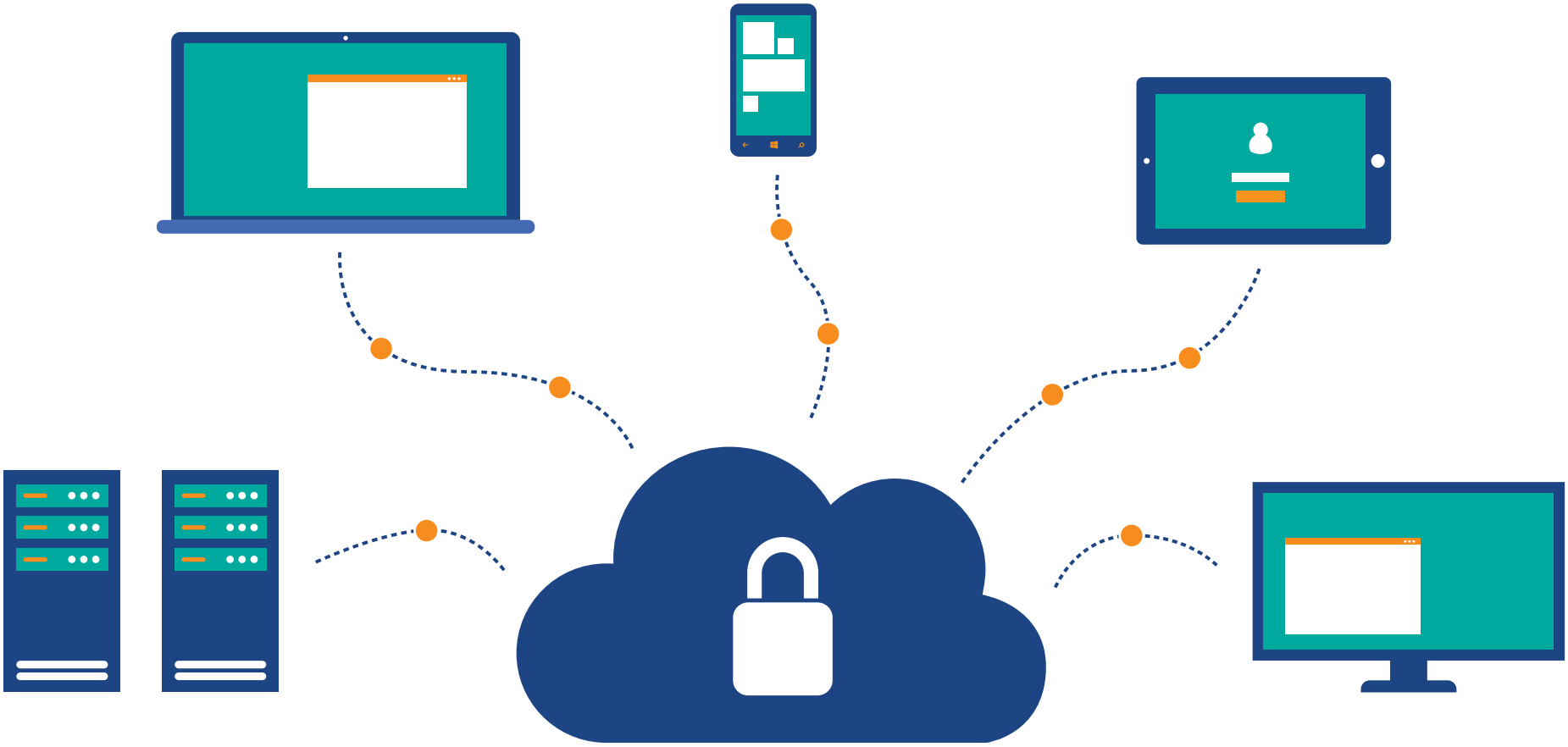
Microsoft Intune

Microsoft



Enterprise Mobility Suite Guide:

Implement Mobile Device and Application Management

The Enterprise Mobility Suite (EMS) provides organizations with robust and flexible solutions to meet the challenges created by proliferation of mobile devices and the desire to use them in the workplace.

This guide provides a comprehensive series of practical walkthroughs that show you how to configure Intune and other related cloud-based services to bring mobile devices into management and ensure compliance when used to access company resources. By performing the walkthroughs in this guide, you will learn how mobile devices, whether owned by the organization or by the users, can be used to increase productivity and at the same time ensure that access to corporate resources is both secure and compliant with the organization's policies.

Produced by HynesITe, Inc.

Table of Contents

Part One: Introduction

Part One:

Introduction

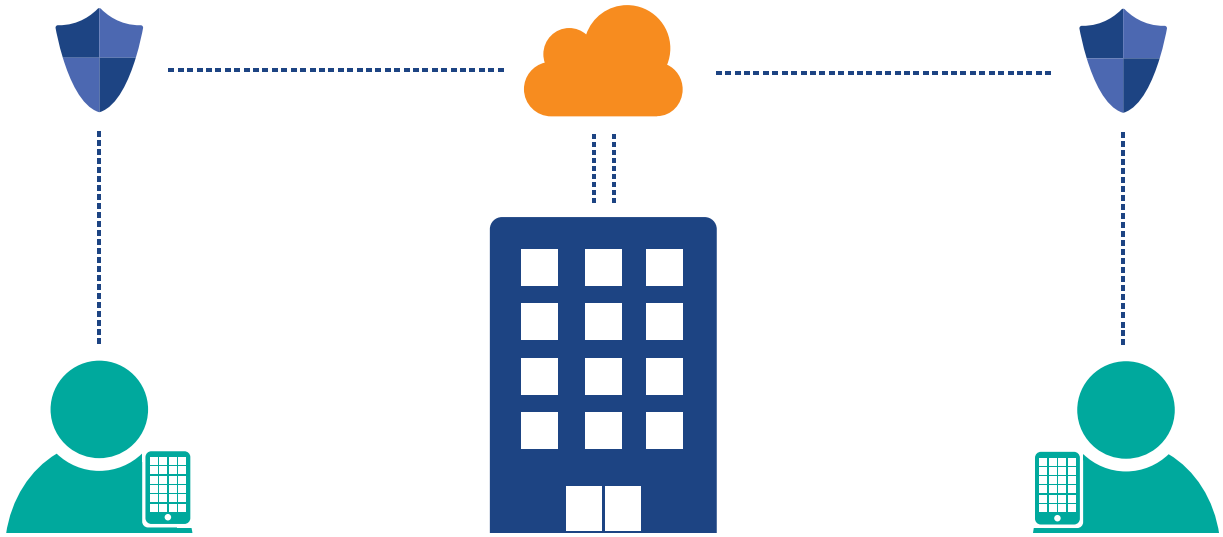
As the popularity of mobile devices, such as smartphones and tablets, has grown rapidly in the past few years and as more cloud-based mobile apps that enable work-related productivity become available, the pressure exerted by end users at all levels of the organization to use their personal mobile devices for work-related tasks has increased tremendously. Likewise, many organizations see numerous advantages in allowing and, in fact, promoting the use of personal mobile devices for work-related tasks. This pressure to incorporate personal devices for work-related tasks is so prevalent that it even has its own catch phrase: the consumerization of IT.

The consumerization of IT creates challenges for organizations. Foremost among these challenges is ensuring that the use of personal mobile devices and the data on those devices is compliant with business and security requirements established by the organization or required by law and government regulation. While meeting these requirements, organizations have to ensure that they are also able to meet users' expectations with regard to being able to use a variety of devices that are not limited to a single vendor or operating system version.

To meet these challenges, organizations need to adopt and enable enterprise mobility strategies and solutions that:

- Allow users the ability to use a variety of devices of choice, either their own choice or the organization's choice.
- Ensure IT has some variable degree of control over those devices and the data on those devices, ranging from complete control of both the device and data or partial control of the device and corporate data on that device at the very least.
- Provide users with a common identity to gain access to applications and corporate data regardless of the device they are using.
- Give IT the ability to deploy and manage applications for all types of devices.
- Protect the confidentiality, integrity, and availability of corporate data, both at rest and in transit.
- Ensure regulatory compliance when required by government legislation.
- Provide flexibility for policies and policy enforcement, allowing for a range of restrictions and controls to be applied according to particular contexts and factors, such as location, device type, device ownership, and so on.

To address these challenges and to enable a robust and secure and enterprise mobility strategy, Microsoft offers a cloud-based solution known as the Enterprise Mobility Suite (EMS). EMS comprises three separate cloud services and one on-premises software solution:



1. Microsoft Intune. Provides a mobile application (MAM) and mobile device management (MDM) solution to enable management of devices and applications from the cloud or on-premises through integration with System Center 2012 R2 Configuration Manager. Some of the features of Microsoft Intune include:

- Mobile device and application management for Windows, Windows Phone, iOS, and Android devices.
- Management and control of access to corporate resources based on enrollment policies and compliance policies.
- Simplified administration through a single management console in the cloud with Intune or on-premises through integration with System Center 2012 R2 configuration manager.

2. Azure Active Directory (AAD) Premium. Provides a hybrid identity and access management solution to enable users to gain access to on-premises or cloud-based resources and applications using a single set of credentials. Some of the features available with AAD include:

- Cloud-based self-service password reset
- Group management
- Group-based provisioning and access management Software as a Service (SaaS) applications.
- Multi-factor (MFA) options.
- Synchronization of users' identities from on-premises directories, including write back of changes.

3. Azure Rights Management (Azure RMS). Azure RMS is a cloud-based service that is integrated into other Microsoft cloud services, such as Office 365 and Azure Active Directory, and can be used with on-premises application and services. Using encryption, identity, and authorization policies, Azure RMS provides protection of data from unauthorized access, whether in transit or at rest.

4. Advanced Threat Analytics. An on-premises software solution that provides continuous monitoring of activities to learn and differentiate between normal and abnormal behavior and to alert to the presence of suspicious activity and to block attacks.

In this guide, you will focus on two of the cloud services available in the Enterprise Mobility Suite: Microsoft Intune and Azure Active Directory Premium. This guide will show how easy it is to enable robust and flexible policies for mobile device users to protect your corporate data and to meet your organizational or regulatory requirements.

What You Will Learn:

In the subsequent walkthroughs presented in this guide, you will learn how to implement Microsoft Intune and Azure Active Directory Premium to enable mobile device management and mobile application management scenarios. This guide comprises exercises on the following topics:

Configure Intune for Mobile Device Management and Enroll Devices

Intune can manage iOS, Android, Mac OS X, and Windows Phone devices. In addition, it can manage Windows RT, Windows 8.1, and Windows 10 as mobile devices. In order to manage those devices, you must perform some basic setup, such as configuring policies, and then enrolling devices to bring them under Intune management.

Configure Conditional Access to Exchange

Microsoft Intune polices allows you to control and manage settings and features on mobile devices and computer. Conditional access policies allow you to restrict access to Exchange email (both on-premises and Exchange online) to devices that are managed by your organization and compliant with other policies that you define.

Configure ActiveSync Email Profiles

Email profile configuration policies allow you to create, deploy, and manage Exchange ActiveSync settings on a variety of devices. When email configuration policies are deployed, users can gain access to their corporate email without having to perform any configuration and setup on their part, aside from enrolling their devices and bringing them under control of the organization.

Configure Mobile Application Management (MAM) Policies

MAM policies allow you to protect corporate data by giving you the ability to modify the functionality of apps to align them with compliance and security policies. Some of the policies you can enforce with mobile application management are:

- Encrypt corporate data.
- Prevent Save as.
- Restrict cut, copy, and paste operations.
- Prevent Android or iTunes or iCloud backups.
- Require a simple PIN or corporate credentials for app access.
- Open in-app website links in a managed browser application.

Configure Mobile Application Management Without Enrolling Devices

In some cases, users are not comfortable with the requirement to enroll their personal devices and bring them under various degrees of control of the organization in order to gain access to corporate data and application. However, using the mobile application management policies in Microsoft Intune, IT administrators can manage applications and corporate data on users' devices without requiring those devices to enroll in mobile device management. With this model, users do not have to give up control over many aspects of their devices in order to gain access to corporate resources. Furthermore, this functionality can work in combination both with Intune and third-party mobile application management solutions.

Deploy MSI Applications to Windows 10 Using Intune and Mobile Device Management (MDM)

Among the benefits of using Microsoft Intune is the ability to deploy applications to managed devices, such as PCs, phones, and tablets. Until recently, it was possible to deploy only .xap., .appx, and .appxbundle file types to managed mobile devices, including Windows 10 devices that were enrolled in mobile device management. It is now possible to deploy Windows Installer (*.msi) file types to Windows 10 devices that are enrolled in and managed by Intune.

Configure Multi-Factor Authentication for Mobile Device Management (MDM)

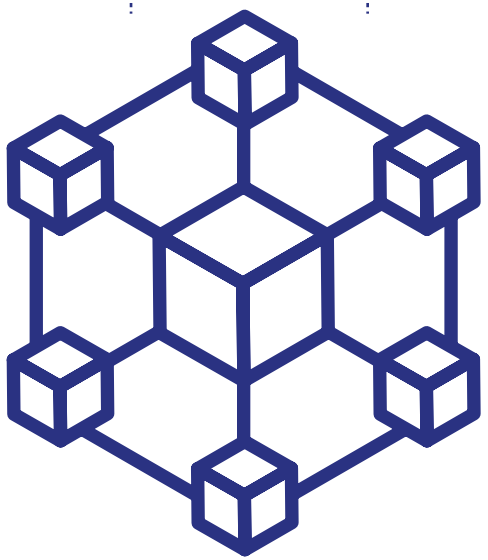
Azure Multi-Factor Authentication provides additional security to corporate resources by requiring a second factor of authentication in addition to a username and password combination. Multi-Factor Authentication requires two or more of the following authentication methods:

- Something you know (password).
- Something you possess and that is associated with you (phone or other trusted device).
- Something you are (biometrics).

By implementing two or more authentication factors, you can provide greater assurance of the identity of the person who is attempting to get authorization to access corporate resources.

Intended Audience:

This guide is intended as an introduction to mobile device and application management using Windows Intune and Azure Active Directory Premium. Anyone who has an interest in learning how to configure and test Intune policies to enable MAM and MDM scenarios can use this book and, it is hoped, find some value in it.



Hardware and Software Requirements:

The following are the minimum hardware and software requirements to perform the exercises in this guide:

A computer running Windows 7 or higher.

This computer will be used as your management computer to connect to the management portals. If you use a computer running Windows 10, it can be used both as a management and test computer to demonstrate enrollment into Intune, MSI installation and multi-factor authentication.

.NET Framework 4.

The Microsoft Intune Software Publisher requires that .NET Framework 4 be installed on your management computer.

A browser with Microsoft Silverlight plug-in installed.

At the time of this writing, the Microsoft Intune portal requires a browser that has the Silverlight plug-in installed. This means that you cannot use Microsoft Edge or recent versions of Chrome for many of the lab exercises. Please consider that these lab exercises were tested using Internet Explorer and, consequently, assume the use of Internet Explorer. However, the lab exercises should work using Firefox or Safari, assuming you have installed the Silverlight plug-in. For more information, please see https://www.microsoft.com/getsilverlight/Get-Started/Install/Default.aspx.

A mobile device that can receive text messages.

A number of the lab exercises require that you respond to text messages sent to a mobile device.

An Android and/or iOS device.

Most of the exercises are focused on policies for Android and iOS devices. If you wish to test the results of your Intune configurations, you will need access to an Android or iOS device. The following provides information on the recommended OS version of the iOS and Android devices you can use for the walkthroughs in this guide.

