

Configure and Deploy Intune MDM

November 19, 2018 Brad Wyatt Comments 5 comments

Table of Contents

Description

Solution

Configure MDM Authority

Configure APN Certificate

Configure MDM DNS Records

Configure Company Portal

Configure Portal Terms and Conditions

Device Enrollment Administrator

Device Enrollment and Type Restrictions

Device Group Mappings

Step 1: Device Categories

Step 2: Create Azure Active Directory Dynamic Device Security Groups

Step 3: Select Device Category

Windows

iOS

Intune Policies

Compliance Policies

Configuration Policies

Basic Configuration Policy Overview

Uninstall Restricted Applications

Configure Email Profiles

Modify iOS Dock

Software Update Policies

Windows

iOS

Enable Windows 10 automatic enrollment

Enroll Devices into Intune

iOS

Windows

Online Portal

Microsoft Store App

Windows Settings App

Deploy Client Apps to Managed Intune Devices

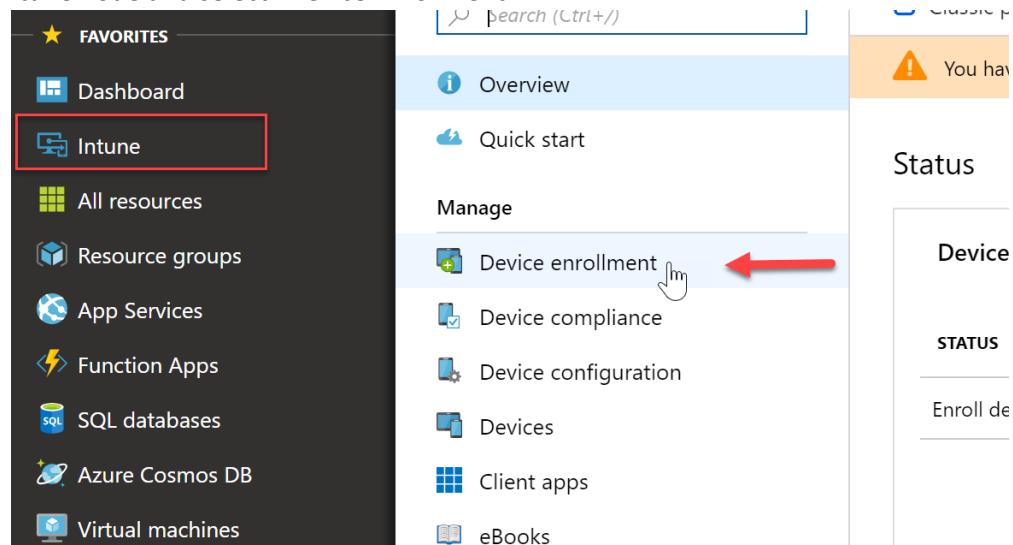
Description

In this article I will be configuring and deploying Intune as a stand-alone MDM solution. This article will walk you through deploying applications to devices, configuring your Company Portal, enrolling end user devices, creating policies and more.

Solution

Configure MDM Authority

First we must configure Intune as my MDM authority. Since I am doing a stand alone I want Intune as the only authority and not Configuration Manager. By logging into portal.azure.com I can expand the Intune node and select “Device Enrollment”



Select “Intune MDM Authority” and then click “Choose”

Choose MDM Authority

Mobile Device Management Authority

Choose whether Intune or Configuration Manager is your mobile device management authority.

Choose Intune as your MDM authority to manage mobile devices with Microsoft Intune only.

Choose Configuration Manager as your MDM authority to manage mobile devices with System Center Configuration Manager and Microsoft Intune.

Mobile devices cannot be managed if an MDM authority is not chosen.

Learn more about [choosing your MDM Authority](#).

- Intune MDM Authority
- Configuration Manager MDM Authority
- None



Choose



I will get a notification that my changes were saved successfully

MDM Authority is successfully chosen. 8:55 AM

Your MDM Authority has been set to Microsoft Intune

Configure APN Certificate

To manage iOS devices you must have an Apple Push certificate.

In the Intune blade we want to go to Device Enrollment and then Apple Enrollment and select “Apple MDM Push Certificate”

The screenshot shows the Microsoft Intune interface for Device enrollment - Apple enrollment. On the left, there's a navigation sidebar with various options like Overview, Quick start, Manage (with Device enrollment and Apple enrollment highlighted), and Help and support. The main content area has two main sections: 'Device enrollment' and 'Apple enrollment'. Under 'Prerequisites', there's a box for 'Apple MDM Push certificate' which is described as 'Certificate required to manage Apple devices'. A red arrow points to this box. Below it, there are sections for 'Bulk enrollment methods' (Apple Configurator) and 'Enrollment program tokens'.

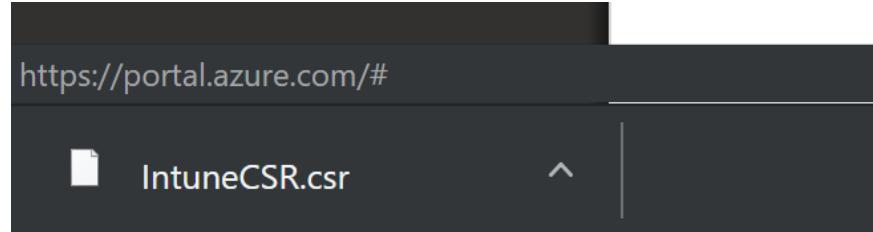
Agree to the terms in step 1 and then download the CSR

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:			
1. I grant Microsoft permission to send both user and device information to Apple. More information.			
<input checked="" type="checkbox"/> * I agree.			
<hr/>			
2. Download the Intune certificate signing request required to create an Apple MDM push certificate.			
 Download your CSR 			
<hr/>			
3. Create an Apple MDM push certificate. More information.			
Create your MDM push Certificate 			
<hr/>			
4. Enter the Apple ID used to create your Apple MDM push certificate.			
 * Apple ID <input type="text" value="Apple ID"/>			
<hr/>			

It will download the file, “IntuneCSR.csr”



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

Apple ID

Sign in with your Apple ID into the Apple Push Certificates Portal

Apple Mac iPad iPhone Watch TV Music Support Q □

Apple Push Certificates Portal

Sign In.

MDM@thelazyadministrator.com

Forgot your Apple ID?

.....

Forgot your password?

[Sign In](#)



Shop the Apple Online Store (1-800-MY-APPL), visit an [Apple Retail Store](#), or find a [reseller](#).

[Apple Info](#) | [Site Map](#) | [Hot News](#) | [RSS Feeds](#) | [Contact Us](#) | [!\[\]\(7784bf410a8668d4bdc1caeae116d31c_img.jpg\)](#)

Copyright © 2018 Apple Inc. All rights reserved. [Terms of Use](#) | [Privacy Policy](#)

Now click "Create a Certificate" after you have successfully signed into the portal with your Apple ID.

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 icon. Below the navigation bar is the title "Apple Push Certificates Portal" and a user account section showing "bradleywyatt1@gmail.com" and a "Sign out" button. The main content area has a large blue globe graphic with a green dot over North America and a yellow dot over South America. On the left, there are two sections: "Get Started" with the sub-instruction "Create a push certificate that enables your third-party server to work with the Apple Push Notification Service and your Apple devices." and a "Create a Certificate" button, and "FAQ" with links to "Learn more about Mobile Device Management" and "What about OS X Server?". At the bottom, there's footer information including links to the Apple Online Store, Apple Info, Site Map, Hot News, RSS Feeds, Contact Us, and a U.S. flag icon.

Store Mac iPod iPhone iPad iTunes Support

Apple Push Certificates Portal

bradleywyatt1@gmail.com Sign out

Get Started

Create a push certificate that enables your third-party server to work with the Apple Push Notification Service and your Apple devices.

Create a Certificate

FAQ

Learn more about Mobile Device Management

What about OS X Server?

Shop the [Apple Online Store](#) (1-800-MY-APPLE), visit an [Apple Retail Store](#), or find a [reseller](#).

[Apple Info](#) | [Site Map](#) | [Hot News](#) | [RSS Feeds](#) | [Contact Us](#) |

Copyright © 2018 Apple Inc. All rights reserved. [Terms of Use](#) | [Privacy Policy](#)

Navigate to your CSR file that you downloaded from the Intune portal above and then select "Upload"

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, Support, and a search icon. Below the navigation bar, the title "Apple Push Certificates Portal" is displayed, along with a user account link "bradleywyatt1@gmail.com" and a "Sign out" button. The main content area has a heading "Create a New Push Certificate". A sub-instruction says "Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate." Below this, there's a "Notes" section with an empty text area. To the right of the notes is a large graphic of a globe with blue and white continents, centered over North America, with a green dot at the North Pole and a yellow sun-like circle at the South Pole. In the center of the page, there's a file upload interface. It includes a red-bordered "Choose File" button labeled "IntuneCSR.csr", a "Cancel" button, and an "Upload" button with a downward-pointing arrow. A hand cursor is hovering over the "Upload" button. At the bottom of the page, there's footer text: "Shop the [Apple Online Store](#) (1-800-MY-APPLE), visit an [Apple Retail Store](#), or find a [reseller](#).", followed by links for "Apple Info", "Site Map", "Hot News", "RSS Feeds", "Contact Us", and a small American flag icon.

Once you have a green confirmation, download your certificate

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 icon. Below the navigation bar is the title "Apple Push Certificates Portal". On the right side of the title, it shows the user's email (bradleywyatt1@gmail.com) and a "Sign out" button. The main content area has a heading "Confirmation" with a green checkmark icon. It says "You have successfully created a new push certificate with the following information:" followed by a table:

Service	Mobile Device Management
Vendor	Microsoft Corporation
Expiration Date	Oct 31, 2019

Below the table are two buttons: "Manage Certificates" and "Download". The "Download" button is highlighted with a red box and a cursor icon pointing at it. To the right of the "Download" button is a large graphic of Earth with blue and yellow highlights. At the bottom of the page, there's a footer with links for Apple Online Store, Apple Retail Store, reseller, Apple Info, Site Map, Hot News, RSS Feeds, Contact Us, and a USA flag.

Go back to the Intune portal and in step 4, enter your Apple ID you used to create the certificate. In step 5 browse to the downloaded certificate and then press “Upload”

The screenshot shows the Microsoft Intune "Configure MDM Push Certificate" page. The URL in the address bar is "Home > Microsoft Intune > Device enrollment - Apple enrollment > Configure MDM Push Certificate". On the right, there's a message box with a green checkmark and the text "Upload Completed for MDM_ Microsoft C... 9:23 AM" and "1.91 KiB | Streaming upload".

The page has several steps listed:

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
MDM@thelazyadministrator.com
5. Browse to your Apple MDM push certificate to upload
* Apple MDM push certificate
"MDM_Microsoft Corporation_Certificate.pem"

At the bottom left, there's a blue "Upload" button with a red arrow pointing to it.

Once we finish the upload, we can scroll up and see details regarding our certificate, including the expiration date

Home > Microsoft Intune > Device enrollment - Apple en

Configure MDM Push Certificate

Status:



Active

Last Upd

10/31/20

Expiration:

10/31/2019

Subject I

com.app

Configure MDM DNS Records

For Windows devices, there are two DNS CNAME records you need to create (pictured below):

^ CNAME records

One or more of these records haven't been added correctly yet. [step-by-step instructions](#)

[Copy this table](#)

Expected vs actual record	Host name	Points to address or value	TTL	Status
✓ Expected re...	autodiscover	autodiscover.outlook.com	3600	Correct
✗ Expected re...	enterpriseregistration.windows.net	enterpriseregistration.windows.net	3600	No records found Missing record
✗ Expected re...	enterpriseenrollment.manage.micros...	enterpriseenrollment.manage.micros...	3600	No records found Missing record

There are two CNAME records you will need to add. Once

Add a CNAME Record for "thelazyadministrator.com"

Name
enterpriseregistration.thelazyadministrator.com.

CNAME
enterpriseregistration.windows.net

Add a CNAME Record Cancel

Name
enterpriseenrollment.thelazyadministrator.com.

CNAME
enterpriseenrollment.manage.microsoft.com

Add a CNAME Record Cancel

Checking my DNS for MDM again, I can see that the records are now in place and valid

thelazyadministrator.com
Domain managed outside Office 365

Set as default DNS management Check DNS Remove

All DNS records are correct, no errors found. Nameservers used: ns1.mylhsns.net, ns2.mylhsns.net

Required DNS settings
Your DNS records must be set to the following values for your Office 365 services to run smoothly.
You can also download or print this data.
Export options

Exchange Online

Type	Priority	Host name	Points to address or value	TTL	Actions
MX	0	@	thelazyadministrator-com.mail.protection.outlook...	1 Hour	
TXT	-	@	v=spf1 include:spf.protection.outlook.com -all	1 Hour	
CNAME	-	autodiscover	autodiscover.outlook.com	1 Hour	

Mobile Device Management for Office 365

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	

Back in the Intune azure portal, under Device Enrollment, go to Windows enrollment and then CNAME Validation

The screenshot shows the Microsoft Intune Device enrollment - Windows enrollment page. The left sidebar has a navigation menu with several options: Overview, Quick start, Manage (with Apple enrollment, Android enrollment, and Windows enrollment), Terms and conditions, Enrollment restrictions, Device categories, Corporate device identifiers, Device enrollment managers, Monitor, Audit logs, Help and support, and Help and support. The 'Windows enrollment' option is highlighted with a red box. The main content area has a heading 'Use the following to help enroll Windows devices.' followed by sections for General, Windows Hello for Business, CNAME Validation (which is highlighted with a red box), Enrollment Status Page (Preview), Windows Autopilot Deployment Program, Deployment Profiles, and Devices.

