



Desktop-as-a-Service (DaaS) Using Windows Virtual Desktop (WVD)

BYOD with M365 & Intune

Prepared for:

Service Provider Partners

Oct. 2019

Prepared by:

Microsoft – One Commercial Partner (OCP)

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation. Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers. © 2016 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

1. Overview	5
2. Prerequisites	5
Azure & Windows Active Directory Prerequisites	5
General Best Practices	6
Azure Networking	6
Azure Architectural Diagram	6
3. Setup Mobile Device Management (MDM) Services	7
Configure MDM Authority	7
Preparation for enrolling iOS devices	9
Preparation for enrolling Windows devices	14
4. Configure Company Portal	16
Device Enrollment Administrator	17
Device Group Categories	18
Creating Azure Active Directory Dynamic Device Security Groups	20
Create an AAD Dynamic Device Security Group	21
5. Device enrollment experience	22
Windows Devices	22
iOS Devices	24
6. Device Compliance Policies	24
Create a compliance policy	24
Assign a compliance policy	26
Configuration Policies	28
Create a configuration policy	28
Uninstall restricted applications policy iOS	32
Software Update Policies	35
Create a Windows software update policy	35
Create an iOS software update policy	40

7. Device Enrollment	43
Enable automatic enrollment for Windows 10.....	43
Enable automatic enrollment for iOS	44
Enrolling Windows devices manually	48
Microsoft Store App.....	50
Deploy Client Apps to Managed Intune Devices	53
8. Device Actions	57
Remotely erase data from a device.....	57
9. ATP and Intune Integration	58
Enable Microsoft Defender ATP in Intune	58
On-board devices by using a configuration profile	61
Create a device configuration profile.....	61
Assign a device profile	63
Create and assign a compliance policy.....	64
Create the compliance policy.....	64
Assign the device compliance to user/groups.....	66
Create a Conditional Access policy	67
Monitor device compliance.....	72
10. Support	72
11. Appendix	73
Device security and data protection security.....	73
Basic Security.....	73
Advanced Security	73

1. Overview

This document is a walk-through of implementing MDM, Intune, and ATP Azure Protection on Endpoints. Together, they let you manage smartphones, laptops, tablets, and desktops and multiple operating systems such as iOS, Android, Windows, macOS, and Chrome OS.

This document will cover deploying applications to devices, configuring your Company Portal, enrolling end user devices, creating policies, and more.



The image above shows the integrated cloud services designed to protect data and control access. In this document we will work with the majority of these tools to protect, analyze and track threats, and enforce security and update compliance for accessing the sensitive data of your organization.

Learn [more](#) about the device security and data protection services available for BYOD.

2. Prerequisites

Azure & Windows Active Directory Prerequisites

Before getting started, **all** items listed below **must** be checked/validated to ensure the most basic requirements are in place to proceed with executing the remaining steps in this guide.

- An Azure Active Directory
- A Windows Server Active Directory in sync with Azure Active Directory. This can be enabled through:
 - Azure AD Connect
 - Azure AD Domain Services
- An Azure subscription, containing a virtual network that either contains or is connected to the Windows Server Active Directory

General Best Practices

Since everyone's business and technical requirements vary across the board, it is always a good idea to familiarize yourselves with the standard best practices across the different Azure technologies & services.

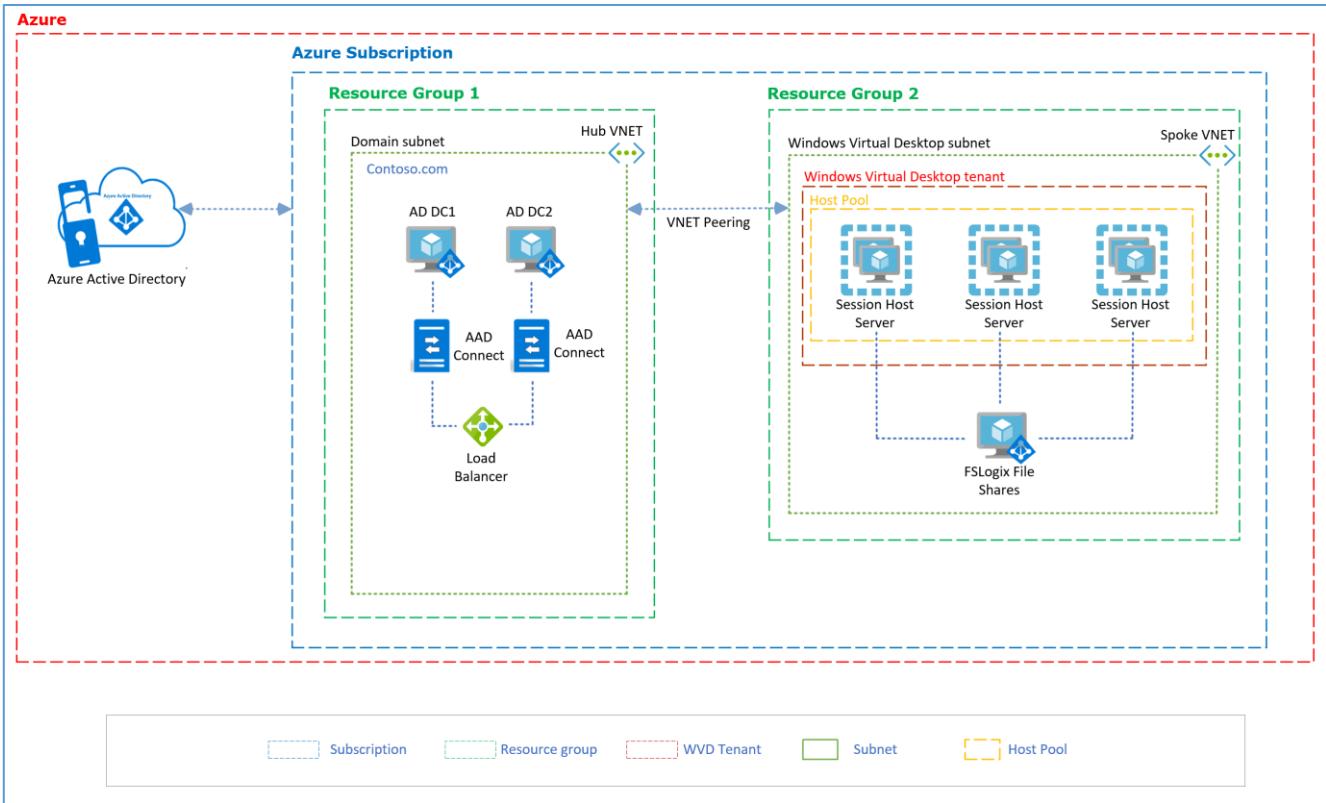
- Please follow the guidance [here](#) to maintain a consistent naming convention across your resources, unless you are already using a naming system.
- [Azure security best practices and patterns](#)
- Azure Active Directory Hybrid Identity [best practices](#)
- [Azure identity management and access control security best practices](#)
- Azure Networking & security [Best Practices](#)
- Azure Storage security [overview](#)
- [Best practices for Azure VM security](#)

Azure Networking

The recommendation is to design your Azure Networking using a [Hub-Spoke topology](#). Consider the HUB like a DMZ deployed with your Virtual network Gateways and other security/edge appliances like Firewalls Etc. while the Spoke will act as the backend zone where your session hosts servers are deployed to and is peered with the HUB. This is our design for this walk-through, so you'll need this already setup before proceeding.

Azure Architectural Diagram

Below is a diagram of the Azure environment that we'll use. It shows the objects created in Azure and their relationships within the environment. In this example, the company name will be Contoso.



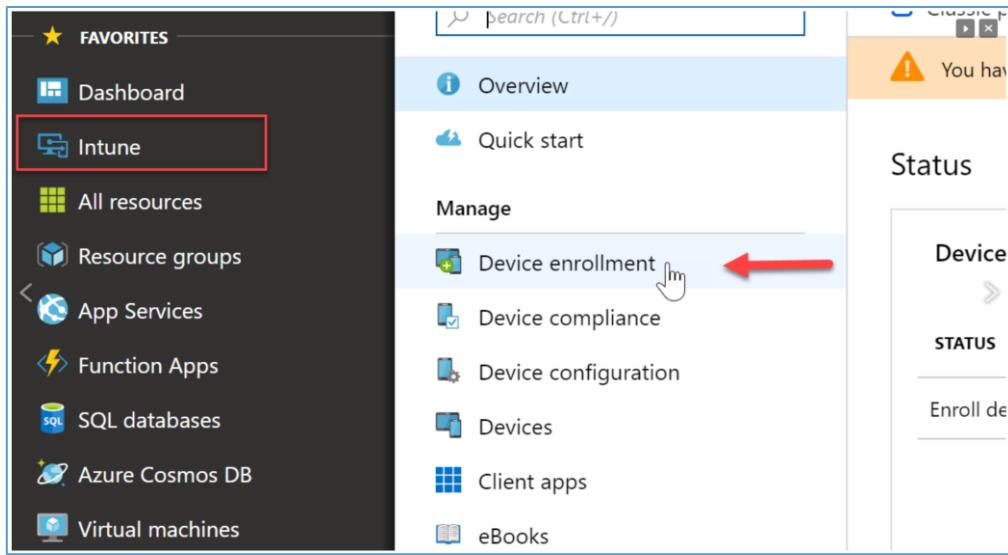
3. Setup Mobile Device Management (MDM) Services

In this section we'll implement Azure Mobile Device Management (MDM) Services. This includes setting up the enrollment processes for the various device types.

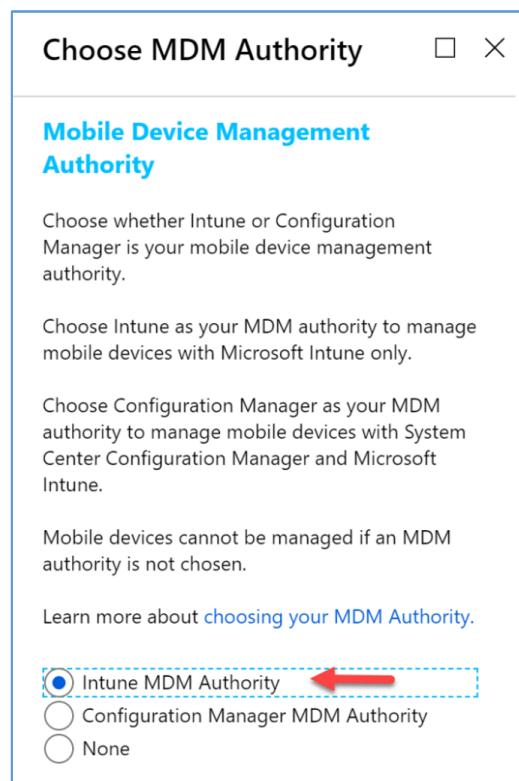
Configure MDM Authority

First, we must configure Intune as our MDM authority. We are setting up MDM as stand-alone, so we'll use Intune as the only authority, and not Configuration Manager.

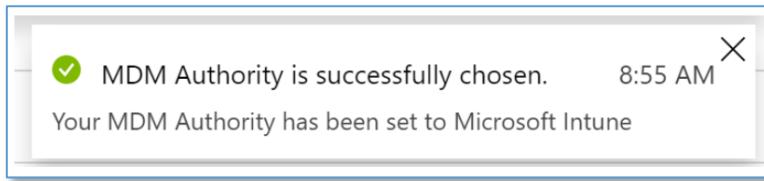
1. Logon to portal.azure.com, and search for “Intune”.
2. Open the service console, then expand the Intune node and select “Device Enrollment”.



3. Select "**Intune MDM Authority**" and then click "**Choose**":



1. We will get a notification that the changes were saved successfully



After the MDM Authority is configured, we go next to Configuring APN Certificate. These steps are necessary for managing iOS devices.

Preparation for enrolling iOS devices

To manage iOS devices, we must create an Apple Push certificate:

1. In the Intune blade, go to **Device Enrollment > Apple Enrollment**, select “Apple MDM Push Certificate”

The screenshot shows the Microsoft Intune interface. On the left, there's a navigation sidebar with links like Overview, Quick start, Manage, Device enrollment (which is selected and highlighted with a red box), Device compliance, Device configuration, Devices, Client apps, eBooks, Conditional access, On-premises access, Users, Groups, Roles, Software updates, Help and support, and Troubleshoot. The main content area is titled "Device enrollment - Apple enrollment". It contains sections for Prerequisites (with a callout to "Apple MDM Push certificate" which is also highlighted with a red box and has a red arrow pointing to its "Manage" button), Bulk enrollment methods (listing Apple Configurator and Enrollment program tokens), and other management tools like Terms and conditions, Enrollment restrictions, Device categories, Corporate device identifiers, Device enrollment managers, Monitor, Audit logs, Help and support, and Help and support. A note at the top states: "Intune requires an Apple MDM Push certificate to manage Apple devices, and supports multiple enrollment methods. Set up the MDM push certificate to begin. Learn More."

2. Agree to the terms and then download the CSR:

Configure MDM Push Certificate

Delete

Status: ? Not set up	Days Until Expiration: Not available
Last Updated: Not available	Expiration: Not available
Apple ID: Not set up	Subject ID Not set up

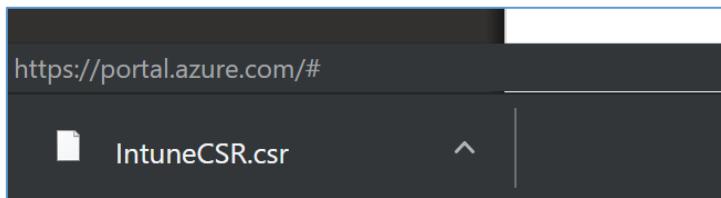
^

You need an Apple MDM push certificate to manage Apple devices with Intune.

Steps:

1. I grant Microsoft permission to send both user and device information to Apple. [More information.](#)
 * I agree.
2. Download the Intune certificate signing request required to create an Apple MDM push certificate.
[Download your CSR](#)
3. Create an Apple MDM push certificate. [More information.](#)
[Create your MDM push Certificate](#) ↗

3. The file, "IntuneCSR.csr" will be downloaded.



4. Click **Create your MDM push certificate**. You will need to have an Apple ID so if you do not have one you will need to create one.

Home > Microsoft Intune > Device enrollment - Apple enrollment > Configure MDM Push Certificate

Configure MDM Push Certificate

Status: ? Not set up	Last Updated: Not available	Apple ID: Not set up	Days Until Expiration: Not available
Expiration: Not available	Subject ID: Not set up		

You need an Apple MDM push certificate to manage Apple devices with Intune.

Steps:

- I grant Microsoft permission to send both user and device information to Apple. [More information.](#)
 * I agree.
- Download the Intune certificate signing request required to create an Apple MDM push certificate.
[Download your CSR](#)
- Create an Apple MDM push certificate. [More information.](#)
→ [Create your MDM push Certificate](#) 
- Enter the Apple ID used to create your Apple MDM push certificate.
* Apple ID

5. Sign in with your Apple ID into the Apple Push Certificates Portal:



6. Now click "Create a Certificate" after you have successfully signed into the portal:

The screenshot shows the Apple Push Certificates Portal. At the top, there's a navigation bar with links for Store, Mac, iPod, iPhone, iPad, iTunes, and Support, along with a search bar. Below the navigation bar is the title "Apple Push Certificates Portal" and a sign-in link for "bradleywyatt1@gmail.com". A "Sign out" button is also visible. The main content area features a large globe graphic with a green dot over North America and a yellow dot over South America, symbolizing global reach. On the left, there's a "Get Started" section with a "Create a Certificate" button, which has a red box and a cursor icon indicating it's the target for step 6. Below this is an "FAQ" section with links to "Mobile Device Management" and "What about OS X Server?". At the bottom of the page, there are links for the Apple Online Store, Apple Info, Site Map, Hot News, RSS Feeds, Contact Us, and a US flag icon.

7. Navigate to the CSR file that we downloaded from the Intune portal, & select "Upload"

This screenshot shows the "Create a New Push Certificate" page. The top navigation bar and user information are identical to the previous screenshot. The main form is titled "Create a New Push Certificate" and contains instructions: "Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate." Below this is a "Notes" section with an empty text area. Further down is a "Vendor-Signed Certificate Signing Request" field with a "Choose File" button labeled "IntuneCSR.csr", which has a red box and a cursor icon. To the right of this field is a "Cancel" button and an "Upload" button, with a red arrow pointing to the "Upload" button. The right side of the page features the same globe graphic as the homepage. The footer links and flags are also present.

