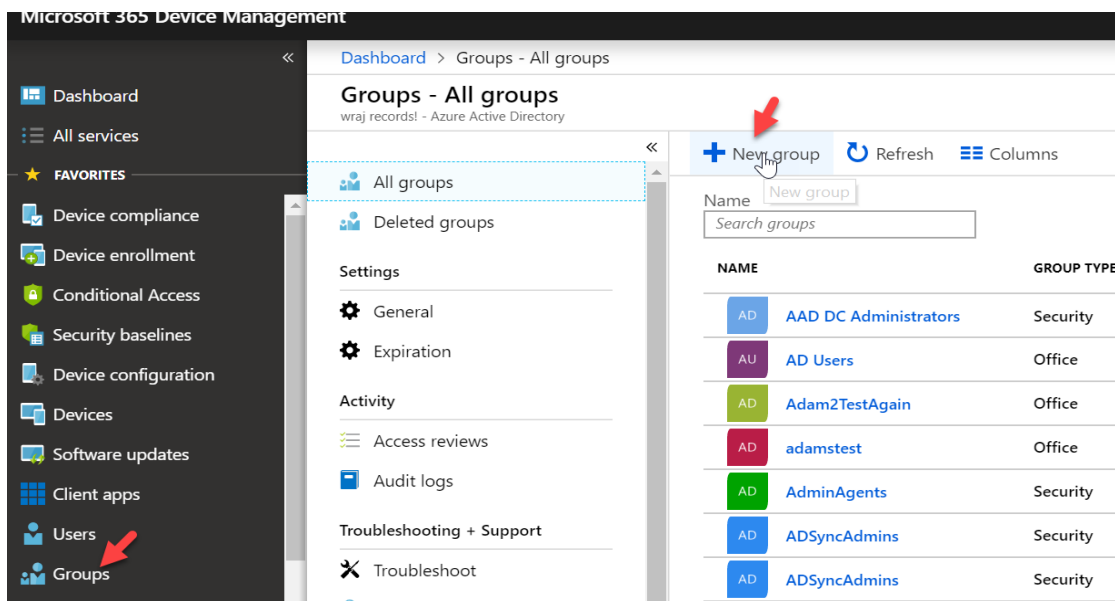
## Create Groups

Create a group for an Intune Pilot Create different groups if you want to separate out different people into different Intune Policies.

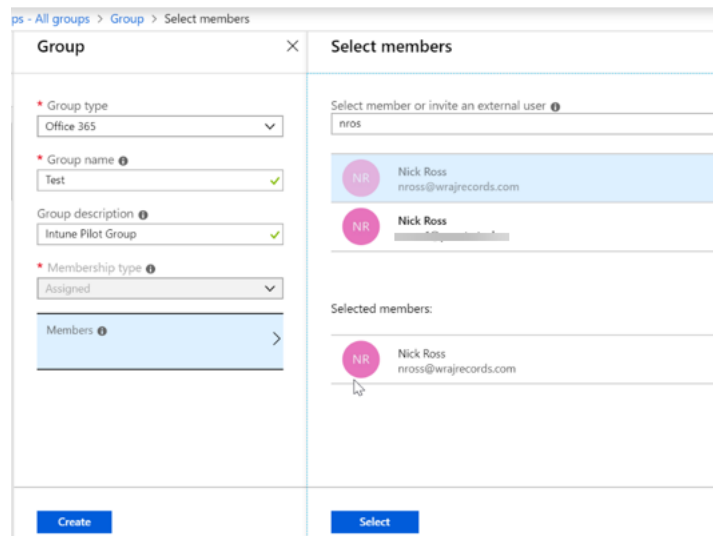
- a. Scroll Down in the 365 Admin Portal and Go to the **Device Management Portal**



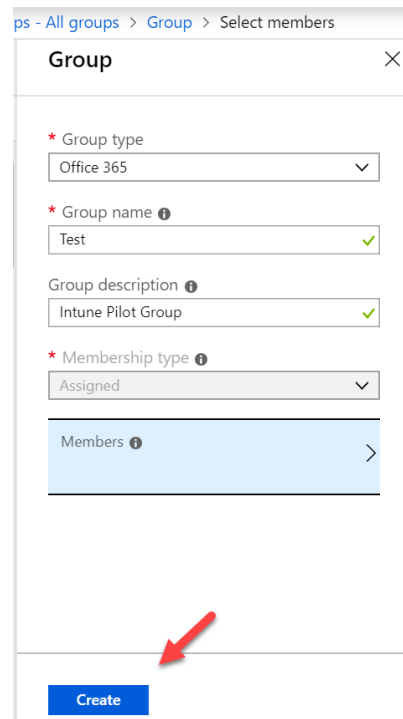
- b. Click on **Groups** and click **New Group**



- c. Group Type can be 365 or security. You can add whatever users you would like for this group. This is my test group, so I am going to add my pilot user