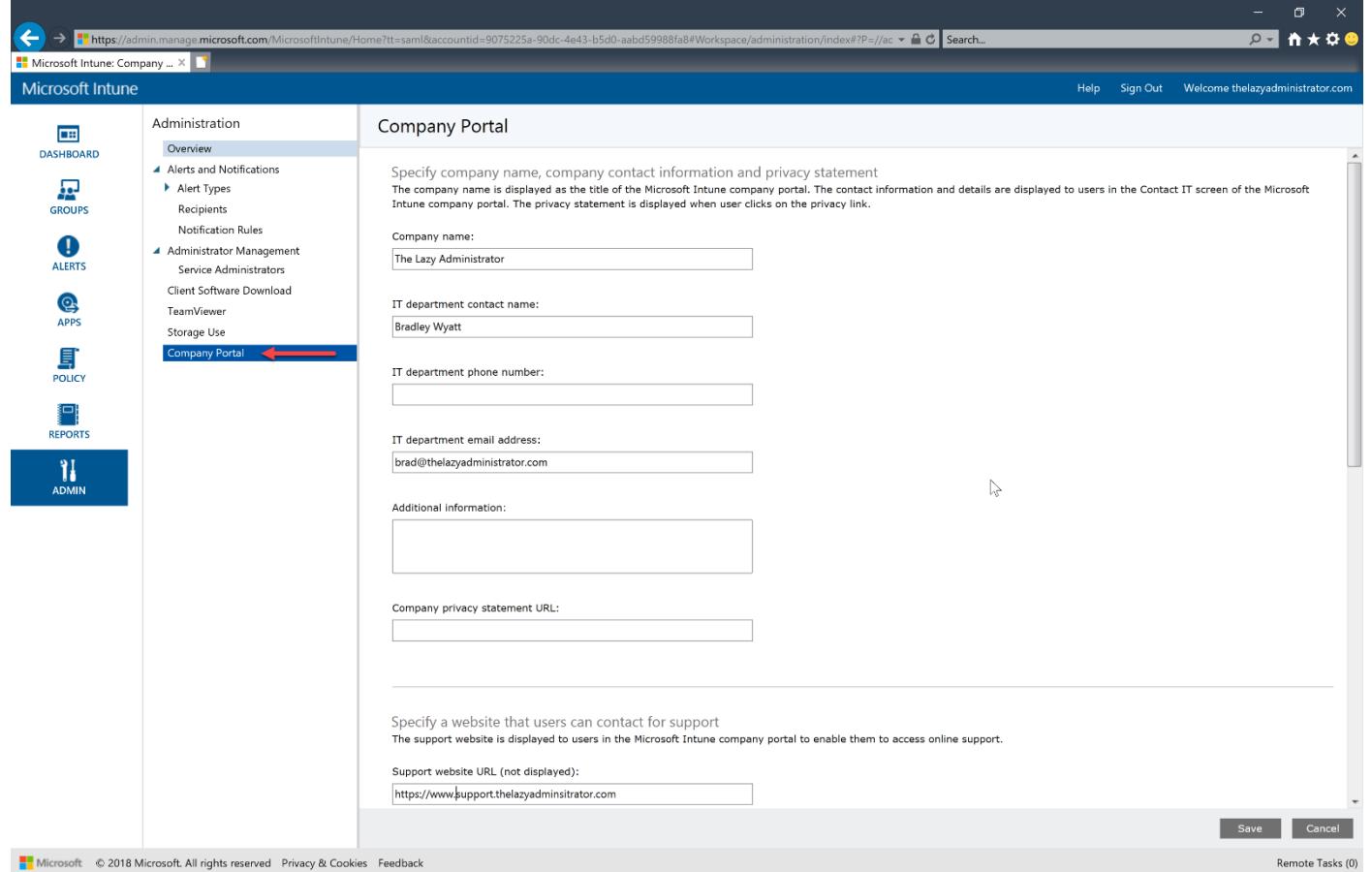
Verify that your domain comes back successful

The screenshot shows the 'CNAME' configuration page. It has a header 'CNAME' and 'Test CNAME'. Below is a text block explaining that configuring a CNAME in DNS saves users from entering the MDM server address. It then instructs to enter the domain here to confirm configuration. A note states that changes might take up to 72 hours to propagate. There is a 'Domain' input field with the value 'thelazyadministrator.com' and a green checkmark. Below is a 'Test' button with a blue dotted border. At the bottom, a message says 'CNAME for thelazyadministrator.com is configured correctly.'

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.

Currently the Company Portal can be configured on the legacy Intune Portal at admin.manage.microsoft.com



The screenshot shows the Microsoft Intune Company Portal configuration page. The URL in the browser is https://admin.manage.microsoft.com/MicrosoftIntune/Home?t=saml&accountid=9075225a-90dc-4e43-b5d0-aabd59988fa8#Workspace/administration/index#/P=/ec. The page title is "Microsoft Intune: Company ...". The left sidebar has links for DASHBOARD, GROUPS, ALERTS, APPS, POLICY, and REPORTS, with ADMIN selected. The main content area is titled "Company Portal" and contains fields for company name, IT department contact name, phone number, email address, and additional information. At the bottom, there's a section for support website URL with a value of "https://www.support.thelazyadministrator.com". There are "Save" and "Cancel" buttons at the bottom right.

On the iOS Company Portal application under support you can see the email and website we specified for help. This is handy for end users as they have a very simple and clear way to contact you or your IT

team.

The screenshot shows a mobile application interface. At the top, there's a blue header bar with the text "The Lazy Administrator". Below this, the main content area has a light gray background. A section titled "Support" is displayed, followed by the contact information: "Contact Name" and "Bradley Wyatt". Below this, there are two links: "✉ brad@thelazyadministrator.com" and "🌐 Help Me". At the bottom of the screen, there's a navigation bar with five items: "Apps" (represented by a grid icon), "Device" (represented by a monitor icon), "Support" (represented by a headphones icon, which is highlighted in black), "Notifications" (represented by a flag icon), and "More" (represented by three dots). The overall theme is clean and modern.

At the bottom, once you save your Company Portal changes you can launch the portal website (<https://portal.manage.microsoft.com/>)

Customization

You can customize your company portal with your company logo, company name, theme color and background. [Learn more about customizations.](#)

Theme color:

Blue ▾

Include company logo:

Choose a background for Windows 8 Company Portal app:

Default background Solid white background

Microsoft Intune company portal
[Open the Microsoft Intune company portal website](#)

Save Cancel

Here I can see the basic portal

The screenshot shows the Microsoft Intune Company Portal homepage. At the top, there is a navigation bar with links for Apps, Bookmarks, 3Points, and PSM. On the left, a sidebar menu includes Home (selected), Apps, Devices, Helpdesk, Brad Wyatt (user profile), and Sign out. The main content area displays a message: "No apps yet" and "There are no apps available to you on this device." Below this, it says "You might let your organization access other company resources such as email and documents. Go to Devices".

Configure Portal Terms and Conditions

The Terms and Conditions can be prompted to users prior to them accessing the Intune Company Portal. In the Azure Intune portal you can configure your policies, apply to users or groups, and review the acceptance reporting.

[Log into the Azure Intune Portal](#)

Navigate to the Intune blade, then Device Enrollment > Terms and Conditions and then click "Create"

The screenshot shows the Microsoft Intune interface. On the left, there's a sidebar with various management options like Device enrollment, Device compliance, Device configuration, etc. The 'Device enrollment' option is selected and highlighted with a red box. On the right, the main content area is titled 'Device enrollment - Terms and conditions'. It shows a list of terms and conditions with columns for NAME, ASSIGNED, and LAST MODIFIED DATE. A purple banner at the top right encourages upgrading company terms with Azure Active Directory Terms of Use. A prominent blue 'Create' button is located at the top right of the main content area, also highlighted with a red arrow.

Create the required information regarding your Terms and Conditions and then press OK

The screenshot shows two overlapping dialog boxes. The first dialog is titled 'Create Terms and Conditions' and contains fields for 'Display name' (set to 'The Lazy Administrator Terms and COnditions'), 'Description' (checkbox checked), and 'Define term of use' (set to 'Defined'). A 'Create' button is at the bottom. The second dialog is titled 'Terms and Conditions' and contains fields for 'Title' (set to 'The Lazy Administrator Terms and COnditions'), 'Summary of Terms' (checkbox checked), and 'Terms and Conditions' (checkbox checked). Both dialogs have an 'Ok' button at the bottom right, which is highlighted with a red arrow.

You will get a notification that your policy must be assigned to users or groups in your environment

✓ The Lazy Administrator Terms and COndition... 10:19 AM 

This term has not been assigned to any users.

Under your Terms and Conditions overview select “Assignments”

The Lazy Administrator Terms and COnditions - Overview 

Terms and conditions

Search (Ctrl+/
)

Overview

Manage

Properties

Assignments  

Last Modified: 10/31/2018, 10:19:40 AM

Created: 10/31/2018, 10:19:40 AM

Version: 1

Assignments: 0

Acceptance Reporting

Select the Users or Groups you want to assign the Terms and Conditions to and then press Save

The Lazy Administrator Terms and CConditions - Assignments  

Terms and conditions

Search (Ctrl+/
)

Overview

Manage

Properties

Assignments  

Assign to

All Users 

Acceptance Reporting

Next time you or your users log into the Company Portal they will be greeted with the Terms and Conditions that were assigned to them.

The Lazy Administrator

Terms

The Lazy Administrator Terms and Conditions

You agree that I can watch you do everything and look through all your files whenever I please. It may be in the middle of the night, you never know. All your devices belong to us!

[Read Terms](#)

Privacy Policy

Contact your IT department about your company's privacy policies.



[The Lazy Administrator Privacy Terms](#) [Feedback](#) © 2018 Microsoft. All rights reserved.

Device Enrollment Administrator

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

Navigate to the Azure Portal and expand the Intune blade

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 links like Overview, Quick start, Manage, Help and support, and Troubleshoot. Under the Manage section, 'Device enrollment' is selected and highlighted with a blue background. The main content area is titled 'Device enrollment' and contains sections for Overview, Quick start, Manage, Monitor, and Help and support. In the 'Manage' section, 'Device enrollment managers' is listed and also highlighted with a blue background. A mouse cursor is hovering over this link.

Microsoft Intune

Home > Microsoft Intune > Device enrollment

Device enrollment

Microsoft Intune

Search (Ctrl+ /)

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

Device enrollment

Search (Ctrl+ /)

Overview

Quick start

Manage

- Apple enrollment
- Android enrollment
- Windows enrollment
- Terms and conditions
- Enrollment restrictions
- Device categories
- Corporate device identifiers
- Device enrollment managers**

Monitor

- Audit logs

Help and support

- Help and support

Click Add and then enter your users UserPrincipalName and then select the “Add” button on the bottom

The screenshot shows the Microsoft Intune interface for managing device enrollment managers. On the left, there's a sidebar with 'Device enrollment managers' selected. The main area has a header 'Add User' with navigation icons. Below the header, there's a form with a 'User name' field containing 'enduser1@thelazyadministrator.com', which is highlighted with a red box. At the bottom right of the form, there's a blue 'Add' button with a red arrow pointing to it, indicating where to click.

Device Enrollment and Type Restrictions

The default amount of devices a regular users can enroll into Intune is 5 unless you have granted the user to be a Device Enrollment Administrator (above). You can also change the default amount for users in the Portal.

Log into the Azure portal and select the Intune blade

Select “Device Enrollment” and then click “Enrollment Restrictions”

The screenshot shows two side-by-side views of the Microsoft Intune interface. The left view is the main Microsoft Intune dashboard, and the right view is a detailed "Device enrollment - Enrollment restrictions" page.

Left View (Microsoft Intune Dashboard):

- Search bar: Search (Ctrl+/)
- Overview
- Quick start
- Manage**
 - Device enrollment** (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
 - Help and support
 - Troubleshoot

Right View (Device enrollment - Enrollment restrictions):

- Search bar: Search (Ctrl+/)
- Overview
- Quick start
- Manage**
 - Apple enrollment
 - Android enrollment
 - Windows enrollment
 - Enrollment restrictions** (highlighted with a red box and a cursor icon)
 - Device categories
 - Corporate device identifiers
 - Device enrollment managers
- Monitor
 - Audit logs
- Help and support
 - Help and support

Here you can either edit your restriction policies or create a new restriction policy

Device enrollment - Enrollment restrictions

Microsoft Intune

Search (Ctrl+ /)

+ Create restriction

Overview

Quick start

Manage

- Apple enrollment
- Android enrollment
- Windows enrollment
- Terms and conditions
- Enrollment restrictions**
- Device categories
- Corporate device identifiers
- Device enrollment managers

Monitor

Audit logs

Help and support

Help and support

A device must comply with the highest priority enrollment restrictions assigned to its user. You can drag a device restriction to change its priority. Default restrictions are lowest priority for all users and govern userless enrollments. Default restrictions may be edited, but not deleted. [Learn More](#).

Device Type Restrictions

Define which platforms, versions, and management types can enroll.

PRIORITY	NAME	ASSIGNED
Default	All Users	Yes

Device Limit Restrictions

Define how many devices each user can enroll.

PRIORITY	NAME	DEVICE LIMIT	ASSIGNED
Default	All Users	5	Yes

Here I am changing the device limit from the default of 5 to 3 and then saving my changes

All Users - Properties

Search (Ctrl+ /)

Save Discard

Overview

Manage

Properties

* Name

Description

* Restriction type

Device Limit

Specify the maximum number of devices a user can enroll.

3

If I want to change the Device Type Restriction Policy I can go back to the Enrollment Restrictions pane and select the Device Type Restriction policy

Device enrollment - Enrollment restrictions

Microsoft Intune

Search (Ctrl+ /)

[Create restriction](#)

[Overview](#)

[Quick start](#)

Manage

- [Apple enrollment](#)
- [Android enrollment](#)
- [Windows enrollment](#)
- [Terms and conditions](#)
- [Enrollment restrictions](#) **Selected**
- [Device categories](#)
- [Corporate device identifiers](#)
- [Device enrollment managers](#)

Monitor

- [Audit logs](#)

Help and support

- [Help and support](#)

A device must comply with the highest priority enrollment restrictions assigned to its user. You can drag a device restriction to change its priority. Default restrictions are lowest priority for all users and govern userless enrollments. Default restrictions may be edited, but not deleted. [Learn More](#).

Device Type Restrictions

Define which platforms, versions, and management types can enroll.

PRIORITY	NAME	ASSIGNED
Default	All Users	Yes

Device Limit Restrictions

Define how many devices each user can enroll.

PRIORITY	NAME	DEVICE LIMIT	ASSIGNED
Default	All Users	5	Yes

Here I am making a change to the Android Work Profile (seen in purple) and saving my changes
restrictions > All Users - Properties > Select platforms

The screenshot shows the Microsoft Intune 'All Users - Properties' blade. In the center, there is a modal window titled 'Select platforms'. The 'Name' field is set to 'All Users'. The 'Description' field contains the text: 'This is the default Device Type Restriction applied with lowest priority to all users regardless of group membership.' The 'Restriction type' dropdown is set to 'Device Type Restriction'. Below this, a section titled 'Select platforms' shows '4 platforms selected'. A dashed blue box highlights the 'Configure platforms' link, which is followed by the word 'Configured'. On the right side of the 'Select platforms' dialog, there is a message: 'You have allowed new platforms. Consider updating Platform Configurations.' Below this message, it says: 'You can allow enrollment of the following platforms. Only block platforms you will not support. Allowed platforms can be configured with additional enrollment restrictions.' A table lists five platforms with 'Allow' and 'Block' buttons: Android (Allow), Android work profile (Allow), iOS (Allow), macOS (Allow), and Windows (MDM) (Allow). At the bottom right of the dialog is a blue 'Ok' button with a hand cursor icon.

Device Group Mappings

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

Step 1: Device Categories

In my example I am going to create two (2) device categories. One category is for BYOD devices, or personal devices. These will be devices that end users own but may use them for work. The other category will be Company Owned Devices. These devices are purchased by the company, and given to the end users through the IT department.

In the Azure Portal, expand the Intune blade.