8. Once you have a green confirmation, download your certificate:



9. Go back to the Intune portal, and in **step 4**, enter your **Apple ID**. In **step 5** browse to the downloaded **certificate** and then press "**Upload**":

A screenshot of the Microsoft Intune portal. The URL in the address bar is "Home > Microsoft Intune > Device enrollment - Apple enrollment > Configure MDM Push Certificate". The page title is "Configure MDM Push Certificate". There are five steps listed:

1. * I agree.
2. Download the Intune certificate signing request required to create an Apple MDM push certificate.
[Download your CSR](#)
3. Create an Apple MDM push certificate. [More information](#).
[Create your MDM push Certificate](#)
4. Enter the Apple ID used to create your Apple MDM push certificate.
* Apple ID
5. Browse to your Apple MDM push certificate to upload
* Apple MDM push certificate

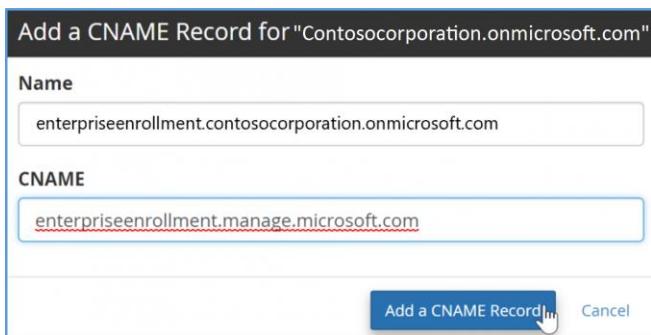
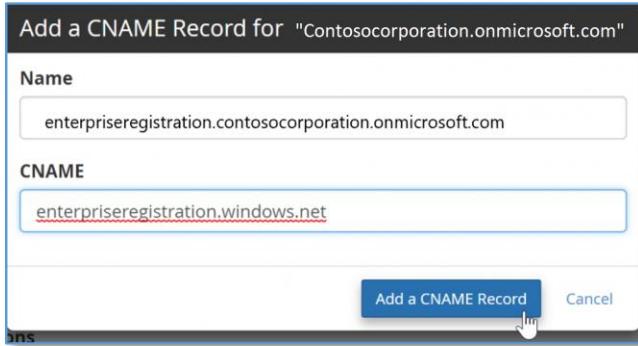
A red box highlights the "Apple ID" input field, and another red box highlights the "Apple MDM push certificate" input field. A red arrow points to the "Upload" button at the bottom left of the form. A status message in the top right corner says "Upload Completed for MDM_Microsoft_C... 9:23 AM 1.91 KiB | *Streaming upload*".

iOS device enrollment is now setup.

Preparation for enrolling Windows devices

For Windows devices, there are two DNS CNAME records that need to be created within your domains DNS zone. These will redirect the devices to the Intune servers for automatic device management. In our example, we're adding them to Contosocorporation.onmicrosoft.com:

1. Add **enterpriseregistration.[domain name]** and **enterpriseenrollment.[domain name]**



2. Check DNS for MDM, to see that the records are now in place and valid:

The screenshot shows the Microsoft 365 Admin Center with a green banner indicating 'All DNS records are correct, no errors found. Nameservers used: ns1.mylhsns.net, ns2.mylhsns.net'. Below the banner, under 'Required DNS settings', it says 'Your DNS records must be set to the following values for your Office 365 services to run smoothly.' There are sections for 'Exchange Online' and 'Mobile Device Management for Office 365'. The 'Mobile Device Management for Office 365' section lists two CNAME records:

Type	Host name	Points to address or value	TTL	Actions
CNAME	enterpriseregistration	enterpriseregistration.windows.net	1 Hour	
CNAME	enterpriseenrollment	enterpriseenrollment.manage.microsoft.com	1 Hour	

3. In the Intune Azure portal, open **Device Enrollment**
4. Click **Windows enrollment > CNAME Validation**

The screenshot shows the Microsoft Intune Azure portal interface. The left sidebar has a tree view with 'Device Enrollment' selected. The main content area is titled 'Device enrollment - Windows enrollment'. It includes sections for 'Windows Hello for Business', 'CNAME Validation' (which is highlighted with a red box), 'Enrollment Status Page (Preview)', and 'Windows Autopilot Deployment Program'.

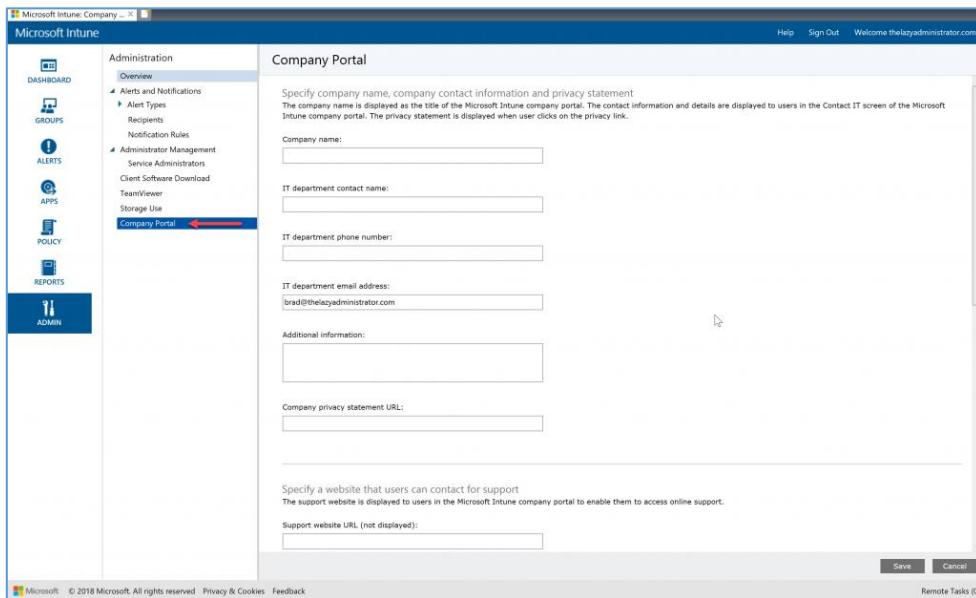
5. Test that the domain is verified successfully:

The screenshot shows a 'Test CNAME' dialog box. It contains the following text:
 Configuring a CNAME in your DNS saves your users from having to enter the address of the MDM server when enrolling their Windows devices. [Learn More](#).
 After configuring the CNAME resource records in your DNS, enter the corresponding domain here to confirm that it has been configured correctly. Changes to DNS records might take up to 72 hours to propagate.
 Domain: contosocorporation.onmicrosoft.com
 Test
 ✓ CNAME for contosocorporation.onmicrosoft.com is configured correctly.

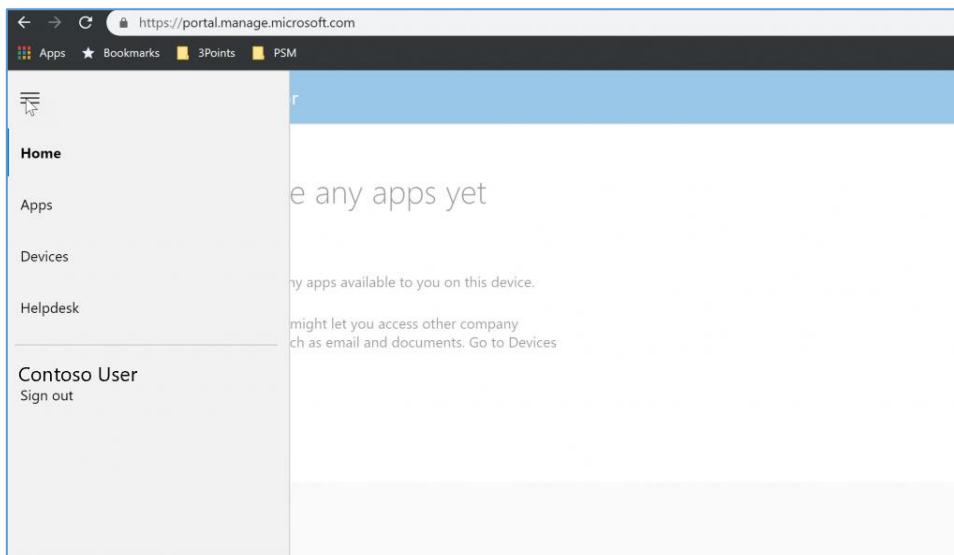
4. Configure Company Portal

The Company Portal is a web page and a mobile device application that supports BYOD users. It gives them a centralized location to install published applications, self-management, and retrieve information.

The Company Portal is configured on the Intune Portal at <https://portal.manage.microsoft.com/>



Once the administrator saves the Company Portal changes, you can launch the portal website (<https://portal.manage.microsoft.com/>) and get the apps and devices registered to the user.



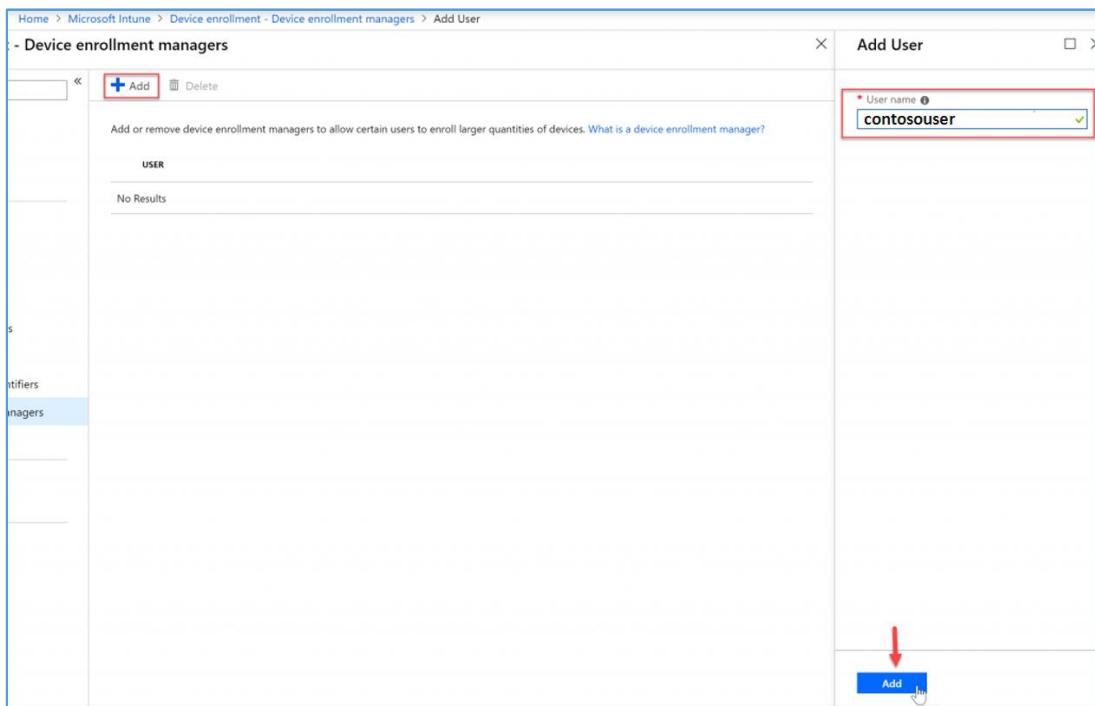
Device Enrollment Administrator

Device Enrollment Administrators are users that are able to enroll more than the default of 5 devices to Intune (which is meant for a standard user and not an Administrator account.)

1. Navigate to the Azure Portal and expand the Intune blade
2. Expand "Device Enrollment" and select "Device Enrollment Managers"

The screenshot shows the Microsoft Intune interface. On the left, there's a sidebar with various navigation options like Overview, Quick start, Manage, Help and support, and Troubleshoot. Under Manage, 'Device enrollment' is selected. On the right, the main content area is titled 'Device enrollment' and lists several management options: Apple enrollment, Android enrollment, Windows enrollment, Terms and conditions, Enrollment restrictions, Device categories, Corporate device identifiers, and Device enrollment managers. The 'Device enrollment managers' option is highlighted with a blue selection bar and a small circular arrow icon to its right.

3. Click Add and then enter your users UserPrincipalName and then select the "Add" button on the bottom. In this case we're adding "contosouser":



Device Group Categories

Use Microsoft Intune **device categories** to automatically add devices to groups based on properties that you define. This makes it easier for you to manage those devices as a group.

In this walk-through, we'll create two device categories.

- **Company Owned Devices.** These devices are purchased by the company, and given to the end users through the IT department.
- **BYOD** devices, or personal devices. These will be devices that end users own but may use them for work.

1. In the Azure Portal, expand the **Intune** blade.
2. Select “**Device Enrollment**” and then click “**Device Categories**”

The screenshot shows the Microsoft Intune interface. On the left, there's a sidebar with various management options like Overview, Quick start, Manage, Help and support, and Troubleshoot. Under Manage, the 'Device enrollment' link is highlighted with a red box. On the right, there's a 'Device enrollment - Device categories' section with links for Apple enrollment, Android enrollment, Windows enrollment, Terms and conditions, Enrollment restrictions, Device categories, Corporate device identifiers, and Device enrollment managers. The 'Device categories' link is also highlighted with a red box and has a cursor icon pointing to it. Below these sections are Monitor, Help and support, and Audit logs.

3. To add a new category, click **Create Device Category**, supply a valid name, and press “**Create**”. We’re adding the category called Company Owned Devices:

The screenshot shows the 'Create device category' dialog box. It has a 'Category' field containing 'Company Owned Device' which is highlighted with a red box. There's also a 'Description' field with the word 'Company'. At the bottom, there's a 'Create' button which is also highlighted with a red box and has a cursor icon pointing to it.

Repeat this step for each category you wish to add.

Creating Azure Active Directory Dynamic Device Security Groups

In this section, you will create dynamic groups in the Azure portal, based on the device category and device category name.

Use the information in this section to create a device group with an advanced rule, by using the **deviceCategory** attribute. For example: **device.deviceCategory -eq "Personal Device"**.

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

Windows users should also use the Company Portal website to select a category.

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

After choosing a category, the device is automatically added to the corresponding group.

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

Create an AAD Dynamic Device Security Group

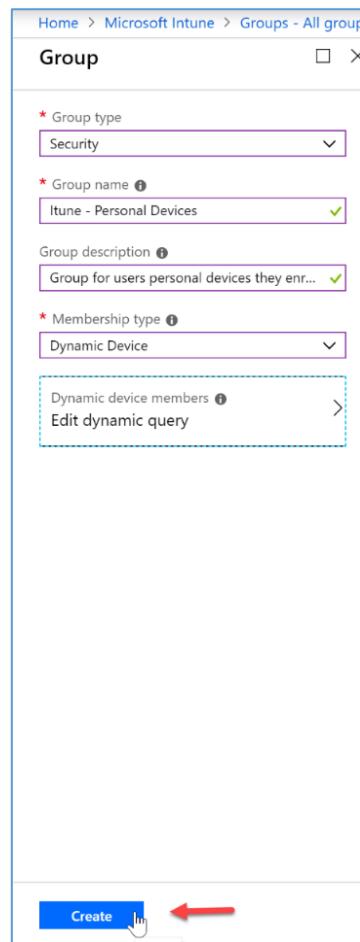
1. In the Intune blade, select **Groups**, and then select “**All Groups**” and click “**New Group**”:

The screenshot shows the Microsoft Intune Groups - All groups interface. On the left, there's a sidebar with navigation links: 'All groups' (selected), 'Deleted groups', 'Settings' (with 'General', 'Expiration', 'Naming policy'), 'Activity' (with 'Access reviews', 'Audit logs'), and 'Troubleshooting + Support' (with 'Troubleshoot', 'New support request'). The main area displays a table of groups with columns: NAME, OBJECT ID, GROUP TYPE, MEMBERSHIP TYPE, EMAIL, and SOURCE. The table lists 15 groups, mostly named 'AD Sync' followed by various suffixes like 'Admins', 'Browse', 'Operators', 'Passwor...', 'DnsAdmins', and 'DnsUpdateProxy'. Most groups are of type 'Security' and have 'Assigned' membership type, with sources ranging from 'Cloud' to 'Windows server AD'.

2. Give your group the required properties like type, name and description. We will want to add a dynamic membership rule. Our example below will contain all devices that a user selects as their Personal Device.

The screenshot shows the Microsoft Intune Group - Dynamic membership rules configuration page. On the left, under 'Group', the 'Group type' is set to 'Security', 'Group name' is 'Intune - Personal Devices', 'Group description' is 'Group for users personal devices they enr...', and 'Membership type' is 'Dynamic Device'. Below this, 'Dynamic device members' has an option 'Add dynamic query'. On the right, the 'Dynamic membership rules' section is open, showing a configuration for 'Add dynamic membership rule'. It includes a 'Simple rule' tab selected, a dropdown for 'Add devices where' set to 'deviceCategory', an 'Equals' operator, and a value 'personal device'. There's also a link to 'Learn more about creating an Advanced Rule'.