- iOS release 9.2.1 or higher. There is an issue with iOS 9.2 that could cause problems with the exercises in this guide. For more information, please see http://blogs.technet.com/b/microsoftintune/archive/2015/12/11/important-issue-with-the-ios-9-2-release.aspx.
- Android version 5.0.2 or higher. The exercises in this guide were tested against a Samsung device running Android version 5.0.2. Please note that if you want to test email profiles on an Android device you will need to use a Samsung device running KNOX standard 4.0 or higher.

Microsoft Intune is compatible with iOS 7.1 and higher and Google Android 4.0. For more information on mobile device management capabilities, please see https://technet.microsoft.com/en-ca/library/dn600287.aspx.

IMPORTANT: You use your own device at your own risk. Once you bring it under Intune management, you will be able to perform remote wipe operations. Additionally, because some labs in this series require that you start with clean device configurations, you may want to wipe your devices before you begin a particular lab. Please make sure you can afford to lose the data on your device if you make an error or wish to reset it to a factory default state. Please ensure you perform a backup of your device before performing any of the steps to verify your Intune configuration.

Windows 10 device.

Some of the steps in the walkthroughs require that you have access to a Windows 10 device. The device should not be domain-joined. This device can also be used as your management computer to connect to the Office 365, Azure, and Microsoft Intune portals. If you do not have access to Windows 10 device, you will not be able to test the deployment of MSI files to the Windows 10 device via Intune.

Windows Phone (optional).

If you have access to a Windows Phone device, you can use it to test some of the scenarios, for example, conditional access and email profiles.

Apple ID.

To enroll iOS and Mac OS X devices and deploy policies and applications to them, you must acquire an Apple Push Notification (APN) certificate using your Apple ID. If you do not have an Apple ID, you can sign up for one here: https://appleid.apple.com.

> Even if you do not have an iOS device to use for these walkthroughs, it is recommended you acquire an Apple ID so that you can perform the steps to request and upload an APN certificate.

Personal OneDrive account.

To test separation of personal data from corporate data, you will need access to a personal OneDrive account that contains at least one document. The OneDrive account can be associated with any Microsoft account that have for your own personal use and are not using to set up trial accounts as part of the steps in this guide. If you do not have personal OneDrive account, you can sign up for an additional Microsoft account after you complete the Get Started section.

How to Use This Guide

This guide provides a series of practical walkthroughs (exercises) that show you how to configure Intune for mobile device and mobile application management. Each of the walkthroughs provides steps, replete with screenshots, to configure Windows, iOS, and Android devices, as appropriate, to test the results of the Intune configurations.

The topics are presented in a logical sequence that, when followed, allow you to build a solid foundation to start managing mobile devices.
Each section of this guide is dependent on the section that precedes it. You must perform each section in the sequence presented in this guide. For example, in order to configure and test managed applications, you must first have configured mobile application policies.

One notable exception to this rule is the device-specific instructions to test the results of your configurations. For example, if you have only an Android device to test and verify your Intune and Azure Active Directory configurations, you can skip any instructions that specifically require you to perform configuration tasks on a Windows Phone or iOS device. This said, within the Intune administrative console you should configure settings for all device types as provided in this guide.

> Please note that the instructions contained in the walkthroughs that follow were valid at the time of this writing. However, over time, some discrepancies may be introduced by changes in the various sign-up pages and management portals for Azure, Intune, and Office 365 as well as the OS versions in mobile devices. As a consequence, you may need to make some minor allowances and adjustments, depending on when you are using this guide.

Part Two:
Get Started

Part Two:

Get Started

In order to perform the exercises in this guide, you will need to have access to the following free trial accounts:

- Enterprise Mobility Suite (EMS) trial account. This gives you access to trial Microsoft Intune and to Azure Active Directory Premium licenses.
- Azure free trial account. This gives you access to Azure Active Directory.
- Office 365 Trial account. This gives you access to mobile applications licenses for Office applications.

To acquire these trial accounts, you will need to create a dedicated Microsoft account, a Hotmail.com, Outlook.com, or Live.com account, to sign up for the free EMS, Azure, and Office 365 trial accounts.

Once you have signed up for the free trial accounts, you will need to create users, create an Azure Active Directory security group, and assign licenses to the users.

The steps that follow walk you through configuring these requirements.

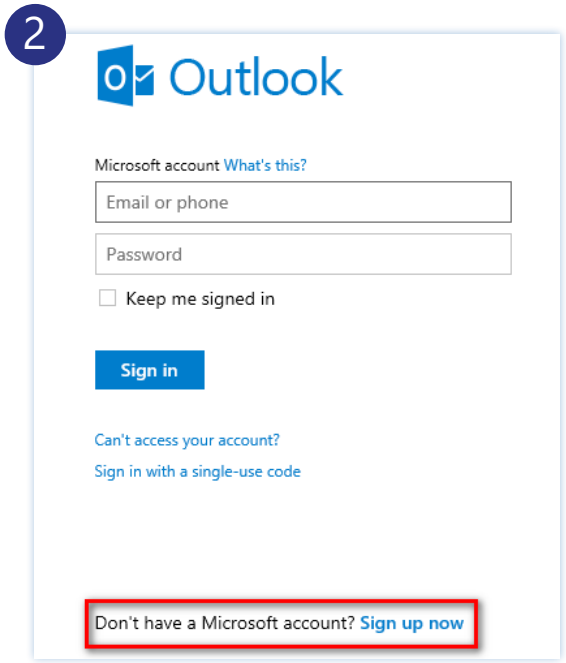
Sign Up for a Microsoft Account

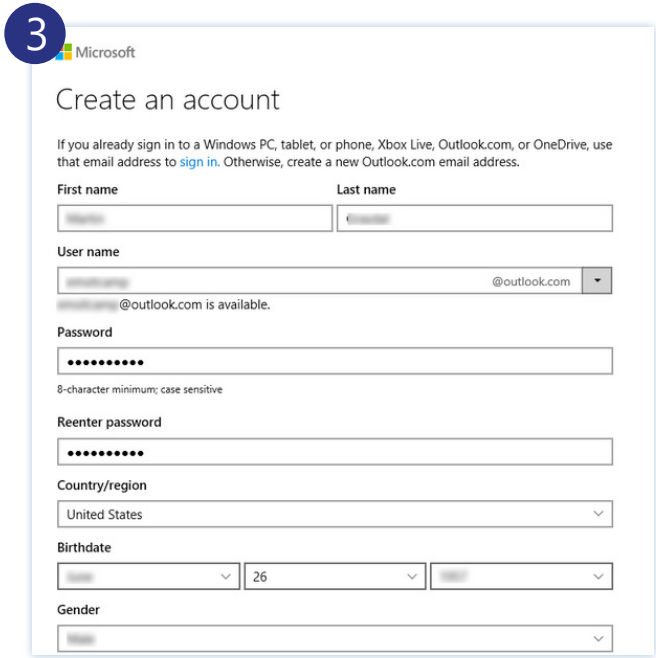
A Microsoft account is one that has hotmail.com, outlook.com, or live.com suffix. You will not be able to sign up for a free Azure trial account if you use any Microsoft account that has been previously associated with an Azure subscription. If you have a Microsoft account that has never been associated with an Azure subscription and wish to use that account, you can skip this task and continue to the next one.

- For best results, please use inPrivate, Incognito, or equivalent browser mode to ensure you are not automatically logged on with previously cached credentials.
- Perform this task using Internet Explorer or other compatible browser.

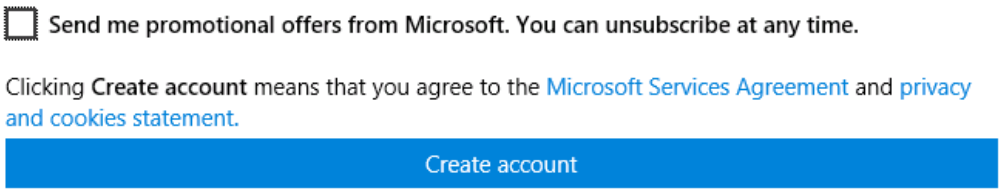
1. Open a browser and navigate to https://outlook.com.
2. Click Sign up now.
3. On the Create an account page, enter your first name, last name, unique username, password, country, birthdate, gender, phone country code, phone number, alternate email address, and verification characters.

- Please make sure you enter a real phone number and alternate email address.
- For best results, please ensure you do not choose a user name that has a country code in the DNS suffix, such as .ca, .de, .uk, etc. The DNS suffix should be Hotmail.com, live.com, or Outlook.com.
- NOTE: In this and subsequent lab steps, you will be prompted to enter your country. Please make sure that you enter the same country as your credit card billing address. In a subsequent lab exercise to create an Azure free trial account, you will be prompted for your credit card. You must enter accurate billing information on this page. You won't be able to enter your billing address if you specify a country other than the one used for your credit card billing address.
- Please note that your credit card will incur only a small, temporary charge when you sign up this account.

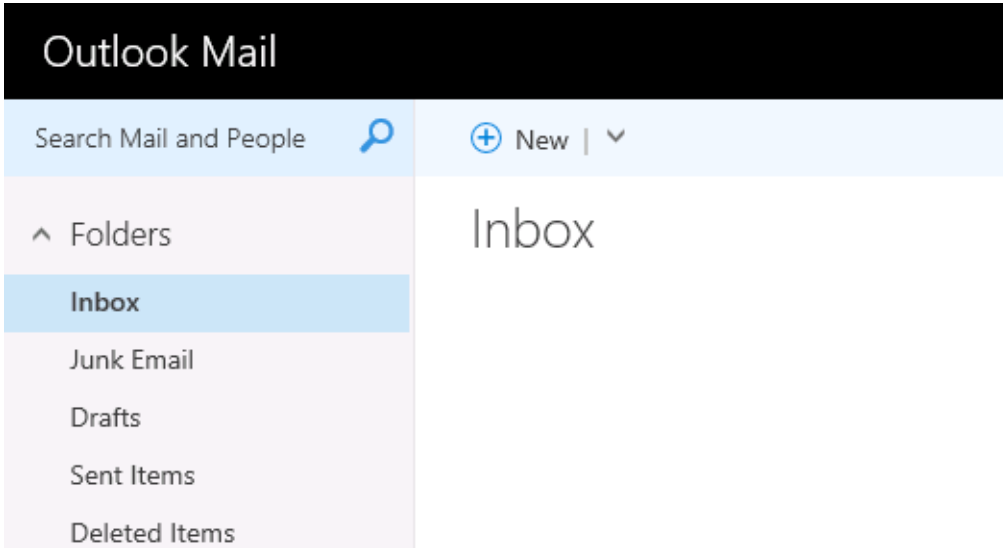


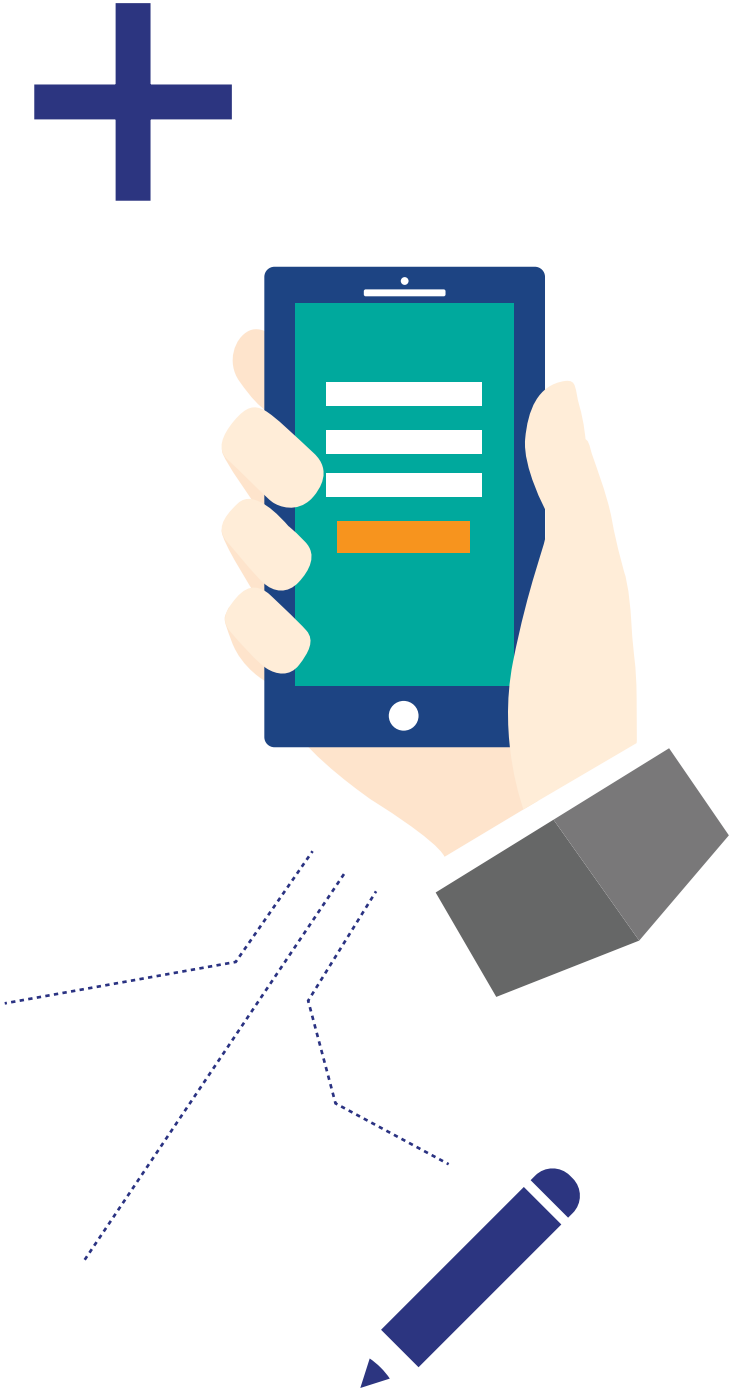


4. Clear the Send me promotional offers from Microsoft check box, and then click Create Account.



5. Close any welcome pop-ups or messages that may appear, and follow the prompts to open new inbox. Leave Outlook Mail Inbox open for subsequent steps.





Sign Up for Enterprise Mobility Suite Trial Account

As noted earlier, the Enterprise Mobility Suite (EMS) comprises 3 cloud-based services: Microsoft Azure Active Directory (AAD) Premium, Microsoft Intune, and Microsoft Azure Rights Management. And, more recently, it now includes Advanced Threat Analytics. Although it is possible to purchase these products individually, you will achieve cost savings by purchasing them bundled as EMS.

In this task, you will sign up for an EMS trial account using the Microsoft account you created previously.

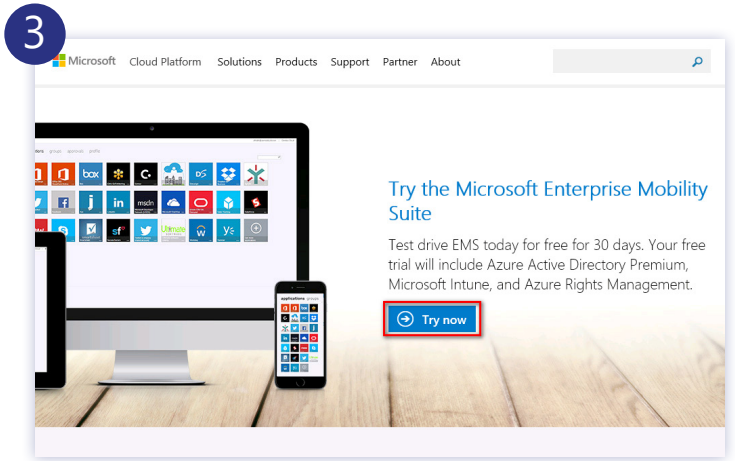
- If you skipped the previous exercise, please ensure you use a Microsoft account that has never been associated with an Azure subscription.
- For the best results, please use the same browser session that is open to your Outlook Mail Web page.