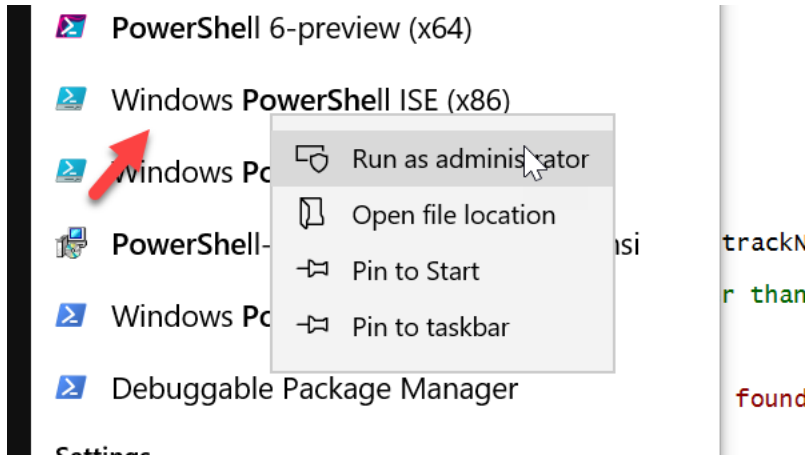


- d. Click **Create** when finished

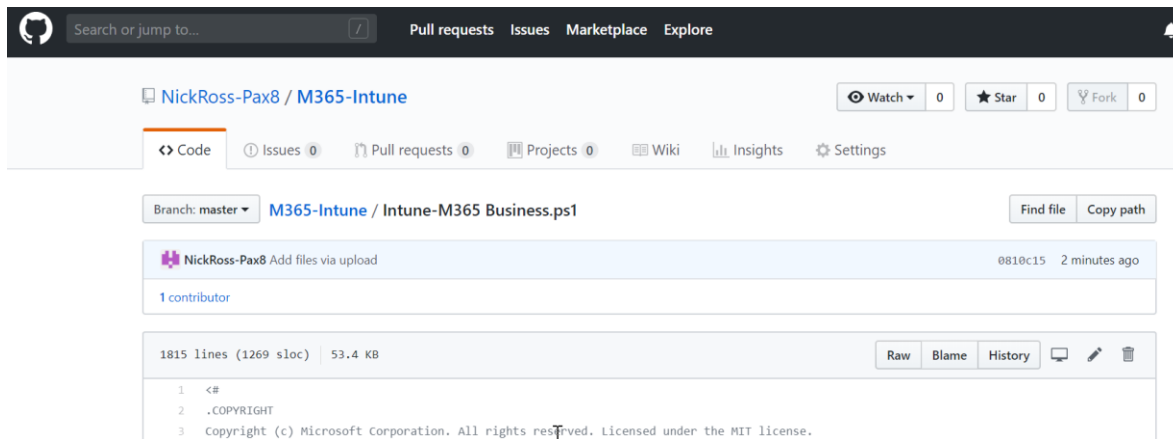


## Running the Powershell Script

1. Run Powershell ISE as Administrator



2. Copy and Paste the script from GitHub that I created. Here is the [link](#)



- If you want to modify any of the settings for any of the policies, you can view their respective lines:

```

4 | See LICENSE in the project root for license information.
5 | #>
6 |
7 | <#
8 | .SYNOPSIS
9 | After you run this script, you will have
10 |
11 | 1. A device compliance policy for:
12 |    iOS (Configure line 1413)
13 |    Android (Configure line 1388)
14 |    Windows (Configure line 1435)
15 | 2. A device configuration policy for Windows Devices to have BitLocker (Configure line 1460)
16 | 3. Terms and Conditions for when users enroll (Configure line 1479)
17 | 4. Office 365 Business pushed out as a required App to Windows 10 devices (Configure line 1491)
18 | 5. Microsoft Authenticator pushed out as a required App for iOS and Android devices (Configure line 1526)
19 |
20 | #>
21 |
22 | #####
23 |
24 | function Get-AuthToken {
25 |
26 | <#
27 | .SYNOPSIS
28 | This function is used to authenticate with the Graph API REST interface
29 | .DESCRIPTION
30 | The function authenticates with the Graph API interface with the tenant name
31 | .EXAMPLE
32 | Get-AuthToken
33 | Authenticates you with the Graph API interface
34 | .NOTES

```

### Ex. iOS

```

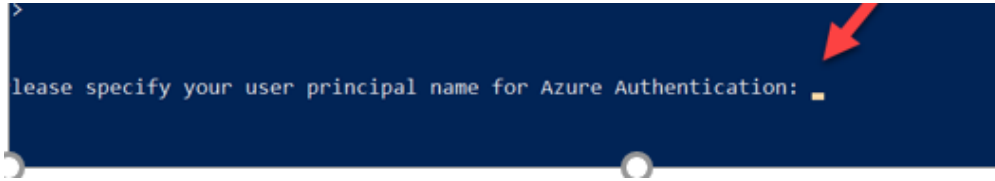
1400 | #####
1410 | #####
1411 |
1412 | $JSON_iOS = @"
1413 | {
1414 |   "@odata.type": "microsoft.graph.iosCompliancePolicy",
1415 |   "description": "iOS Compliance Policy",
1416 |   "displayName": "iOS Compliance Policy",
1417 |   "scheduledActionsForRule": [{"ruleName": "PasswordRequired", "scheduledActionConfigurations": [{"actionType":
1418 |     "passwordBlockSimple": true,
1419 |     "passwordExpirationDays": 90,
1420 |     "passwordMinimumLength": 4,
1421 |     "passwordMinutesOfInactivityBeforeLock": 15,
1422 |     "passwordPreviousPasswordBlockCount": 8,
1423 |     "passwordMinimumCharacterSetCount": null,
1424 |     "passwordRequiredType": "numeric",
1425 |     "passwordRequired": true,
1426 |     "securityBlockJailbrokenDevices": true,
1427 |     "deviceThreatProtectionEnabled": true,
1428 |     "deviceThreatProtectionRequiredSecurityLevel": "Low"
1429 |   }
1430 | }
1431 | "@
1432 | #####

```

- When you run the commands, you will be prompted for a User principal name. Enter the user principal name of a global administrator:

```

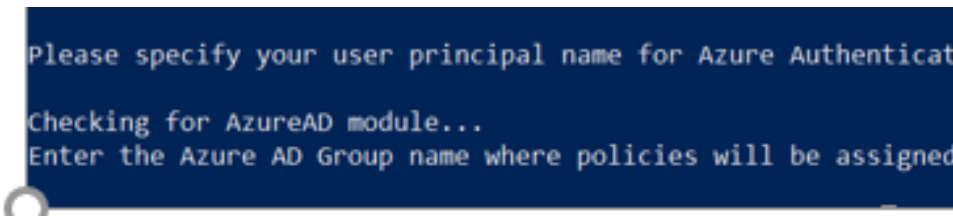
>
Please specify your user principal name for Azure Authentication:
  