Select “Device Enrollment” and then click “Device Categories”

The screenshot shows the Microsoft Intune interface with the title "Device enrollment - Device categories". The left sidebar has a search bar and links for "Overview" and "Quick start". Under "Manage", "Device enrollment" is highlighted with a red box and a cursor is hovering over "Device categories" which is also highlighted with a red box. Other options in the "Manage" section include "Device compliance", "Device configuration", "Devices", "Client apps", "eBooks", "Conditional access", "On-premises access", "Users", "Groups", "Roles", and "Software updates". Below "Manage" are sections for "Help and support" (with "Help and support" and "Troubleshoot" links) and "Monitor" (with "Audit logs"). The right pane lists "Apple enrollment", "Android enrollment", "Windows enrollment", "Terms and conditions", "Enrollment restrictions", "Corporate device identifiers", and "Device enrollment managers".

To add a new category, click Create Device Category and then supply a valid name and press “Create”
You can create any device categories you want. For example:

Point-of-sale device

Demonstration device

Sales

Accounting

Manager

The screenshot shows the Microsoft Intune interface for creating a device category. On the left, there's a sidebar with 'Device categories' and a 'Create device category' button. The main area displays a table of existing device categories:

CATEGORY	DESCRIPTION
Personal Device	BYOD

A modal window titled 'Create device category' is open on the right. It contains fields for 'Category' (set to 'Company Owned Device') and 'Description' (set to 'Optional'). A red box highlights the 'Category' field, and a red arrow points to the 'Create' button at the bottom of the modal.

Step 2: Create Azure Active Directory Dynamic Device Security Groups

In this step, 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 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. The user 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 you created. 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.

In the Intune blade, select Groups, and the select “All Groups” and click “New Group”

The screenshot shows the Microsoft Intune interface. On the left, there's a navigation bar with links like Overview, Quick start, Manage (Device enrollment, Device compliance, Device configuration, Devices, Client apps, eBooks, Conditional access, On-premises access), Users, Groups (which is selected and highlighted with a red box), Roles, and Software updates. Below that is Help and support (Help and support, Troubleshoot). The main area is titled 'Groups - All groups' and shows a list of existing groups. At the top right of this area, there's a 'New group' button (highlighted with a blue box) and other buttons for Refresh and Columns. The 'All groups' section is also highlighted with a red box. The list of groups includes:

NAME	GROUP TYPE
DG distro group 1	Distribution
DG distro group 2	Distribution
G5 group 5	Office
O3 Office 365 Group	Office
PR Projects	Office
SE Security	Security
SG sgroup	Mail enabled security
SP Stinky People	Office
TE TEST	Office
TE test1	Office
TE test2	Office
TH TheLazyAdministrator	Distribution

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

Home > Microsoft Intune > Groups - All groups > Group > Dynamic membership rules

Group X

Dynamic membership rules X

* Group type
Security

* Group name ⓘ
Itune - Personal Devices

Group description ⓘ
Group for users personal devices they enr...

* Membership type ⓘ
Dynamic Device

Dynamic device members ⓘ
Add dynamic query >

Add dynamic membership rule
[Learn more about creating an Advanced Rule](#)

[Simple rule](#) [Advanced rule](#)

Add devices where

deviceCategory Equals personal device

[Create](#) [Add query](#)

Once you have your new Group with the correct properties and query, click "Create"

Home > Microsoft Intune > Groups - All groups

Group □ X

* Group type Security ▾

* Group name Itune - Personal Devices ✓

Group description Group for users personal devices they enr... ✓

* Membership type Dynamic Device ▾

Dynamic device members >

[Edit dynamic query](#)

Create 

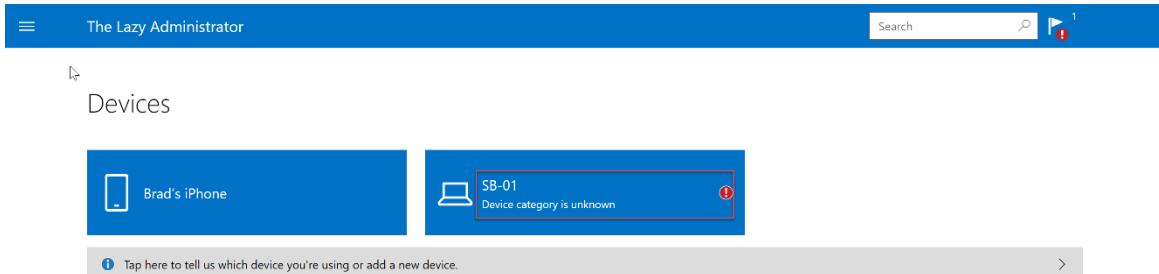
Now back in my Azure Groups pane, I can see my newly created groups

 Intune - Company Devices	Security	Dynamic	...
 Itune - Personal Devices	Security	Dynamic	...

Step 3: Select Device Category

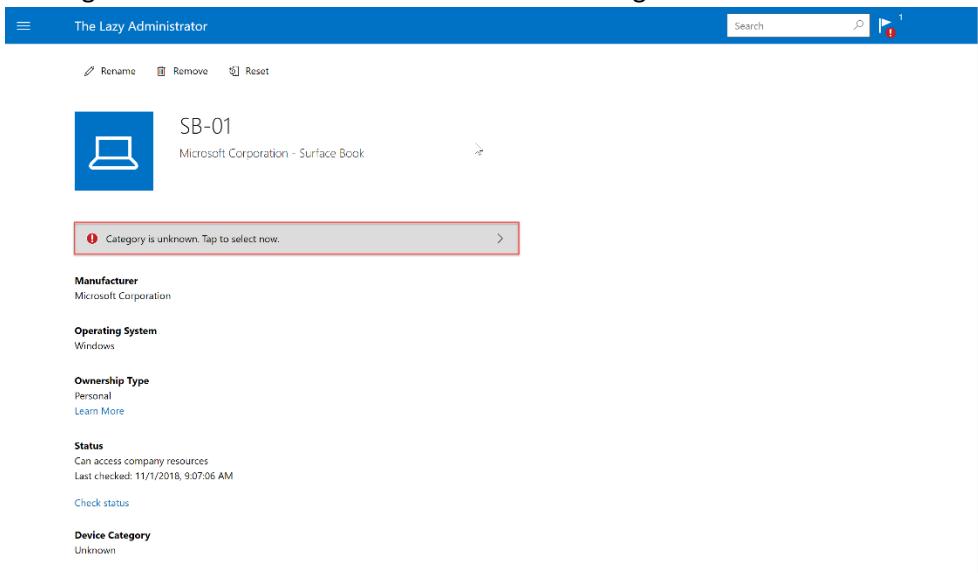
Windows

When users enroll their Windows devices they will need to assign a category in the online Intune portal



The screenshot shows the Microsoft Intune portal's 'Devices' section. At the top, there's a search bar and a notification icon with a '1'. Below the header, the word 'Devices' is displayed. Two devices are listed: 'Brad's iPhone' and 'SB-01'. The 'SB-01' card has a red border around it, and a small red exclamation mark icon is visible in the top right corner of the card. Below the cards, a message says 'Tap here to tell us which device you're using or add a new device.' A navigation arrow is at the bottom right.

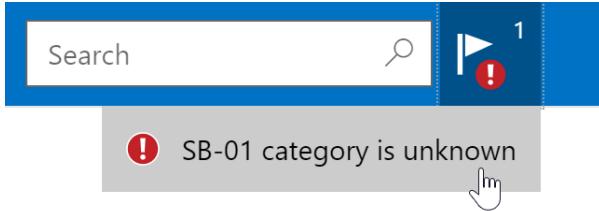
Clicking on the device will show them the outstanding notification and allow them to select a category



This screenshot shows the detailed view for the device 'SB-01'. At the top, there are buttons for 'Rename', 'Remove', and 'Reset'. Below the device name, it says 'Microsoft Corporation - Surface Book'. A message box at the top left says 'Category is unknown. Tap to select now.' with a red border and a red exclamation mark icon. The device details are listed as follows:

- Manufacturer:** Microsoft Corporation
- Operating System:** Windows
- Ownership Type:** Personal
[Learn More](#)
- Status:** Can access company resources
Last checked: 11/1/2016, 9:07:06 AM
[Check status](#)
- Device Category:** Unknown

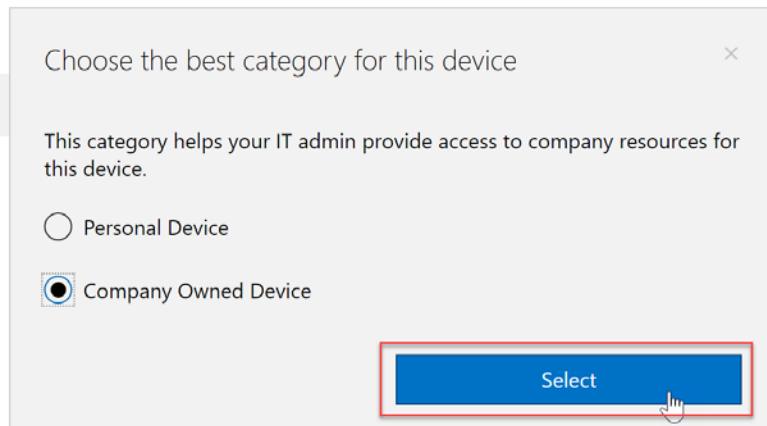
In the top right of the portal they will also see a notification



This screenshot shows a notification in the top right corner of the Microsoft Intune portal. It displays the message 'SB-01 category is unknown' next to a red exclamation mark icon. A hand cursor is shown pointing at the notification.

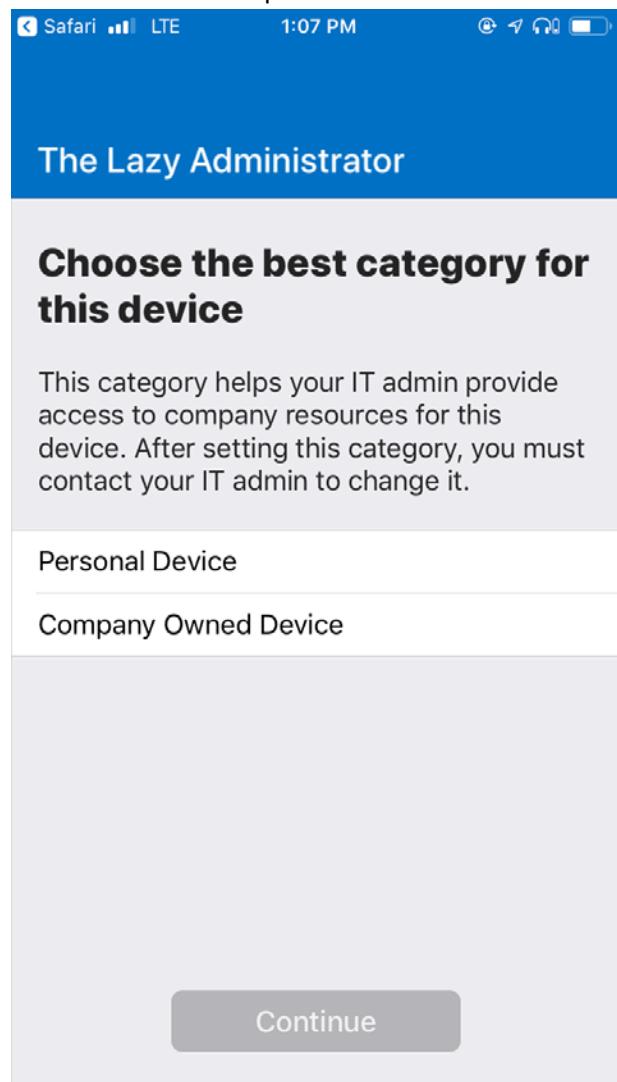
Here we see the two categories I set up for the users to select. Since this machine is a Company Owned Device I will select the category. Behind the scenes, this device is added to that dynamic group and

allows for a better management experience.



iOS

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



Intune Policies

Compliance Policies

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.

Navigate to the Azure portal and select the Intune blade

Select “Device Compliance” and then “Policies”

The screenshot shows the Microsoft Intune interface in the Azure portal. On the left, there's a sidebar with various navigation options like Overview, Quick start, Device enrollment, Device compliance (which is highlighted with a red box), Device configuration, Devices, Client apps, eBooks, Conditional access, On-premises access, Users, Groups, Roles, and Software updates. Below that is a Help and support section with links for Help and support and Troubleshoot. The main content area is titled "Device compliance - Policies". It has sections for Manage (with Policies highlighted in a blue box and a red border), 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). At the bottom of the content area, there's a "Help and support" link.

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. Once we specify a name and platform we

will have different compliance settings that we can configure become available.

The screenshot shows the Microsoft Intune Device compliance - Policies page. A new policy is being created, highlighted by a red box. The policy is named "iOS - Personal Devices Policy L1" and has a description "Compliance policy for end user personal iOS devices". The platform is set to "iOS". The "Configure" button is visible, and the "Actions for noncompliance" section shows "1 configured". The "Scope (Tags)" section shows "0 scope(s) selected".

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

The screenshot shows the "iOS compliance policy" configuration screen. Under "System Security", there are sections for "Password" and "Device Security". In "Password", settings include "Require" (selected), "Simple passwords" (selected), "Minimum password length" (set to 6), "Required password type" (set to "Alphanumeric"), "Number of non-alphanumeric characters in password" (set to "Not configured"), "Maximum minutes after screen lock before password is required" (set to "Immediately"), "Maximum minutes of inactivity until screen locks" (set to "Immediately"), "Password expiration (days)" (set to 30), and "Number of previous passwords to prevent reuse" (set to 3). In "Device Security", there is a "Restricted apps" section with fields for "App name" and "App Bundle ID", both currently set to "Not configured". The "OK" button is highlighted with a red arrow pointing to it.