1. In your browser, stay logged on to your Outlook Mail Web page, and open a new tab.

- By remaining in the same browser session, you may be able to leverage your currently logged on credentials to save time and avoid errors.

2. In the new tab, navigate to https://www.microsoft.com/en-us/server-cloud/enterprise-mobility/ems-trial.aspx.

3. On the Try the Microsoft Enterprise Mobility Suite page, click Try now.



4. On the Welcome, Let's get to know you page, select the county used for your credit card billing address.

> 📌 Please ensure you use the same country as the billing address for your credit card, which you will need to sign up for a free Azure trial later on.

5. Enter your first and last names, the email address of the Microsoft account your created earlier, and your cell phone number.

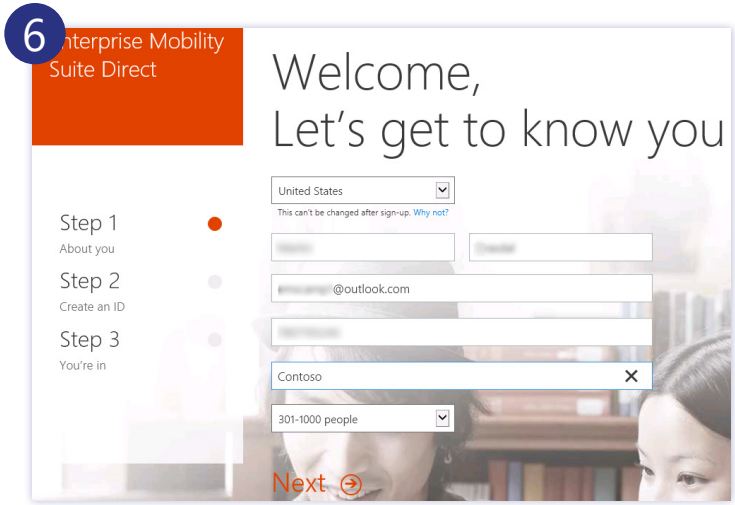
6. Enter a company name, select 301-1000 people as the organization size, and click Next.

7. On the Create your user ID page, in the Enter a user name field, type Admin.

> 📌 You may use any name you wish for the user account. However, subsequent lab steps will refer to this account by the name Admin.

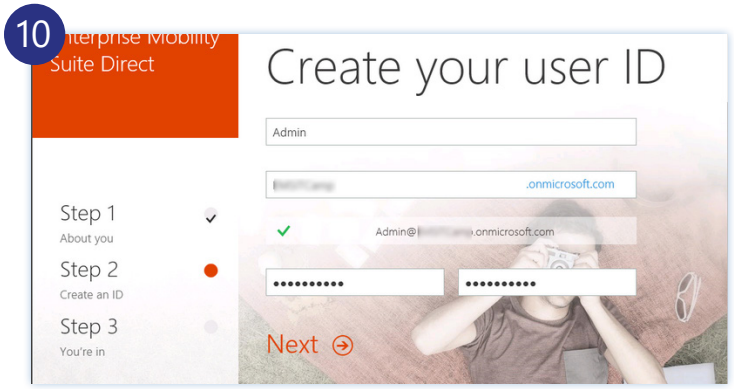
8. In the Yourcompany field, enter a unique name.

9. In the password and confirm password fields, enter a password of your choosing.



10. Record the username and password and click Next.

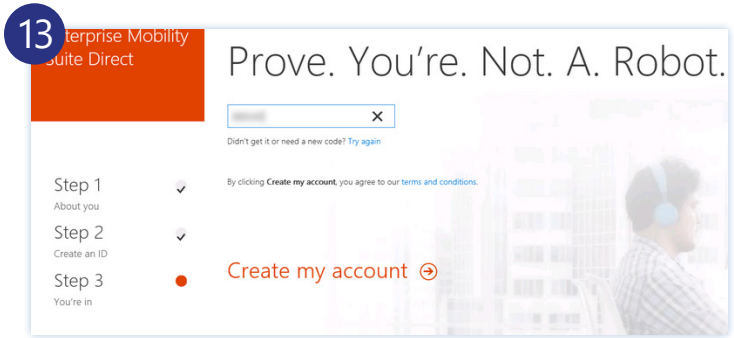
- Make sure you record your user name and password. In subsequent steps, your user name will be referred to as Admin@[OrgName].onmicrosoft.com. This account is also known as your tenant admin account and will be also referred to by this name in this guide.
- You will use this account exclusively to perform administrative tasks in Microsoft Intune, Office 365, and Azure Active Directory.



11. On the Prove. You're. Not. A. Robot. Page, enter a valid cell phone number, and then click Text me.

12. Wait to receive the verification code.

13. On the Prove. You're. Not. A. Robot. Page, enter the verification code, and click Create my account.

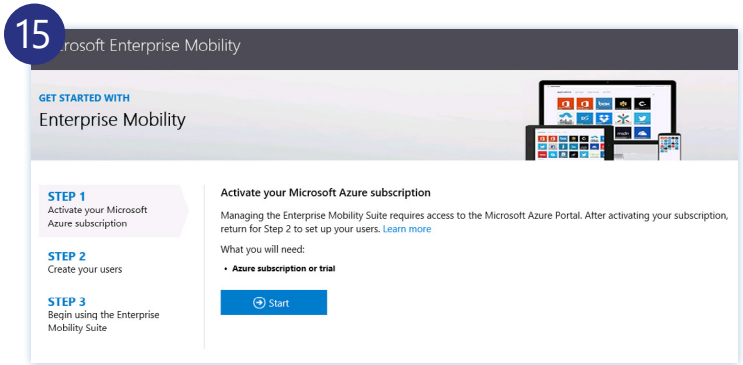


14. On the Save this info page, note the Office 365 sign in page and your user ID, and then click You're ready to go.

- Once you complete this page, the Activate your Microsoft Azure subscription page opens. In the next task, you will create your Azure trial subscription.

15. Leave the browser open and logged onto the Activate your Azure subscription page.

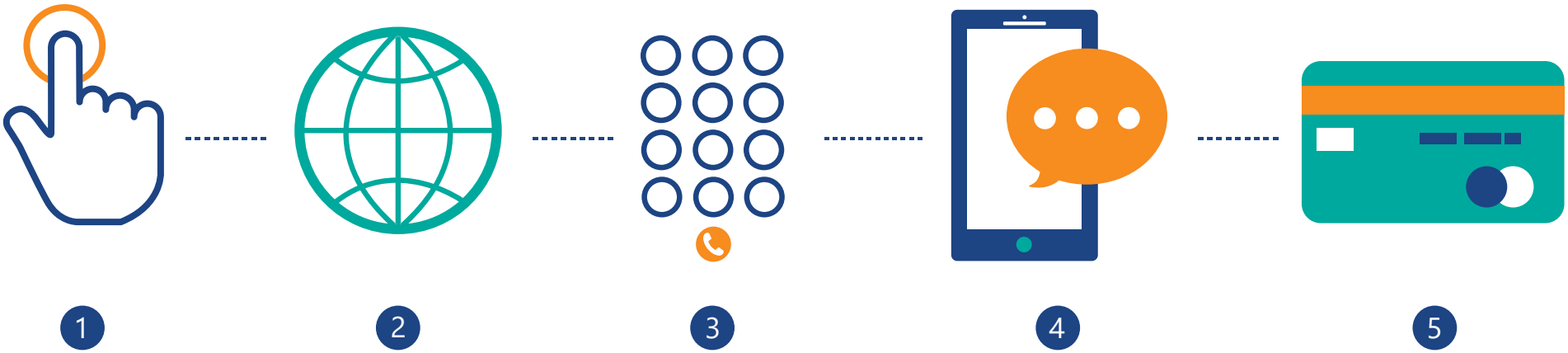
- Please ensure you leave this page open for the next task.



Sign Up for Azure Free Trial Account

When you created your EMS trial subscription, you also received an Azure Active Directory instance to provide identity services. However, you need to be able to gain access to this directory in the Azure management portals. This access requires that you have an Azure account. For this lab, you will use a free Azure trial subscription.

- NOTE: Signing up for an Azure trial requires that you provide a credit card that has NEVER been used previously to sign up for an Azure subscription to verify your identity. Your credit card will be charged $1.00 initially to prove it is valid. The charge will later be reversed. You may have only one trial account that uses the same billing information. If you already have a valid Azure trial account, you must use that for the labs, or use a different credit card.
- Please ensure that you begin this task using the browser page you left open in the previous task.



1. On the Activate your Microsoft Azure subscription page, click Start.

2. On the Oops! Access to Azure Active Directory is not available page, select your country (the same country as your credit card billing address), and then click Azure subscription.

- IMPORTANT: Please make sure that you select the country associated with your credit card billing address. You must enter accurate credit card billing address information in subsequent lab steps. For example, if your credit card billing address is in the UK, and you leave United States as the default country, you will not be able to enter a UK address in subsequent steps.
- WARNING: If you proceed with the incorrect country selected and cannot enter a valid billing address, you will have to redo all of the previous steps in the lab and create a new Microsoft and EMS trial account.

3. On the Microsoft Azure Free Trial signup page, in the WORK PHONE and the Verification by phone fields, enter your cell phone number, and then click Send text message.

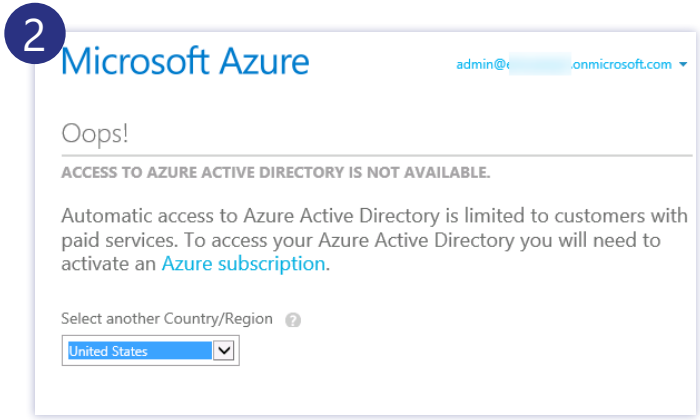
- IMPORTANT: Please make sure you change the country to the one used for your credit card billing address, if different from United States. If the country is not the same as the billing address on your credit card, you will not be able to enter the correct billing address.

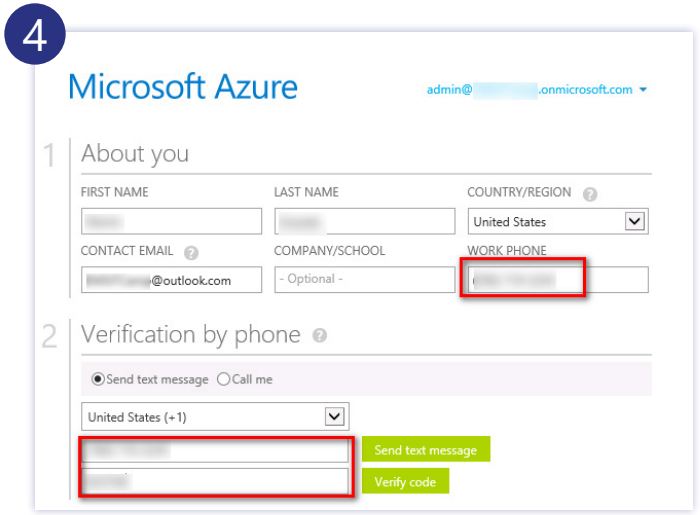
4. When you receive the phone verification code, enter it in the Verify code field, and then click Verify code.

- After a few moments, the payment information section expands.

5. In the Verification by card section, enter your credit card details. In the Agreement section, clear the Microsoft may use my email and phone to provide special Microsoft Azure offers checkbox. Click Sign up.

- IMPORTANT: Wait for the Microsoft Signup status page to show that your subscription is ready. Do not proceed to the next steps until you receive a notice that your subscription is ready.
- Leave the browser page open for the next steps.





Verify EMS Licenses and Features

When you signed up for an EMS trial account, you automatically received access to Azure Active Directory Premium. In this task, you will verify the EMS license assignment and then verify access to Azure Active Directory Premium features.

> For this task, please use the browser page that you left open in the previous task.

1. On the Welcome to Microsoft Azure page, click Start managing my service.
2. Follow the prompts to open the Azure portal.

> If prompted to sign in to Azure, sign in as admin@[OrgName].onmicrosoft.com using the password you created for this account earlier.

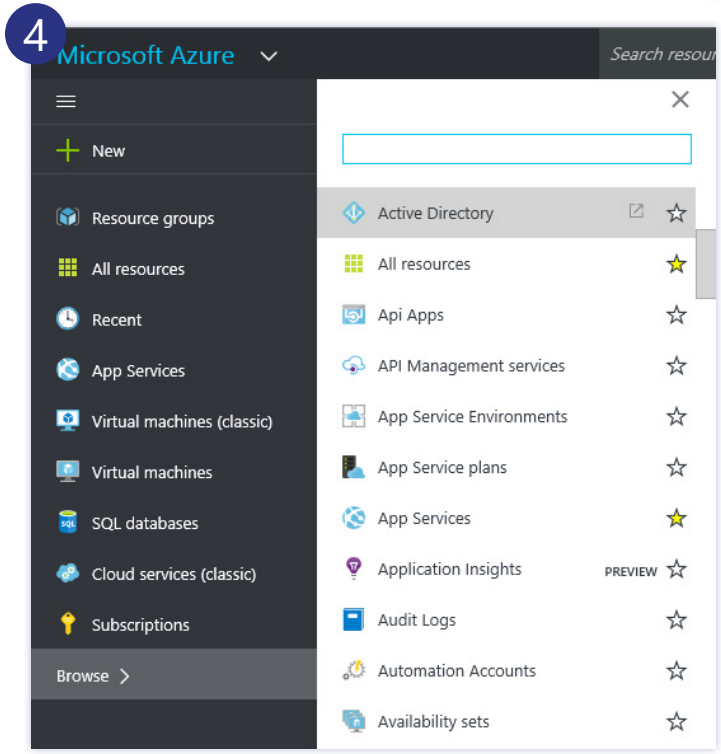
> As of December 2, 2015, the Azure portal, formerly known as the Azure preview portal, is the default portal. The older default portal is now called the Azure classic portal.

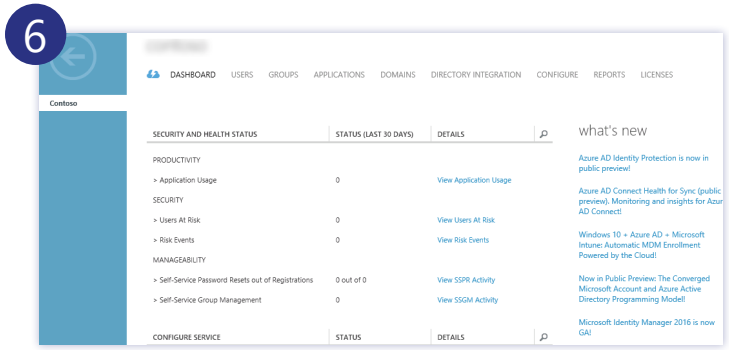
3. In the Azure portal, click Browse, and then click Active Directory.
4. As of this writing, Azure Active Directory is managed in the Azure classic portal.