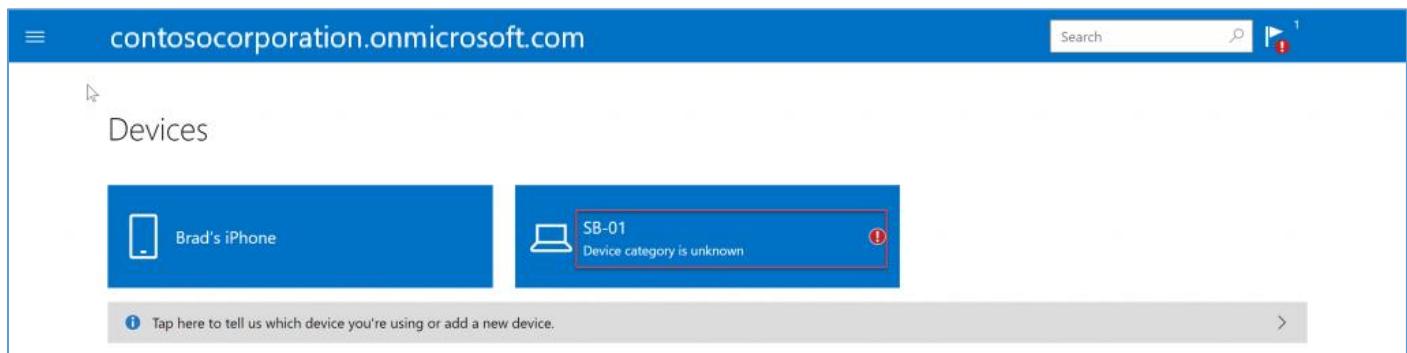
3. Once you have your new Group with the correct properties and query, click “**Create**”



5. Device enrollment experience

Windows Devices

When users enroll their Windows devices, they must select a category in the online Intune portal:



Clicking on the device will show them the outstanding alert and allow them to select a category:

SB-01

Microsoft Corporation - Surface Book

Category is unknown. Tap to select now.

Manufacturer
Microsoft Corporation

Operating System
Windows

Ownership Type
Personal
Learn More

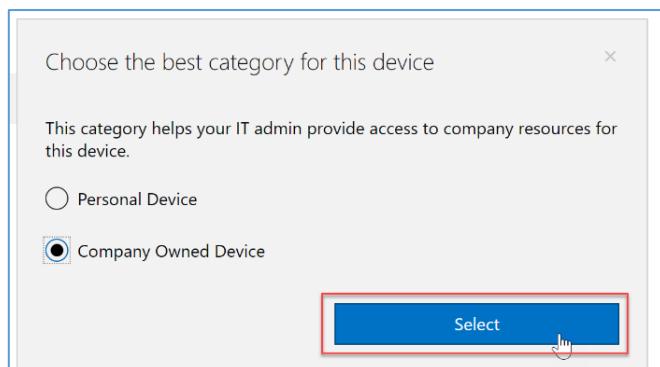
Status
Can access company resources
Last checked: 11/1/2018, 9:07:06 AM
Check status

Device Category
Unknown

In the top right of the portal they will also see a notification:

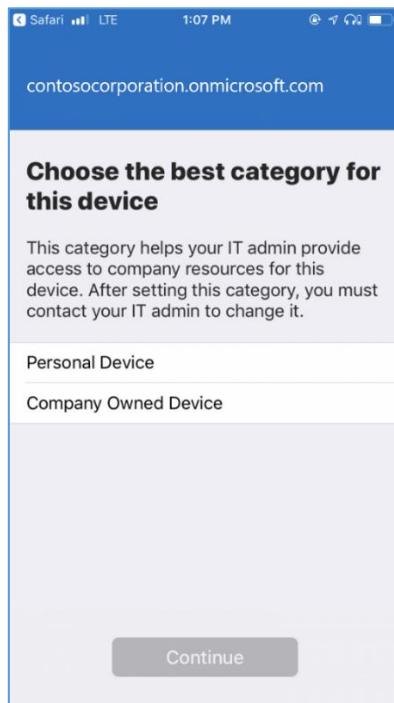


Here we see the two categories I set up for the users to select. Since this machine is a Company Owned Device, I will select that category. Behind the scenes, this device is added to that dynamic group and allows for a better management experience.



iOS Devices

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



6. Device Compliance Policies

Create a compliance policy

Compliance policies in Intune define the rules and settings that a device must comply with in order to be considered compliant by conditional access policies. In this walk-through, we'll create, and enforce, a policy that requires a user to enable password protection:

1. Navigate to the Azure portal and select the Intune blade
2. Select "**Device Compliance**" and then "**Policies**"

The screenshot shows the Microsoft Intune interface. On the left, there's a navigation sidebar with sections like Overview, Quick start, Manage (Device enrollment, Device compliance, Device configuration, Devices, Client apps, eBooks, Conditional access, On-premises access, Users, Groups, Roles, Software updates), Help and support (Help and support, Troubleshoot), and Help and support (Help and support). The 'Device compliance' link under 'Manage' is highlighted with a red box. The main content area is titled 'Device compliance - Policies'. It has sections for Manage (Policies, Notifications, Locations), Monitor (Device compliance, Devices without compliance po..., Setting compliance, Policy compliance, Audit logs, Windows health attestation rep..., Threat agent status), Setup (Compliance policy settings, Windows Defender ATP, Mobile Threat Defense, Partner device management), and Help and support (Help and support).

3. Click “**Create Policy**” and then I am going to create a policy that I will apply to my end users personal devices. This will be a policy for the group we created earlier.

The screenshot shows the 'Create Policy' dialog in Microsoft Intune. On the left, there's a list of existing policies with a 'Create Policy' button highlighted with a red box. The right panel contains fields for creating a new policy: Name (iOS - Personal Devices Policy L1), Description (Compliance policy for end user personal iOS devices), Platform (iOS), Settings (Configure), Actions for noncompliance (1 configured), and Scope (Tags) (0 scope(s) selected). A 'Create' button is at the bottom right of the dialog.

4. Once you have configured all of the Compliance settings, save the policy.

Create Policy

Name: iOS - Personal Devices Policy L1

Description: Compliance policy for end user personal iOS devices

Platform: iOS

Settings Configure

Actions for noncompliance: 1 configured

Scope (Tags): 0 scope(s) selected

iOS compliance policy

Select a category to configure settings.

- Email: 1 setting available
- Device Health: 1 of 2 settings configured
- Device Properties: 1 of 2 settings configured
- System Security: 10 settings available

System Security

Password

Require a password to unlock mobile devices.

Require	Not configured
Block	Not configured

Simple passwords: Not configured

Minimum password length: 6

Required password type: Alphanumeric

Number of non-alphanumeric characters in password: Not configured

Maximum minutes after screen lock before password is required: Immediately

Maximum minutes of inactivity until screen locks: Immediately

Password expiration (days): 30

Number of previous passwords to prevent reuse: 3

Device Security

Restricted apps:

App name: Not configured

App Bundle ID: Not configured

You have not restricted any apps.

OK

Assign a compliance policy

5. To assign this policy to devices or users. Click the **Assignments** item under Manage:

iOS - Personal Devices Policy L1

Device compliance policy

Overview

Manage

- Properties
- Assignments**
- Monitor

 - Device status
 - User status
 - Per-setting status

Delete

Assign profile to at least one group. Click assignments.

Profile type: iOS compliance policy

Platform supported: iOS

Groups assigned: 0

Groups excluded: 0

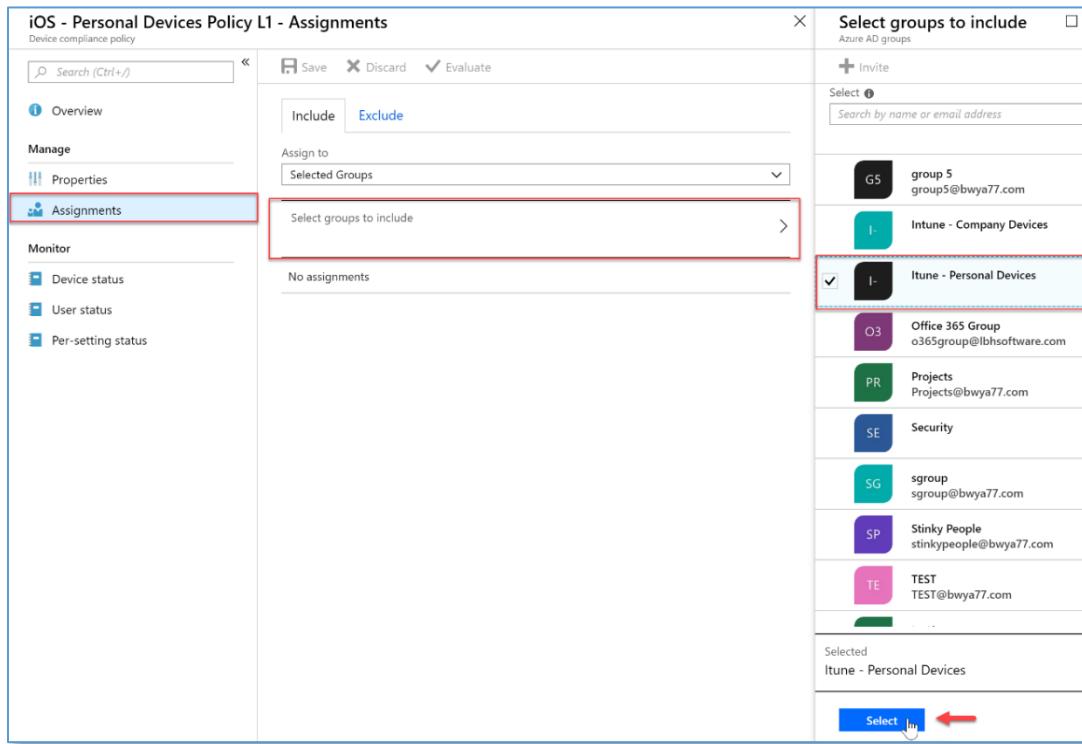
Policy assignment status — iOS devices

Succeeded	Error	Conflict
0	0	0

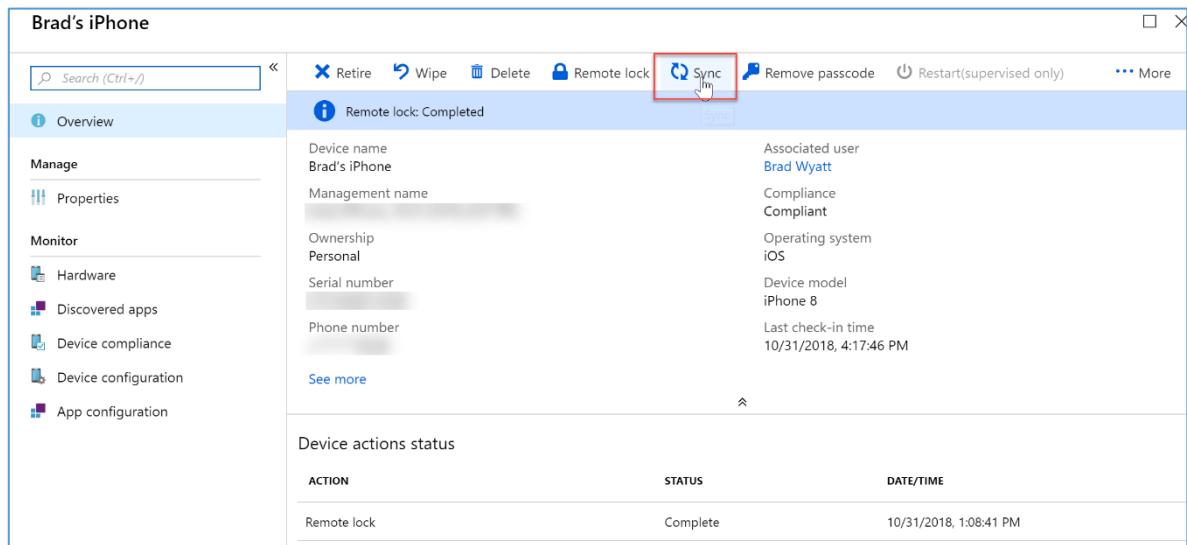
Assigned to non-iOS devices

0

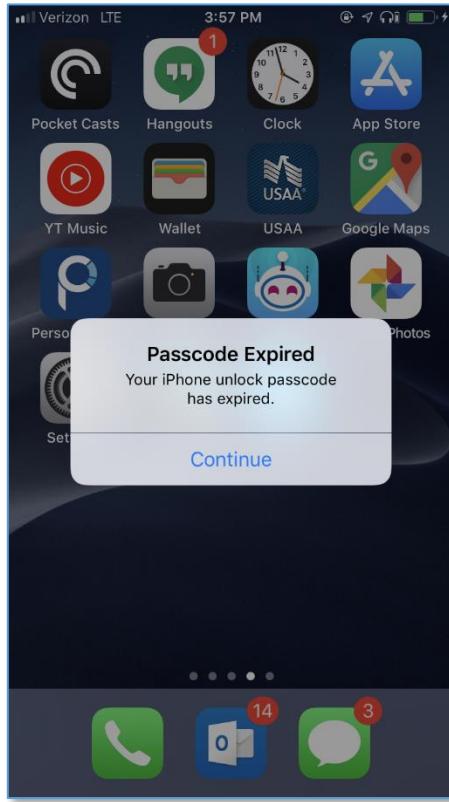
6. Once I click “**Select groups to include**” I can select my Intune – **Personal Devices** dynamic group and then **save**:



- As an added example, I want to make sure the policy goes into effect immediately on some device. I simply go to **All Devices**, find that device, and click **Sync**:



- If you set a passcode and the users current passcode does not match, they will be greeted with a password expiration notification. From there they can set their own passcode:



Configuration Policies

Commonly used to manage security settings and features on your devices, including access to company resources. In this walk-through, we'll create a policy for a Windows 10 device, that requires a complex password, sets a screen-lock time limit, and enables Windows Hello!:

Create a configuration policy

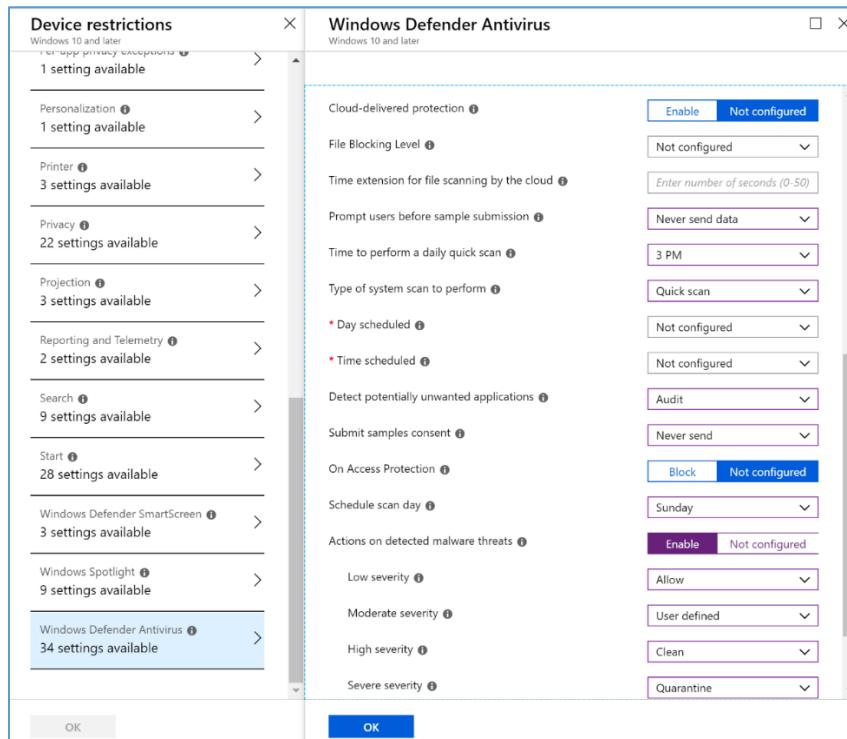
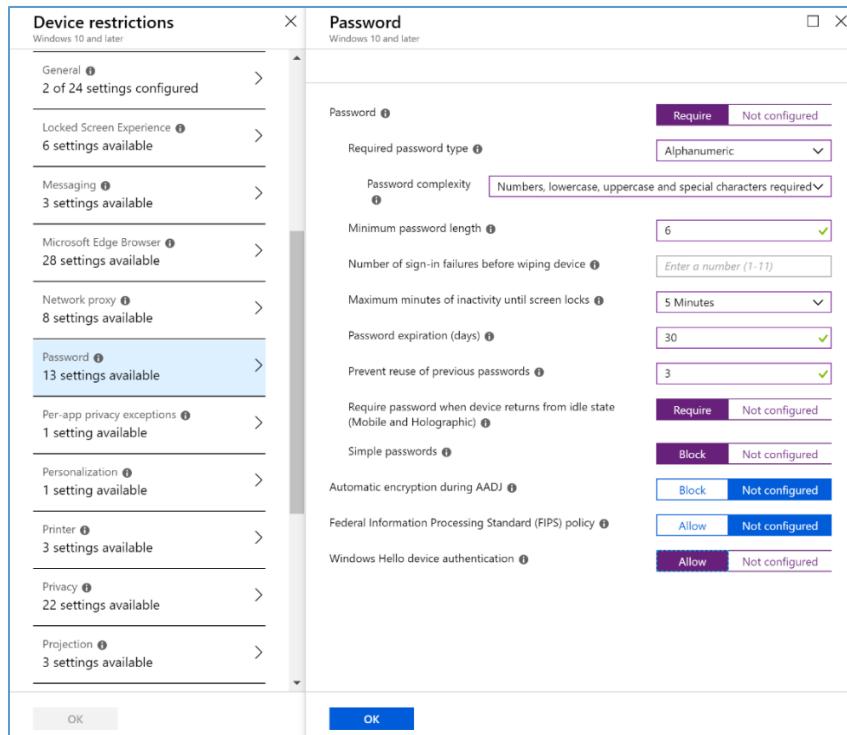
1. Expand the Intune blade and then select “**Device Configuration**”, “**Profiles**” and then click “**Create Profile**” to create a new device configuration profile:

The screenshot shows the Microsoft Intune interface. On the left, there's a navigation sidebar with various options like Overview, Quick start, Manage (Device enrollment, Device compliance, Device configuration), Devices, Client apps, eBooks, Conditional access, On-premises access, Users, Groups, Roles, Software updates, Help and support, and Troubleshoot. The 'Device configuration' link is highlighted with a red box. The main content area is titled 'Device configuration - Profiles'. It has a search bar, a 'Create profile' button, and filters for columns like Profile Name, Platform, Profile Type, Assigned, and Last modified. A table lists one profile: 'iOS Configuration Lockdown 1' for iOS, Device restrictions type, assigned, and last modified on 10/31/1. Below the table are sections for Monitor (Assignment status, Audit logs, Devices with restricted apps), Setup (Certification Authority, Telecom Expense Management), and Help and support.