Next, we will need to assign this policy to devices or users. Click the Assignments item under Manage

iOS - Personal Devices Policy L1

Device compliance policy

Search (Ctrl+ /) <>

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: 0

Error: 0

Conflict: 0

Assigned to non-iOS devices: 0

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

iOS - Personal Devices Policy L1 - Assignments

Device compliance policy

Search (Ctrl+ /) <>

Save Discard Evaluate

Overview

Manage

Properties

Assignments

Monitor

Device status

User status

Per-setting status

Select groups to include

Azure AD groups

+ Invite

Select

Search by name or email address

G5 group 5 group5@bwya77.com

I- Intune - Company Devices

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

No assignments

Selected
Itune - Personal Devices

Select

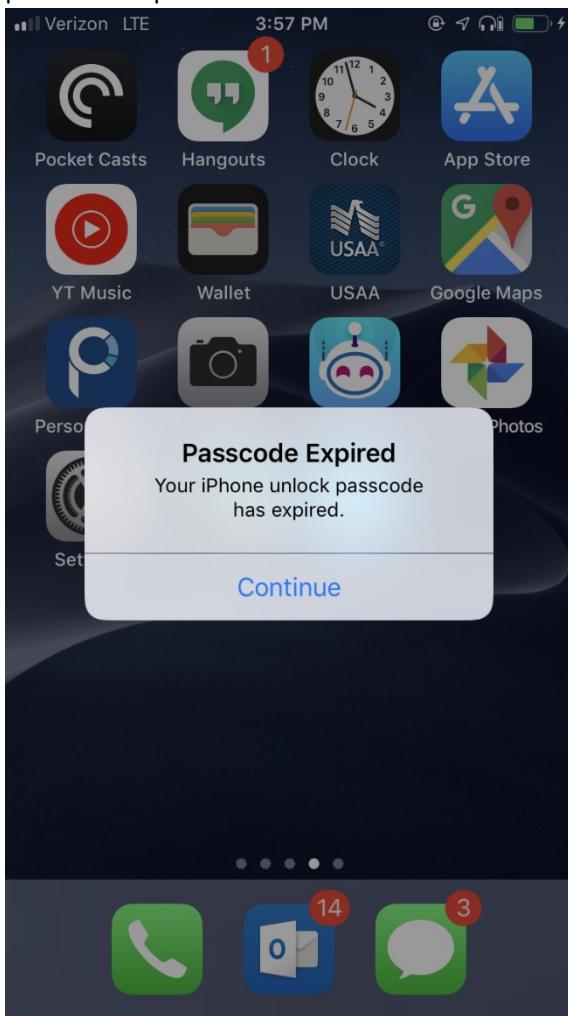
If I want to make sure the policy goes into effect immediately on a device, I can go to All Devices and find my device and force a resync.

Brad's iPhone

The screenshot shows the 'Overview' tab for 'Brad's iPhone' in the Intune portal. The top navigation bar includes buttons for Retire, Wipe, Delete, Remote lock, Sync (which is highlighted with a red box), Remove passcode, Restart(supervised only), and More. Below the navigation bar, a message indicates 'Remote lock: Completed'. The main content area displays device details such as Device name (Brad's iPhone), Management name (redacted), Associated user (Brad Wyatt), Ownership (Personal), Compliance (Compliant), Serial number (redacted), Operating system (iOS), Device model (iPhone 8), Phone number (redacted), and Last check-in time (10/31/2018, 4:17:46 PM). A 'See more' link is present. At the bottom, a 'Device actions status' table shows a single entry: Remote lock (Status: Complete, Date/Time: 10/31/2018, 1:08:41 PM).

ACTION	STATUS	DATE/TIME
Remote lock	Complete	10/31/2018, 1:08:41 PM

If you set a passcode setting 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.

Basic Configuration Policy Overview

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. The left sidebar has a navigation tree with sections like Overview, Quick start, Manage (Device enrollment, Device compliance, Device configuration), and Help and support (Help and support, Troubleshoot). The 'Device configuration' section is expanded, and 'Profiles' is selected and highlighted with a red box. The main content area is titled 'Device configuration - Profiles'. It includes a search bar, a 'Create profile' button (also highlighted with a red box), and a table with columns: PROFILE NAME, PLATFORM, PROFILE TYPE, ASSIGNED, and LAST MODIFIED. One row is visible: 'iOS Configuration Lockdown 1' (Platform: iOS, Type: Device restrictions, Assigned: Yes, Last modified: 10/31/1).

PROFILE NAME	PLATFORM	PROFILE TYPE	ASSIGNED	LAST MODIFIED
iOS Configuration Lockdown 1	iOS	Device restrictions	Yes	10/31/1

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

Create profile X

* Name

Win10 - Corp - Device Restrictions ✓

Description

Policy for Windows 10 corp. owned devices ✓

* Platform

Windows 10 and later ▼

* Profile type

Device restrictions ▼

Settings

Configure >

Scope (Tags)

0 scope(s) selected >

Create

Configure the necessary settings for your specific policy

Device restrictions X

Windows 10 and later

- General ⓘ >
2 of 24 settings configured
- Locked Screen Experience ⓘ >
6 settings available
- Messaging ⓘ >
3 settings available
- Microsoft Edge Browser ⓘ >
28 settings available
- Network proxy ⓘ >
8 settings available
- Password ⓘ** >
13 settings available
- Per-app privacy exceptions ⓘ >
1 setting available
- Personalization ⓘ >
1 setting available
- Printer ⓘ >
3 settings available
- Privacy ⓘ >
22 settings available
- Projection ⓘ >
3 settings available

OK

Password X

Windows 10 and later

Password ⓘ

Required password type ⓘ Require Not configured

Required password type ⓘ Alphanumeric

Minimum password length ⓘ 6

Number of sign-in failures before wiping device ⓘ Enter a number (1-11)

Maximum minutes of inactivity until screen locks ⓘ 5 Minutes

Password expiration (days) ⓘ 30

Prevent reuse of previous passwords ⓘ 3

Require password when device returns from idle state (Mobile and Holographic) ⓘ Require Not configured

Simple passwords ⓘ Block Not configured

Automatic encryption during AADJ ⓘ Block Not configured

Federal Information Processing Standard (FIPS) policy ⓘ Allow Not configured

Windows Hello device authentication ⓘ Allow Not configured

OK

Device restrictions

Windows 10 and later

1 setting available

- Personalization 1 setting available
- Printer 3 settings available
- Privacy 22 settings available
- Projection 3 settings available
- Reporting and Telemetry 2 settings available
- Search 9 settings available
- Start 28 settings available
- Windows Defender SmartScreen 3 settings available
- Windows Spotlight 9 settings available
- Windows Defender Antivirus 34 settings available

OK

Windows Defender Antivirus

Windows 10 and later

Cloud-delivered protection Not configured

File Blocking Level

Time extension for file scanning by the cloud

Prompt users before sample submission

Time to perform a daily quick scan

Type of system scan to perform

* Day scheduled

* Time scheduled

Detect potentially unwanted applications

Submit samples consent

On Access Protection Not configured

Schedule scan day

Actions on detected malware threats

Low severity

Moderate severity

High severity

Severe severity

OK

Once you have configured all of the settings you'd like, press "Create" under the create profile blade.

Create profile

□ X

* Name
Win10 - Corp - Device Restrictions ✓

Description
Policy for Windows 10 corp. owned devices ✓

* Platform
Windows 10 and later

* Profile type
Device restrictions

Settings >
24 configured

Scope (Tags) >
0 scope(s) selected

 Create

Next, click “Assignments” so we can assign this policy

Win10 - Corp - Device Restrictions
Device configuration profile

Profile assignment status — Windows 10 and later devices

Status	Count
Succeeded	0
Error	0
Conflict	0
Pending	0
Not Applicable	0

Assigned to non-Windows 10 and later devices
0

From there I will select my Intune – Company Devices group to apply this policy to.

Win10 - Corp - Device Restrictions - Assignments
Device configuration profile

Select groups to include

Selected groups

Intune - Company Devices

Select

Uninstall Restricted Applications

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 and then select your profile you want to edit or create a new one. In my example I will modify the profile applied to iOS devices.

Microsoft Intune

Device configuration - Profiles

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

Create profile

Columns

Filter

Refresh

Export

Search by name

PROFILE NAME	PLATFORM	PROFILE TYPE	ASSIGNED	LAST
iOS Configuration Lockdown 1	iOS	Device restrictions	Yes	10/3
Win10 - Corp - Device Restrictions	Windows 10 a...	Device restrictions	Yes	11/01

In the profile select Settings > Restricted Apps, and then under type of restricted apps list select Prohibited Apps. In the next section we will configuring the application we are going to restrict

- Properties

X



Save



Discard

* Name

iOS Configuration Lockdown 1

Description

Enter a description...

* Platform

iOS



* Profile type

Device restrictions



Settings



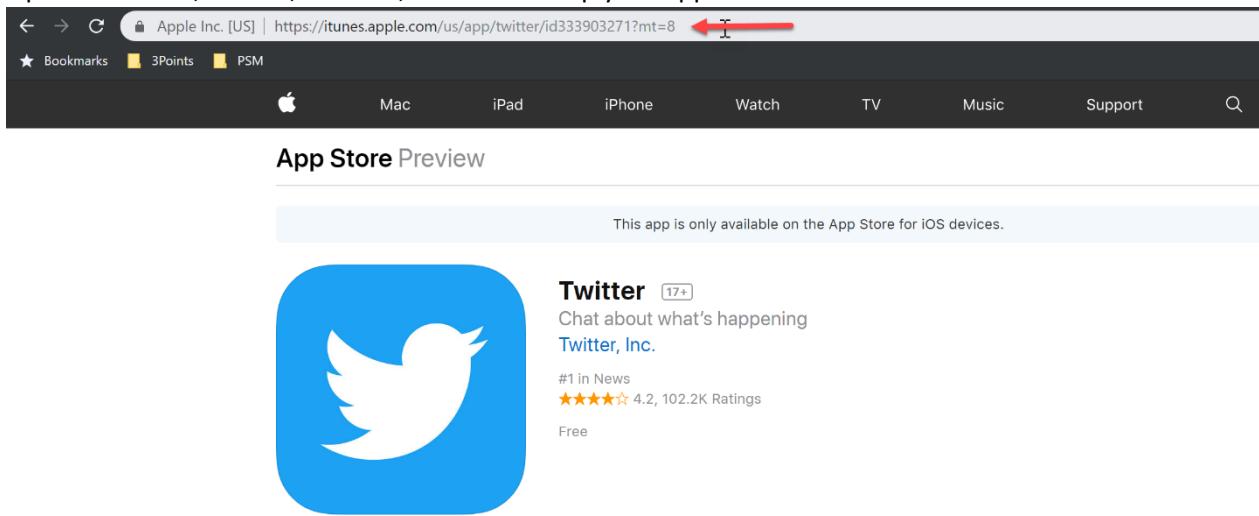
10 configured

Scope (Tags)



0 scope(s) selected

Open a tab in IE, Firefox, Chrome, etc and look up your application and note the itunes store URL



Apple Inc. [US] | https://itunes.apple.com/us/app/twitter/id333903271?mt=8

Bookmarks 3Points PSM

Mac iPad iPhone Watch TV Music Support

App Store Preview

This app is only available on the App Store for iOS devices.

Twitter 17+
Chat about what's happening
Twitter, Inc.
#1 in News
★★★★★ 4.2, 102.2K Ratings
Free

Back in the Azure Portal, past the link and then click "Add"

Restricted Apps

iOS

Use these settings to stay informed about which users install apps that are not approved for use in your company. Select the type of restricted app list:

Prohibited apps - A list of apps that you want to be informed about when users install them.
Approved apps - A list of apps that are approved for use in your company. When users install an app that is not in this list, you will be informed.

Type of restricted apps list ⓘ Prohibited apps ↴

* Apps list ⓘ Import Export

APP URL	APP BUNDLE ID	* APP NAME	PUBLISHER	Add
https://itu...	e.g. com.a...	Twitter	Not configur	

APP URL APP BUNDLE ID APP NAME PUBLISHER Add

No apps

When you have finished your restricted apps list, click OK at the bottom and then save your profile / policy.

Restricted Apps

iOS



Use these settings to stay informed about which users install apps that are not approved for use in your company. Select the type of restricted app list:

Prohibited apps - A list of apps that you want to be informed about when users install them.

Approved apps - A list of apps that are approved for use in your company. When users install an app that is not in this list, you will be informed.

Type of restricted apps list

Prohibited apps



* Apps list

Import

Export

App URL

App Bundle ID

App Name

Publisher

e.g. https://it...

e.g. com.appl...

Not configured

Not configured

Add

APP URL

↑↓

APP BUNDLE ID

↑↓

APP NAME

↑↓

PUBLISHER

↑↓

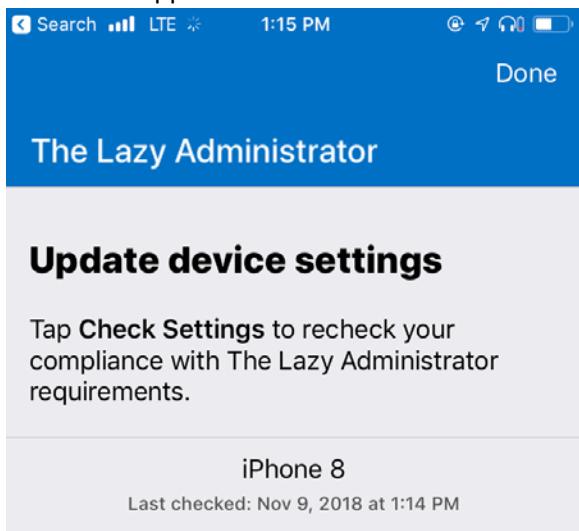
https://itunes.appl...

Twitter

...

OK

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



Uninstall disallowed apps



Uninstall the following apps:

- Twitter

Check Settings

Configure Email Profiles

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. The left sidebar has sections for Overview, Quick start, Manage (with Device enrollment, Device compliance, and Device configuration selected), 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. The main content area is titled "Device configuration - Profiles". It has a search bar, a "Create profile" button (highlighted with a red box), and a table with columns: PROFILE NAME, PLATFORM, PROFILE TYPE, ASSIGNED, and LAST MODIFIED. One row is visible: "iOS Configuration Lockdown 1" (Platform: iOS, Type: Device restrictions, Assigned: Yes, Last modified: 10/31/1).

Give your new profile a name and description. Select the platform that best fits your needs. under profile type select “Email”. In the email blade configure the email profile and then press OK and then

Create to create the profile.