> The Azure classic portal opens and displays the Windows Azure Tour pop-up.

5. Click Cancel (X) to close the Windows Azure Tour.
6. Close all other menus or banners that appear.

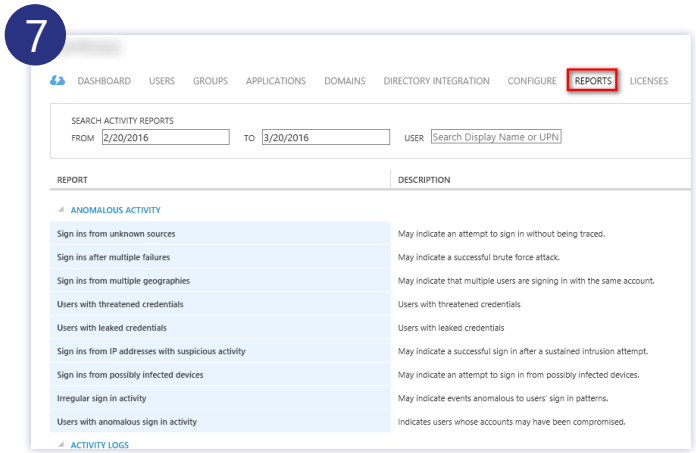
> The dashboard for your Azure Active Directory instance appears.





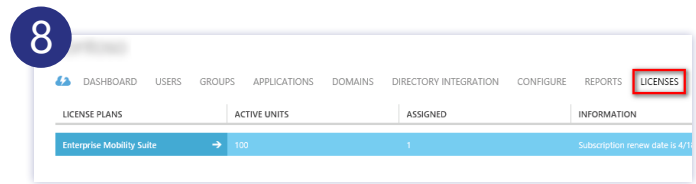
7. Click REPORTS.

- The following reports are available only with Azure Active Directory Premium Sign ins from IP addresses with suspicious activity: Sign ins from possibly infected devices, Irregular sign in activity, Users who have anomalous sign in activity, Password reset activity, Password reset registration activity, Groups activity, Application usage
- Most of these reports help to identify potential security threats. For a complete list of features that are available with Azure Active Directory Premium, please see https://msdn.microsoft.com/library/azure/dn532272.aspx and https://www.microsoft.com/en-us/server-cloud/products/azure-active-directory/features.aspx.



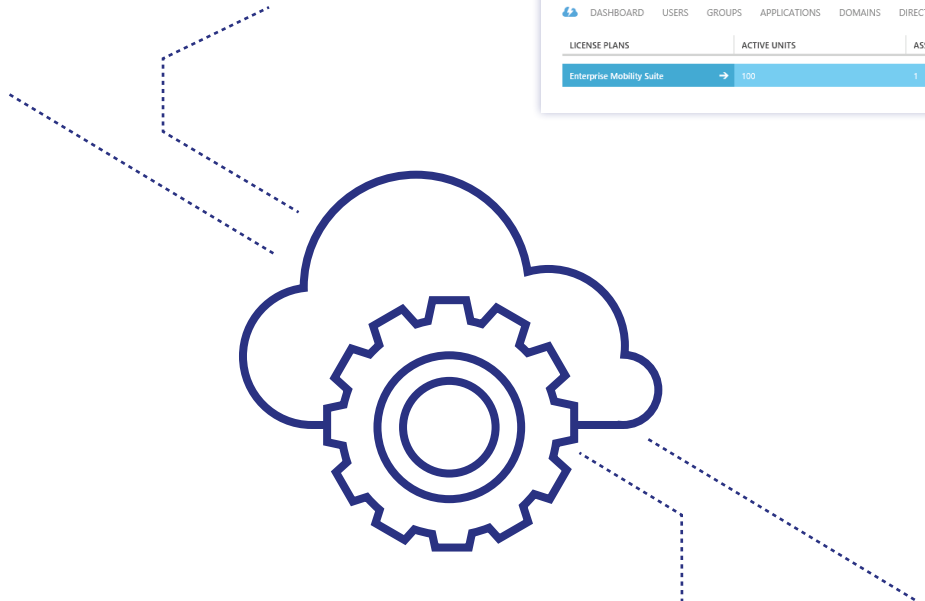
8. Click LICENSES.

- The license plans is listed as Enterprise Mobility Suite.



9. Leave your browser open for the next task.

- Do not close your browser at this time.



Sign Up for Office E3 Trial Account

In subsequent tasks, you will deploy Office applications to your demonstration mobile users. To manage and deploy Office applications, you will need to sign up for an Office 365 E3 trial account.

> Please ensure you use the same browser session that you left open in the previous task.

1. In the browser you left open in the previous task, open a new tab and leave the other tabs open.
2. In your browser, navigate to https://products.office.com/en-us/business/office-365-enterprise-e3-business-software.

> TIP: You can also get to this page by performing an Internet search on Office 365 Enterprise E3 trial.

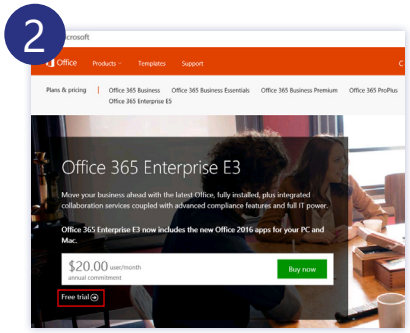
3. On the Office 365 Enterprise E3 Trial, click Free trial.

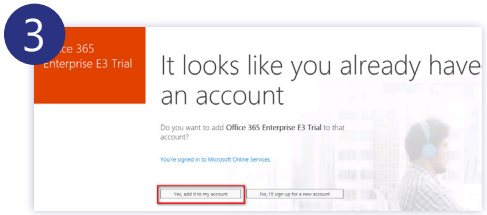
> A page should appear indicating that you already have an account.

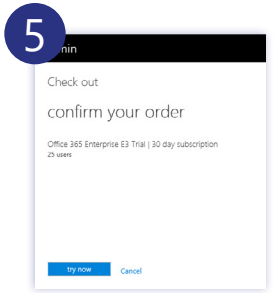
4. Click Yes, add it to my account.
5. On the Check out page, click Try Now.
6. On the order receipt page, click continue.

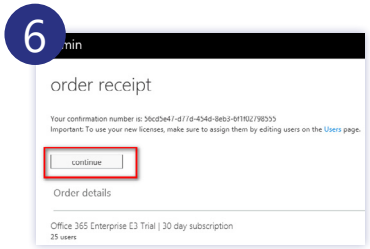
> Upon clicking continue, you will be redirected to the Office 365 admin center.

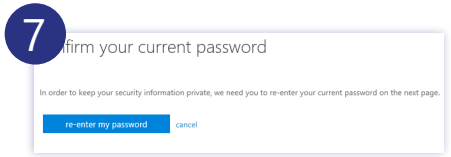
7. If the confirm current password page appears, click re-enter my password, and then sign in as admin@[OrgName].onmicrosoft.com.











8. On the don't lose access to your account page, beside Authentication phone is set to [phone number], click Verify. Then, click text me.

9. When you receive the verification code, enter it and then click verify.

10. On the don't lose access to your account page, click Set it up now.

11. In the authentication email field, enter the email address for the Microsoft account you set up at the beginning of the Getting started section, and then click email me.

12. Switch the tab showing your email inbox that you left open in a previous step.

13. Open the email from the Microsoft Online Services team, and record the code.

14. Switch to the tab showing the don't lose access to your account page.

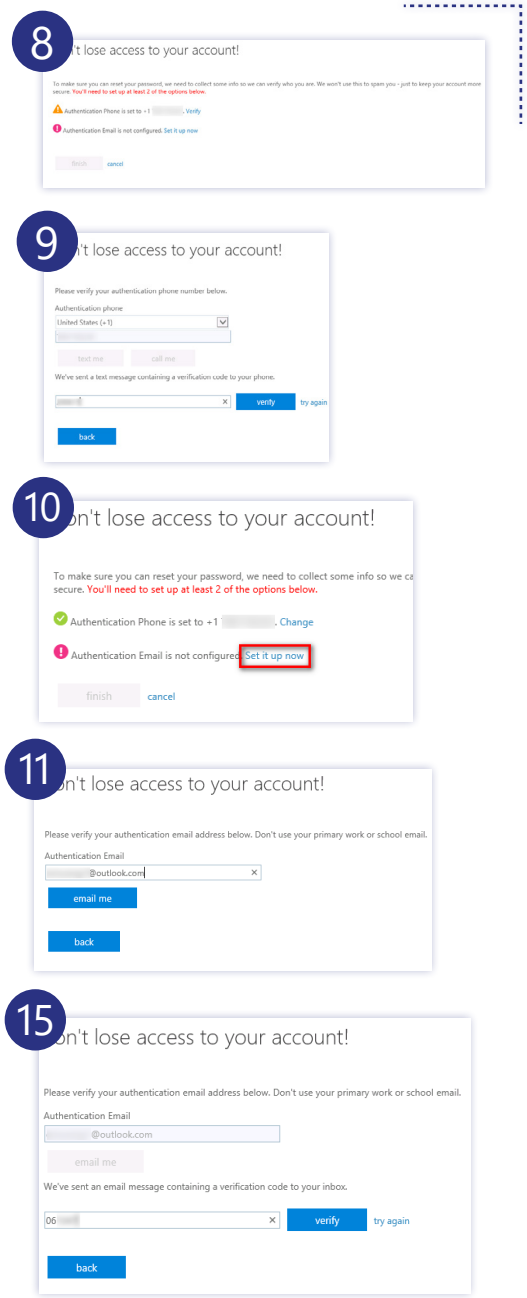
15. Enter the verification code, and click verify.

16. Click finish.

> The Office 365 admin center opens. At the time of this writing, the admin center has not changed over to the new version, which is still in Preview. The subsequent steps assume the use of the older admin center.

17. Close any pop-ups or informational messages that appear.

18. Leave the browser open for the next exercise.

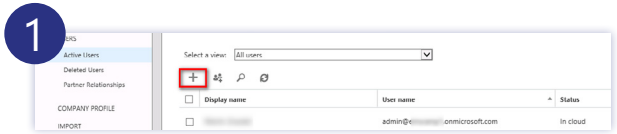


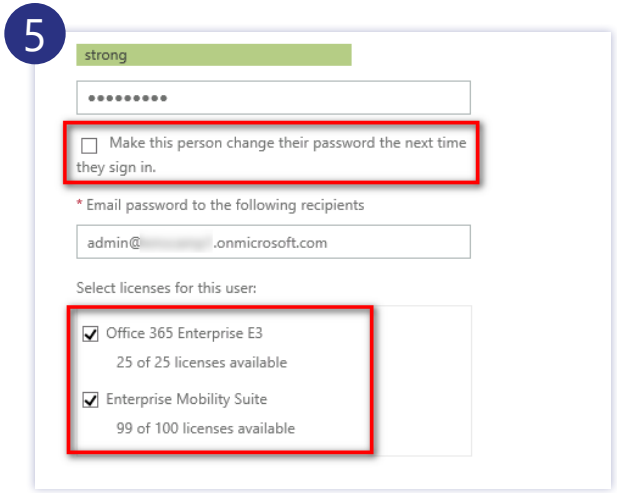
Add Users, Assign Licenses, and Create AAD Groups

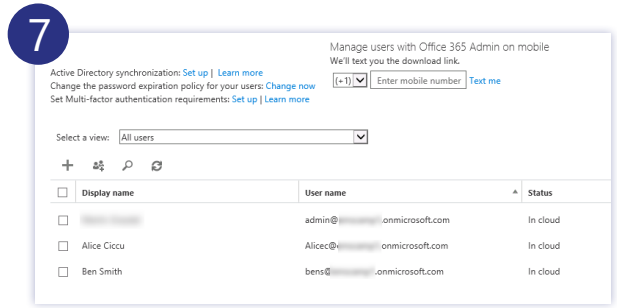
To perform subsequent steps to test mobile device and mobile application management policies, you will need to create some test users, assign licenses to them, create an Azure Active Directory group, and then add the users to the group.

> Ensure you are logged on the Office 365 admin center portal in the browser window you left open in the last step.

1. In Office 365 Admin center, in the left navigation, expand Users, and then click Active Users.
2. Click Add (plus sign).
3. On the Create new user account page, click Type password, clear Make this person change their password the next time they sign in check box.
4. Enter the account information as shown below:
   - First name: Alice
   - Last name: Ciccu
   - Display name: Alice Ciccu
   - UserName: alicec@[OrgName].onmicrosoft.com
   - Password: Passw0rd!
   - Re-enter password: Passw0rd!
5. Check Office 365 Enterprise E3 and Enterprise Mobility Suite.
6. Click Create, and then click Close.
7. Repeat steps 2–6 to create a user named Ben Smith (alias = bens@[OrgName].onmicrosoft.com).
8. Optionally, repeat steps 2–6 to create additional users.







9. On the ACTIVE USERS page, select admin@[OrgName].onmicrosoft.com, and then click EDIT.

📌 This is your tenant admin account. In the next step, you will assign this account an Office 365 Enterprise E3 license.

10. On your tenant admin page, click Licenses.
11. Under Assign licenses, check Office 365 Enterprise E3, and then click Save.

📌 In this task, you are assigning an E3 license to your admin account so that the account will have a valid email address. This step is necessary to configure the Intune to Exchange service-to-service connector in upcoming steps.

12. In your browser, switch to the tab that displays Azure Active Directory in the classic portal.

📌 In the next steps, you will add an Azure AD security group and add members to the group. Although you could perform these tasks in the Office 365 portal, they are easier to do if performed in the Azure portal.

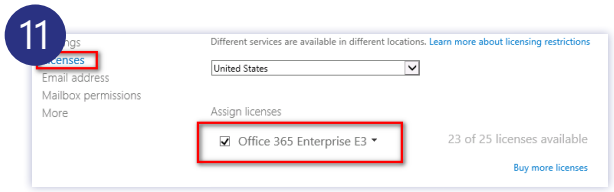
📌 TIP: If you accidentally closed the classic Azure portal, you can navigate to it from the Office 365 Admin portal. In the left navigation pane, scroll to the bottom, expand ADMIN, and then click Azure AD.

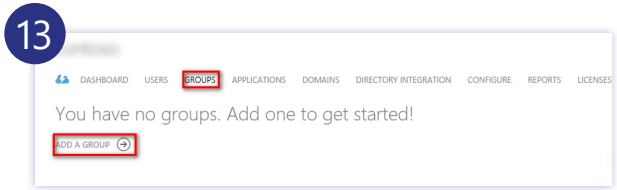
13. On the domain page, click GROUPS, and then click ADD A GROUP.
14. In the Add Group dialog box, in NAME, type Mobile Users, and then click OK (check mark).
15. Click Mobile Users, and then click ADD MEMBERS.
16. On the Add Members page, click the plus sign to the left of Alicec@[OrgName].onmicrosoft.com.
17. Repeat the previous step for all users you created, with the exception of your tenant admin account.
18. Click OK (bottom right check mark).