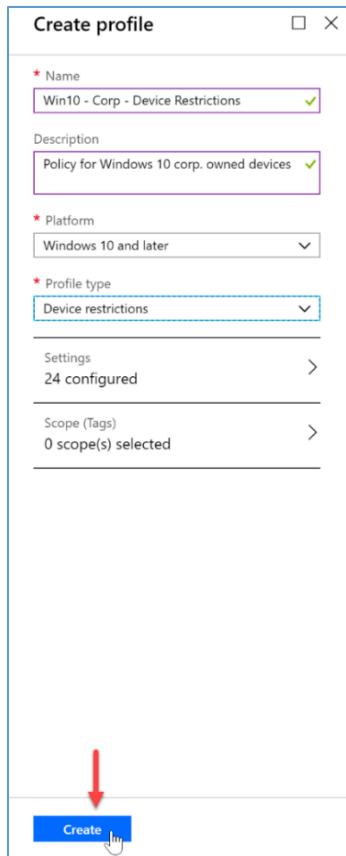
2. Enter the appropriate information regarding your profile/policy. In our example I will be making a policy that is applied to corporate owned Windows 10 devices:

The 'Create profile' dialog box is open. It has fields for Name (filled with 'Win10 - Corp - Device Restrictions'), Description (filled with 'Policy for Windows 10 corp. owned devices'), Platform (set to 'Windows 10 and later'), and Profile type (set to 'Device restrictions'). There are sections for Settings (with a 'Configure' button) and Scope (Tags) (showing '0 scope(s) selected').

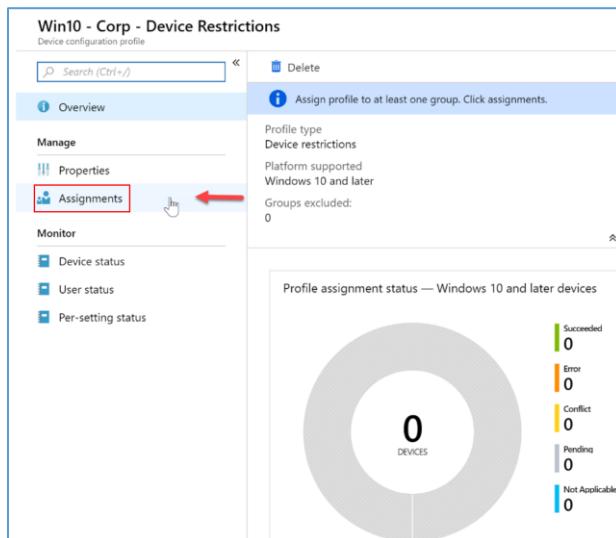
3. Select the required settings for this policy:



4. Once you have configured all of the settings, press “**Create**” under the create profile blade:



5. Next, click “**Assignments**” so we can assign this policy:



- From there I will select my Intune – **Company Devices** group to apply this policy to:

The screenshot shows the 'Win10 - Corp - Device Restrictions - Assignments' blade in the Intune portal. The 'Assignments' tab is selected. On the right, a modal window titled 'Select groups to include' is open, showing a list of Azure AD groups. The 'Intune - Company Devices' group is selected and highlighted with a red border. A blue arrow points from the 'Selected' section to a 'Select' button at the bottom.

Uninstall restricted applications policy iOS

In this example I will be configuring a restricted application and applying it to my iOS devices. Restricted applications are applications that users are not allowed to install and run. Users are not prevented from installing a prohibited app, but if they do so, this is reported to you.

- In the Intune blade select **Device configuration** > **Profiles**, then select the profile you want to edit, or create a new one. In our example, we will modify the profile applied to iOS

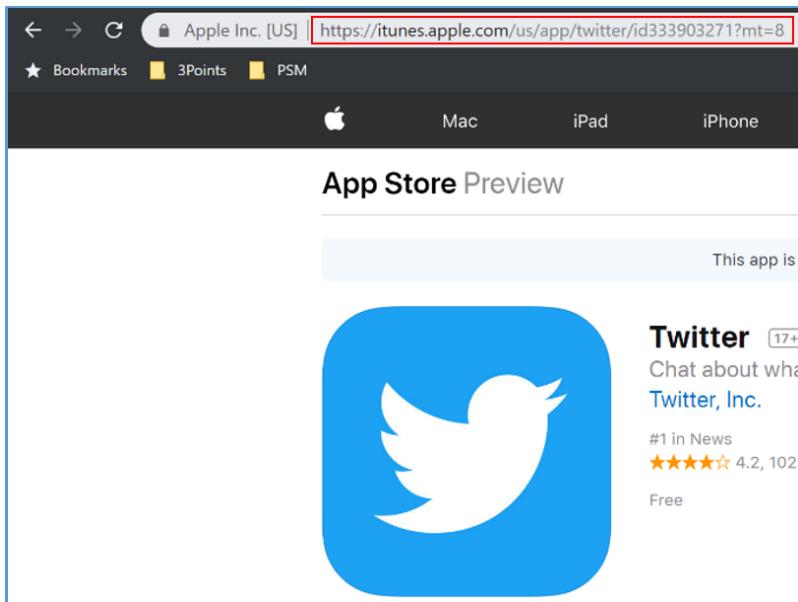
devices:

The screenshot shows the Microsoft Intune interface. In the top navigation bar, the path is Home > Microsoft Intune > Device configuration - Profiles > iOS Configuration Lockdown 1 - Properties > Device restrictions > Restricted Apps. On the left, there's a sidebar with Overview, Quick start, Manage (Device enrollment, Device compliance, Device configuration, Devices), and a search bar. The main area has a title 'Device configuration - Profiles' and a 'Create profile' button. Below it is a table with columns: PROFILE NAME, PLATFORM, PROFILE TYPE, ASSIGNED, and LAST. Two rows are visible: 'iOS Configuration Lockdown 1' (iOS, Device restrictions, Yes, 10/3) and 'Win10 - Corp - Device Restrictions' (Windows 10 a..., Device restrictions, Yes, 11/01). A red box highlights the 'Device configuration' link in the sidebar.

2. In the profile select **Settings** > **Restricted Apps**, and then under type of restricted apps list select **Prohibited Apps**.

This screenshot shows the 'Device restrictions' settings for an iOS profile. The left pane shows general profile details: Name (iOS Configuration Lockdown 1), Description, Platform (iOS), Profile type (Device restrictions), Settings (10 configured), and Scope (Tags) (0 scope(s) selected). The right pane lists various settings categories like General, Password, and Built-in Apps, each with its own configuration options. A red box highlights the 'Settings' section in the left pane. The 'Restricted Apps' section is expanded, showing a table with columns: APP URL, APP BUNDLE ID, APP NAME, and PUBLISHER. A dropdown menu indicates the type is set to 'Prohibited apps'. A red box highlights this dropdown. The table currently shows 'No apps'.

3. Open a tab in a browser, look up the application you want to block, and Copy the itunes store URL:



4. Back in the Azure Portal, paste the link into **App URL** and then click “**Add**”:

APP URL	APP BUNDLE ID	APP NAME	PUBLISHER	
https://itunes.apple.com/us/app/twitter/id333903271?mt=8	e.g. com.apple.Twitter	Twitter	Not configured	Add

5. When you have finished your apps list, click **OK** at the bottom and then save your policy.

- The company portal will display a message that I must uninstall the Twitter application since it is now a disallowed application:



Software Update Policies

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

Create a Windows software update policy

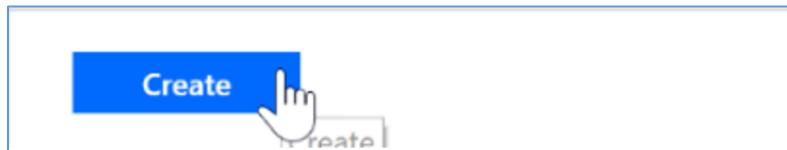
- From the Intune blade, click **Software Updates** > **Windows 10 Update Rings**, and **Create**

The screenshot shows the Microsoft Intune interface for managing software updates. On the left, the navigation pane includes links for Overview, Quick start, Manage (Device enrollment, Device compliance, Device configuration, Devices, Client apps, eBooks, Conditional access, On-premises access, Users, Groups, Roles, Software updates), Help and support (Help and support, Troubleshoot), and a Home link. The 'Software updates' link is highlighted with a red box. The main content area is titled 'Software updates - Windows 10 Update Rings' and shows a table with one row: 'Windows 10 Update Rings'. A red box highlights the '+ Create' button in the top right corner of the table header. The table has columns for NAME, FEATURE DEFERRED, QUALITY DEFERRED, and FEATURE. A message at the bottom states 'There are no Windows 10 Update Rings to show.'

2. Give your policy a name and description. In our example, I'm putting my devices on the Windows Insider update ring. They will also get Microsoft product updates, and drivers. You can configure a deferral period which may be recommended for a production environment. In the User Experience Settings administrators can configure maintenance hours, in my environment I am auto installing the updates anywhere from 3PM to 11PM:

The screenshot shows two overlapping windows. The top window is titled 'Create Update Ring' and contains fields for 'Name' (Company Devices - Windows 10) and 'Description' (Company devices on Windows Insider). It also has sections for 'Settings' (Configure) and 'Scope (Tags)' (0 scope(s) selected). The bottom window is titled 'Settings' and is for 'Windows 10 and later'. It includes sections for 'Update settings' (Servicing channel: Release Windows Insider, options for Microsoft product updates, Windows drivers, Quality update deferral period, Feature update deferral period, and Set feature update uninstall period), 'User experience settings' (Automatic update behavior: Auto install at maintenance time, Active hours start: 3 PM, Active hours end: 11 PM, Restart checks: Allow, Require user's approval to restart outside of work hours: Required, Remind user prior to required auto-restart with dismissible reminder (hours): 4, and Remind user prior to required auto-restart with permanent reminder (minutes): 15), and a 'Create' button.

- Once you have the policy settings configured to your needs you can add scope tags and then press "**Create**" to create the policy.



- Once the policy has been created, click "**Assignments**" to assign the policy to devices or groups.

Company Devices - Windows 10
Windows 10 Update Ring

Overview

Manage

- Properties
- Assignments** (highlighted with a red arrow)
- Monitor
- Device status
- User status

Created: 11/09/18, 8:21:01 AM **Feature:** Running
Last Modified: 11/09/18, 8:21:01 AM **Quality:** Running
Groups assigned: 0

Profile assignment status — Windows 10 and later devices

Succeeded: 0 Error: 0 Conflict: 0

5. You can apply to all devices using the “Assign to” drop down, or in my case I will apply it to one of my dynamic groups I created earlier by clicking the “Select groups to include” and then selecting my “Intune – Company Devices” group:

Company Devices - Windows 10 - Assignments
Windows 10 Update Ring

Overview

Manage

- Properties
- Assignments**
- Monitor
- Device status
- User status

Include **Exclude**

Assign to: Selected Groups

Select groups to include

No assignments

Select groups to include

Azure AD groups

+ Invite

Select **I**

Search by name or email address

- G5 group 5 group5@bwya77.com
- I** Intune - Company Devices (highlighted with a red box)
- I Itune - Personal Devices
- O3 Office 365 Group o365group@lbhsoftware.com
- PR Projects Projects@bwya77.com
- SE Security
- SG sgroup sgroup@bwya77.com
- SP Stinky People stinkypeople@bwya77.com
- TE TEST TEST@bwya77.com
-

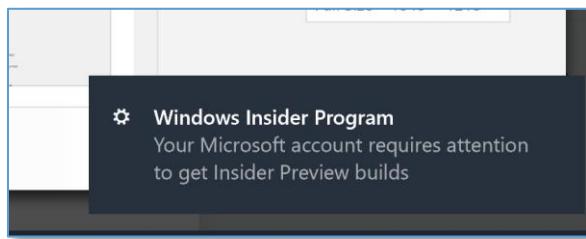
Selected: Intune - Company Devices

Select

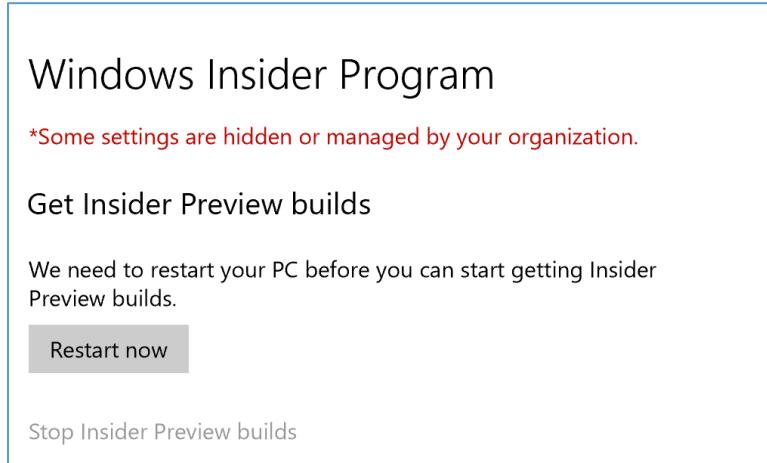
6. In my Group settings I can see that my windows machine SB-01 is a member of that group so I can be sure that the policy will be applied to that machine:

The screenshot shows the 'Intune - Company Devices - Members' page. On the left, there's a sidebar with sections like 'Overview', 'Manage' (which is currently selected), 'Properties', 'Owners', 'Group memberships', 'Applications', 'Licenses', 'Azure resources', 'Dynamic membership rules', 'Activity' (with 'Access reviews' and 'Audit logs'), and 'Troubleshooting + Support' (with 'Troubleshoot' and 'New support request'). The main area has a header with '+ Add members' and a 'Refresh' button. A table below lists a single member: 'NAME' (SB-01) and 'TYPE' (Device). The entire row for SB-01 is highlighted with a dashed blue border.

7. A few minutes later, that machine gets a toast notification regarding my build change:



8. In the Settings application on the device I can see that my computer is pending a reboot. After the reboot I will be on the correct build:



Create an iOS software update policy

1. Select the Intune blade > **Software Updates** > **Update Policies for iOS**, and then "Create"

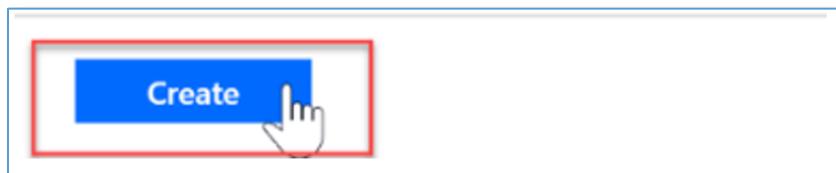
The screenshot shows the 'Software updates - Update policies for iOS' blade in Microsoft Intune. On the left, the 'Manage' sidebar has 'Software updates' selected. The main area shows a list of update policies for iOS, with a red box around the 'Create' button. The table columns are 'NAME' and 'RESTRICTED DAYS'. A message at the bottom states: 'There are no iOS update policies to display.'

- Give the policy a name and a description and then configure your settings. In my example I am disabling users from updating to the newest iOS during the work week and during work hours. iOS updates are also deferred for 2 weeks:

The screenshot shows two windows side-by-side. On the left is the 'Create update policy' blade with a title bar 'Create update policy'. It has fields for 'Name' (Company Policy - iOS) and 'Description' (Enter a description...). Below these are sections for 'Settings' (Configure) and 'Scope (Tags)' (0 scope(s) selected). At the bottom are 'Create' and 'OK' buttons, with 'OK' highlighted by a red box.

On the right is a settings overlay titled 'Settings' with a subtitle 'iOS'. It contains a descriptive text about update profiles, a 'Learn More' link, and a section for 'Select times to prevent update installations'. This section includes dropdowns for 'Days' (Mon,Tue,Wed,Thu,Fri), 'Time zone' (UTC-6), 'Start time' (8 AM), and 'End time' (5 PM). Below this is a section for 'End user experience settings' with a note about delaying visibility of software updates for 14 days. The 'OK' button at the bottom of the overlay is also highlighted by a red box.