Create profile

* Name
iOS Email Profile

Description
Office 365 Email Profile

* Platform
iOS

* Profile type
Email

Settings
1 configured

Scope (Tags)
0 scope(s) selected

[Create](#)

Email

iOS

* Email server ⓘ
outlook.office365.com

* Account name ⓘ
The Lazy Administrator

* Username attribute from AAD ⓘ
User Principal Name

* Email address attribute from AAD ⓘ
Primary SMTP Address

* Authentication method ⓘ
Username and password

SSL ⓘ
[Enable](#) [Disable](#)

OAuth ⓘ
[Enable](#) [Disable](#)

S/MIME ⓘ
[Disable S/MIME](#)

Amount of email to synchronize ⓘ
Two Weeks

Allow messages to be moved to other email accounts ⓘ
[Enable](#) [Disable](#)

Allow email to be sent from third party applications ⓘ
[Enable](#) [Disable](#)

Synchronize recently used email addresses ⓘ
[Enable](#) [Disable](#)

[OK](#)

Click Assignments to assign your profile to a group or all devices.

iOS Email Profile
Device configuration profile

Search (Ctrl+ /) Delete

Overview

Manage

Properties

Assignments ← jm

Monitor

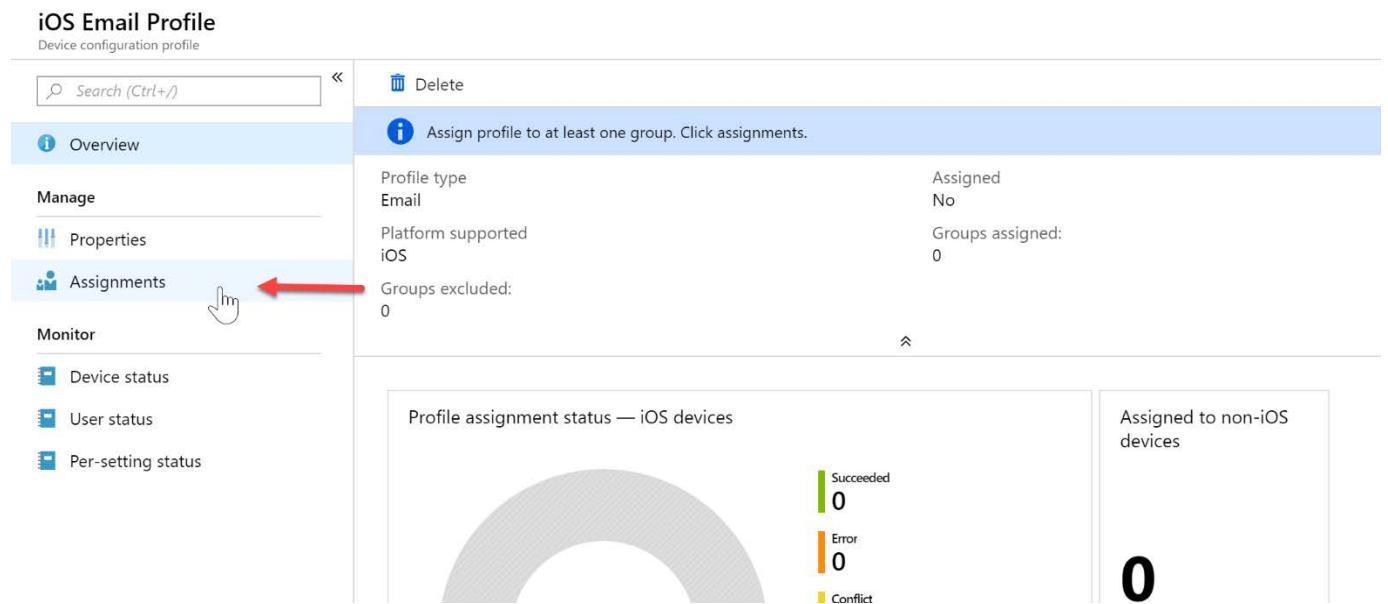
Device status User status Per-setting status

Profile type: Email **Assigned:** No
Platform supported: iOS **Groups assigned:** 0
Groups excluded: 0

Profile assignment status — iOS devices

Succeeded	Error	Conflict
0	0	0

Assigned to non-iOS devices 0



In my example, I am applying it to all devices. This will apply to all iOS devices. If there are other devices, such as Android, it will just list as not applicable.

iOS Email Profile - Assignments
Device configuration profile

Search (Ctrl+ /)

Overview

Manage

Properties

Assignments

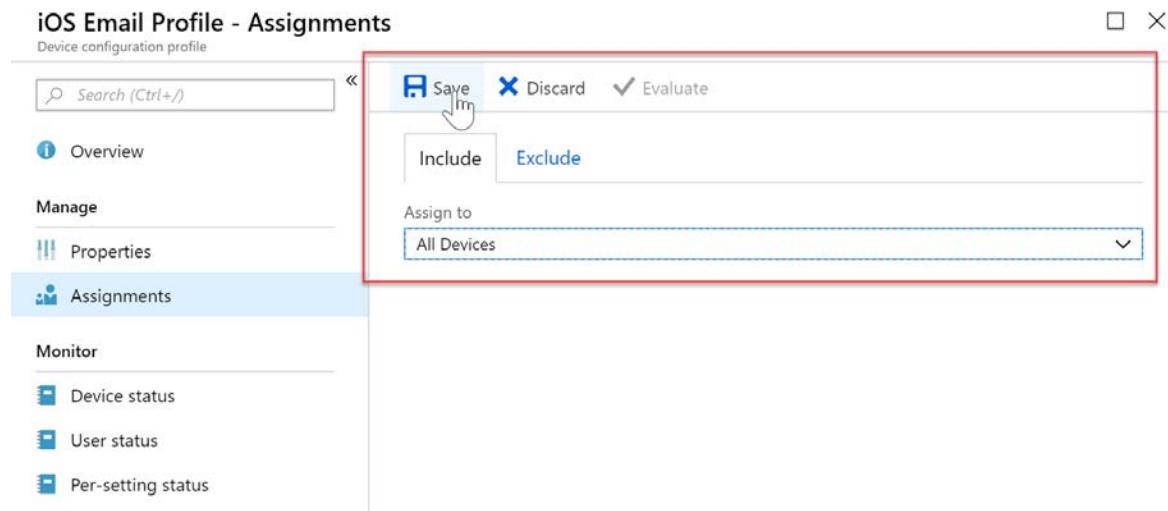
Monitor

Device status User status Per-setting status

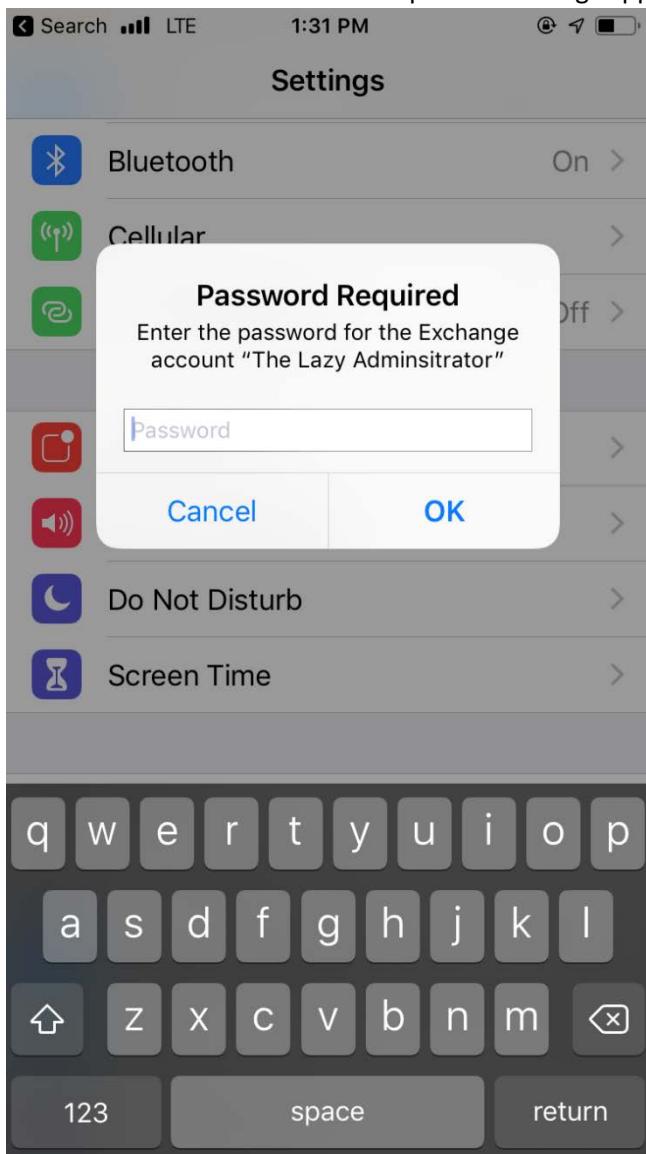
Save ← **Discard** **Evaluate**

Include **Exclude**

Assign to: All Devices



Back on my iOS device it will automatically add the account. On an iOS device the account is in Settings > Password and Accounts. When I open the settings application it immediately asks me for my password



When I go to Passwords and Accounts I can see that the account was automatically added

The screenshot shows the 'EXCHANGE' section of the 'Passwords & Accounts' settings. It lists an account for 'brad@thelazyadministrator.com' with several sync options enabled:

- Mail: On
- Contacts: On
- Calendars: On
- Reminders: On
- Notes: On

Below this, there is a 'Mail Days to Sync' setting set to '2 Weeks'. Under 'Automatic Reply', it says 'Loading...'. A note at the bottom states: 'These settings are installed by the profile 'Eas Profile - outlook.office365.combrad@thelazyadministrator.com''.

Modify iOS Dock

In this example I will be showing you how Intune can modify users home docks. I will be making a profile / policy that will ensure the default Phone application is on the dock.

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), Help and support, and Troubleshoot. The 'Device configuration' section is selected and highlighted with a red box. In the main content area, there's a search bar, a 'Create profile' button (also highlighted with a red box), and a table showing existing profiles. The table columns include PROFILE NAME, PLATFORM, PROFILE TYPE, ASSIGNED, and LAST MODIFIED. One profile named 'iOS Configuration Lockdown 1' is listed, assigned to iOS with a Device restrictions type, last modified on 10/31/1.

The platform must be iOS and the Profile type is going to be “Device Features”. In the device features blade select Home Screen Layout and select Dock.

The screenshot shows the 'Add Phone to iOS Dock - Properties' blade. In the 'Properties' section, fields for Name (set to 'Add Phone to iOS Dock') and Description (set to 'Enter a description...') are shown. The 'Platform' dropdown is set to 'iOS' and highlighted with a red box. The 'Profile type' dropdown is set to 'Device features' and highlighted with a red box. In the 'Device features' section, categories like AirPrint, Home Screen Layout (supervised only), App Notifications, Shared Device Configuration, Single Sign On, and Web Content Filter are listed. The 'Home Screen Layout (supervised only)' category is expanded, showing 'Dock' settings with 1 app and 0 folders. A note says 'Find out how this can impact different form factors here.'

When adding a new application you will need to know the App Bundle ID. If the application is not a default iOS application you can follow these steps to obtain the bundle ID.

The screenshot shows two windows side-by-side. The left window is titled 'Dock' and contains instructions for selecting apps or folders to add to the dock. It includes a note about a maximum of 6 items and a link for 'Apps and folders'. The right window is titled 'Edit Row' and is specifically for adding apps and folders. It has a field for 'Type' set to 'App', an 'App Name' field containing 'Phone', and an 'App Bundle ID' field containing 'com.apple.mobilephone'. Both windows have an 'OK' button at the bottom.

The application will automatically be placed on the dock on iOS devices once the profile gets pushed to the device.

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.

Windows

To create a Windows Software Update policy first select the Intune blade > Software Updates > Windows 10 Update Rings, and then “Create”

The screenshot shows the Microsoft Intune interface. On the left, there's a sidebar with various management options like Overview, Quick start, Device enrollment, and Software updates. The Software updates option is highlighted with a red box. The main content area is titled "Software updates - Windows 10 Update Rings". It has a search bar at the top right. Below it is a table header with columns: NAME, FEATURE DEFERRED, QUALITY DEFERRED, FEATURE, and Q!. A red box highlights the "+ Create" button in the top right corner of the table area. The table body below says "There are no Windows 10 Update Rings to show."

Give your policy a name and description. In the Settings you can begin configuring the policy settings. Below I am 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.

Create Update Ring

X

Set

Wind

* Name

Company Devices - Windows 10



Description

Company devices on Windows Insider



Settings



Configure

Scope (Tags)



0 scope(s) selected

* Mi

* Wi

* Qu

* Fea

* Set
days

Use

Auto

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

Create Update Ring

* Name
Company Devices - Windows 10 

Description
Company devices on Windows Insider 

Settings
14 configured >

Scope (Tags)
0 scope(s) selected >

Create 

Once the policy has been created, click “Assignments” to assign the policy to devices or groups.

Company Devices - Windows 10

Windows 10 Update Ring

Search (Ctrl+ /) <>

Delete Pause Resume Extend Uninstall

Overview

Manage

Properties

Assignments 

Monitor

Device status

User status

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

Click Assignments to assign this ring to at least one group.

Profile assignment status — Windows 10 and later devices

Succeeded	0
Error	0
Conflict	0

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 click the “Select groups to include” and then selecting my “Intune –

Company Devices" group.

Company Devices - Windows 10 - Assignments

Windows 10 Update Ring

Save Discard Evaluate

Include Exclude

Assign to Selected Groups

Select groups to include >

No assignments

Select groups to include

Azure AD groups

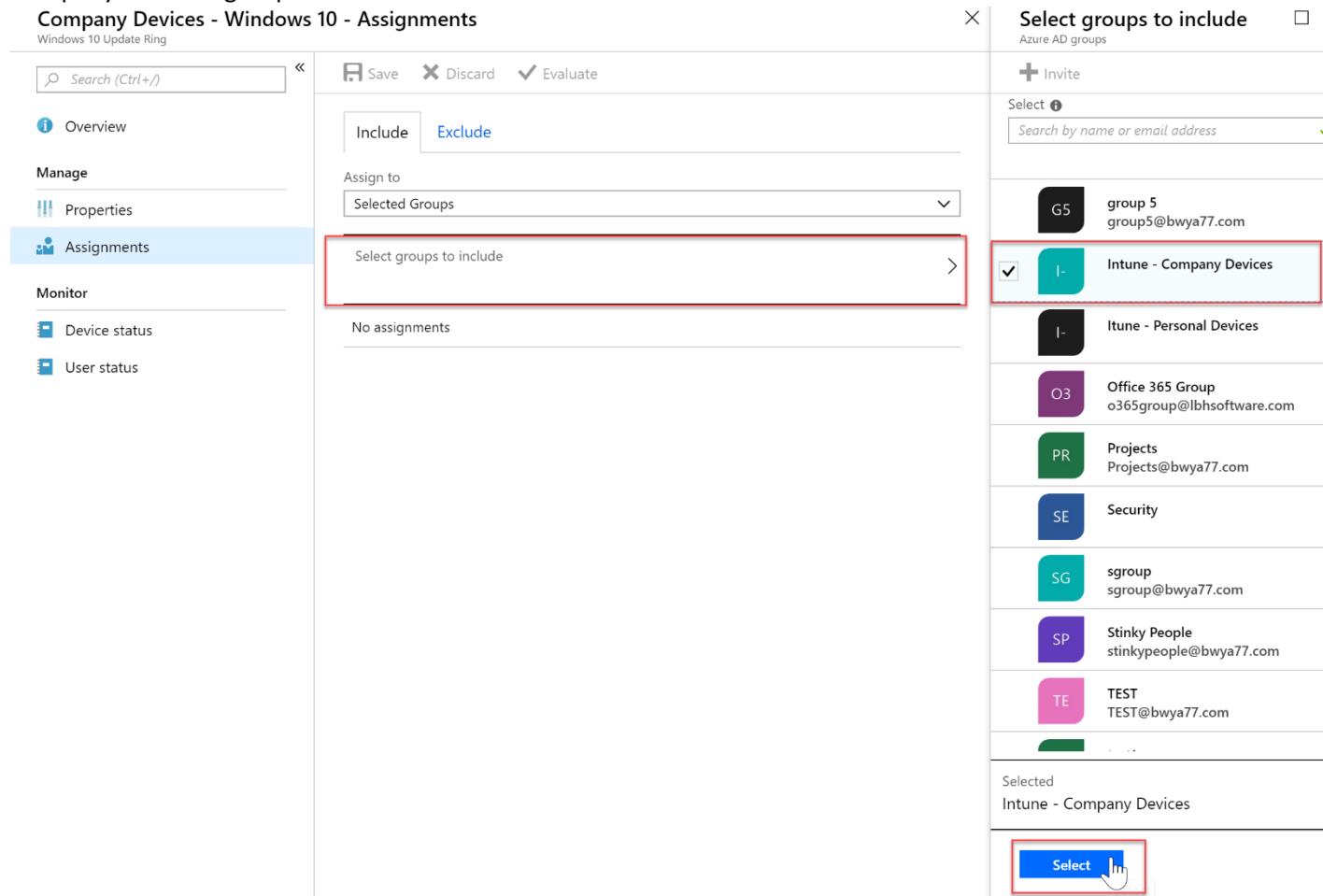
+ Invite

Select *i* Search by name or email address

Group	Description
G5	group 5 group5@bwya77.com
I-	Intune - Company Devices
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 



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.