```



- Next, enter the group you created in the beginning of this document that contains your pilot users:

```

Please specify your user principal name for Azure Authentication:
Checking for AzureAD module...
Enter the Azure AD Group name where policies will be assigned
  
```



- You will see all the policies, apps, and Terms created. Once complete you will get a new commandline:

```

Adding Terms and Conditions from JSON...
Creating Terms and Conditions via Graph
Terms and Conditions created with id e657cddb-e818-49be-8870-a0ca552e43fb

Assigning Terms and Conditions to AAD Group 'Nicks Test'
Assigned 'Nicks Test' to Customer Terms and Conditions/e657cddb-e818-49be-8870-a0ca552e43fb

Adding Android Compliance Policy from JSON...
Compliance Policy created as dcb93565-9c63-4e1b-bbf1-c927b07cff5d

Assigning Compliance Policy to AAD Group 'Nicks Test'
Assigned 'Nicks Test' to Android Compliance Policy/dcb93565-9c63-4e1b-bbf1-c927b07cff5d

Adding iOS Compliance Policy from JSON...
Compliance Policy created as fda8bad0-8a0a-4822-ae9e-2c3e664b64cf

Assigning Compliance Policy to AAD Group 'Nicks Test'
Assigned 'Nicks Test' to iOS Compliance Policy/fda8bad0-8a0a-4822-ae9e-2c3e664b64cf

Adding Windows Compliance Policy from JSON...
Compliance Policy created as 783dec58-c2f4-45ec-a39e-d059f57e8310

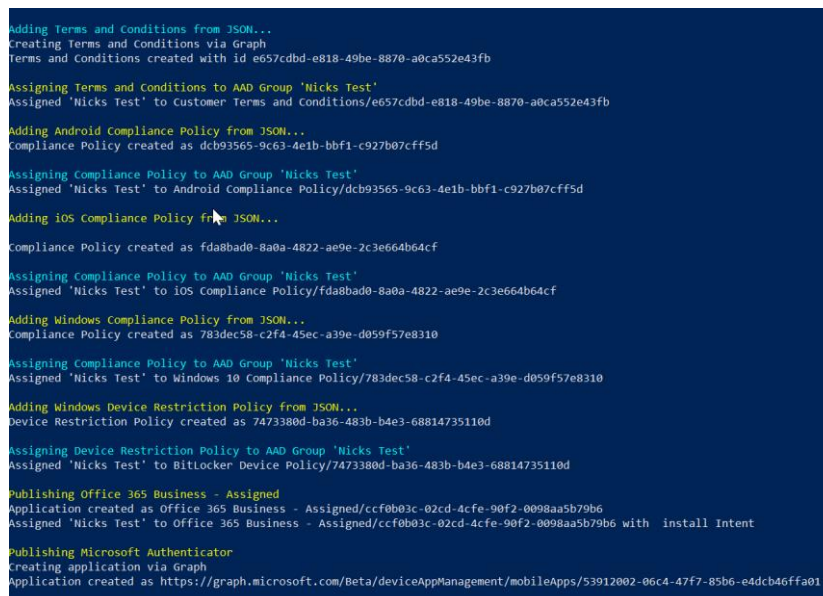
Assigning Compliance Policy to AAD Group 'Nicks Test'
Assigned 'Nicks Test' to Windows 10 Compliance Policy/783dec58-c2f4-45ec-a39e-d059f57e8310

Adding Windows Device Restriction Policy from JSON...
Device Restriction Policy created as 7473380d-ba36-483b-b4e3-68814735110d

Assigning Device Restriction Policy to AAD Group 'Nicks Test'
Assigned 'Nicks Test' to BitLocker Device Policy/7473380d-ba36-483b-b4e3-68814735110d

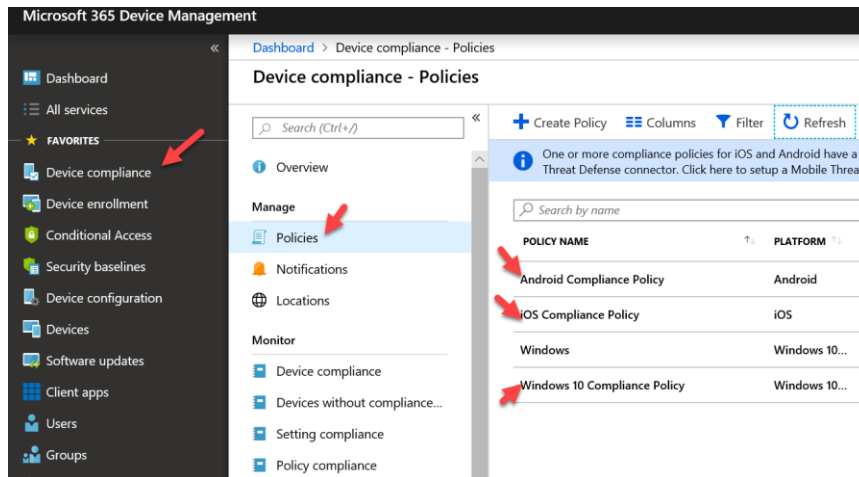
Publishing Office 365 Business - Assigned
Application created as Office 365 Business - Assigned/ccf0b03c-02cd-4cfe-90f2-0098aa5b79b6
Assigned 'Nicks Test' to Office 365 Business - Assigned/ccf0b03c-02cd-4cfe-90f2-0098aa5b79b6 with install Intent

Publishing Microsoft Authenticator
Creating application via Graph
Application created as https://graph.microsoft.com/Beta/deviceAppManagement/mobileApps/53912002-06c4-47f7-85b6-e4dcb46ffa01
  
```





- When you go back to the Device Admin portal, you will be able to see the policies, profile, apps, and terms.