- Once you have your policy set to your liking, press the **Create** bottom of the blade:



4. Click "**Assignment**" to assign your policy to groups or devices.

Company Policy - iOS
iOS Updates

Overview

Manage

Properties

Assignments (highlighted with a red box)

Delete

Assign this iOS update policy to at least one group. Click Assignments

Created: 11/09/18, 9:45:58 AM **Last Modified:** 11/09/18, 9:45:58 AM

Groups assigned: 0 **Days Delayed:** 14

RESTRICTED DAYS: Mon, Tue, Wed, Thu, Fri

TIME ZONE: UTC-6

START TIME: 8:00 AM

END TIME: 5:00 PM

UPDATES VISIBILITY DELAY DAYS: 14

In my example I will apply this policy to Company Devices only:

Company Policy - iOS - Assignments
iOS Updates

Overview

Manage

Properties

Assignments

Save **Discard** **Evaluate**

Include **Exclude**

Assign to: Selected Groups

Select groups to include

No assignments

Select groups to include (right pane):

- G5 group 5 group5@bwya77.com
- I- Intune - Company Devices (highlighted with a red box)
- I- Intune - Personal Devices
- O3 Office 365 Group o365group@lbhsoftware.com
- PR Projects Projects@bwya77.com
- SE Security
- SG sgroup sgroup@bwya77.com
- SP Stinky People stinkypeople@bwya77.com
- TE TEST TEST@bwya77.com

Selected: Intune - Company Devices

Select

5. You will now see your newly created policy:

The screenshot shows a table with columns: NAME, RESTRICTED DAYS, TIME ZONE, START TIME, END TIME, and ASSIGNED. A search bar at the top is labeled 'Search by name'. The table has one row for 'Company Policy - iOS'.

NAME	RESTRICTED DAYS	TIME ZONE	START TIME	END TIME	ASSIGNED
Company Policy - iOS	Mon, Tue, Wed, Thu, Fri	UTC-6	8:00 AM	5:00 PM	Yes

7. Device Enrollment

Enable automatic enrollment for Windows 10

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

1. In the Azure Portal select **Azure Active Directory** and then click "**Mobility (MDM and MAM)**" and select "**Microsoft Intune**":

The screenshot shows the Azure portal navigation menu on the left with 'Azure Active Directory' selected. The main content area shows the 'Mobility (MDM and MAM)' section with 'Microsoft Intune' listed under it. Both 'Mobility (MDM and MAM)' and 'Microsoft Intune' are highlighted with red boxes.

2. 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.

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

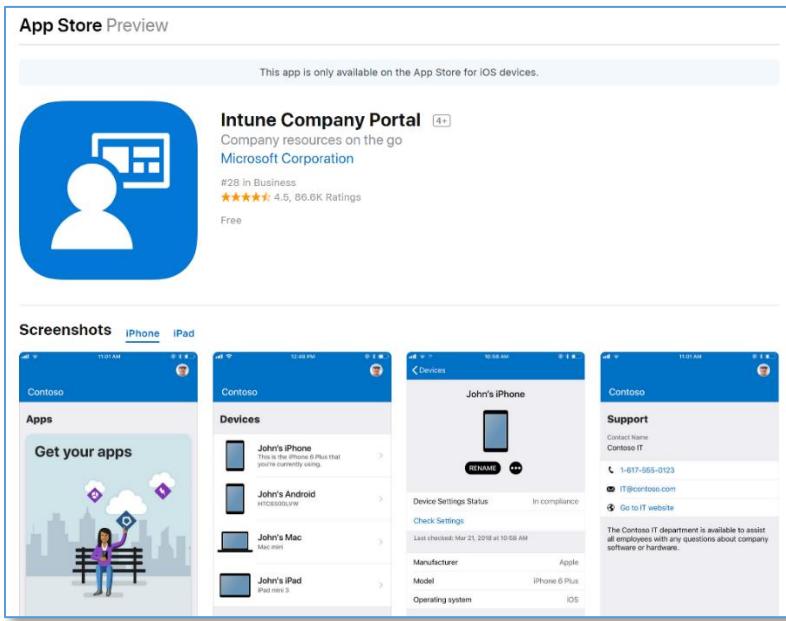
The screenshot shows the 'Configure' page for Microsoft Intune. At the top, there's a breadcrumb navigation: Home > bwya77 - Mobility (MDM and MAM) > Configure. Below the title 'Configure Microsoft Intune', there are two main sections: 'MDM user scope' and 'MAM User scope'. In the 'MDM user scope' section, three buttons are shown: 'None', 'Some', and 'All', with 'All' being the selected option and highlighted with a red box. A red arrow points to the 'Save' button at the top left of this section. Below the MDM section, there are four URL fields: 'MDM terms of use URL' (https://portal.manage.microsoft.com/TermsofUse.aspx), 'MDM discovery URL' (https://enrollment.manage.microsoft.com/enrollmentserver/discover...), 'MDM compliance URL' (https://portal.manage.microsoft.com/?portalAction=Compliance), and a 'Restore default MDM URLs' link. In the 'MAM User scope' section, three buttons are shown: 'None', 'Some', and 'All', with 'None' being the selected option. There are four corresponding URL fields below it: 'MAM Terms of use URL' (empty), 'MAM Discovery URL' (https://wip.mam.manage.microsoft.com/Enroll), 'MAM Compliance URL' (empty), and a 'Restore default MAM URLs' link.

Important:

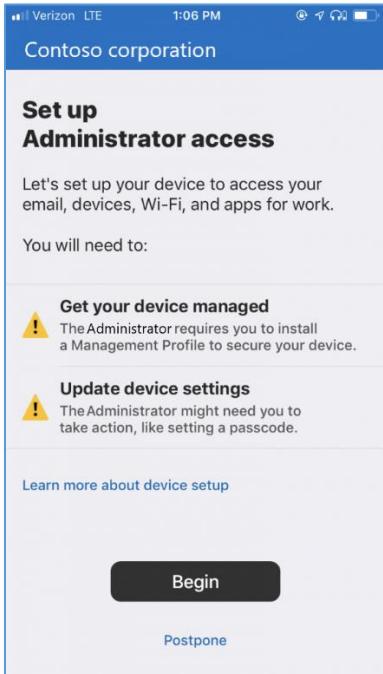
If *both* InTune Mobile Application Management (MAM) user scope and automatic MDM enrollment (MDM user scope) are enabled for a group, MAM takes precedence. In that case, only MAM is applicable to users in that group when they workplace join personal device. When MAM applies, devices are not automatically MDM enrolled.

Enable automatic enrollment for iOS

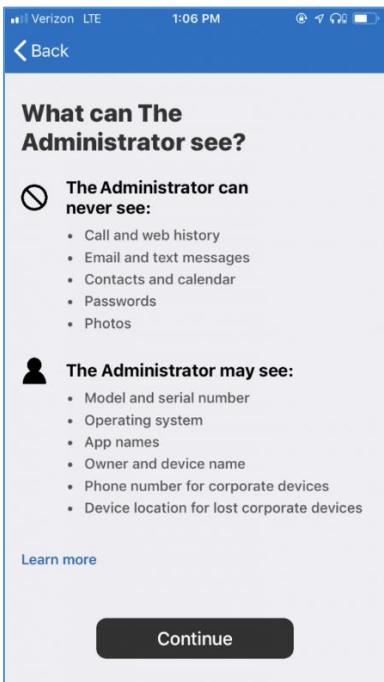
1. Users must download and install the Company Portal from the iOS App Store



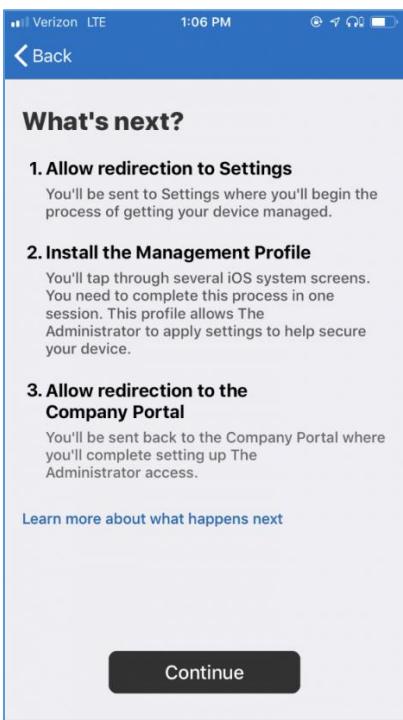
2. Once they launch the application and sign in they can begin to Intune enrollment process:



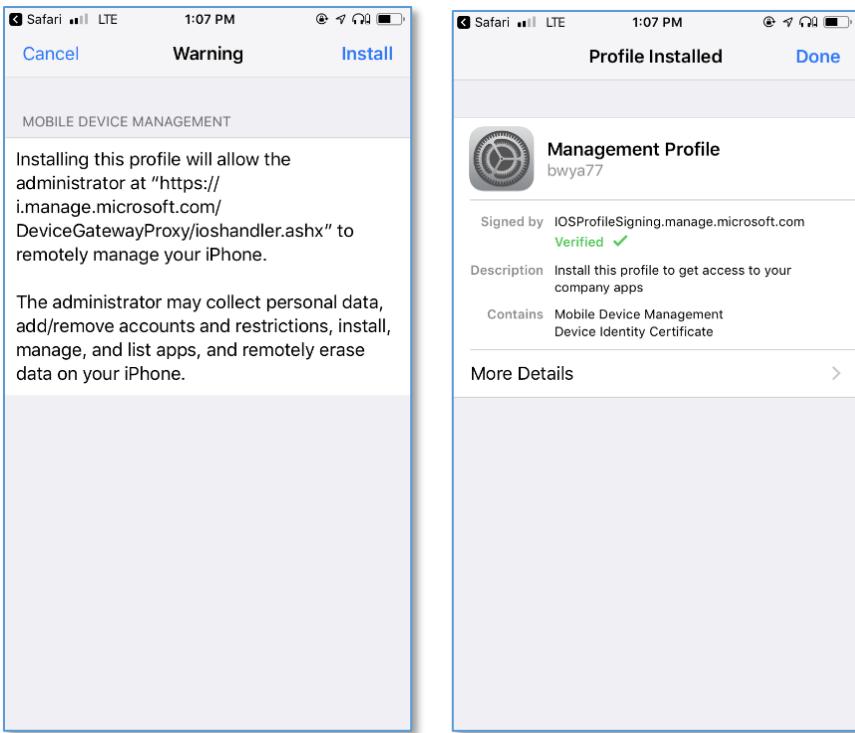
3. The application will show the end user the permissions the IT Administrator will have on the device:



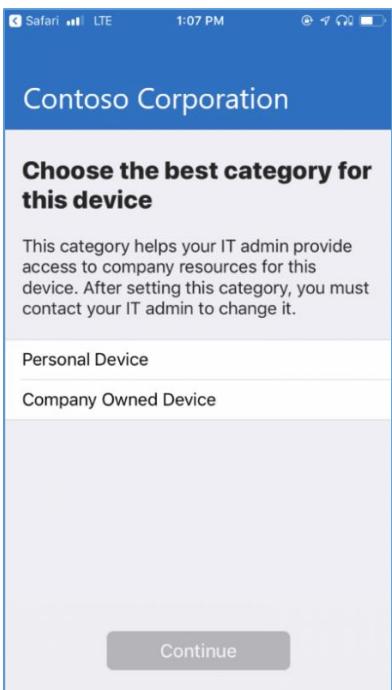
4. They will then be shown the step by step instructions that the application will take to enroll the device:



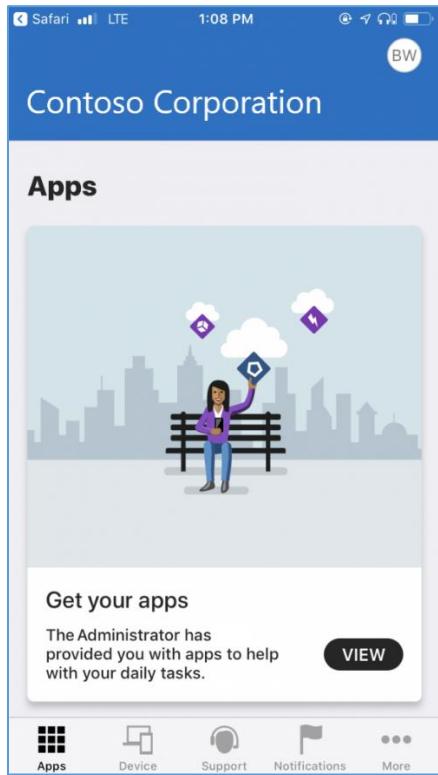
5. An MDM iOS Profile will be installed on the device:



6. And finally, the user will select a category (set up earlier) to put their device under. This allows for a better administrator management experience:



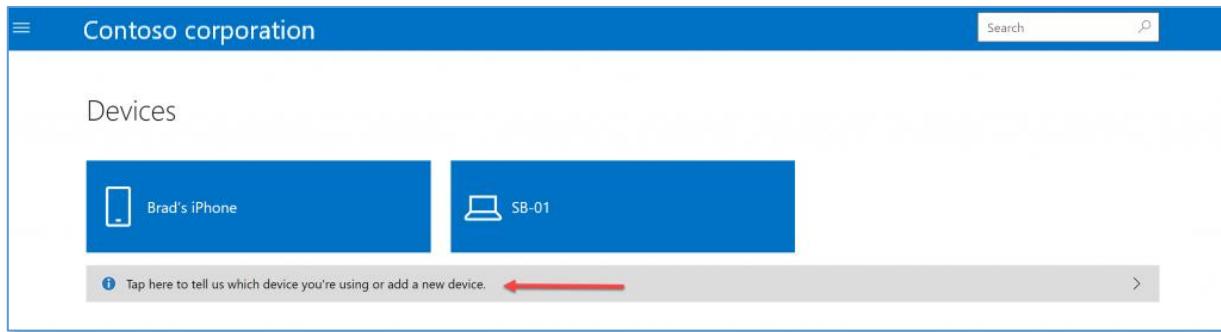
The Company Portal will show the end users any available apps you have granted them, all of their Intune devices, support options we set up previously and notifications:



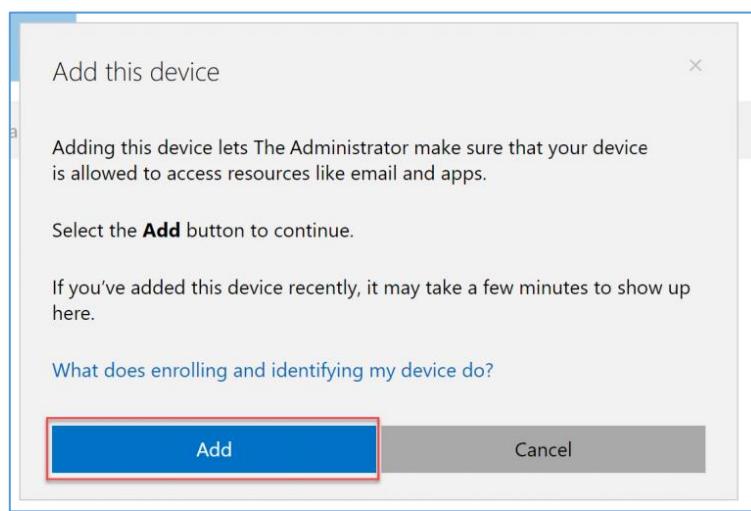
Enrolling Windows devices manually

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

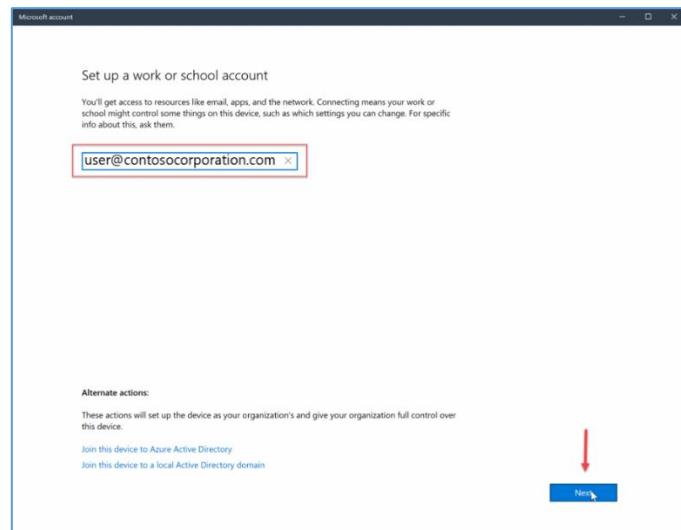
1. Navigate to the online Company Portal at <https://portal.manage.microsoft.com>
2. Once the user signs into the Company Portal they can add a device under Devices