Intune - Company Devices - Members

Group

Overview

Add members Refresh

Manage

Properties

Members (selected)

Owners

Group memberships

Applications

Licenses

Azure resources

Dynamic membership rules

Activity

Access reviews

Audit logs

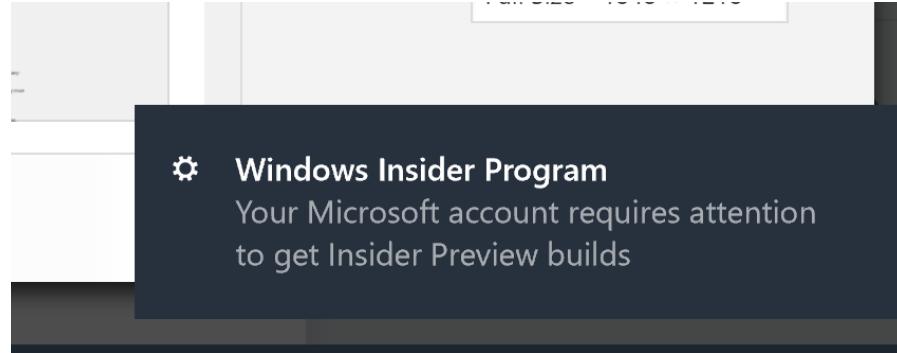
Troubleshooting + Support

Troubleshoot

New support request

NAME	TYPE
SB-01	Device

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



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.

Windows Insider Program

*Some settings are hidden or managed by your organization.

Get Insider Preview builds

We need to restart your PC before you can start getting Insider Preview builds.

Restart now

Stop Insider Preview builds

iOS

To create a Windows Software Update policy first select the Intune blade > Software Updates > Update Policies for iOS, and then “Create”

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), Help and support (Help and support, Troubleshoot), and Software updates (which is highlighted with a red box). The main content area is titled "Software updates - Update policies for iOS". It has a search bar, a "Create" button (also highlighted with a red box), and columns for NAME and RESTRICTED DAYS. A message says "There are no iOS update policies to display". Below the table, there are sections for Monitor (Per update ring deployment sta..., Installation failures for iOS devi..., Audit logs) and Help and support (Help and support).

Give your 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.

Create update policy X

* Name
Company Policy - iOS ✓

Description
Enter a description... ✓

Settings Configure >

Scope (Tags) 0 scope(s) selected >

Settings ios

Use this update profile to force targeted devices to scan and install the latest iOS updates. You can configure settings around when not to install updates and how long to delay the visibility of software updates to the end user. Delaying the visibility of software updates prevents your end users from initiating and installing the latest software update, but does not affect the scheduled updates as configured by the rest of the profile. These updates will only apply to supervised iOS devices.

[Learn More](#)

Select times to prevent update installations:

Days Mon,Tue,Wed,Thu,Fri

Time zone UTC-6

Start time 8 AM

End time 5 PM

End user experience settings:

* Delay visibility of software updates to end users with no change to scheduled updates (days) 14 ✓

Create OK

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

Create update policy

* Name

Company Policy - iOS 

Description

Enter a description... 

Settings

5 configured



Scope (Tags)

0 scope(s) selected



Create 

Click “Assignment” to assign your policy to groups or devices.

Company Policy - iOS
iOS Updates

Overview

Manage

Properties

Assignments 

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 
Azure AD groups

Invite

Select  Search by name or email address

G5 group 5 group5@bwya77.com

I- Intune - Company Devices  

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 

You will now see your newly created policy

[Create](#) [Columns](#) [Refresh](#) [Export](#)

Search by name

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	...

Enable Windows 10 automatic enrollment

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.

In the Azure Portal select Azure Active Directory and then click “Mobility (MDM and MAM) and select “Microsoft Intune”

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is open, with 'Azure Active Directory' highlighted by a red box. Under 'Azure Active Directory', the 'Mobility (MDM and MAM)' option is also highlighted by a red box. The main content area shows the 'bwya77 - Mobility (MDM and MAM)' blade. At the top right, there is a search bar with the placeholder 'intune policies'. Below the search bar, there are two buttons: '+ Add application' and 'Columns'. The main pane displays a table with a single row. The row has a blue icon, the name 'Microsoft Intune', and a small 'Im' label. A red box highlights the 'Microsoft Intune' name. To the right of the table, there is a vertical sidebar with the heading 'Manage' followed by a list of options: Users, Groups, Organizational relationships, Roles and administrators, Enterprise applications, Devices, App registrations, App registrations (Preview), Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings, Properties, and Notifications settings.

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

Home > bwya77 - Mobility (MDM and MAM) > Configure

Configure

Microsoft Intune

MDM user scope All

MDM terms of use URL

MDM discovery URL

MDM compliance URL

[Restore default MDM URLs](#)

MAM User scope All

MAM Terms of use URL

MAM Discovery URL

MAM Compliance URL

[Restore default MAM URLs](#)

Important

If both MAM user scope and automatic MDM enrollment (MDM user scope) are enabled for a group, only MAM is enabled. Only MAM is added for users in that group when they workplace join personal device. Devices are not automatically MDM enrolled.

Enroll Devices into Intune

iOS

Have your users download and install the Company Portal from the iOS App Store

App Store Preview

This app is only available on the App Store for iOS devices.



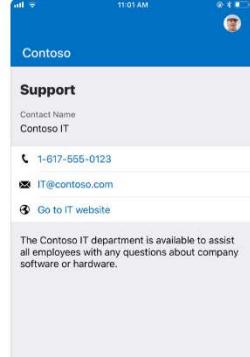
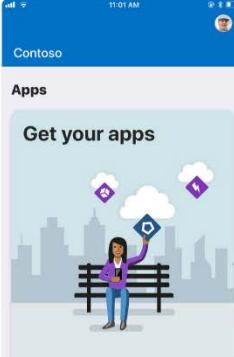
Intune Company Portal 4.4

Company resources on the go
Microsoft Corporation

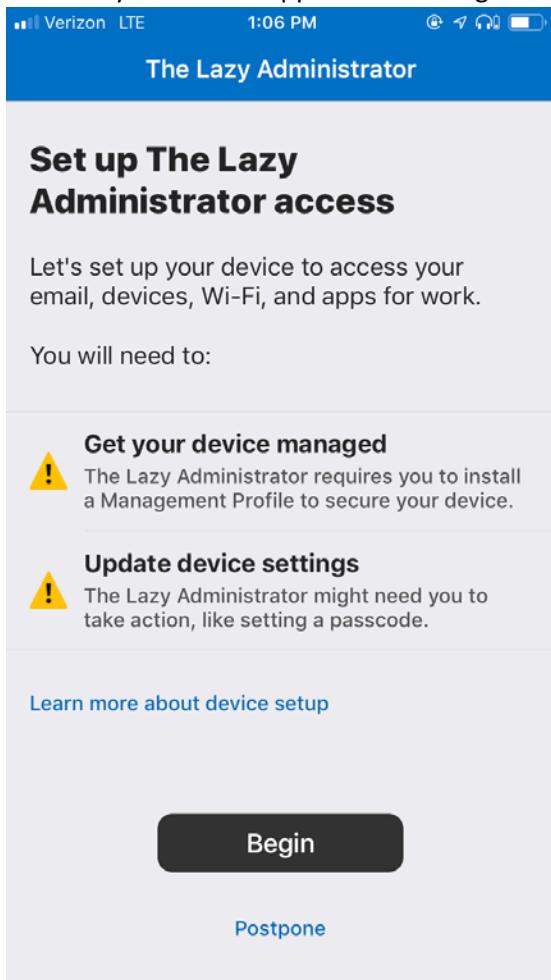
#28 in Business
★★★★★ 4.5, 86.6K Ratings

Free

Screenshots iPhone iPad



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



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

A screenshot of a mobile application interface. At the top, there is a blue header bar with the text "Verizon LTE" and "1:06 PM". Below the header, a back arrow icon and the word "Back" are visible. The main content area has a white background. At the top left of this area, there is a bold title: "What can The Lazy Administrator see?". Below the title, there are two sections: "The Lazy Administrator can never see:" and "The Lazy Administrator may see:". Each section contains a bulleted list of items. At the bottom of the screen, there is a "Continue" button.

Verizon LTE 1:06 PM

Back

What can The Lazy Administrator see?

🚫 The Lazy Administrator can never see:

- Call and web history
- Email and text messages
- Contacts and calendar
- Passwords
- Photos

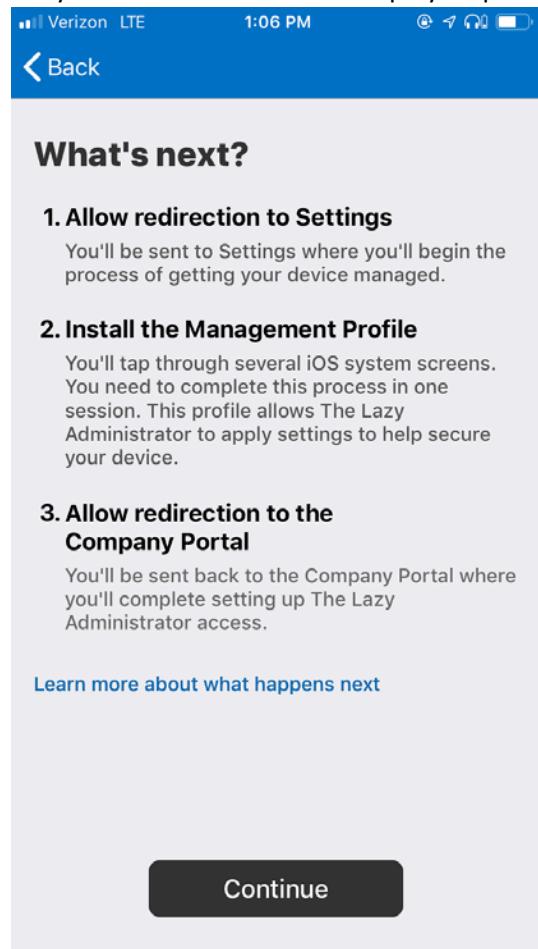
👤 The Lazy Administrator may see:

- Model and serial number
- Operating system
- App names
- Owner and device name
- Phone number for corporate devices
- Device location for lost corporate devices

[Learn more](#)

Continue

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



An MDM iOS Profile will be installed on the device

Safari LTE 1:07 PM

[Cancel](#)

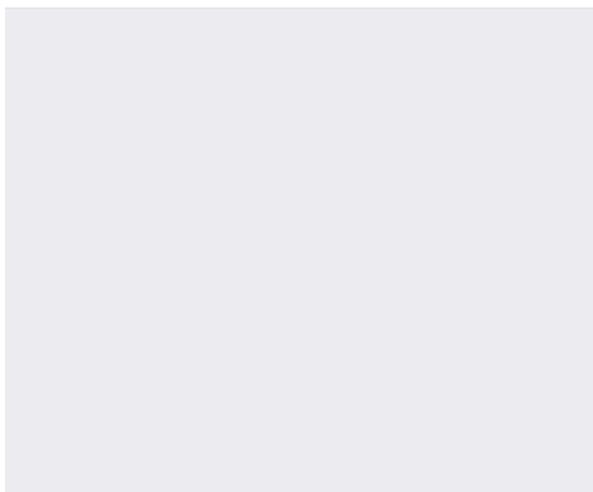
Warning

[Install](#)

MOBILE DEVICE MANAGEMENT

Installing this profile will allow the administrator at "https://i.manage.microsoft.com/DeviceGatewayProxy/ioshandler.ashx" to remotely manage your iPhone.

The administrator may collect personal data, add/remove accounts and restrictions, install, manage, and list apps, and remotely erase data on your iPhone.