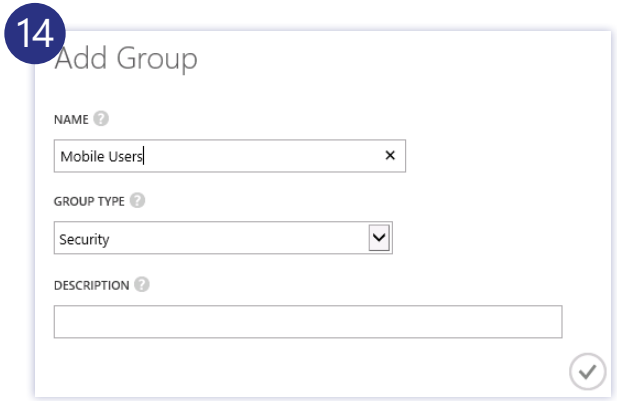
📌 Alice Ciccu and Ben Smith are added to the group.

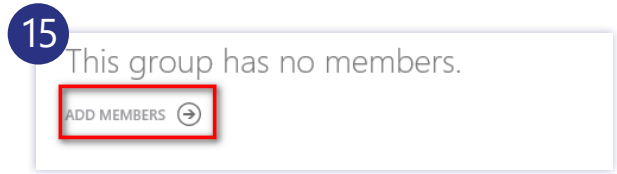
19. Close the tabs in your browser session.

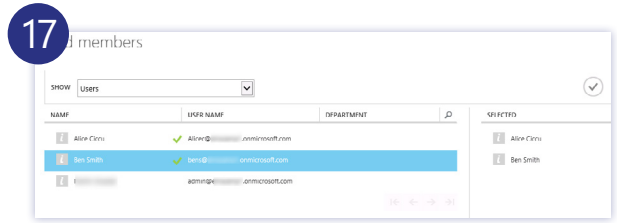
With the completion of this step, you are now ready to begin configuring Microsoft Intune and mobile device and application management policies.











Part Three:
Configure Intune for Device Enrollment

Part Three:

Configure Intune as the Device Management Authority

Now that you have created your trial account, you are ready to prepare Intune to enroll devices. This preparation requires that you configure Intune as the device management authority, create user and device groups, customize the portal, configure an Apple Push Notification Certificate, and create some default security and compliance policies.

You can manage devices from the cloud using the Intune portal or you can manage devices from a single on-premises console by integrating System Center 2012 R2 Configuration Manager with Microsoft Intune. However, the choice between the two is exclusive: You must either manage devices using the cloud-based portal or using the integrated console available through System Center. Furthermore, once you make a choice to use either of these two management options, that choice is irreversible.

In this task, you will configure the Intune portal to be the device management authority.

- To use the Microsoft Intune management portal, you must use a browser that has the Silverlight plug-in installed. This means that you will not be able to use Microsoft Edge or Google Chrome for any steps that require you to use the Intune portal.
- To perform this task, you should open a browser using InPrivate mode to avoid issues with shared credentials in other browser sessions.

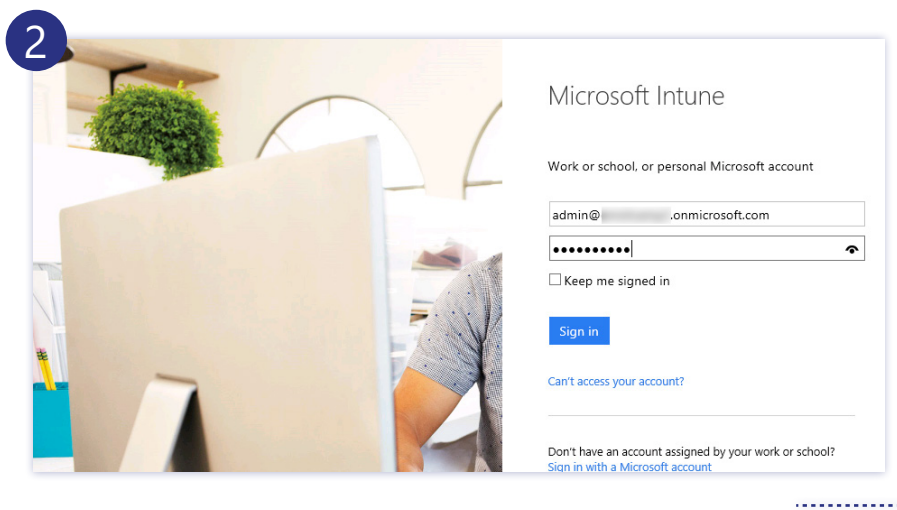
1. Open your browser in InPrivate mode, if possible, and navigate to https://manage.microsoft.com.

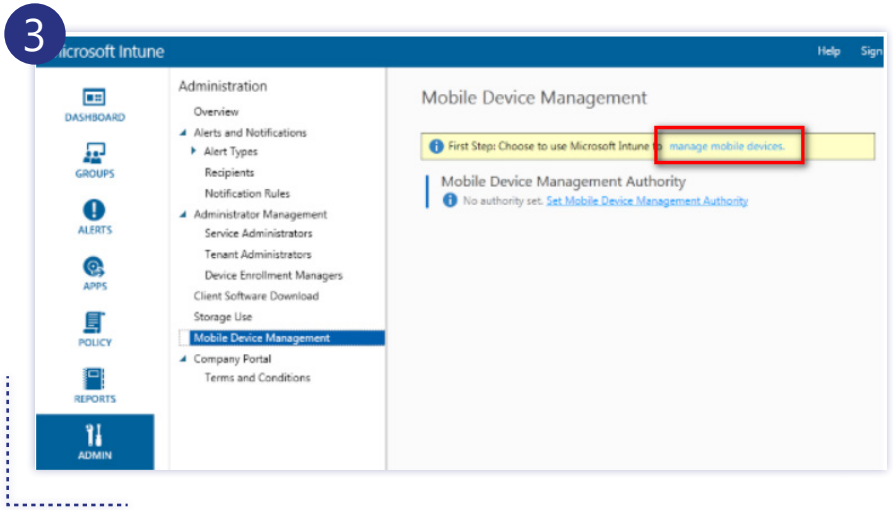
> Note that Office 365 also provides built-in mobile device management. However, the mobile device management in Office 365 is a separate service from Intune and has different capabilities. For example, using Office 365, you can manage iOS, Android, and Windows Phone devices. With Intune, you can manage these devices, as well as Mac OS X devices and Windows PCs. For a side-by-side comparison, please see https://technet.microsoft.com/library/dn957912.aspx

2. When prompted, sign in using the administrative credentials for the tenant admin account that you created previously, admin@[OrgName].onmicrosoft.com.

3. In the Microsoft Intune administration console, in the left navigation pane, click ADMIN. Under Administration, click Mobile Device Management. In the tasks list, click manage mobile devices.

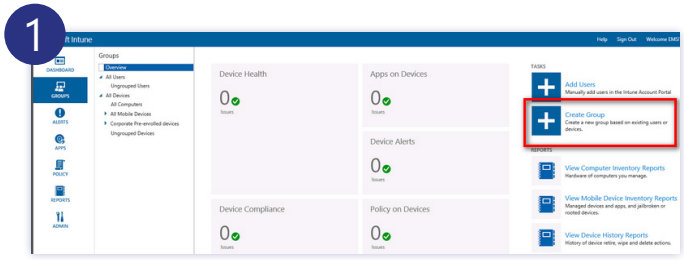
> Intune can manage mobile devices on its own or it can be integrated with System Center Configuration Manager for device management. At the outset, you must decide whether you will use Intune exclusively to manage devices. Setting Intune as the device management authority is an irreversible act. You cannot change this configuration, for example, if you later decided you wanted Configuration Manager to be the device management authority for your mobile devices.





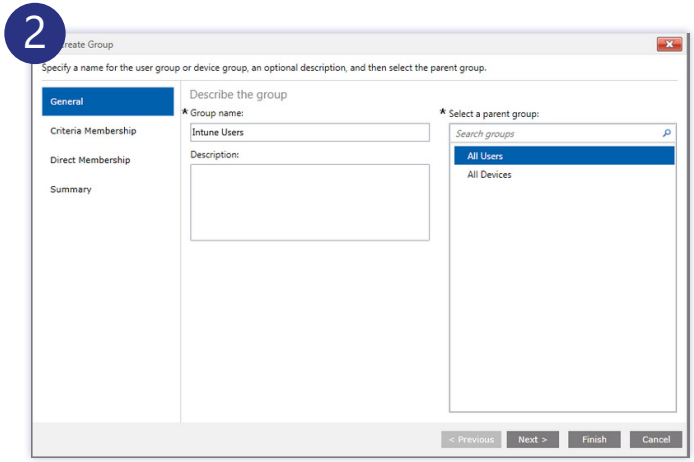
Create User and Device Groups

Groups provide you with flexibility in managing users and devices. You can plan and implement groups according to your organizational needs. For example, you can create groups according to location, security requirements, departments, hardware characteristics, job role, and so on.
In this task, you will create groups that you will subsequently use to target policies that you configure in Intune.



Please ensure you are logged in to the Intune console to perform these steps.

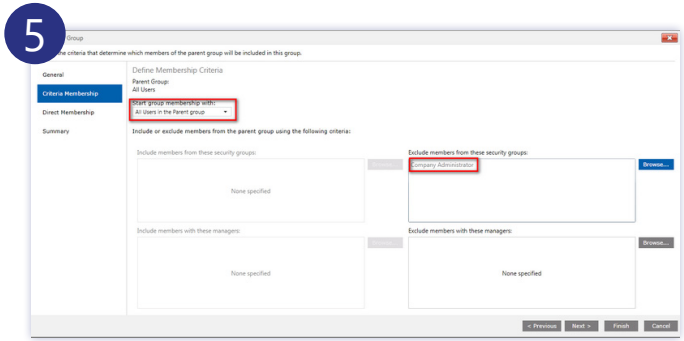
1. In the Intune admin console, click GROUPS, and then click Overview. In the Task lists, click Create Group.



You are creating a user group to assist with the management of your mobile device users. The group you will create includes every user except for the Company Administrator, also known as the tenant administrator.

2. In the Create Group dialog box, in Group Name, type Intune Users. In Select a Parent Group, select All Users, and then click Next.

3. On the Define Membership Criteria tab, in the Start group membership with drop-down list, select All Users in the parent group.
4. Beside Exclude members from these security groups, click Browse and then select Company Administrator.



This exclusion allows you to manage all Intune Users with the exception of the Company Administrator account, also known as the tenant administrator.

5. Click Add, click OK, and then click Next.

6. On the Define Direct Membership page, accept the default settings, and then click Next.

7. On the Summary page, click Finish.

8. In the Intune admin console, click GROUPS, and then click Overview. In the Task lists, click Create Group.

> In this and the next few steps, you will create a device group for assisting with the management of your mobile devices.

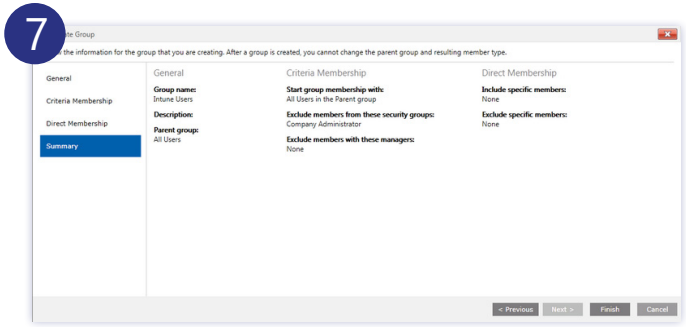
9. On the Describe the group page, in Group name, type All Personal Mobile Devices.

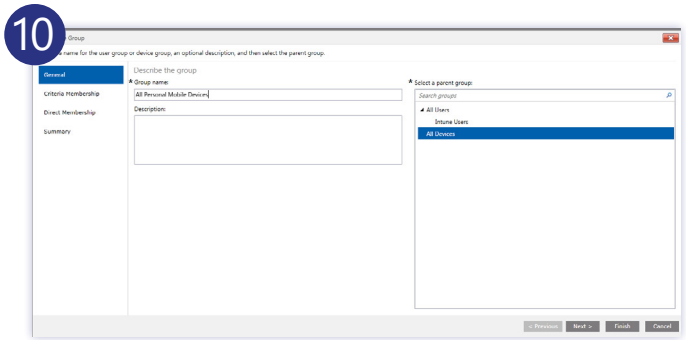
10. In Select a parent group, select All Devices, and then click Next.

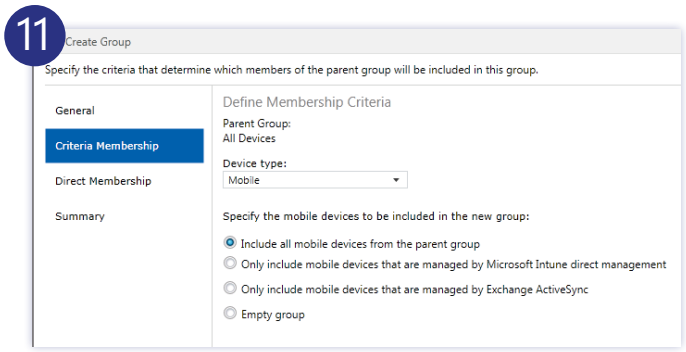
11. On the Criteria Membership page, accept the default setting to Include all mobile devices from the parent group, and then click Next.

12. On the Define Direct Membership page, accept the default settings, and then click Next.

13. On the Summary page, click Finish.







Customize the Company Portal

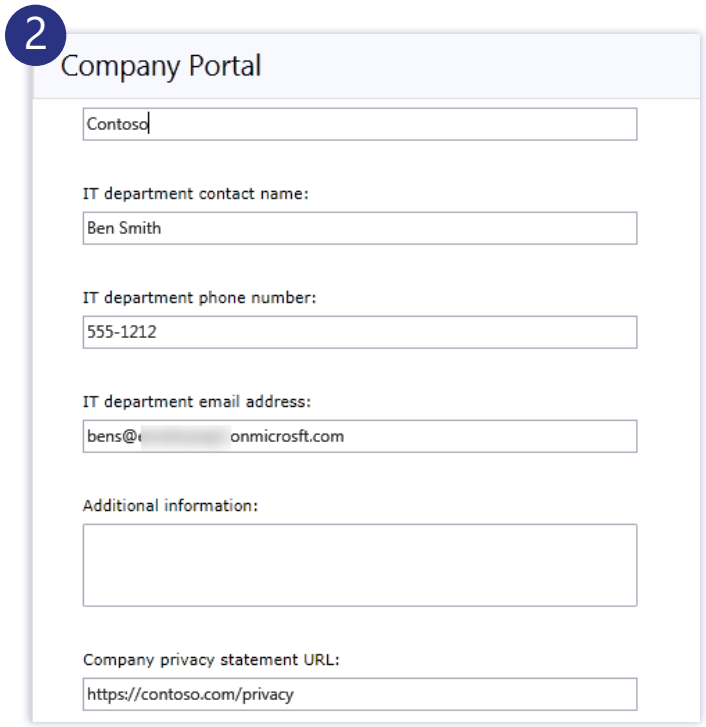
When users enroll devices into Intune, they will interact with the Company Portal. Because the portal represents an important point of contact and information for your users, you should customize it to provide information that is appropriate for your users.

In this task, you will customize the company portal to provide useful information to your end users.

Please ensure you are logged in to the Intune console to perform these steps.

1. In the Intune Admin console, click ADMIN, and then click Company Portal.
2. In the details pane, complete the form using the information as follows:

- Company Name: Contoso
- IT Department Contact Name: Ben Smith
- IT Department phone number: 555-1212
- IT Department email address: bens@[OrgName].onmicrosoft.com.
- Company privacy statement URL: https://contoso.com/privacy
- Support website URL: http://contoso.com/support.
- Website name: Contoso support website.