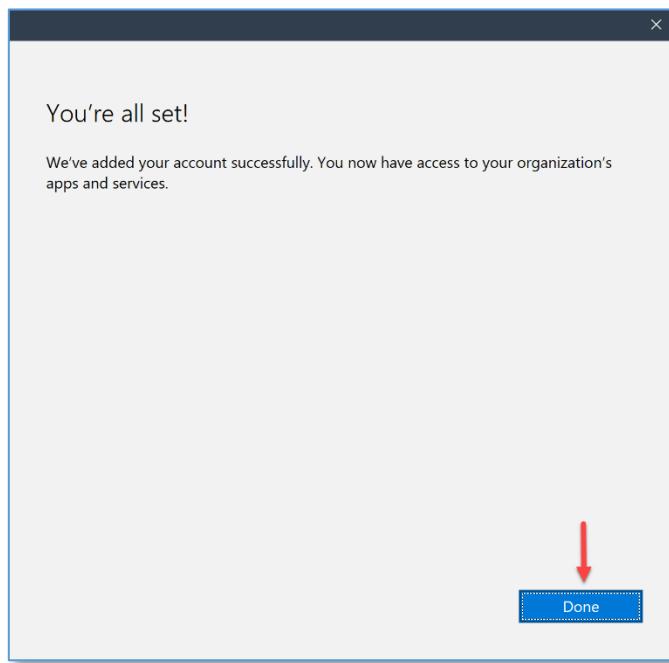
3. Click "Add"



4. Have them sign in and then press Next:

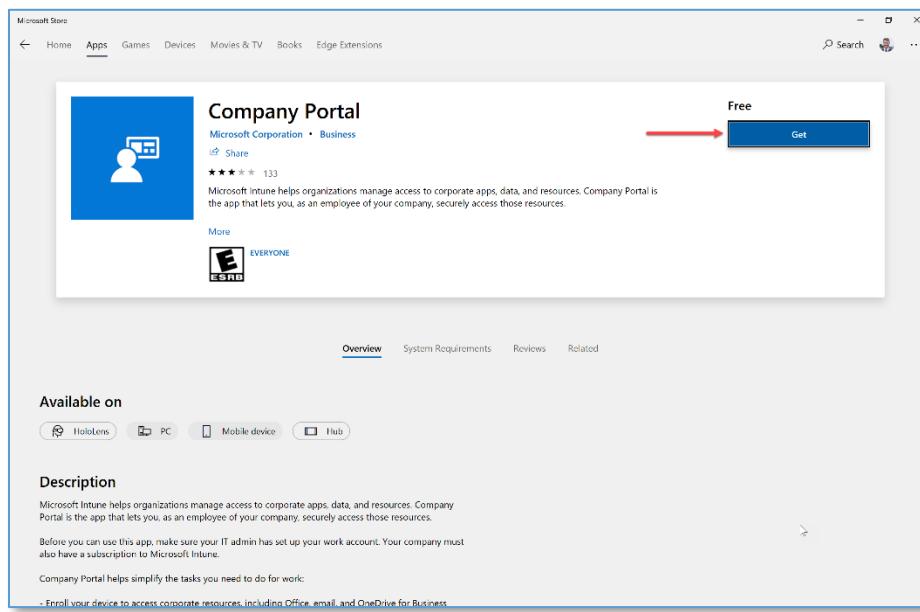


5. The user will be prompted to enter their account password and then press "**Sign In**". Once complete they will be prompted with a successful message.

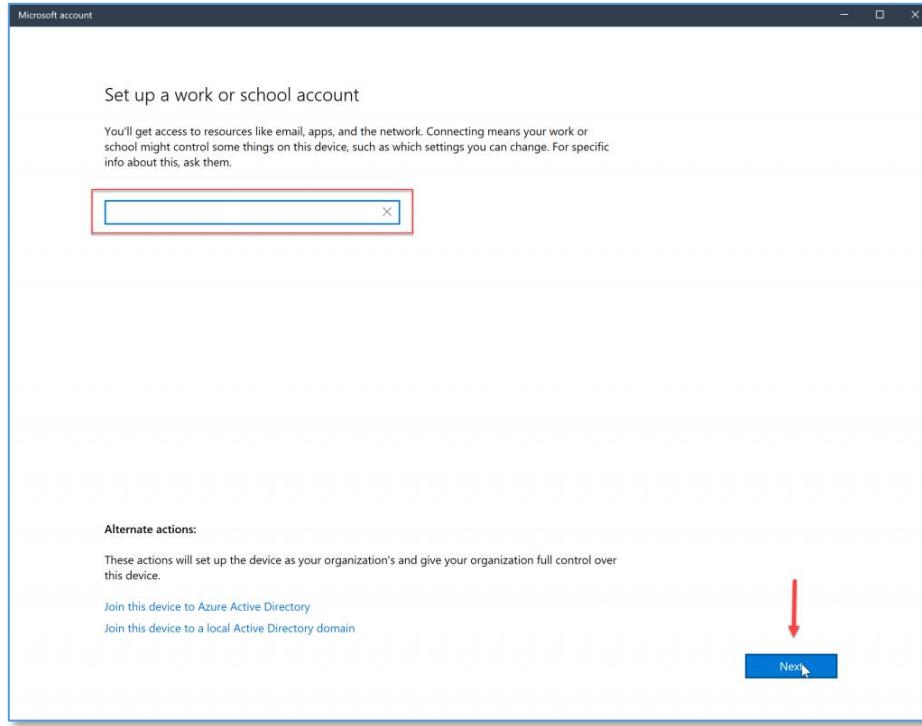


Microsoft Store App

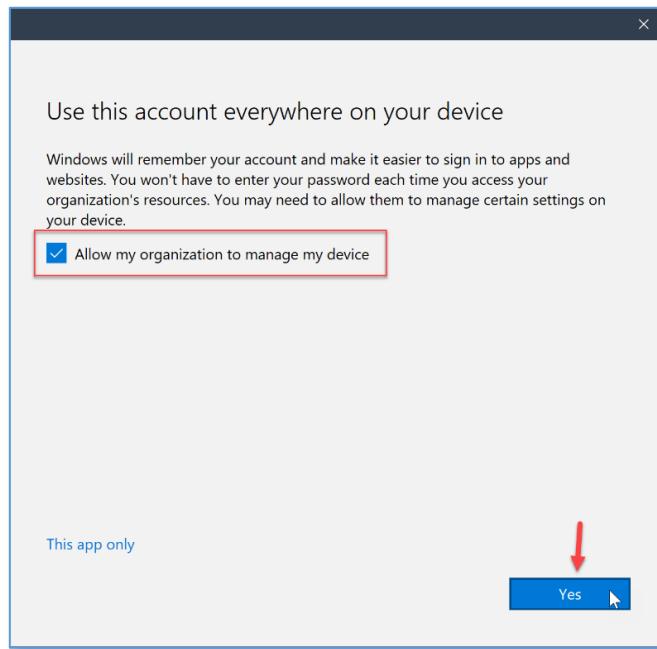
Have your users download and install the Company Portal application from the Microsoft Store:



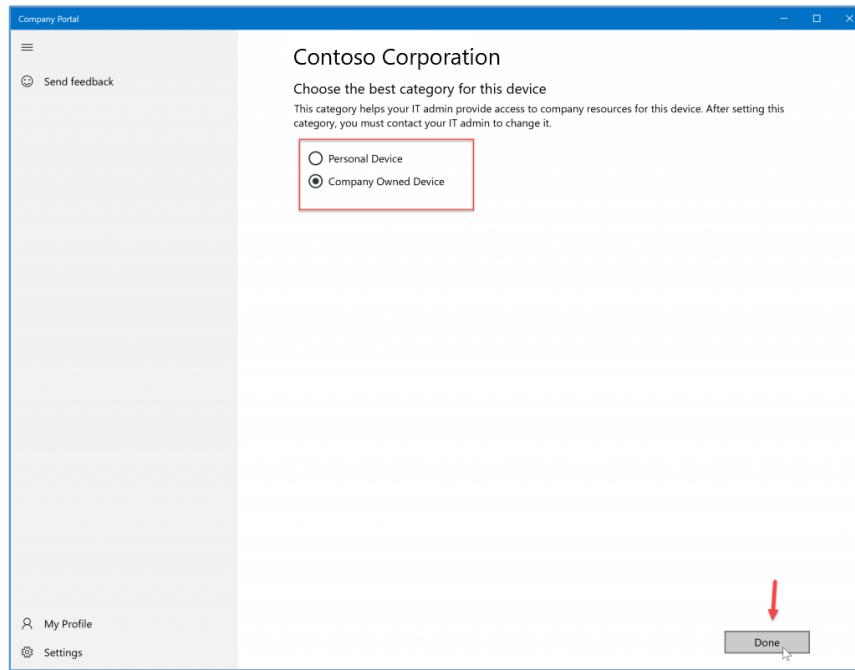
They will be prompted to sign in, then click **Next**:



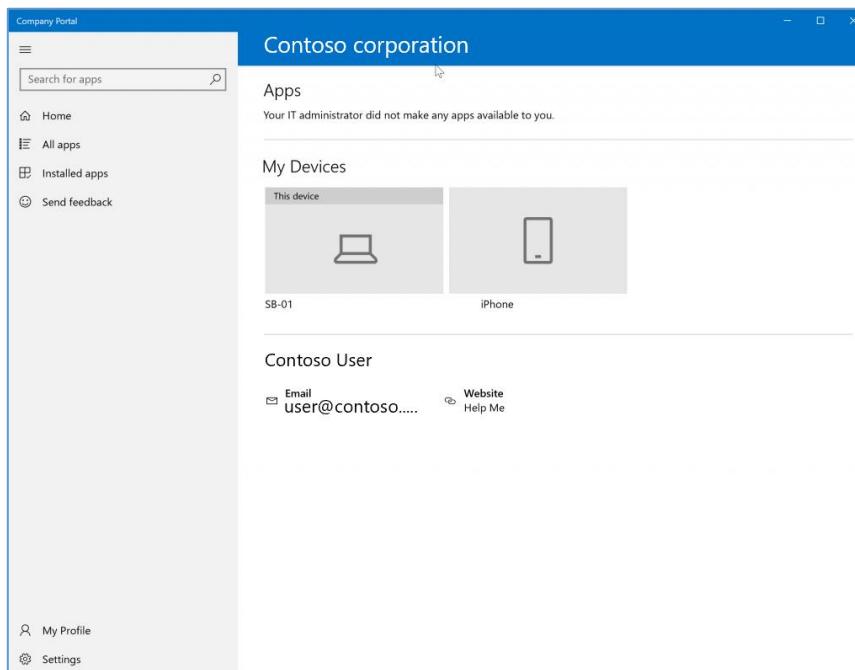
Check "Allow my organization to manage my device" and then click Yes



Finally, the Company Portal will prompt them to select a device category that we set up earlier



The Company Portal will now show the newly enrolled device:



Deploy Client Apps to Managed Intune Devices

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

1. Expand the Intune blade in the Azure portal, go to “**Client Apps**”, “**Apps**” and then select “**Add**”

NAME	TYPE	STATUS	ASSIGNED
Office 365	Office 365 ProPlus Suite (Windows 10)		Yes

2. In my example, I'm deploying Office 365 ProPlus, so I select Windows 10 under Office 365 Suite:

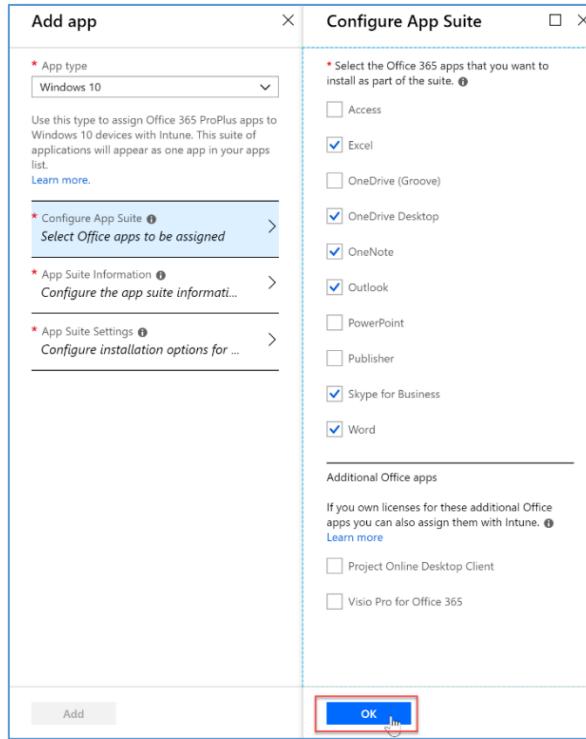
App type
Windows 10

Store app
Android
iOS
Windows Phone 8.1
Windows

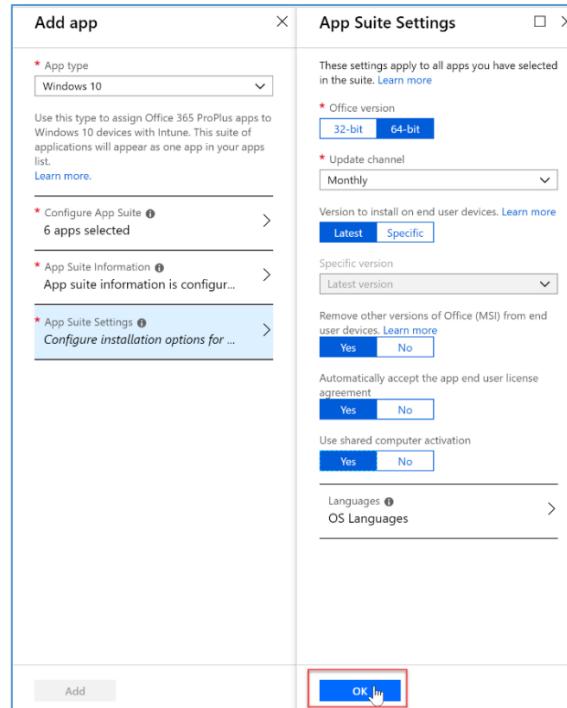
Office 365 Suite
Windows 10
macOS

Other
Web link
Built-In app
Line-of-business app
Windows app (Win32) - preview

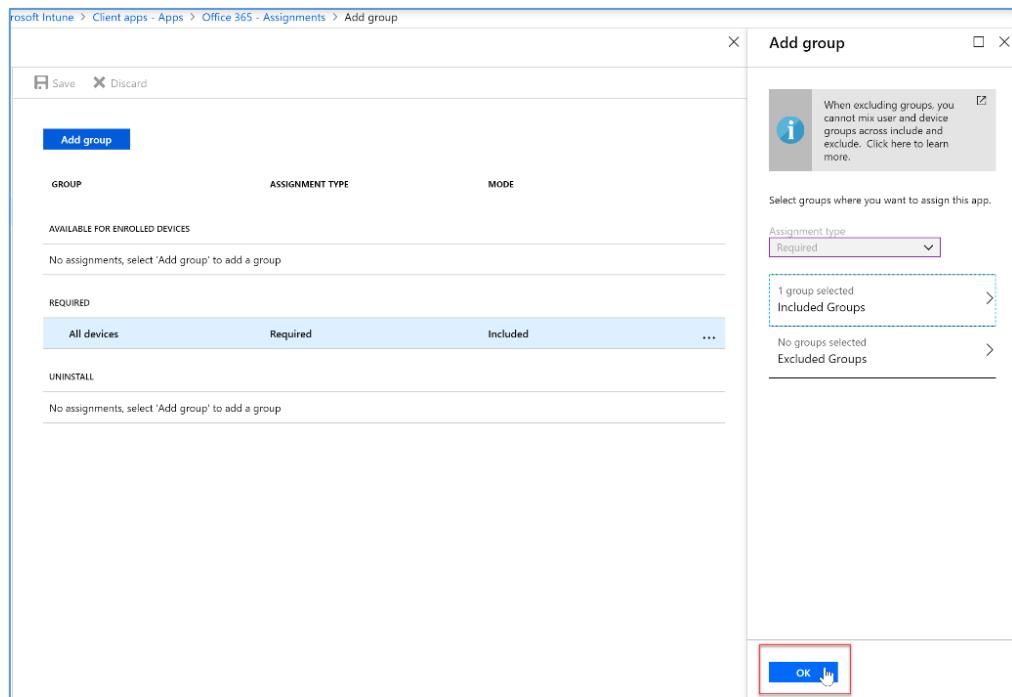
3. Configure the app settings to fit your company needs:



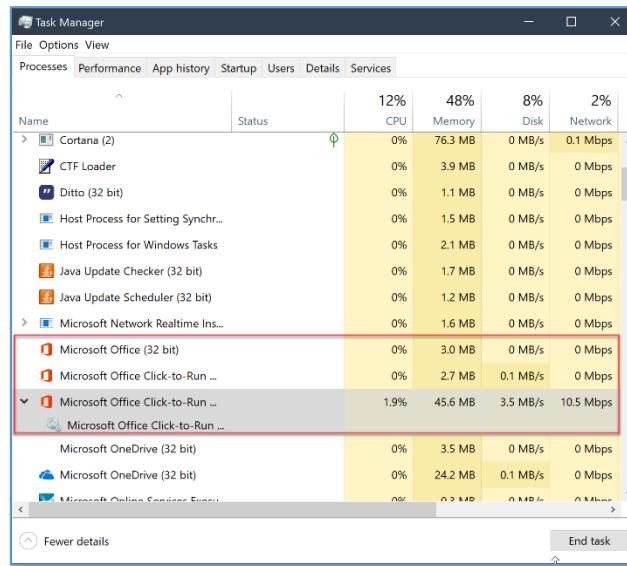
4. We can even configure the update options, EULA, and more:



5. I will make this application required for all users in my assignments setting:

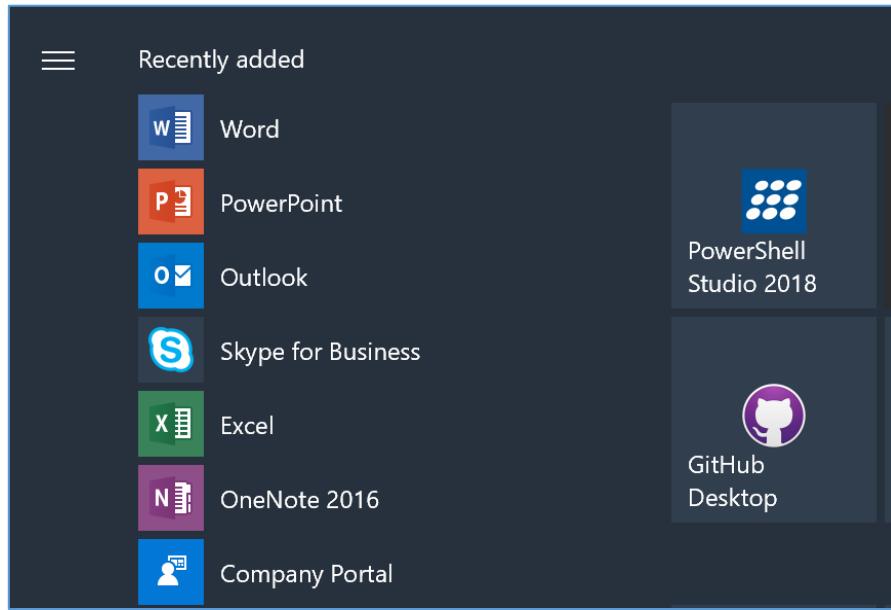


6. After a little bit I can see that Office is installing on my end user machine in Task Manager:

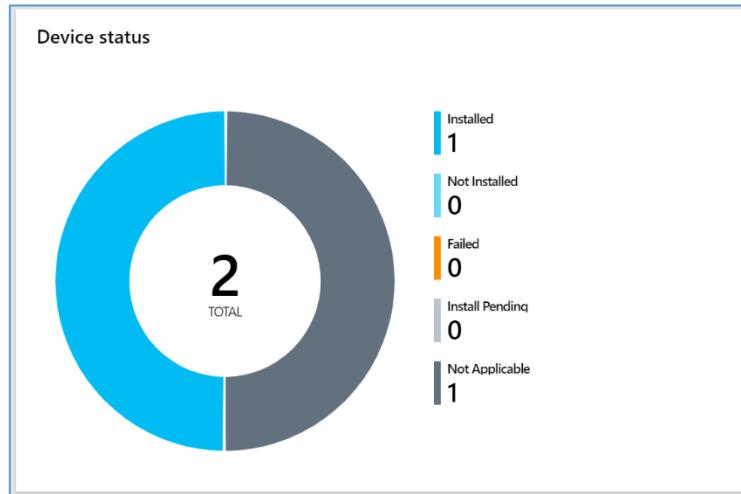


- If I had not made the app required and just made it available, end users could choose to install it from the Company Portal:

- Once the install is complete, I can check the start menu to see all of my newly installed applications:



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



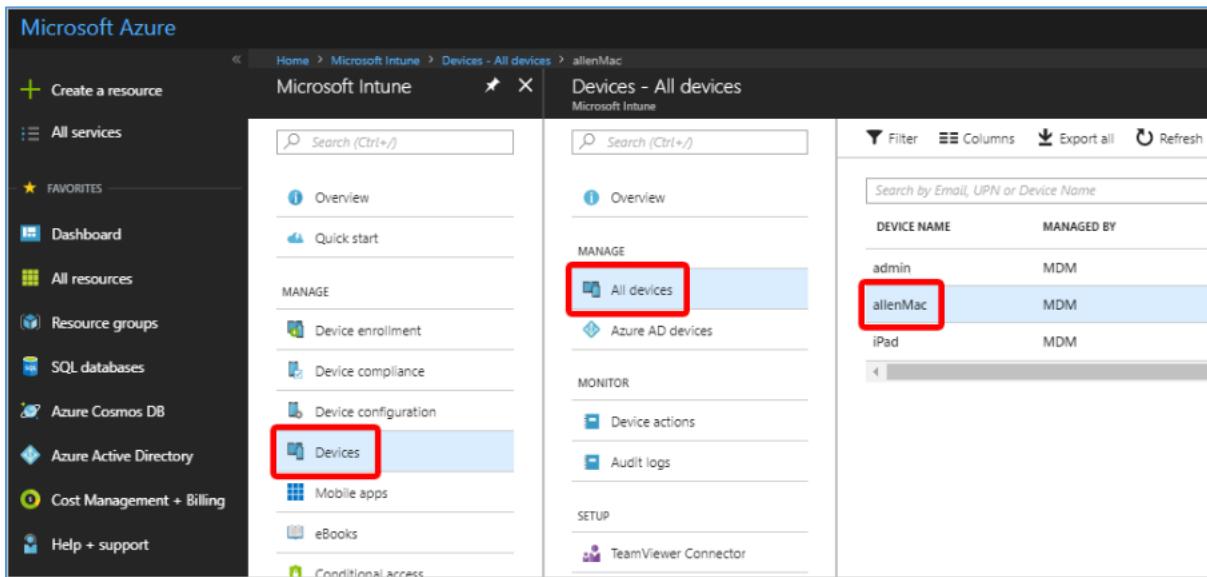
8. Device Actions

Intune also allows you to [remotely manage](#) many aspects of a users device. Using remote actions from the Intune portal, you can restart devices, reset passcodes, locate lost or stolen devices, and more.

Remotely erase data from a device

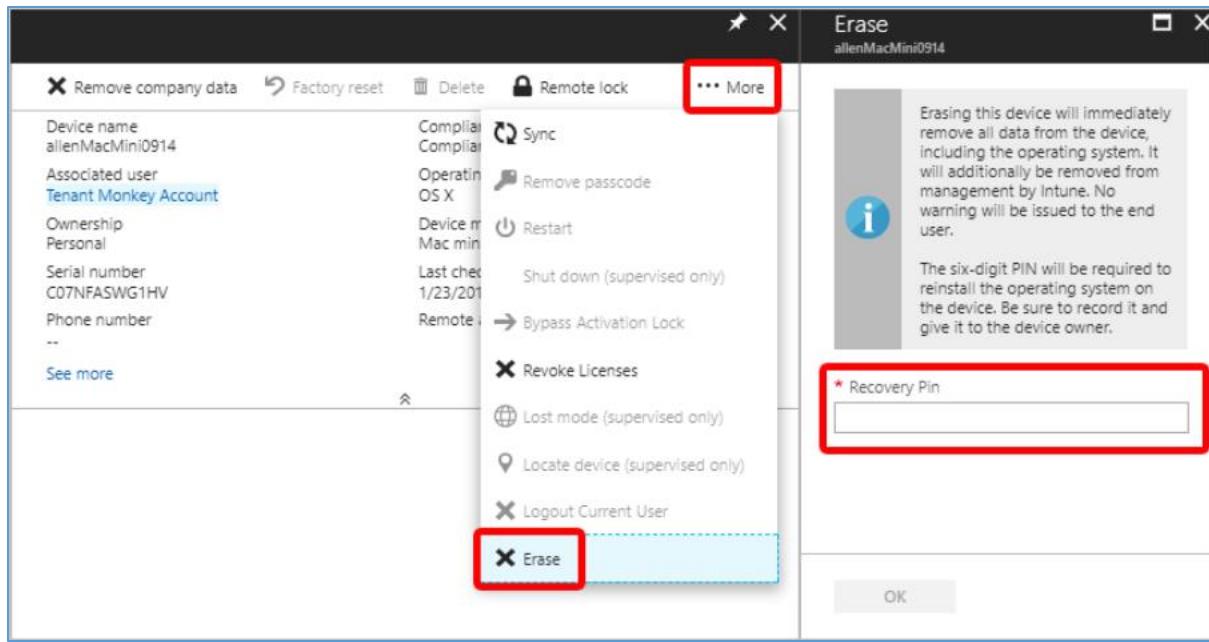
In the following example, we'll force a stolen macOS device to erase it's data and operating system. Further, we'll secure it so that a 6-digit PIN must be entered, before the OS may be re-installed:

1. In **Intune** in the Azure portal, click **Devices > All devices** and select the device to erase. In our example, it is a macOS device called "alienMac":



The screenshot shows the Microsoft Azure Intune portal. On the left, there's a sidebar with various service links like Dashboard, All resources, Resource groups, SQL databases, etc. Below that is a 'FAVORITES' section with links to Azure Active Directory, Cost Management + Billing, and Help + support. The main area has a search bar at the top. Under 'MANAGE', there are links for Overview, Quick start, Device enrollment, Device compliance, Device configuration, Devices (which is highlighted with a red box), Azure AD devices, and Mobile apps. Under 'MONITOR', there are links for Device actions and Audit logs. Under 'SETUP', there's a link for TeamViewer Connector. The right side shows a table titled 'Devices - All devices' with columns for DEVICE NAME and MANAGED BY. It lists three devices: admin (MDM), alienMac (MDM, highlighted with a red box), and iPad (MDM). A 'Filter' button and a 'Refresh' button are at the top of the table.

2. Click **More > Erase** > and provide a 6-digit number as the **Recovery Pin**. This is a pin that you give to the user so that they can re-install the operating system on the device, if it's recovered. Be sure to make a note of this pin because it won't be visible after the erase action completes:



3. Click **OK**, and the device will erase itself, then lock to the Recovery Pin.

9. ATP and Intune Integration

You can integrate Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) with Microsoft Intune as a Mobile Threat Defense solution, to help prevent security breaches and limit the impact of breaches within an organization. Microsoft Defender ATP works with devices that run Windows 10 or later.

To be successful, you use the following configurations in concert:

- Establish a service-to-service connection between Intune and Microsoft Defender ATP. This connection lets Microsoft Defender ATP collect data about machine risk from Windows 10 devices you manage with Intune.
- Use a device configuration profile to onboard devices with Microsoft Defender ATP. You onboard devices to configure them to communicate with Microsoft Defender ATP and to provide data that helps assess their risk level.
- Use a device compliance policy to set the level of risk you want to allow. Risk levels are reported by Microsoft Defender ATP. Devices that exceed the allowed risk level are identified as non-compliant.
- Use a conditional access policy to block users from accessing corporate resources from devices that are non-compliant

Enable Microsoft Defender ATP in Intune

1. Sign in to Intune and select **Device compliance**:

The screenshot shows the Microsoft Intune - Overview page. At the top left, there is a breadcrumb navigation: Home > Microsoft Intune - Overview. Below the breadcrumb is a search bar labeled "Search (Ctrl+/" followed by a magnifying glass icon. To the right of the search bar is a blue circular icon with a white "i" and the text "Microsoft Intune - Overview". On the left side, there is a sidebar titled "Manage" with the following options: Device enrollment, Device compliance (which is highlighted with a red box), Device configuration, Device security, Devices, Client apps, E-books, and Conditional access. The main content area is titled "Status" and contains a section titled "Device compliance status". This section has two columns: "STATUS" and "DEVICES". A callout box with a dashed border contains the text "Enroll devices to view insights".

2. Select **Microsoft Defender ATP**, and then below Connector Settings, select **Open the Microsoft Defender Security Center**:

Home > Microsoft Intune > Device compliance - Microsoft Defender ATP

Device compliance - Microsoft Defender ATP

Search (Ctrl+ /) Refresh

Configure the settings below.

Connector Settings

Toggles are disabled and acting as "off" because Microsoft Defender ATP connection in the Microsoft Defender ATP admin console.

When the connection has returned to a healthy status (Active),

Connect Windows devices version 10.0.15063 and above to Microsoft Defender ATP.

Block unsupported OS versions ⓘ

Number of days until partner is unresponsive ⓘ

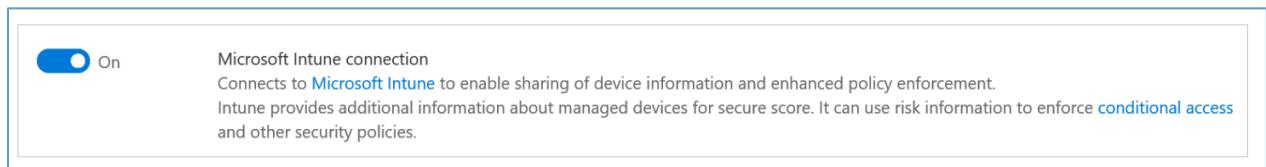
[Open the Microsoft Defender Security Center](#)

Windows 10 devices need to be configured with Microsoft Defender ATP.

0 Devices

3. In Microsoft Defender Security Center, select **Settings** > **Advanced features**.

4. For Microsoft Intune connection, select **On**, then click **Save preferences**:



5. Go back to Intune, **Device compliance** > **Microsoft Defender ATP**.

6. Set Connect Windows devices version 10.0.15063 and above to Microsoft Defender ATP to **On**.

The screenshot shows the 'Connector Settings' page. At the top, there's a note: 'Toggles are disabled and acting as "off" because Microsoft Defender ATP is not actively communicating with Intune for this account. Please check the state of the connection in the Microsoft Defender ATP admin console.' Below this, there are three settings with toggle switches:

- 'Connect Windows devices version 10.0.15063 and above to Microsoft Defender ATP' (switched On)
- 'Block unsupported OS versions' (switched Off)
- 'Number of days until partner is unresponsive' (set to 7)

At the bottom, there's a link 'Open the Microsoft Defender Security Center'.

7. Select **Save**.

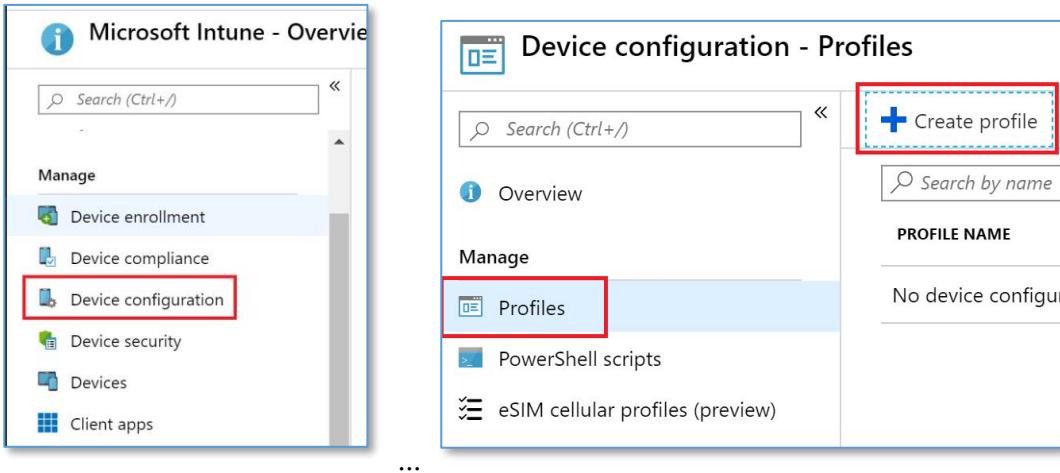
On-board devices by using a configuration profile

After you establish the service-to-service connection between Intune and Microsoft Defender ATP, you onboard your Intune managed devices to ATP so that data about their risk level can be collected. To on-board devices, you use a device configuration profile for Microsoft Defender ATP.

When you established the connection to Microsoft Defender ATP, Intune received an ATP onboarding configuration package from Microsoft Defender ATP. This package is deployed to devices with the device configuration profile. The configuration package configures devices to communicate with Microsoft Defender ATP services to scan files, detect threats, and report the risk to Microsoft Defender ATP.

Create a device configuration profile

1. Sign in to Intune and select **Device Configuration > Profiles > Create profile**:



2. Enter a **Name** and **Description**.

- For **Platform**, select **Windows 10 and later**
- For **Profile type**, select **Microsoft Defender ATP (Windows 10 Desktop)**.