Microsoft 365 Device Management

Dashboard > Device compliance - Policies

### Device compliance - Policies

Search (Ctrl+V)

Overview

Manage

- Policies
- Notifications
- Locations

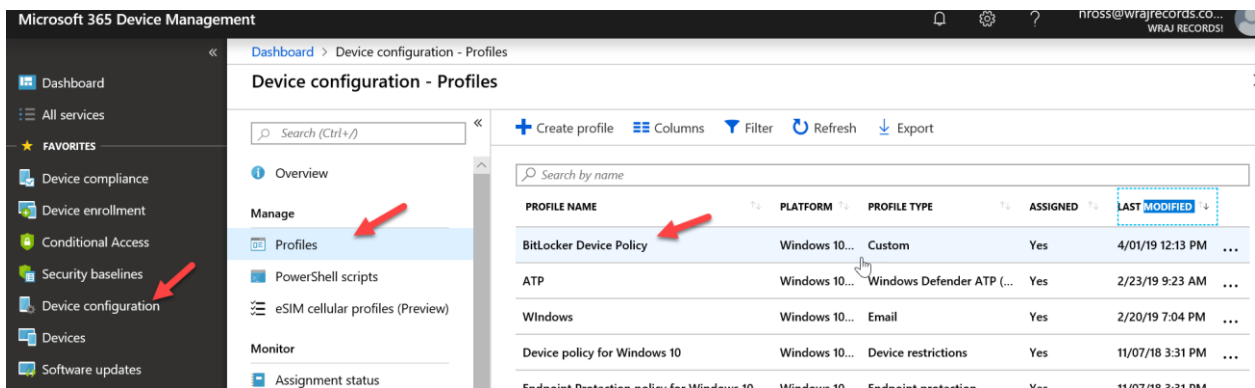
Monitor

- Device compliance
- Devices without compliance...
- Setting compliance
- Policy compliance

One or more compliance policies for iOS and Android have a cc Threat Defense connector. Click here to setup a Mobile Threat...

Search by name

POLICY NAME	PLATFORM	PC
Android Compliance Policy	Android	Ai
iOS Compliance Policy	iOS	iC
Windows	Windows 10...	W
Windows 10 Compliance Policy	Windows 10...	W



Microsoft 365 Device Management

Dashboard > Device configuration - Profiles

### Device configuration - Profiles

Search (Ctrl+V)

Overview

Manage

- Profiles
- PowerShell scripts
- eSIM cellular profiles (Preview)

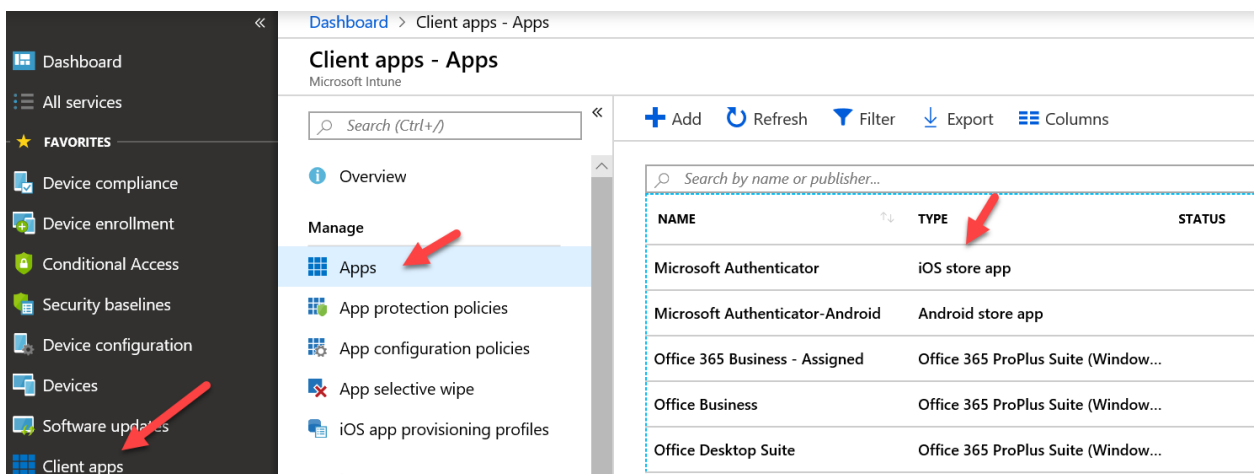
Monitor

- Assignment status

Create profile Columns Filter Refresh Export

Search by name

PROFILE NAME	PLATFORM	PROFILE TYPE	ASSIGNED	LAST MODIFIED
BitLocker Device Policy	Windows 10...	Custom	Yes	4/01/19 12:13 PM ...
ATP	Windows 10...	Windows Defender ATP (...)	Yes	2/23/19 9:23 AM ...
Windows	Windows 10...	Email	Yes	2/20/19 7:04 PM ...
Device policy for Windows 10	Windows 10...	Device restrictions	Yes	11/07/18 3:31 PM ...
Endpoint Protection policy for Windows 10	Windows 10	Endpoint protection	Yes	11/07/18 3:31 PM ...