3. Perform an Internet search for a Contoso logo file and download one of the results to your computer.

> Steps 3–7 are optional.

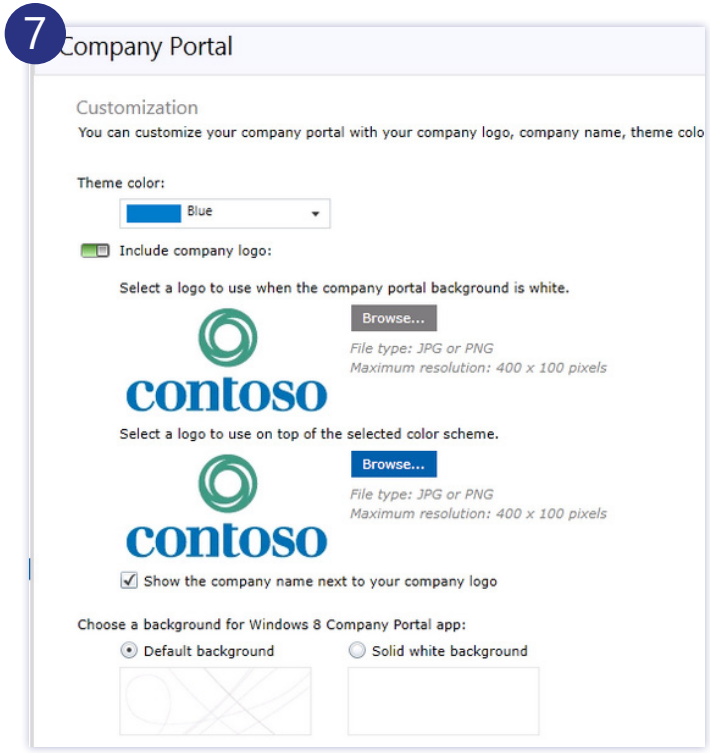
4. Click Include company logo.

5. In the Select a logo to use when the portal background is white field, click Browse.

6. In the Open dialog box, navigate to the folder where you downloaded the graphic file, select the file, and then click Open.

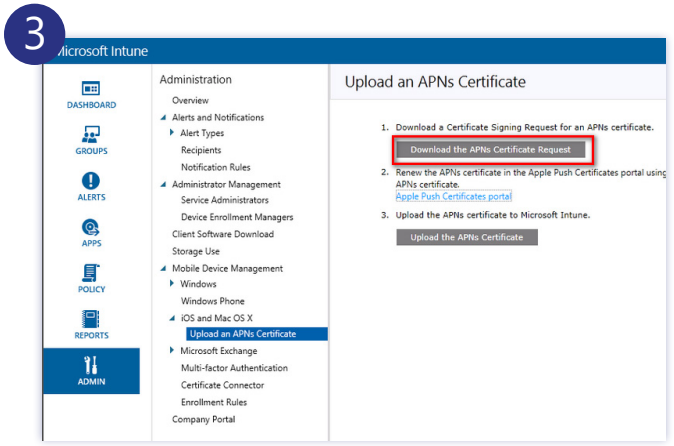
7. Add the same logo to use on top of the selected color theme, and then click Save.

> Typically, you would also add custom terms and conditions that users would see when they first use the company portal. Users would have to accept the terms and conditions before they could enroll their devices. Publishing custom terms and conditions is not part of the configuration steps included here. If you wish to add a terms and conditions, you can do so by navigating the Policy/Terms and Conditions in the Intune console.



Prepare for IOS and Mac Device Enrollment and Management

Intune provides the ability for you to enable enrollment of iOS and Mac OS X devices, allowing your users access to company email and applications using their iPhones, iPads, and Mac devices. After an iOS or Mac OS X device is enrolled, it can be targeted with policies to meet your security and other requirements; however, before you can enroll an iOS or Mac OS X device, you must request and import an Apple Push Notification (APN) service certificate. In this exercise, you will request an APN certificate, and then import it to the Intune service.



IMPORTANT: To complete these steps, you must have an Apple ID. If you do not have an Apple ID, you can skip these steps; however, please keep in mind that you will not be able to enroll any iOS or Mac devices in subsequent steps. You do not need an iOS or Mac device to sign up for an Apple ID. You can sign up for an Apple ID here: https://appleid.apple.com.

Please ensure you are logged in to the Intune console to perform these steps

1. In the Intune admin console, in the left navigation pane, click ADMIN.
2. Under Administration, expand Mobile Device Management, expand iOS and Mac OS X, and then click Upload an APNs certificate.
3. In the details pane, click Download the APNs Certificate Request.

In this step, you are creating a certificate request that is specific to your Intune site. You will use the certificate request in subsequent steps to acquire an APN certificate from Apple.

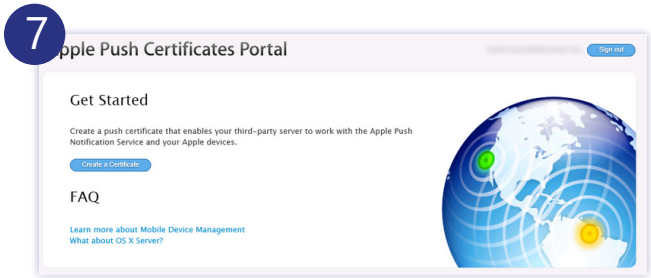
4. In the Save As dialog box, navigate to a convenient folder. In file name, type APNsReq, and then click Save.
5. In the details pane, under the download link, click Apple Push Certificates portal.

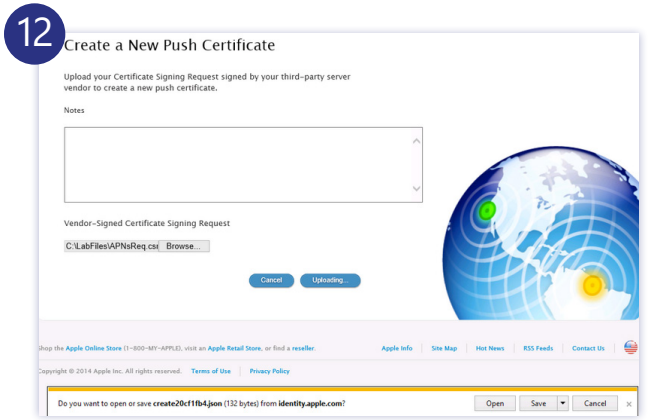
A new tab opens showing the Apple ID sign in page. The Apple ID is the account you create to use to manage Apple devices and services. Organizations that use Intune to manage Apple devices will want to create a special Apple ID to use for this specific purpose.

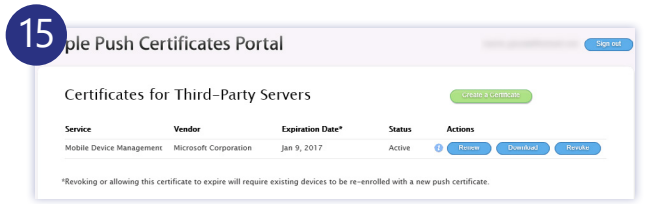
6. In the username and password fields, enter your Apple ID credentials.
7. On the Apple Push Certificates Portal, click Create a Certificate.
8. In the Terms of Use, check I have read and agree to these terms and conditions, and then click Accept.
9. On the Apple Push Certificates Page, under Vendor-Signed Certificate Signing Request, click Browse.
10. In the Choose File to Upload dialog box, select [Path]\APNsReq.csr, and then click Open.
11. Click Upload.
12. When prompted to download a JSON file, click Cancel.

> The page should automatically redirect after a few moments to show the certificate that is created. If the page does not redirect after a minute or two, press F5 to refresh the page.

13. On the Apple Push Certificate Portal, click Download.
14. When prompted to save the MDM_Microsoft Corporation_Certificate.pem file, click Save As.
15. In the Save As dialog box, navigate to a convenient folder, and then click Save.
16. Switch to the Intune admin portal.
17. Click Upload the APNs Certificate.
18. In the Upload the APNs Certificate dialog box, in APNs Certificate, click Browse, and then select [Path]\MDM_Microsoft Corporation_Certificate.pem.
19. In Apple ID, enter your Apple ID, and then click Upload.
20. In the Intune admin console, navigate to Administration / iOS and Mac OS X, and verify that the console displays that the iOS and Mac devices are ready for enrollment.







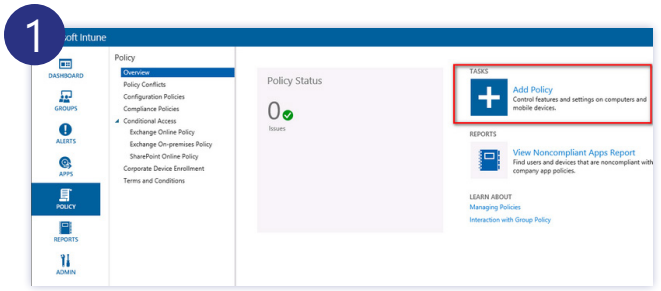
Create Policies for Device Platforms

In this task, you will configure some demonstration security policies for 3 separate mobile platforms: Android, iOS, and Windows 10. You will then configure a compliance policy that devices must conform to in order to access appropriately configured applications and services.

- Intune provides many policy settings. Only a few representative policy settings can be covered in the scope of this guide. For more information on the policy settings available to you for the management of mobile devices and computers, please see https://technet.microsoft.com/en-us/library/dn743712.aspx and https://technet.microsoft.com/en-us/library/dn646984.aspx.

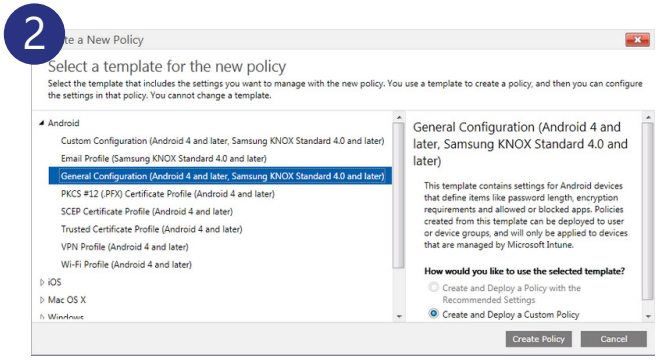
- Please ensure you are logged in to the Intune console to perform these steps.

1. In the Intune admin console, click POLICY, and then click Add Policy



- As a best practice, you should configure security settings and resource access profiles to meet your corporate or organizational policies; however, these policies have no effect on conditional access. To configure and enable conditional access, it will also be necessary to configure a compliance policy that determines the criteria for users to be able to access their email. You will configure a compliance policy in later steps.

2. In the Create a New Policy dialog box, expand Android, select General Configuration (Android 4 and later, Samsung Knox 4.0 and later), ensure Create and Deploy a Custom Policy is selected, and then click Create Policy.

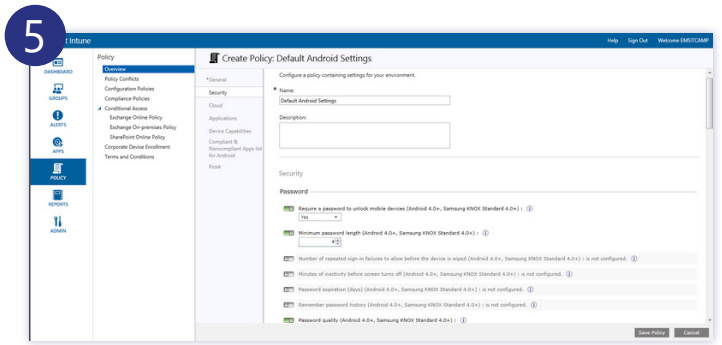


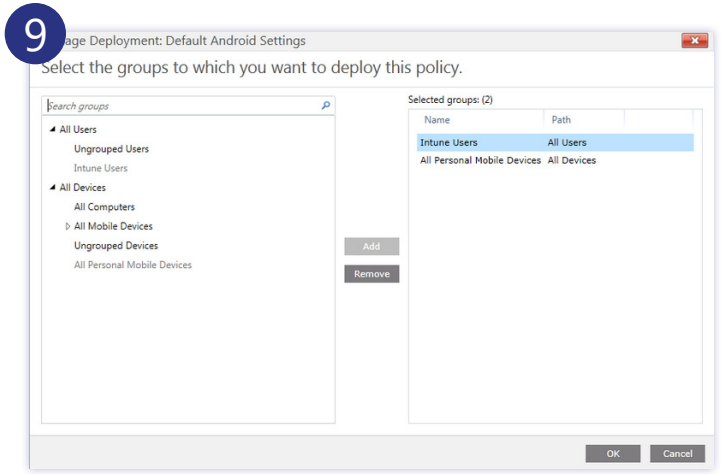
- Although it is possible to configure common mobile device security policy settings for all supported devices under the Common Mobile Device Settings node, Microsoft Intune provides separate configuration policies for each platform. Because the mobile device security policy settings will disappear in the future, the current guidance is to use the separate configuration policies. For more information, please see https://technet.microsoft.com/en-ca/library/dn913730.aspx.

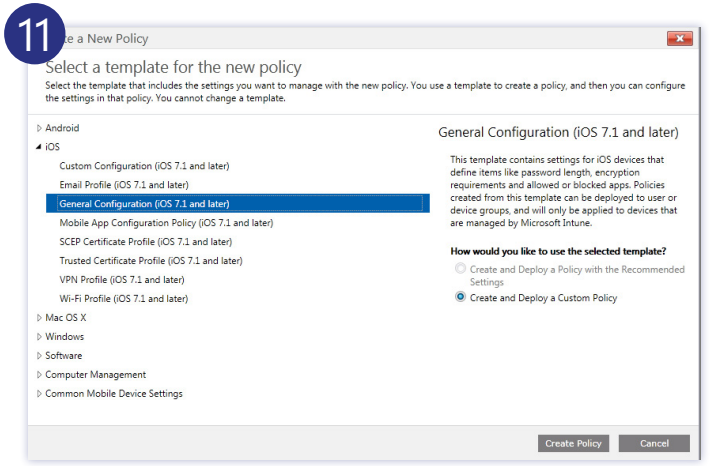
3. On the General page, in name, type Default Android Policy Settings.
4. In the Security section, click the toggle switch to enable Require a password to unlock mobile devices (Android 4.0+, Samsung KNOX Standard 4.0+).
5. Enable the setting to require a minimum password length of 4 characters, and then enable the setting to enable a password quality of At least alphanumeric, as shown in the accompanying screenshot below.
6. Spend a few moments reviewing the Android policies, and then click Save Policy.
7. When prompted to deploy the policy, click Yes.
8. In the Select the groups to which you want to deploy this policy, select Intune Users, and then click Add.
9. Select All Personal Mobile Devices, click Add, and then click OK.
10. In the Intune admin console, under Policy, click Overview, and then in the Tasks pane, click Add Policy.

> In this and subsequent steps, you will add a default iOS policy.