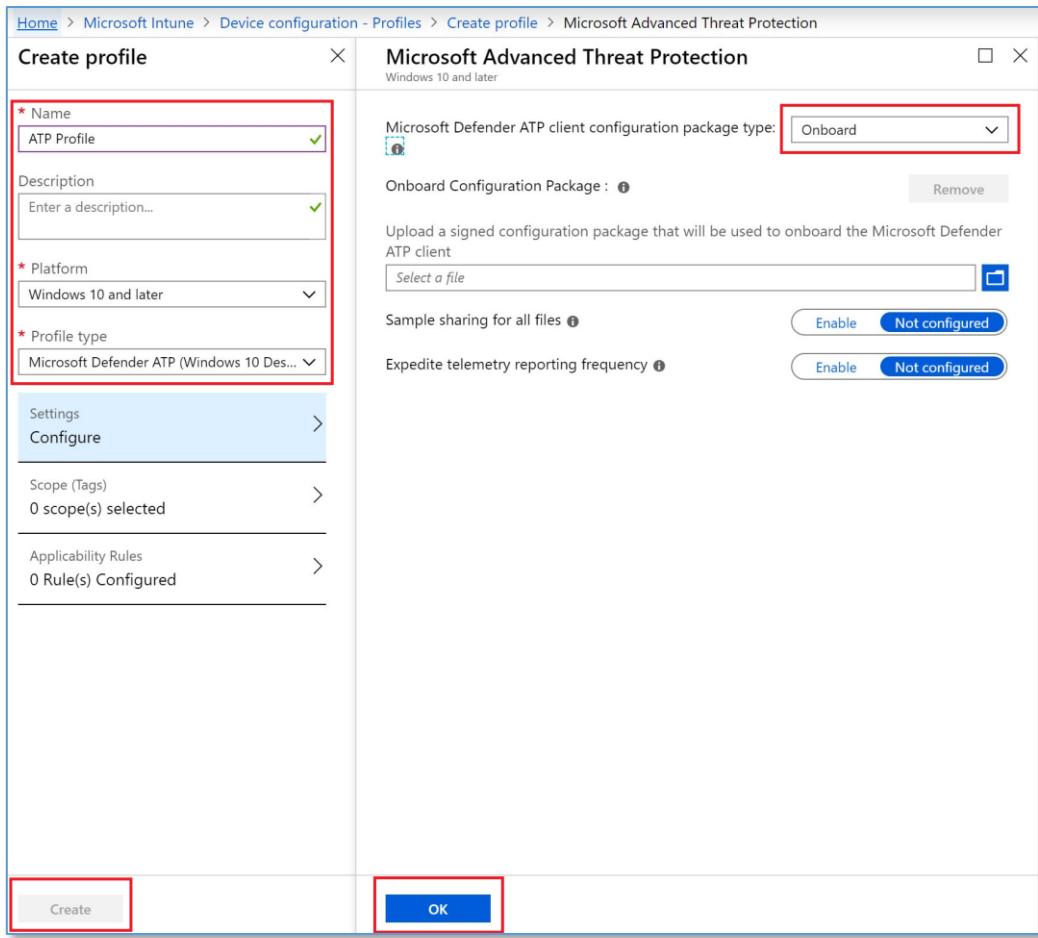
Configure the settings:

- **Microsoft Defender ATP client configuration package type:** Select **Onboard** to add the configuration package to the profile. Select **Offboard** to remove the configuration package from the profile.

Note -

If you've properly established a connection with Microsoft Defender ATP, Intune will automatically **Onboard** the configuration profile for you, and the **Microsoft Defender ATP client configuration package type** setting will not be available.

- **Sample sharing for all files:** **Enable** allows samples to be collected, and shared with Microsoft Defender ATP. For example, if you see a suspicious file, you can submit it to Microsoft Defender ATP for deep analysis. **Not configured** doesn't share any samples to Microsoft Defender ATP.
- **Expedite telemetry reporting frequency:** For devices that are at high risk, **Enable** this setting so it reports telemetry to the Microsoft Defender ATP service more frequently.



3. Select **OK**, and **Create** to save your changes, which creates the profile.

Assign a device profile

Assign the device configuration profile to devices you want to assess with Microsoft Defender ATP.

1. Sign in to Intune and select **Device configuration > Profiles**. All the profiles are listed.
2. Select the profile you want to assign > **Assignments**.
3. Choose to **Include** groups or **Exclude** groups, and then select your groups. When you select your groups, you're choosing an Azure AD group. To select multiple groups, hold down the **Ctrl** key, and select your groups.

4. Save your changes.

Create and assign a compliance policy

The compliance policy determines the level of risk that you consider as acceptable for a device.

Create the compliance policy

1. Sign in to Intune and select **Device compliance > Policies > Create policy**.

Home > Microsoft Intune > Device compliance - Policies

Device compliance - Policies

Search (Ctrl+ /) < Create Policy

Overview

Manage

- Policies
- Notifications
- Locations

POLICY NAME

No compliance policies

2. Enter a **Name** and **Description**.
3. In **Platform**, select **Windows 10 and later**.
4. In the **Microsoft Defender ATP** settings, set **Require the device to be at or under the machine risk score** to your preferred level.

Create Policy

Name: ATPCompliance

Description: Enter a description...

Platform: Windows 10 and later

Settings: Configure

Actions for noncompliance: 1 configured

Scope (Tags): 0 scope(s) selected

Windows 10 compliance policy

Select a category to configure settings.

- Device Health: 3 settings available
- Device Properties: 5 settings available
- Configuration Manager Compliance: 1 setting available
- System Security: 17 settings available

Microsoft Defender ATP

Microsoft Defender Advanced Threat Protection rules

Require the device to be at or under the machine risk score: Low

OK

Threat level classifications are determined by Microsoft Defender ATP.

- **Clear:** This level is the most secure. The device can't have any existing threats and still access company resources. If any threats are found, the device is evaluated as noncompliant. (Microsoft Defender ATP users the value *Secure*.)
- **Low:** The device is compliant if only low-level threats exist. Devices with medium or high threat levels aren't 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.

5. Select **OK**, and **Create** to save your changes (and create the policy).

Assign the device compliance to user/groups

Once a policy is created, the next step is to assign the policy to your groups:

1. Choose a policy you created. Existing policies are in **Device compliance > Policies**.
2. Select the policy > **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 > Choose **Save** to deploy the policy to users.

The screenshot shows the Microsoft Intune ATPCompliance - Assignments page. The URL bar at the top shows the path: Home > Microsoft Intune > Device compliance - Policies > ATPCompliance - Assignments. The main content area is titled "ATPCompliance - Assignments" and "Device compliance policy". At the top right, there are three buttons: "Save" (highlighted with a red box), "Discard", and "Evaluate". Below these buttons is a section titled "Assign to" with two tabs: "Include" and "Exclude". Under "Include", there is a list box containing "Selected Groups" (which is also highlighted with a red box). Below this list box is a placeholder text "Select groups to include". At the bottom of the "Include" section is an "ATP-Group". On the left side, there is a sidebar with the following navigation items: Overview, Properties, **Assignments** (which is highlighted with a blue background), Monitor, Device status, User status, and Per-setting status.

You applied the policy to users. The devices used by the users targeted by the policy are evaluated for compliance.

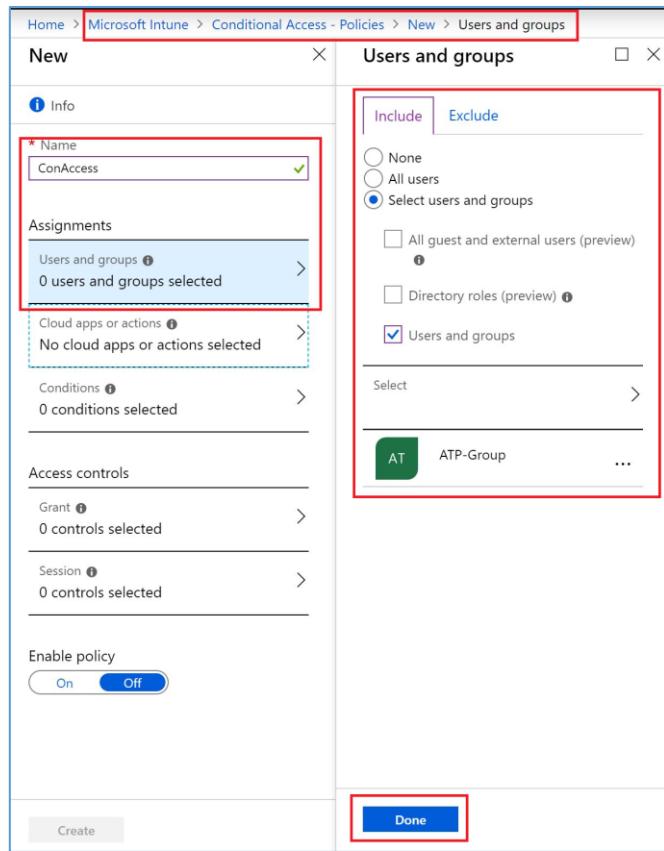
Create a Conditional Access policy

The Conditional Access policy blocks access to resources for devices that exceed the threat level you set in your compliance policy. You can block access from the device to corporate resources, such as SharePoint or Exchange Online.

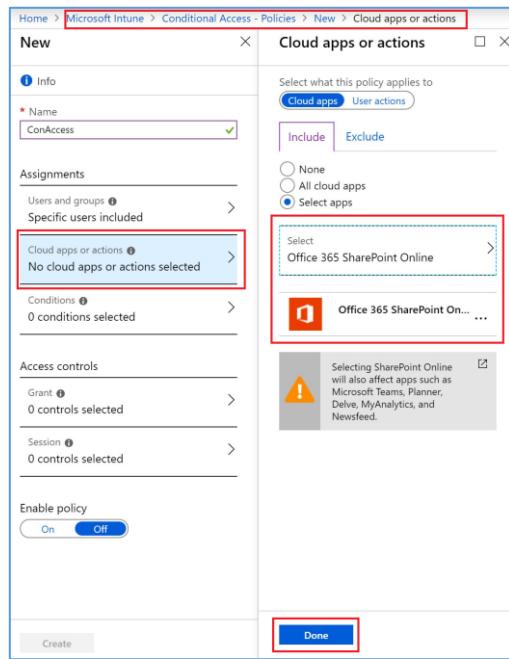
1. Sign in to Intune and select **Conditional Access > New policy**.

The screenshot shows the Microsoft Intune Conditional Access - Policies page. At the top, there is a breadcrumb navigation: Home > Microsoft Intune > Conditional Access - Policies. Below the breadcrumb, there is a sidebar with sections like 'Manage' (Named locations, Custom controls (preview), Terms of use, VPN connectivity, Classic policies) and 'Troubleshooting + Support' (Troubleshoot, New support request). On the right, there is a main content area with a 'POLICY NAME' section containing five listed policies: Baseline policy: Require MFA for admins (Preview), Baseline policy: End user protection (Preview), Baseline policy: Block legacy authentication (Preview), and Baseline policy: Require MFA for Service Management (Preview). At the top right of the main content area, there is a red box highlighting the '+ New policy' button. Above the '+ New policy' button, there are links for 'What If' and 'Got feedback?'. A tooltip message 'Interested in understanding the impact of the policies on a user sign-in?' is visible near the 'What If' link.

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. In our example, we chose **Select apps**, **Office 365 SharePoint Online**, and **Office 365 Exchange Online**.



4. Select **Done** to save your changes.
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:

The screenshot shows the Microsoft Intune Conditional Access - Policies New screen. The top navigation bar is highlighted with a red box, showing the path: Home > Microsoft Intune > Conditional Access - Policies > New > Conditions > Client apps (preview).

The main interface is divided into three columns:

- New Column:** Contains fields for Name (ConAccess), Assignments (Users and groups, Specific users included), Cloud apps or actions (1 app included, Conditions: 0 conditions selected), Access controls (Grant: 0 controls selected), Session (0 controls selected), and Enable policy (On). A red box highlights the 'Conditions' section under Cloud apps or actions.
- Conditions Column:** Shows Sign-in risk (Not configured), Device platforms (Not configured), Locations (Not configured), and Client apps (preview) (Not configured). A red box highlights the 'Client apps (preview)' section.
- Client apps (preview) Column:** This is the active configuration screen. It has a 'Configure' section with a 'Yes' button (highlighted with a red box). Below it, a note says 'Select the client apps this policy will apply to' with checkboxes for 'Browser' (checked) and 'Mobile apps and desktop clients' (checked). Other options include 'Modern authentication clients' (checked), 'Exchange ActiveSync clients' (checked), 'Apply policy only to supported platforms' (unchecked), and 'Other clients' (checked). A warning message at the bottom states 'Exchange ActiveSync currently does not support all other conditions' with an exclamation mark icon.

At the bottom of each column are 'Done' buttons, with the one in the Client apps column highlighted with a red box.

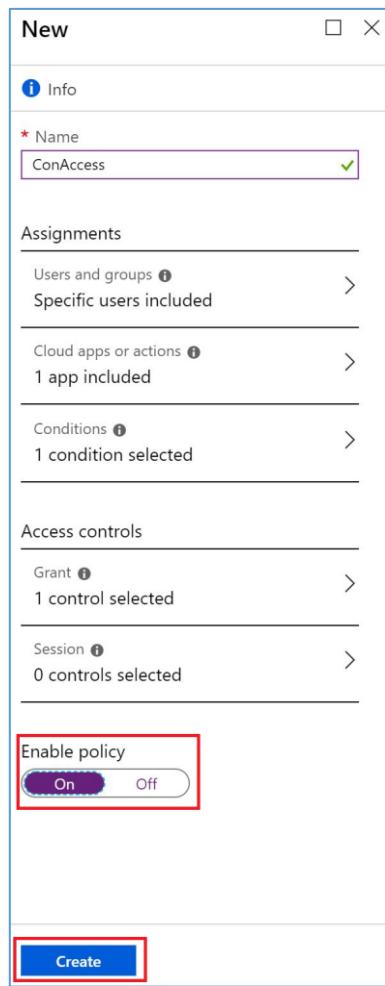
6. Select **Done** to save your changes.
7. Select **Grant** to apply Conditional Access based on device compliance. For example, select **Grant access > Require device to be marked as compliant**:

Home > Microsoft Intune > Conditional Access - Policies > New > Grant

New	X
<p>Info</p> <p>* Name ConAccess</p> <p>Assignments</p> <p>Users and groups > Specific users included</p> <p>Cloud apps or actions > 1 app included</p> <p>Conditions > 1 condition selected</p> <p>Access controls</p> <p>Grant > 0 controls selected</p> <p>Session > 0 controls selected</p> <p>Enable policy</p> <p>On Off</p>	<p>Grant</p> <p>Select the controls to be enforced.</p> <p><input type="radio"/> Block access</p> <p><input checked="" type="radio"/> Grant access</p> <p><input type="checkbox"/> Require multi-factor authentication</p> <p><input checked="" type="checkbox"/> Require device to be marked as compliant</p> <p><input type="checkbox"/> Require Hybrid Azure AD joined device</p> <p><input type="checkbox"/> Require approved client app See list of approved client apps</p> <p><input type="checkbox"/> Require app protection policy (preview)</p> <p>See list of policy protected client apps</p> <p>For multiple controls</p> <p><input checked="" type="radio"/> Require all the selected controls</p> <p><input type="radio"/> Require one of the selected controls</p> <p> Don't lock yourself out! Make sure your device is compliant.</p> <p>Select</p>

8. Choose **Select** to save your settings.

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



Monitor device compliance

Next, monitor the state of devices that have the Microsoft Defender ATP compliance policy.

1. Sign in to Intune.
2. Select **Device compliance > Policy compliance**.
3. Find your Microsoft Defender ATP policy in the list, and see which devices are compliant or noncompliant.

POLICY	COMPLIANT DEVICES	NONCOMPLIANT DEVICES
ATPCompliance	0	0

10. Support

Opening tickets

In case of an issue for Windows Virtual Desktop go to the Azure Portal and open a technical ticket based on your existing support plan at <https://azure.microsoft.com/en-us/support/create-ticket/>

Look for Service under **COMPUTE** and select **Windows Virtual Desktop-Preview**. You will find options to create tickets for the WVD service itself and for Office:

For Office issues you can file tickets during public preview in the Azure Portal when using Office in context of Windows Virtual Desktop.

Information you should provide for failed connection or management interactions when using the service:

- Use the diagnostics service to retrieve the **Activity ID** for failed connections or management interactions.
- Provide the approximate timeframe the issue happened

NOTE: This workflow will change post general availability.

Other resources you can leverage

Windows Virtual Desktop contains a number of knowledge articles as well as trouble shooting guides. Pay attention to the updated diagnostics chapter that provides Error scenarios you can mitigate: <https://docs.microsoft.com/azure/virtual-desktop/overview>

Exchange on our community forum on issues important to you for Windows Virtual Desktop:

<https://techcommunity.microsoft.com/t5/Windows-Virtual-Desktop/bd-p/WindowsVirtualDesktop>

When setting up your environment you will be using other Azure Services. You can watch the health dashboard here to verify health state on any Azure service you are consuming:

<https://azure.microsoft.com/en-us/status/>

11. Appendix

Device security and data protection

Basic Security

[Windows Defender Antivirus](#) Uses the power of the cloud, wide-optics, precise machine learning models, and behavior analysis to protect devices.

[Windows Defender SmartScreen](#) Checks for malicious apps and sites, warning and blocking users from accessing content that could harm their devices.

[Windows Defender Firewall](#) Protects against unauthorized access.

Advanced Security

[Windows Hello](#) Replaces passwords with strong two-factor authentication, providing instant access to your Windows 10 devices using fingerprint or facial recognition. (This is PIN only on a VM)

Windows Information Protection Protects enterprise apps and data against accidental data leak on enterprise-owned devices and personal devices.

Microsoft Defender Advanced Threat Protection Helps detect, investigate, and respond to advanced attacks on your networks. (Requires Windows E5 or M365 E5)