Safari LTE 1:07 PM

Profile Installed Done



Management Profile

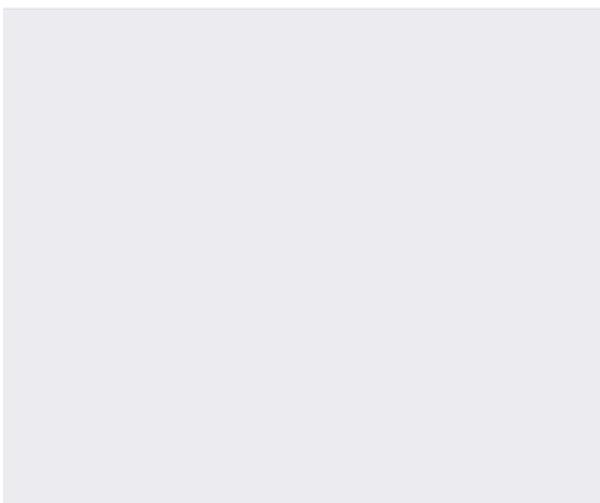
bwya77

Signed by [IOSProfileSigning.manage.microsoft.com](#)
Verified ✓

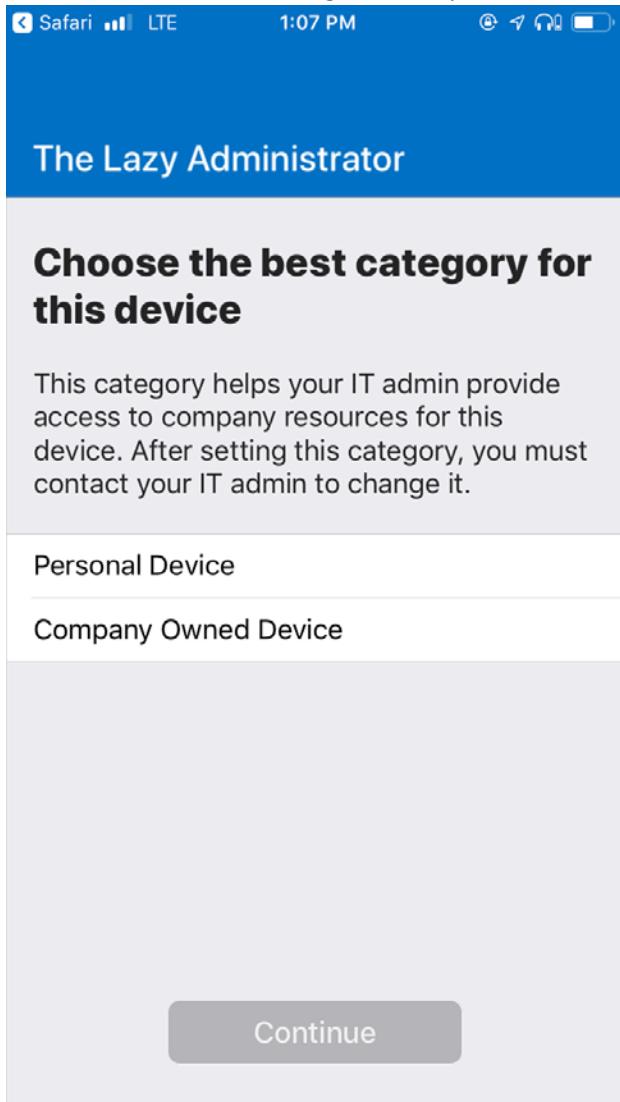
Description Install this profile to get access to your
company apps

Contains Mobile Device Management
Device Identity Certificate

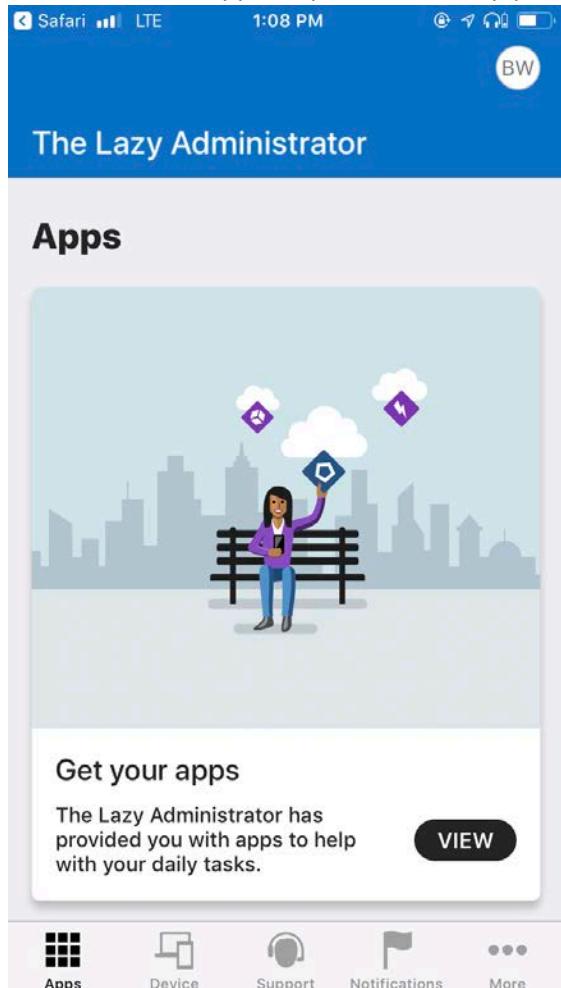
More Details >



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.



Windows

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.

Online Portal

Navigate to the online Company Portal at <https://portal.manage.microsoft.com>

Once the user signs into the Company Portal they can add a device under Devices

A screenshot of the Company Portal web interface. The top navigation bar includes a menu icon, the user name 'The Lazy Administrator', a search bar, and a magnifying glass icon. The main content area is titled 'Devices' and shows two cards: 'Brad's iPhone' (an iPhone icon) and 'SB-01' (a laptop icon). Below the cards is a grey bar with the text 'Tap here to tell us which device you're using or add a new device.' and a red arrow pointing left.

The Lazy Administrator

Search

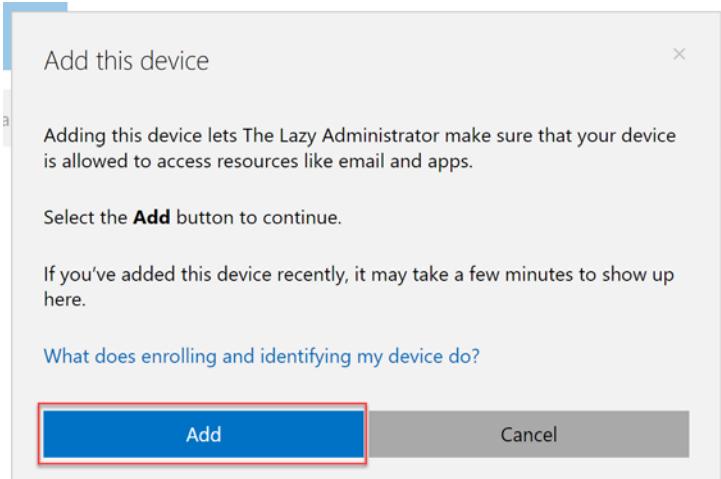
Devices

Brad's iPhone

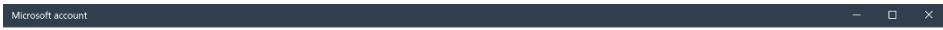
SB-01

Tap here to tell us which device you're using or add a new device. < >

Click "Add"



Have them sign in and then press Next



Set up a work or school account

You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

brad@thelazyadministrator.com

Alternate actions:

These actions will set up the device as your organization's and give your organization full control over this device.

[Join this device to Azure Active Directory](#)
[Join this device to a local Active Directory domain](#)

The user will be prompted to enter their account password and then press “Sign In”



Enter password

Enter the password for brad@thelazyadministrator.com

[Forgot my password](#)

[Need help?](#)

Please sign in using your secure login. If you have any issues please contact the Help Desk at (555) 555-5555

[Sign in with another account](#)

[Privacy statement](#)



[Sign in](#)

Once complete they will be prompted with a successful message.



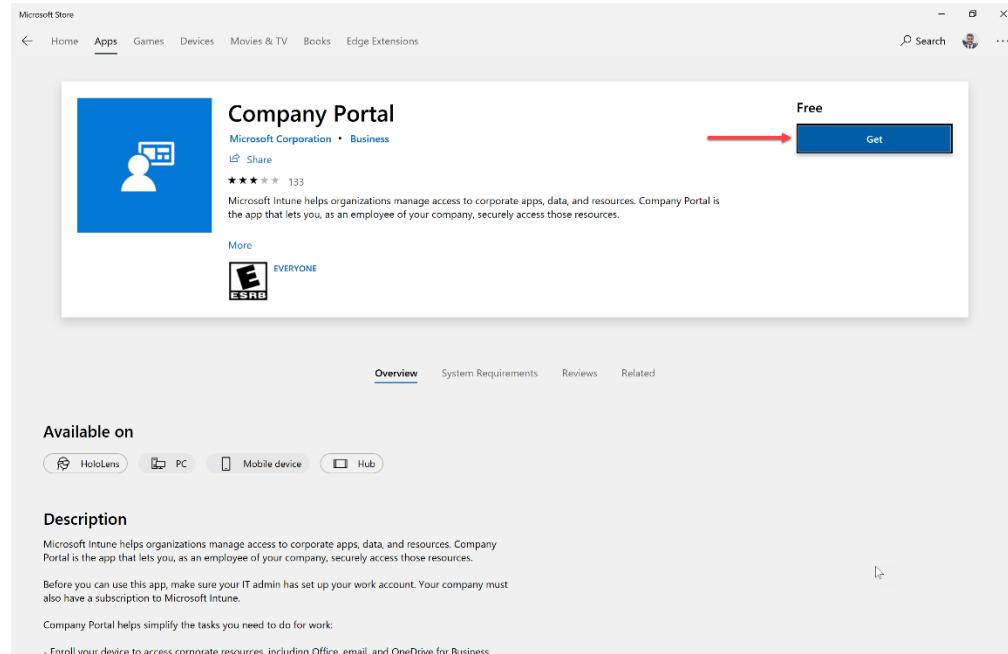
You're all set!

We've added your account successfully. You now have access to your organization's apps and services.

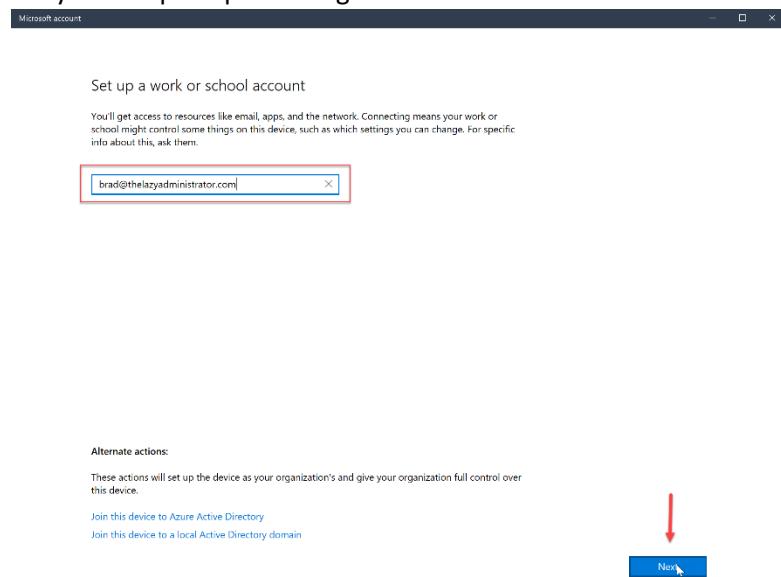
 [Done](#)

Microsoft Store App

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



They will be prompted to sign in



They will be prompted for the password

 X

Enter password

Enter the password for brad@thelazyadministrator.com

[Forgot my password](#)

Need help?

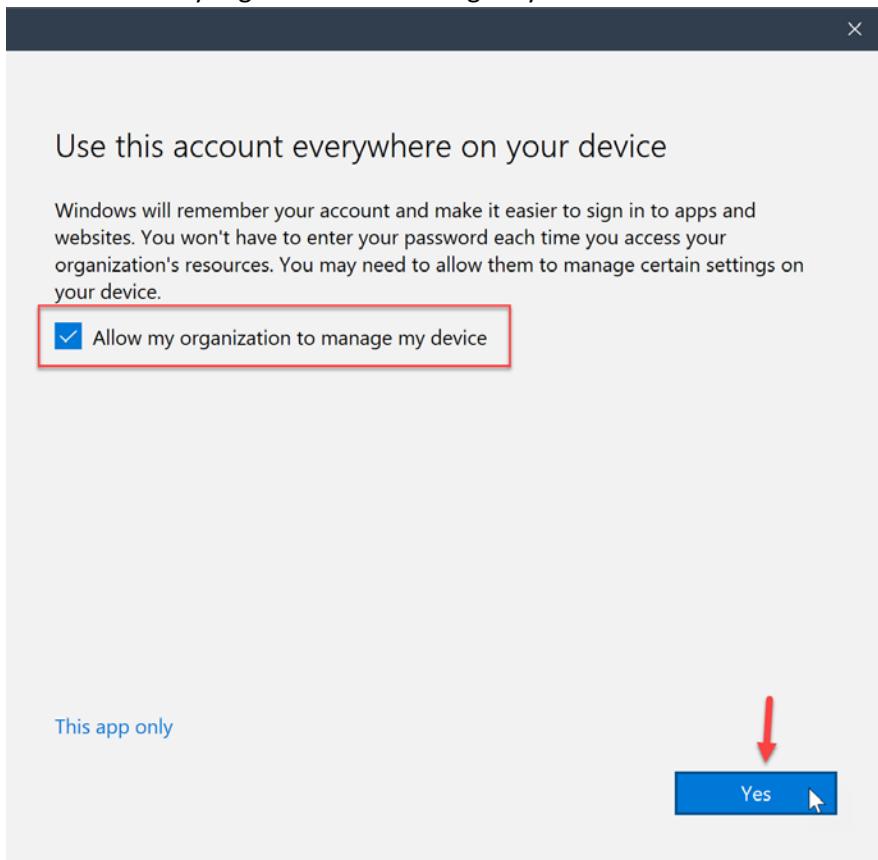
Please sign in using your secure login. If you have any issues please contact the Help Desk at (555) 555-5555

[Sign in with another account](#)

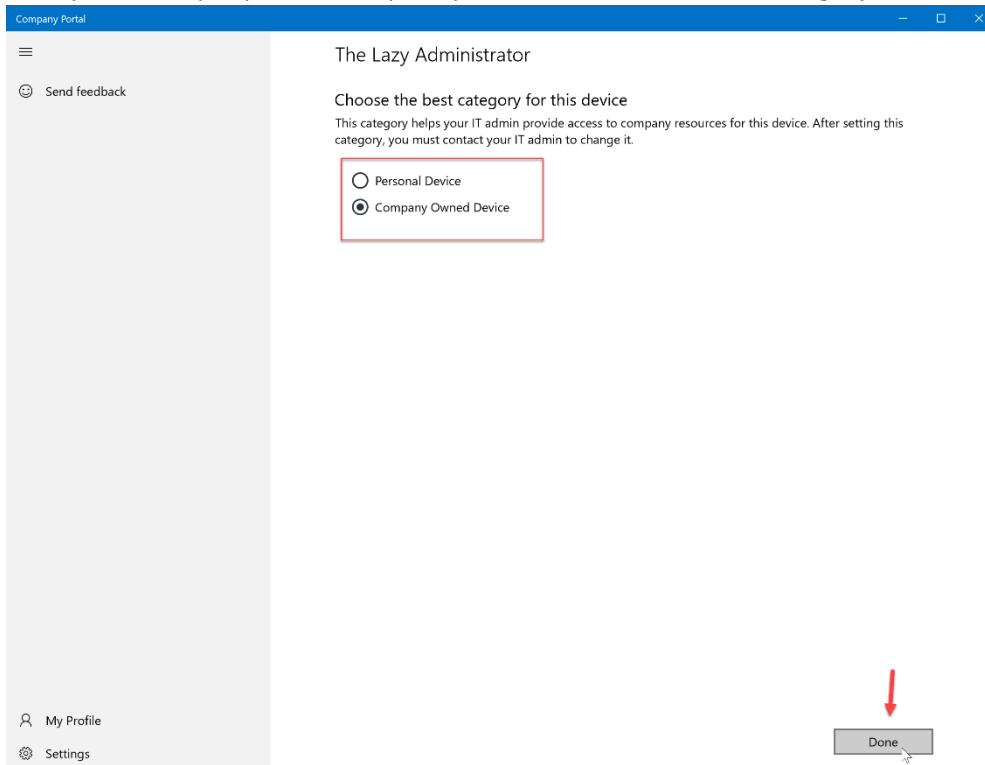
[Privacy statement](#)

 [Sign in](#)

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

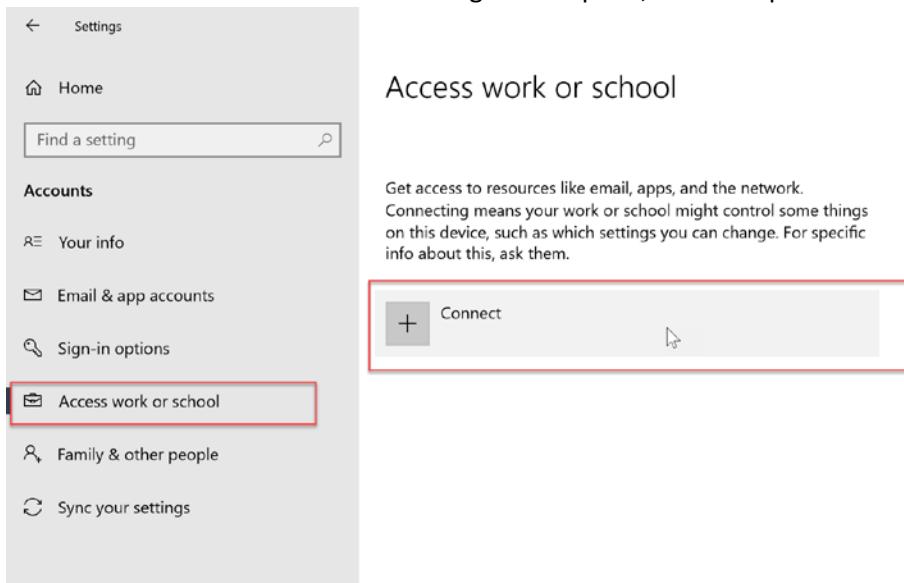
The screenshot shows the Company Portal application window titled "The Lazy Administrator". On the left sidebar, there are links for Home, All apps, Installed apps, and Send feedback. The main content area is titled "My Devices" and shows two devices: "This device" (laptop icon) labeled "SB-01" and "Brad's iPhone" (phone icon). Below this, there is a section for "Bradley Wyatt" with "Email" (brad@thelazyadministrator....) and "Website" (Help Me) links.