Microsoft 365 Device Management

Dashboard > Client apps - Apps

### Client apps - Apps

Microsoft Intune

Search (Ctrl+V)

Overview

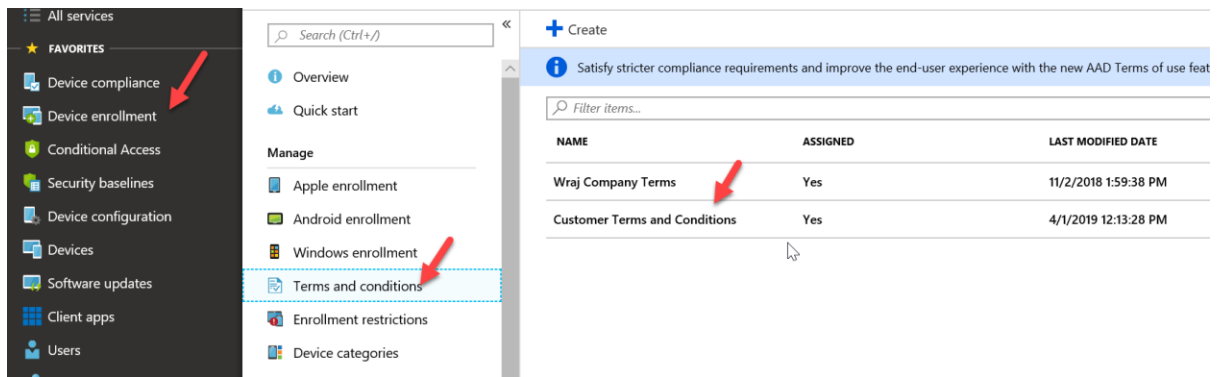
Manage

- Apps
- App protection policies
- App configuration policies
- App selective wipe
- iOS app provisioning profiles

Add Refresh Filter Export Columns

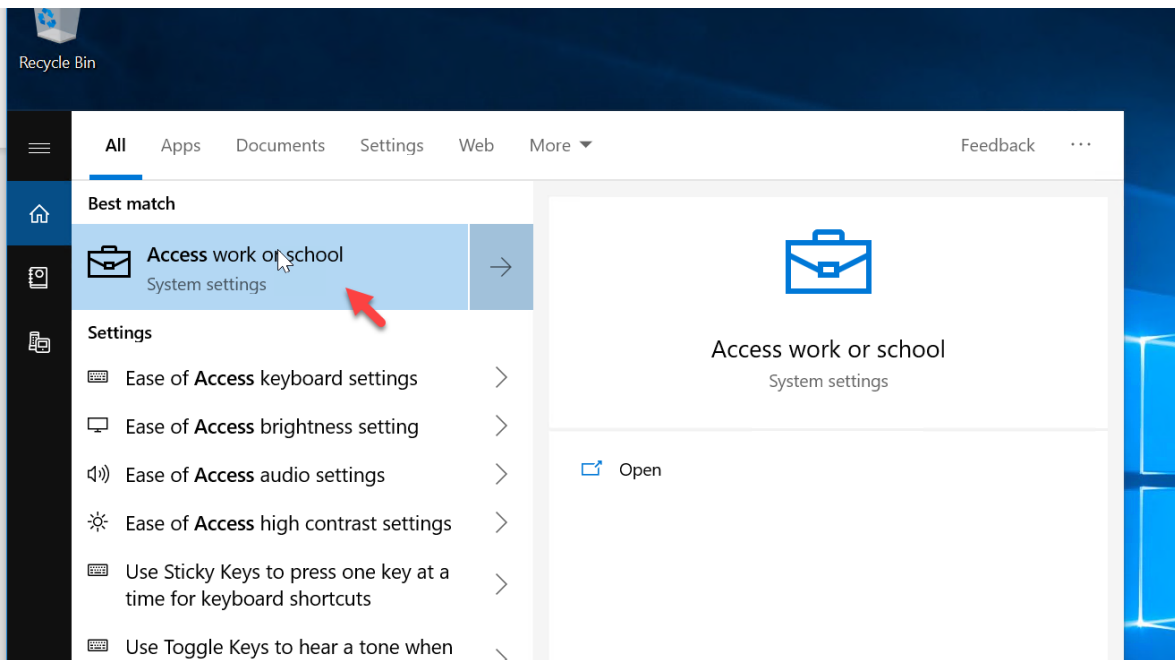
Search by name or publisher...

NAME	TYPE	STATUS
Microsoft Authenticator	iOS store app	
Microsoft Authenticator-Android	Android store app	
Office 365 Business - Assigned	Office 365 ProPlus Suite (Window...	
Office Business	Office 365 ProPlus Suite (Window...	
Office Desktop Suite	Office 365 ProPlus Suite (Window...	