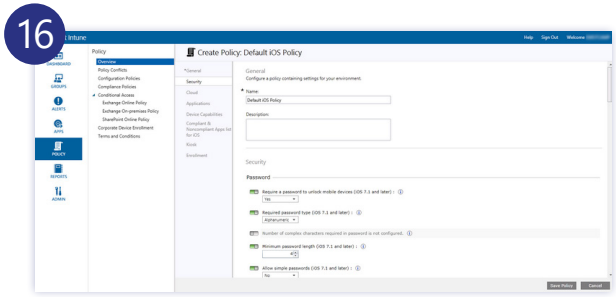
11. In the Create a New Policy dialog box, expand iOS, select General Configuration (iOS 7.1 and later), ensure Create and Deploy a Custom Policy is selected, and then click Create Policy.
12. On the General page, in Name, type Default iOS Policy Settings.
13. In the Security section, click the toggle switch to enable Require a password to unlock mobile devices (iOS 7.1 and later).
14. Enable the Required password type (iOS 7.1 and later) and ensure the setting is Alphanumeric.
15. Enable Minimum password length, and ensure the length is set to 4 characters.





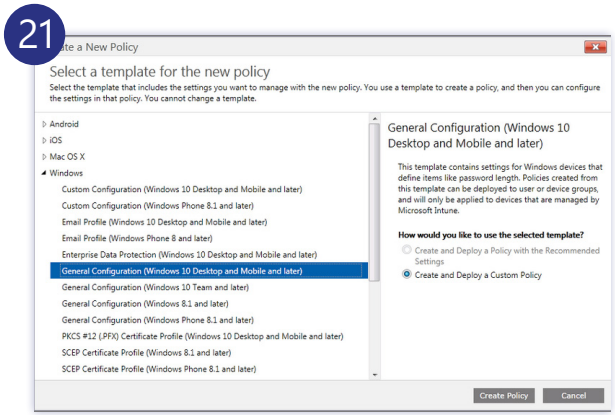


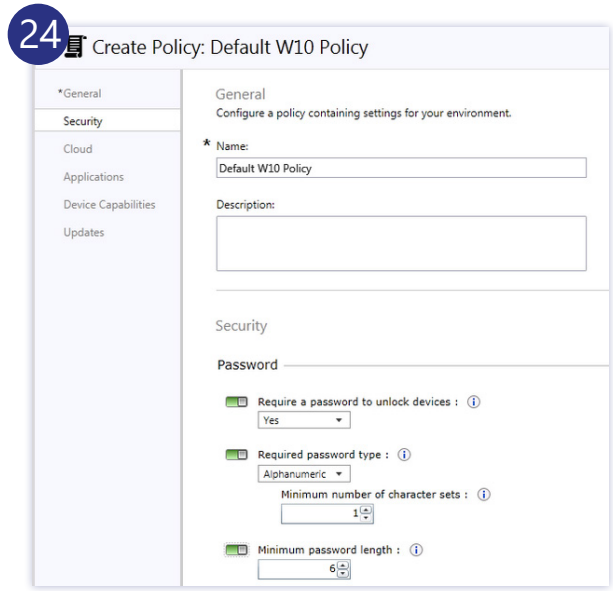
16. Enable Allow Simple passwords, ensure the setting is No, and then click Save Policy.
17. When prompted to deploy the policy, click Yes.
18. In the Select the groups to which you want to deploy this policy, select Intune Users, and then click Add.
19. Select All Personal Mobile Devices, click Add, and then click OK.
20. In the Intune admin console, under Policy, click Overview, and then in the Tasks pane, click Add Policy.



📌 In the next steps, you will create a default policy for Windows 10 devices.

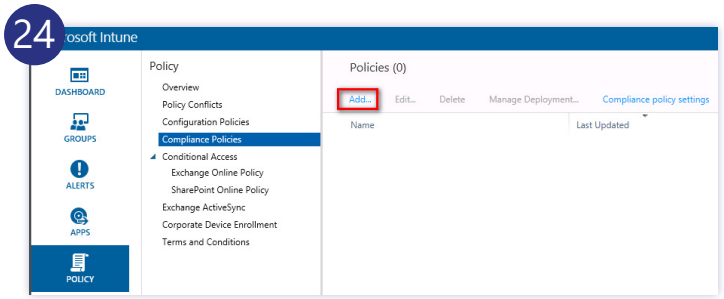
21. In the Create a New Policy dialog box, expand Windows, select General Configuration (Windows 10 Desktop and Mobile and later), ensure Create and Deploy a Custom Policy is selected, and then click Create Policy.
22. On the General page, in name, type Default W10 Policy Settings.
23. In the Security section, click the toggle switch to enable Require a password to unlock devices. Enable the Required password type, and then ensure the setting is Alphanumeric.
24. Enable Minimum password length, ensure the length is set to 6 characters, and then click Save Policy.
25. When prompted to deploy the policy, click Yes. In the Select the groups to which you want to deploy this policy, select Intune Users, and then click Add.
26. Select All Personal Mobile Devices, click Add, and then click OK.
27. In the left navigation pane, click POLICY.





📌 In the next steps, you will create a compliance policy.

28. Under Policy, select Compliance Policies, and then in the details pane, click Add.



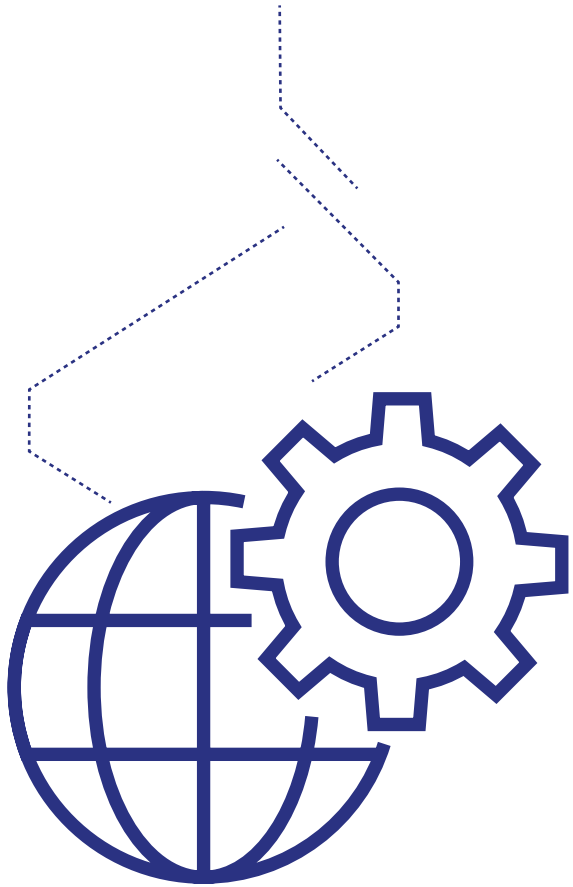
> Compliance policies are necessary to enable conditional access to Exchange ActiveSync. The compliance policy determines what compliance conditions must be met in order for devices to gain complete access to Exchange. Compliance policies can require that passcode settings be applied, that encryption is enabled, that devices not be jailbroken, and that the email profile be managed by Intune.

29. On the Create Policy page, in name, type Default Compliance Policy.
30. Scroll down to the encryption section, set Require encryption on mobile devices to No, and then accept the remaining default settings.

> Please make sure you set Require encryption on mobile devices to No. Although this setting is recommended and desirable in a production environment, it may cause blocking issues in an environment used for testing purposes only.

31. On the Create Policy page, click Save Policy.
32. When prompted to deploy the policy, click Yes.
33. In the Select the groups to which you want to deploy this policy, select Intune Users, click Add, and then click OK.

> Note that you target Intune Groups for the compliance policy. For the conditional access policy, you target Azure Active Directory security groups. You will see this in the next section.



Part Four: Configure and Test Conditional Access Policies

Part Four:

Configure and Test Conditional Access Policies

A conditional access policy restricts access to organizational email to devices that are managed by Microsoft Intune and compliant with organizational policies. To implement conditional access policies, you must have a number of prerequisites in place. You must configure Intune to enroll mobile devices, and you must deploy a compliance policy. Furthermore, you must use an Active Directory security group (not an Intune group) as the target of the conditional access policy. You completed these prerequisite steps earlier in this this guide.

In this section, you will configure other prerequisite settings for conditional access and then configure a conditional access policy. After implementing the conditional access policy, you will have an opportunity to verify the policy on an iOS, Android, or Windows Phone device. You do not need to have any of these devices. The steps include screenshots that will give you a good idea of the user experience. However, to get the most of out of the exercise, having one or more of these devices is preferable.

Create and Send Test Email

In this task, you create and send a test email that you will use throughout this guide to verify your configuration on various devices.

> Please perform these steps using an InPrivate or Incognito browser session.

1. Open an InPrivate or Incognito browser session.

> You need to open an InPrivate browser session because you are going to be logging on to Office 365 Outlook Web access as one of the users you created earlier.

2. Browse to https://outlook.office365.com/owa.
3. When prompted, sign in as bens@[OrgName].onmicrosoft.com using Passw0rd! as the password.

> Ben Smith is a test user you created in an earlier step.

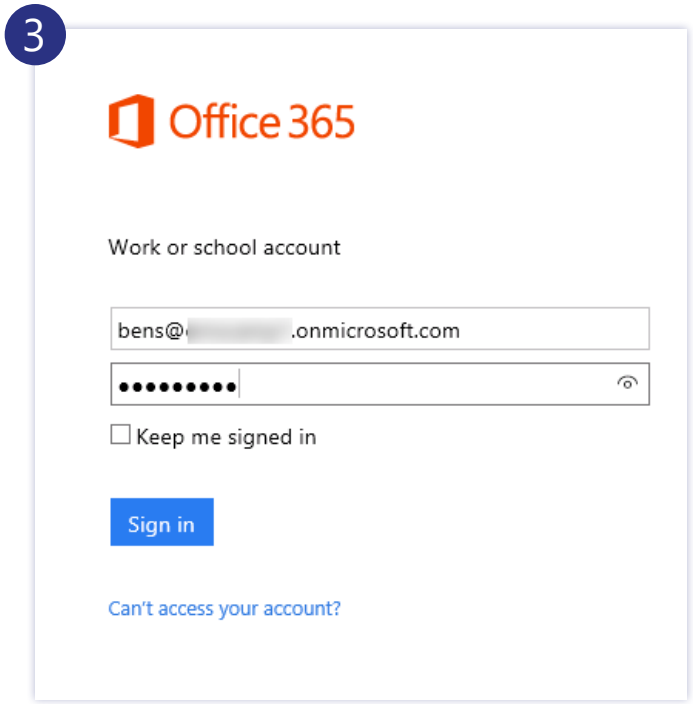
4. When prompted, select a time zone, and click Save.
5. In the Outlook Web Access Inbox, click New.
6. In the To field, type Alice Ciccu, enter a subject for the email, and enter a short message.

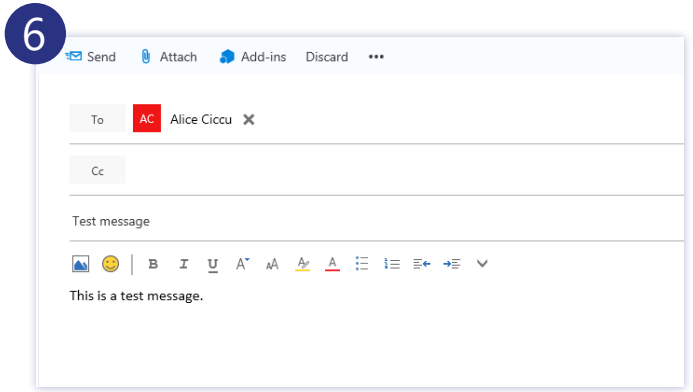
> Alice Ciccu is a test user you created in an earlier step. You can use any test user that you like.

7. Click Send.

> You are sending the test message to verify access to the mailbox once you have configured conditional access to Exchange and enrolled your device(s) in subsequent steps.

8. Close the browser session.





Configure Service-to-Service Connector

An additional prerequisite for enabling conditional access for Exchange ActiveSync is the service-to-service connector. This connector allows you to discover and manage mobile devices that are currently connecting to your Exchange environment but are not managed by Intune.

In this task, you will set up the service-to-service connector.

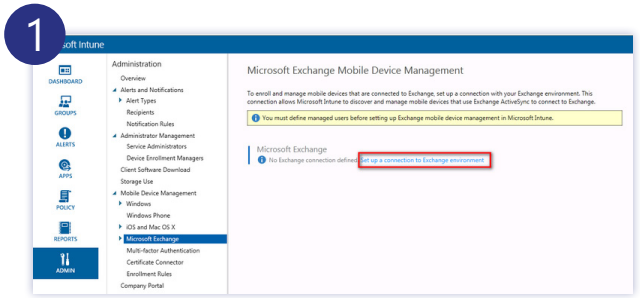
> Please ensure you are signed into the Microsoft Intune administrative console at https://manage.microsoft.com to perform these steps.

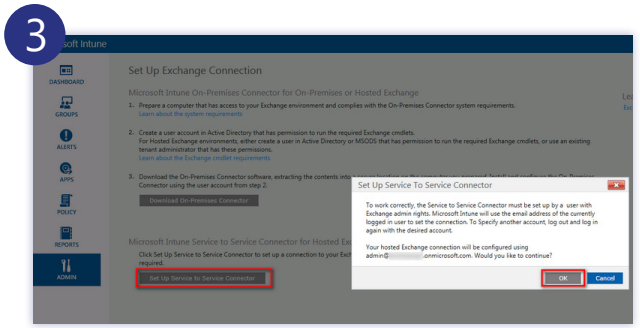
1. In the Intune Admin console, click ADMIN. Under Administration, click Microsoft Exchange, and then in the details pane, click Set up a connection to Exchange environment.
2. On the Set Up Exchange Connection page, click Set Up Service to Service Connector.
3. In the Set Up Service to Service Connector dialog box, read the message, and then click OK.

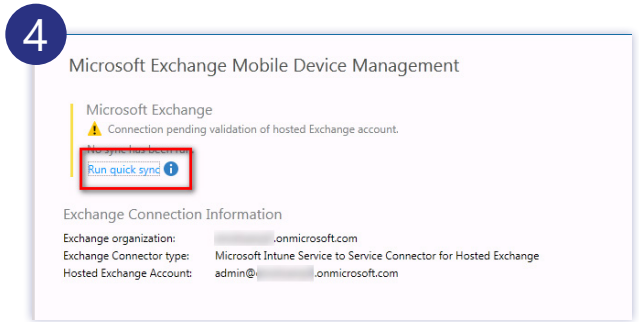
> Note that the user setting up the connector must have Exchange admin rights. Your tenant admin user was granted Exchange admin rights when you assigned an Office 365 E3 license to the user in an earlier step.

4. On the Microsoft Exchange Mobile Device Management page, click Run quick sync, and then click Close.

> If you have any devices that are managed only by Exchange ActiveSync, they will be blocked once you enable the conditional access policy and until they are enrolled. As a best practice, you should alert these users to enroll their devices before you enable the conditional access policy.





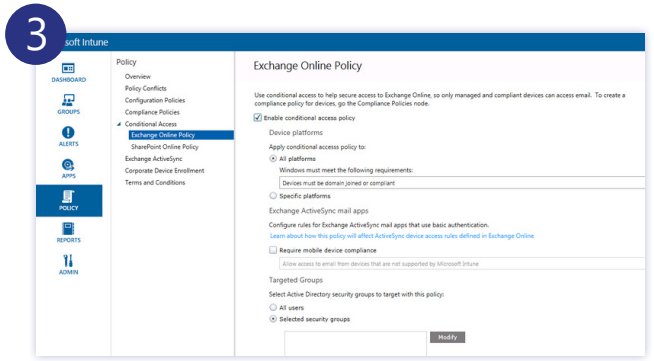


Implement Conditional Access Policy

In this task, you will configure and implement a conditional access policy.