Windows Settings App

Open the Windows Settings application and select “Accounts”

The screenshot shows the Windows Settings application window titled "Windows Settings". At the top is a search bar labeled "Find a setting". Below it are several settings categories: System, Devices, Phone, Network & Internet, Personalization, Apps, Accounts (which is highlighted with a red box), Time & Language, Gaming, Ease of Access, Cortana, Privacy, and Update & Security.

Select “Access work or school” in the right hand pane, and then press “Connect”



Sign in using your work account



Alternate actions:

These actions will set up the device as your organization's and give your organization full control over this device.

[Join this device to Azure Active Directory](#)

[Join this device to a local Active Directory domain](#)

[Next](#)

Enter your work account password and then press Sign In

X

Enter password

Enter the password for brad@thelazyadministrator.com

A password input field containing six dots ('.....') as placeholder text. A red rectangular box highlights the entire input field.

[Forgot my password](#)

[Need help?](#)

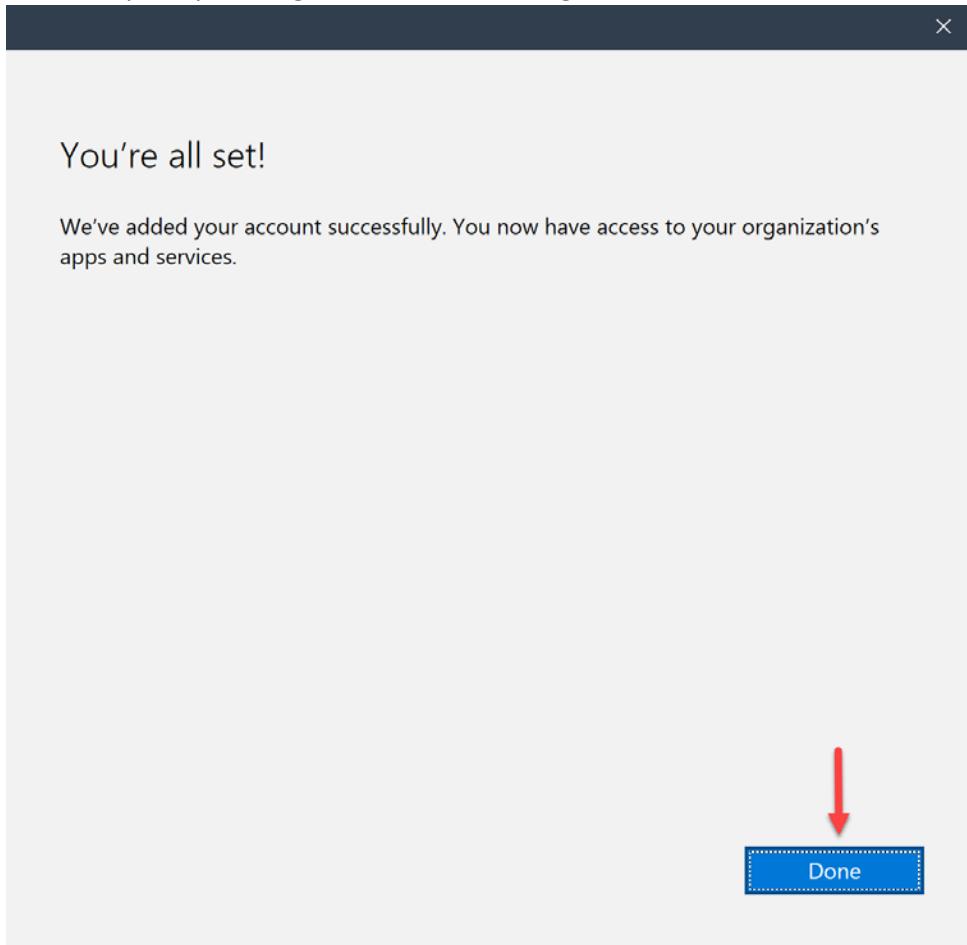
Please sign in using your secure login. If you have any issues please contact the Help Desk at (555) 555-5555

[Sign in with another account](#)

[Privacy statement](#)

 [Sign in](#)

Once complete you will get a successful message



Back in the Settings app you will now see your account

Access work or school

Get access to resources like email, apps, and the network.

Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.



 Work or school account
brad@thelazyadministrator.com

Deploy Client Apps to Managed Intune Devices

The Company Portal allows and 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 is relevant to the device they are on, if they are on an iPhone it will not display your published applications for Windows even if the device is in the same group.

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

Microsoft Intune < Client apps - Apps

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

Troubleshoot

Overview Manage

Search (Ctrl+ /)

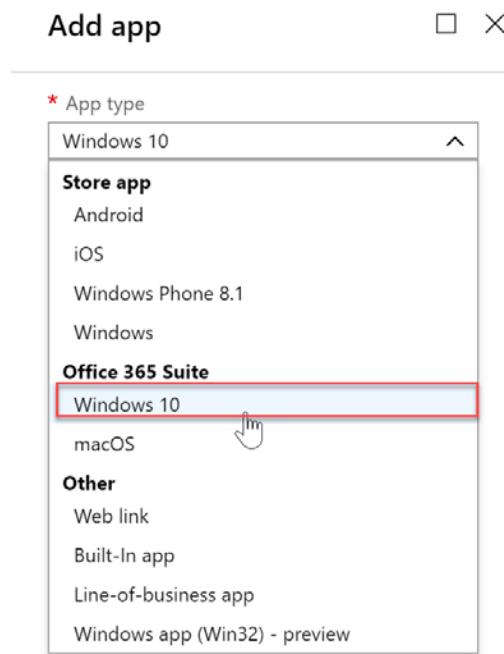
Search (Ctrl+ /)

+ Add Refresh Export Columns

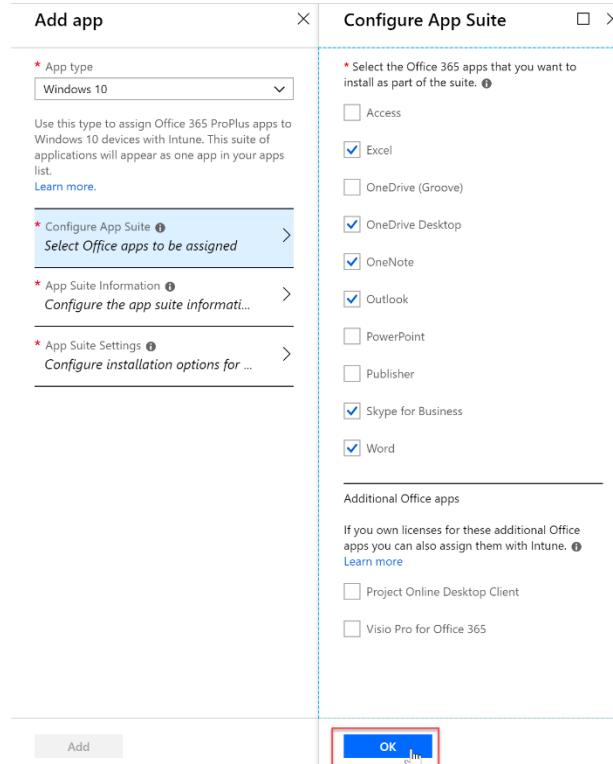
Search by name or publisher...

NAME	TYPE	STATUS	ASSIGNED
Office 365	Office 365 ProPlus Suite (Windows 10)	Yes	
The Lazy Admin Blog	Web link	Yes	
Todoist: Organize your life	iOS store app	Yes	

For my example, I will be deploying Office 365 ProPlus to my devices so I will select Windows 10 under Office 365 Suite



I will configure the app settings to fit my company needs



I can even configure the update channel, EULA and more

The screenshot shows two adjacent configuration pages. On the left is the 'Add app' page, where 'Windows 10' is selected as the app type. On the right is the 'App Suite Settings' page, which includes options for Office version (32-bit or 64-bit), update channel (Monthly), and specific version settings. Both pages feature 'OK' buttons at the bottom.

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

The screenshot shows the 'Add group' assignment settings. It includes sections for 'Assignment type' (set to 'Required'), 'Included Groups' (containing 'All devices'), and 'Excluded Groups'. A note about excluding groups is present. An 'OK' button is highlighted at the bottom.

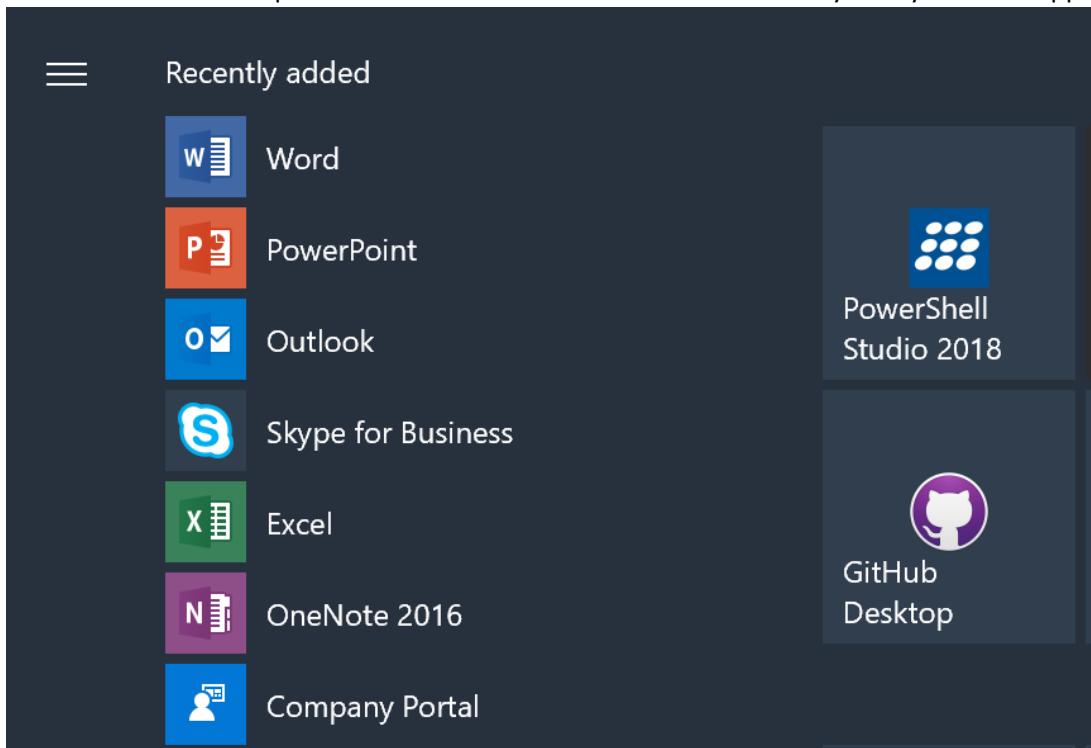
After a little bit I can see that Office is installing on my end user machine in Task Manager

Name	Status	12% CPU	48% Memory	8% Disk	2% Network
> Cortana (2)	ψ	0%	76.3 MB	0 MB/s	0.1 Mbps
CTF Loader		0%	3.9 MB	0 MB/s	0 Mbps
Ditto (32 bit)		0%	1.1 MB	0 MB/s	0 Mbps
Host Process for Setting Synchron...		0%	1.5 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	2.1 MB	0 MB/s	0 Mbps
Java Update Checker (32 bit)		0%	1.7 MB	0 MB/s	0 Mbps
Java Update Scheduler (32 bit)		0%	1.2 MB	0 MB/s	0 Mbps
> Microsoft Network Realtime Ins...		0%	1.6 MB	0 MB/s	0 Mbps
Microsoft Office (32 bit)		0%	3.0 MB	0 MB/s	0 Mbps
Microsoft Office Click-to-Run ...		0%	2.7 MB	0.1 MB/s	0 Mbps
Microsoft Office Click-to-Run	1.9%	45.6 MB	3.5 MB/s	10.5 Mbps
Microsoft Office Click-to-Run ...					
Microsoft OneDrive (32 bit)		0%	3.5 MB	0 MB/s	0 Mbps
Microsoft OneDrive (32 bit)		0%	24.2 MB	0.1 MB/s	0 Mbps
Microsoft Online Services Execu...		0%	0.3 MB	0 MB/s	0 Mbps

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

The screenshot shows the Microsoft Company Portal interface. The top navigation bar is blue with the title "The Lazy Administrator". On the left, there is a sidebar with a search bar and links for Home, All apps, Installed apps, Send feedback, and App categories. The main content area has a header "Apps" with a "Show all" link. It displays a single app card for "Office" by Microsoft. Below this is a section titled "My Devices" showing two devices: "This device" (laptop icon) labeled "SB-01" and "Brad's iPhone" (phone icon). Under the "My Devices" section, there is a profile for "Bradley Wyatt" with an email link to "brad@thelazyadministrator...." and a website link to "Help Me". At the bottom of the sidebar, there are links for "My Profile" and "Settings".

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)