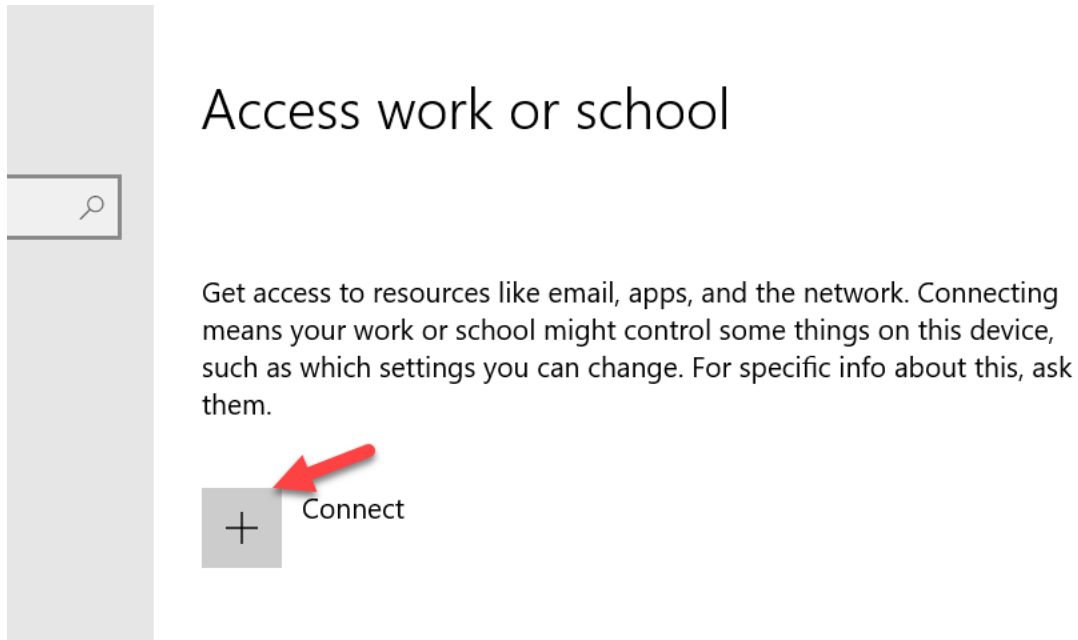
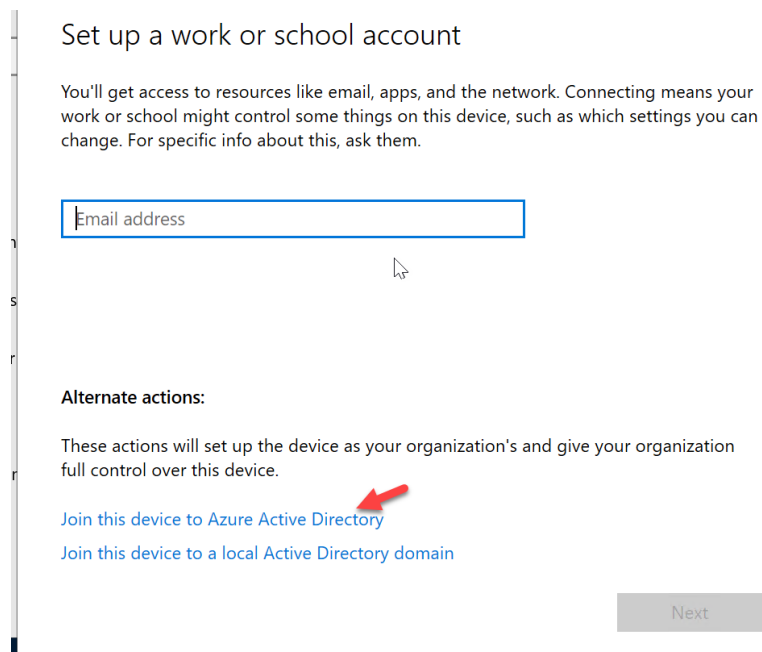


## Enroll Devices: Windows

- a. On the Windows 10 Device, click Start and type Access Work or School



## b. Click Connect

c. Click **Join this device to Azure Active Directory**

d. Sign-In with the Users Azure AD credentials

Let's get you signed in

Work or school account

someone@example.com

Which account should I use?

Sign in with the username and password you use with Office 365 or other business services from Microsoft.

[Privacy statement](#)

Next

e. When prompted, click **Join**

Make sure this is your organization

Make sure this is your organization

If you continue, system policies might be turned on or other changes might be made to your PC.  
Is this the right organization?

Connecting to: wrjrecords.com  
User name: nross@wrjrecords.com  
User type: Administrator

Cancel

Join

- f. You will get a success message when complete. If this is the first device the user is enrolling, you will be first given Terms and Conditions to accept

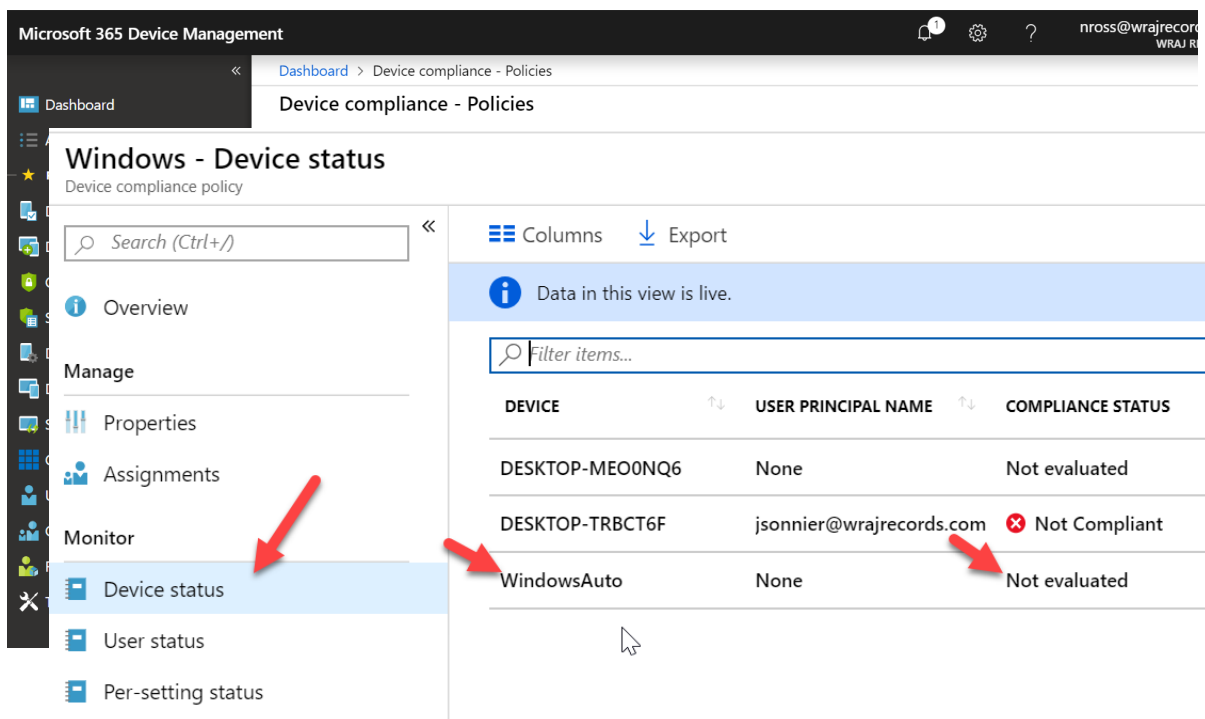
You're all set!

This device is connected to wraj records!

When you're ready to use this new account, select the Start button, select your current account picture, and then select 'Switch account'. Sign in using your nross@wrajrecords.com email and password.

Done

- g. Back in the Intune Portal, you can go to **Device Compliance>Policies>Click on your Windows Policy** (we created earlier in this document)



Microsoft 365 Device Management

Dashboard > Device compliance - Policies

Device compliance - Policies

### Windows - Device status

Device compliance policy

Search (Ctrl+/)

Columns Export

Data in this view is live.

Filter items...

DEVICE	USER PRINCIPAL NAME	COMPLIANCE STATUS
DESKTOP-MEO0NQ6	None	Not evaluated
DESKTOP-TRBCT6F	jsonnier@wrajrecords.com	Not Compliant
WindowsAuto	None	Not evaluated

Overview

Manage

- Properties
- Assignments

Monitor

- Device status
- User status
- Per-setting status

- h. You can click on **Device status** to see compliance status. Note, it can take some time before the evaluation will complete. In this case, I see the device I just joined as "Not Evaluated". We just must wait for that to complete.

## Monitoring

I can come back in later to see that it is in error:

Columns Export

Data in this view is live.

Filter items...

DEVICE	USER PRINCIPAL NAME	DEPLOYMENT STATUS	LAST STATUS UPDATE
DESKTOP-MEO0NQ6	None	Pending	
DESKTOP-TRBCT6F	jsonnier@wrajrecords.com	Failed	1/10/19, 10:57 AM
WindowsAuto	nross@wrajrecords.com	Error	3/30/19, 5:20 PM

a. Click on this line item and the go to **Device Compliance** on the next page:

Dashboard > Device compliance - Policies > Windows > Device status > WindowsAuto

### WindowsAuto

Search (Ctrl+/)

Retire Wipe Delete Remote lock Sync Reset passcode Restart

Overview

Manage

Properties

Monitor

Hardware

Discovered apps

Device compliance

Device configuration

App configuration

Security baselines

Managed Apps

Device name: WindowsAuto

Enrolled by User: Nick Ross

Management name: nross\_Windows\_3/30/2019\_9:01 PM

Compliance: Not Compliant

Ownership: Corporate

Operating system: Windows

Serial number: 0000-0013-4890-0606-7785-1571-70

Device model: Virtual Machine

Phone number: ---

Last check-in time: 3/30/2019, 5:20:18 PM

See more

Device actions status

ACTION	STATUS	DATE/TIME
No results		

- b. Click on **Windows** as it is our policy

Dashboard > Device compliance - Policies > Windows > Device status > WindowsAuto - Device compliance

### WindowsAuto - Device compliance

Search (Ctrl+*/*)

- Overview
- Manage
- Properties
- Monitor
- Hardware
- Discovered apps
- Device compliance

Export

Filter by name

POLICY	USER PRINCIPAL NAME	STATE
Built-in Device Compliance Policy	nross@wrajrecords.com	Compliant
Windows	nross@wrajrecords.com	Error

- c. Here you can see why the device is out of compliance and take action steps to remediate. In this case it looks like we just need to finish setting up BitLocker to encrypt the drive:

Dashboard > Device compliance - Policies > Windows > Device status > WindowsAuto - Device compliance > Windows

### Windows

Policy settings

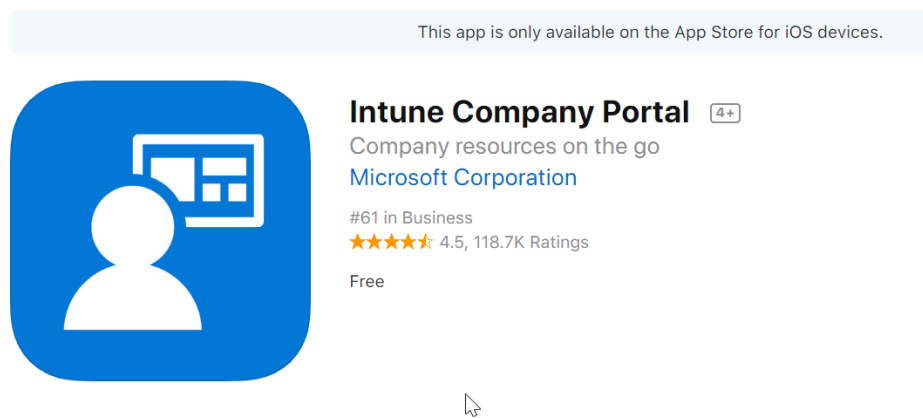
Export

SETTING	STATE	STATE DETAILS
Antispyware	Compliant	
Number of non-alphanumeric characters in passw...	Compliant	
Antivirus	Compliant	
Password expiration (days)	Compliant	
Encryption of data storage on device.	Error	-2016281112 (Remediation failed)
Minimum password length	Compliant	
Maximum minutes of inactivity before password is...	Not applicable	
Password type	Compliant	
Firewall	Compliant	
Require BitLocker	Not applicable	

## Enroll Devices: iOS and Android

iOS and Android device enrollment can be completed by downloading the Intune Company Portal app from the app store or google play store:

### App Store Preview



- a. Users will be walked through a wizard after they enter their Azure AD credentials
- b. For a detailed list of the entire user experience, you can follow this support guide from Microsoft:

[Intune](#)

[Android](#)

## Pilot Testing and Remediation

During our Pilot we want to discover:

- Common FAQs
- Whether we need to tighten or loosen our policies
- End User Experience for Communications to Broad audience
- Common Troubleshooting Techniques for each platform

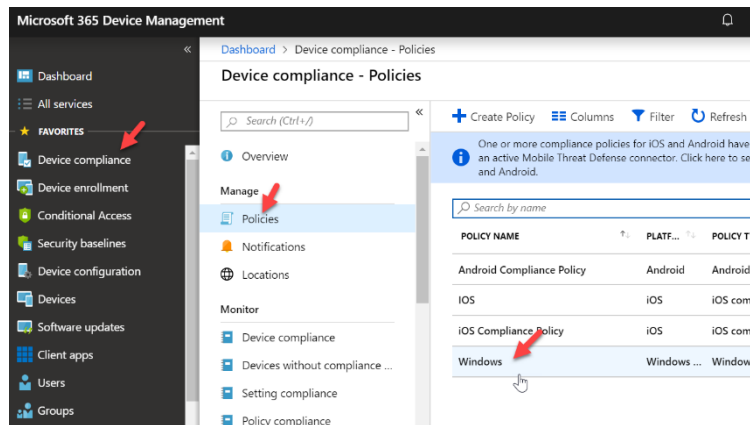
After this is complete, we want to create communications to our audience for enrollment:



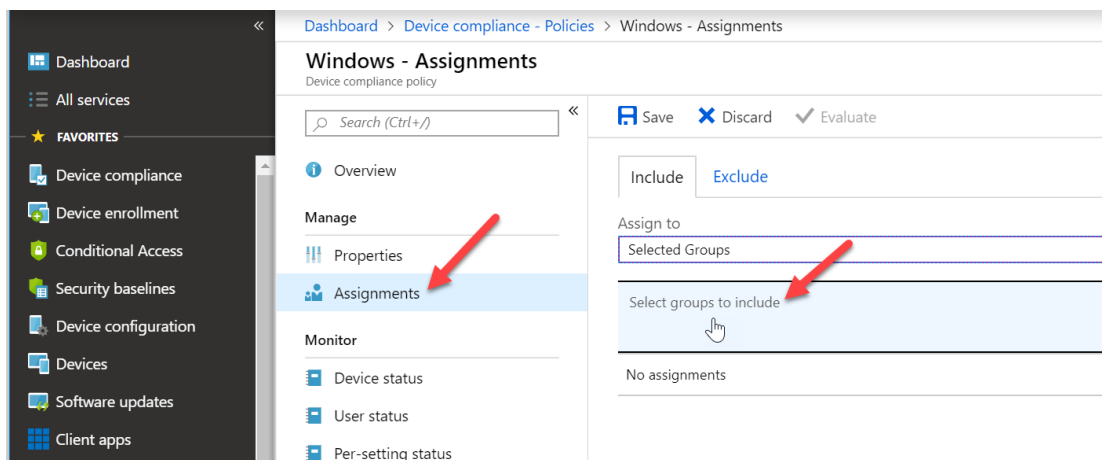
- Why is this service important?
- What pain points will it help them solve?
- What can end users expect?
- What are the steps to get my device enrolled

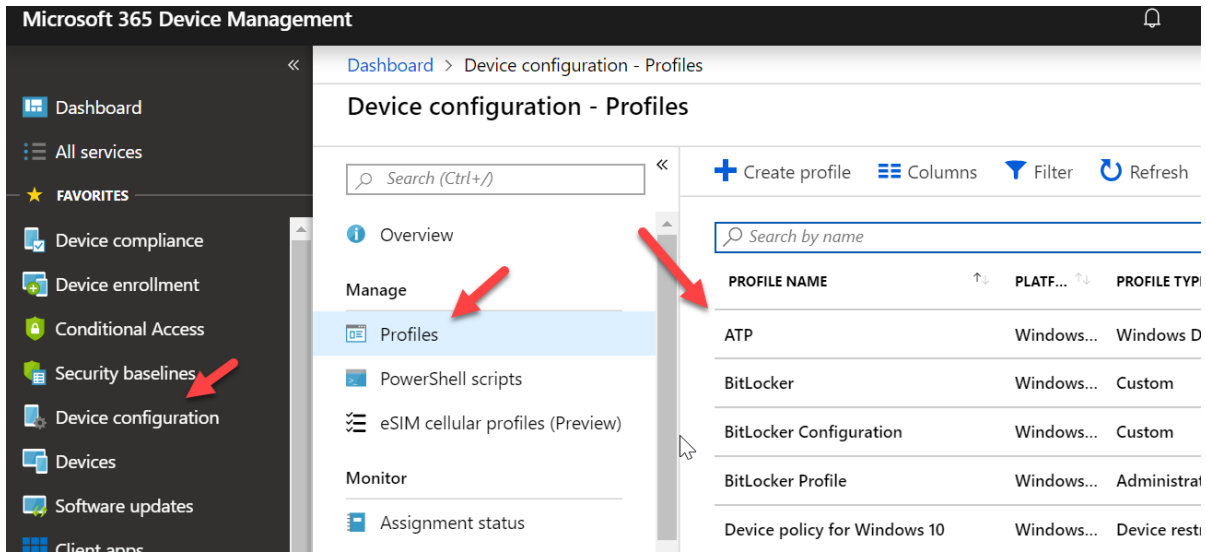
Lastly, after we have this pushed out and a target date for deployment, we can go back into the Device Management Admin Center and begin to add our groups to our policies and profiles:

- Go to Device Compliance and click on policy you want to add a group to:



- Go to **Assignments** and select your groups that you want to apply the policy to. You can do the same with **Device Profiles** by going to the **Device Configuration** section





## Conclusion

I hope this article provided you some targeted guidance on creating a runbook for Intune. Any feedback to improve your experience would be greatly appreciated. I would also like to hear if there is more content that you would like to see in this guide. Any feedback can be sent to my email below:

[Msp4msps@tminus365.com](mailto:Msp4msps@tminus365.com)