> Please ensure you are signed into the Microsoft Intune administrative console at https://manage.microsoft.com to perform these steps.

1. In the Intune Admin console, click POLICY.
2. Under conditional access, select Exchange Online Policy.
3. On the Exchange Online Policy page, check Enable conditional access policy.

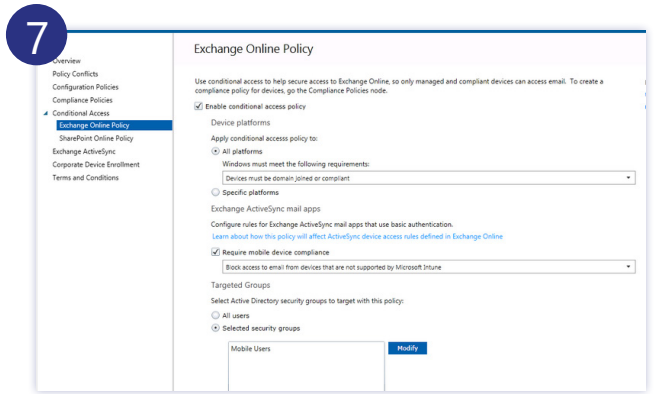


> The page changes to show configuration settings for the conditional access policy.

4. Under Device platforms, ensure All Platforms is selected and that Windows [d]evices must be domain joined or compliant.

> Under this section, you are configuring clients that can use modern authentication, which is enabled by the Active Directory Authentication Library. This enables Office clients to use browser-based authentication and enables conditional access scenarios. For more information, please see https://blogs.office.com/2014/11/12/office-2013-updated-authentication-enabling-multi-factor-authentication-saml-identity-providers/.

5. Under Exchange ActiveSync mail apps, check Require mobile device compliance, and then configure the setting to Block access to email from devices that are not supported by Microsoft Intune.
6. Under Targeted Groups, click Modify. In the Select Security Group dialog box, select Mobile Users, click Add, and then click OK.



> NOTE: You created the Azure Active Directory Mobile Users security group in an earlier step.

7. On the Exchange Online Policy page, leave the remaining settings at their default values, and then click Save.

Verify Exchange Conditional Access on an iOS Device

In this section, you will configure a connection to an Exchange mailbox on an iOS device. You will verify that, because your device is not enrolled and is out of compliance, you are not able to access your email. You will then step through the typical steps an end user would take to enroll the device and bring it into compliance. After enrolling the device and ensuring it is in compliance, you will verify that you are now able to access the Exchange mailbox.

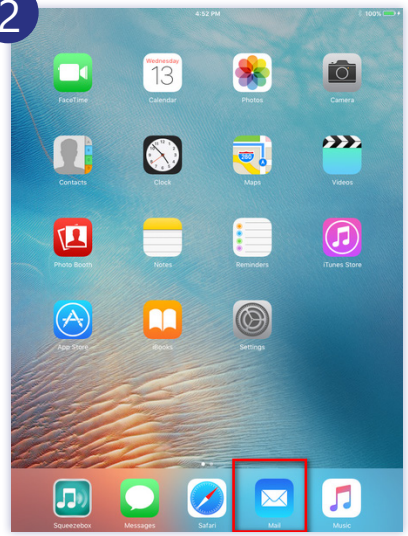
NOTE: To test the compliance rules on your iOS device, you will need to have relatively relaxed passcode settings on the device. If your passcode length is greater than 4 digits, you will not be prompted to enter a new passcode. Additionally, these steps assume you have not previously configured the built-in mail application on your iOS device.

IMPORTANT: After verifying conditional access, you will need to remove the email account, remove the company portal app, and perform a selective wipe of the device to remove it from management. The selective wipe will not remove your personal data. However, please be sure you are willing to do these things before proceeding.

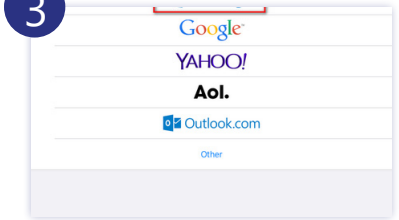
Perform these steps on your iOS device.

1. On your iOS device, enter your passcode to sign in.
2. Tap the Mail icon.
3. On the Welcome to Mail page, click Exchange.
4. In the Email field, type alicec@[OrgName].onmicrosoft.com.
5. In Password, type Passw0rd!, and then tap Next.

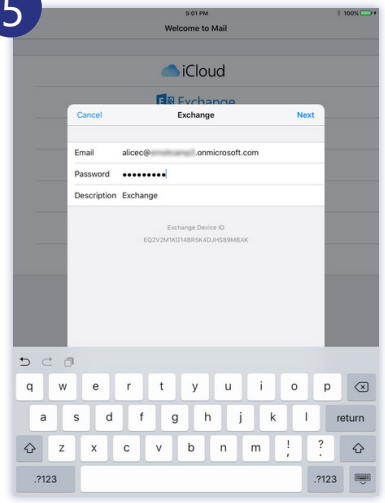
2

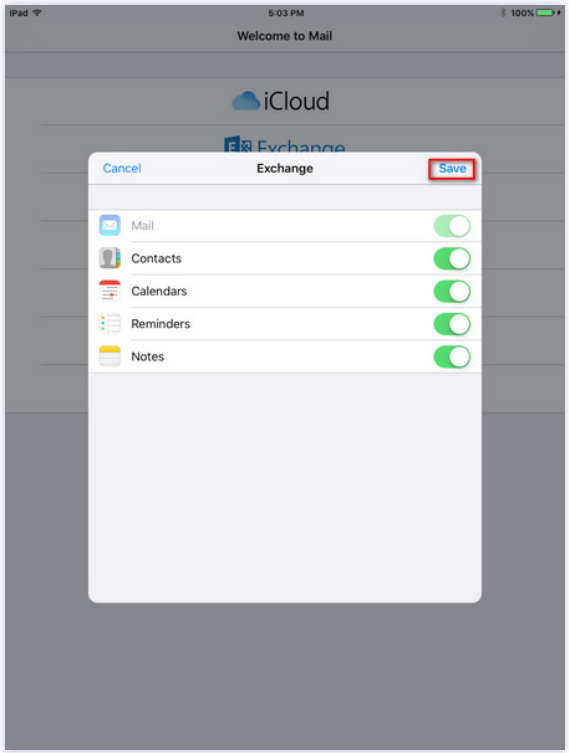


3



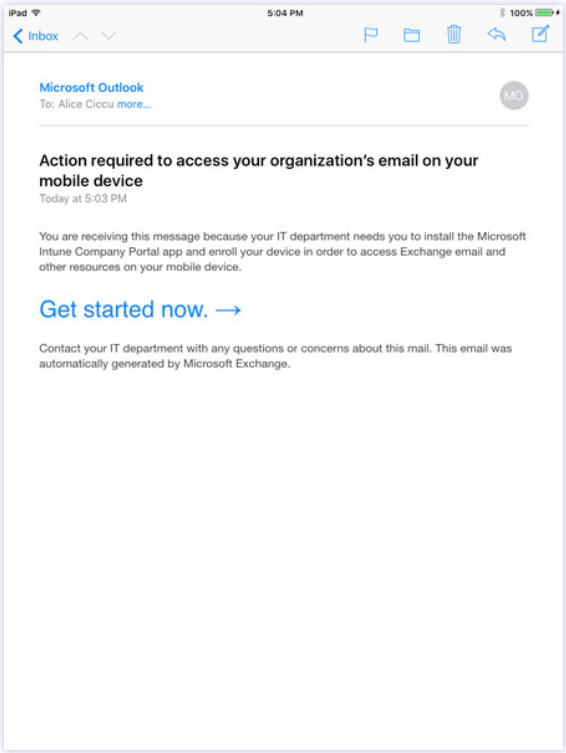
5



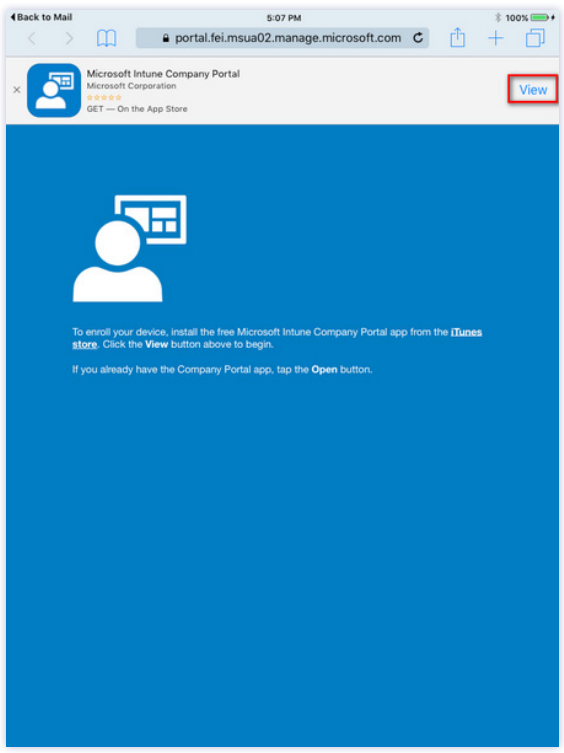


6. After the email account is verified, tap Save.

- The mailbox opens.
- After a few moments, you will receive an email from the system informing you that you need to install the Microsoft Intune Company Portal app and enroll your device before you can access email.



7. In the email, tap Get started now.



8. On the Microsoft Intune Company Portal page, tap View.

- The app store opens the Microsoft Intune Company Portal app in the foreground.

9. Depending on your settings, you may be prompted to sign in to iCloud. If prompted, enter the password for your Apple ID credentials to sign in to iCloud.
10. On the Microsoft Intune Company portal app page, tap download (cloud with down arrow).

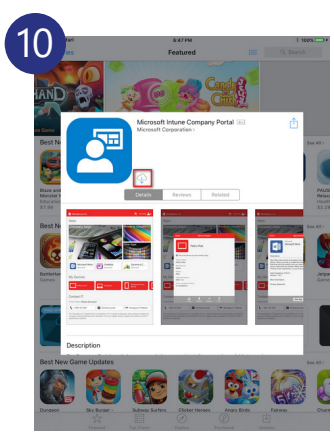
📌 After a few moments, the app is installed.

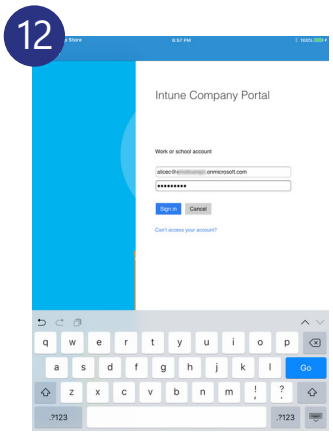
11. On the Microsoft Intune Company Portal app page, tap Open.
12. On the Intune Company Portal page, in user name, type alicec@[OrgName].onmicrosoft.com. In password, type Passw0rd!, and then tap Sign in.
13. On the Company Access Setup page, tap Begin.
14. On the Device Enrollment page, tap Enroll.
15. On the Install Profile page, tap Install.
16. When prompted, enter your passcode, and then tap Install.

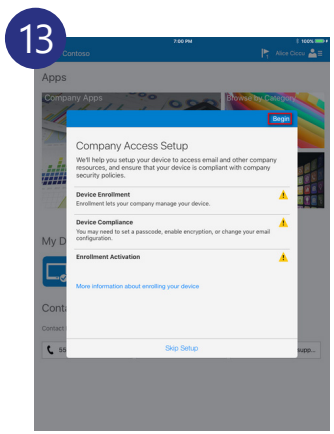
📌 A warning message appears.

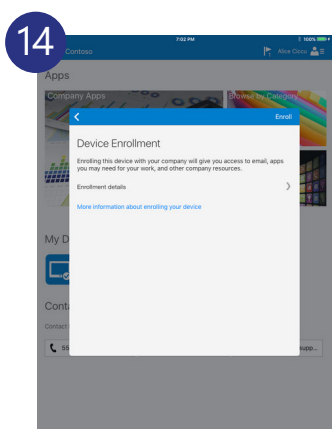
17. Read the warning, and then tap Install.
18. At the Remote Management prompt, tap Trust, and then tap Done.

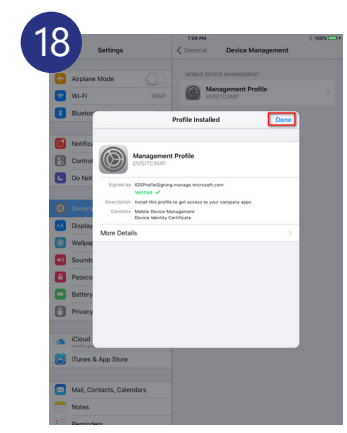
📌 If your passcode does not meet the Intune security requirements, you will be prompted almost immediately to change your passcode. If your passcode meets current security requirements, you will not be prompted to change your passcode. Your passcode must be at least 4 characters long and include both letters and numbers.

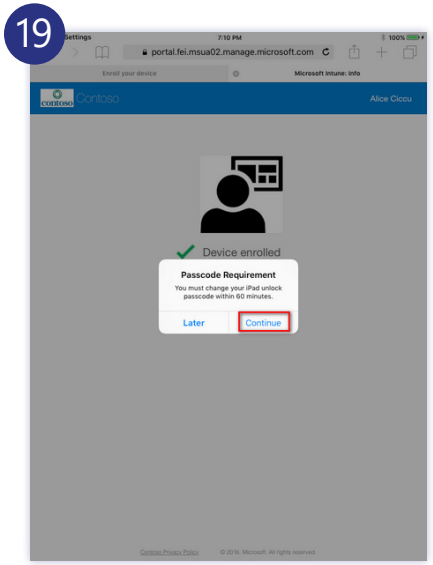


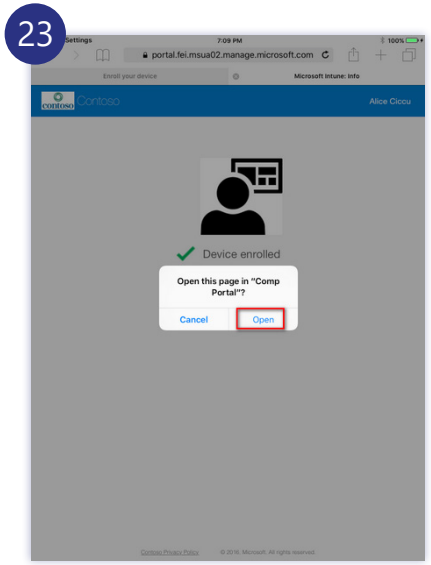


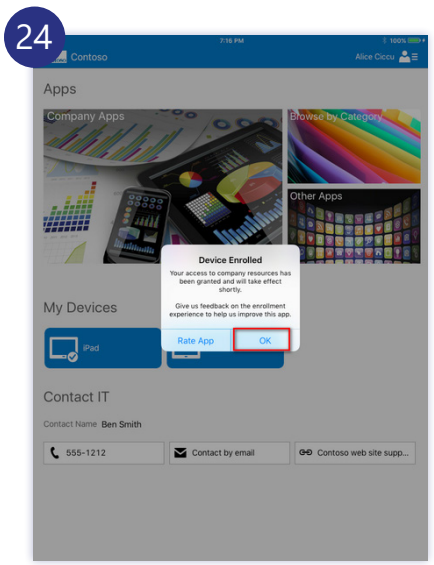


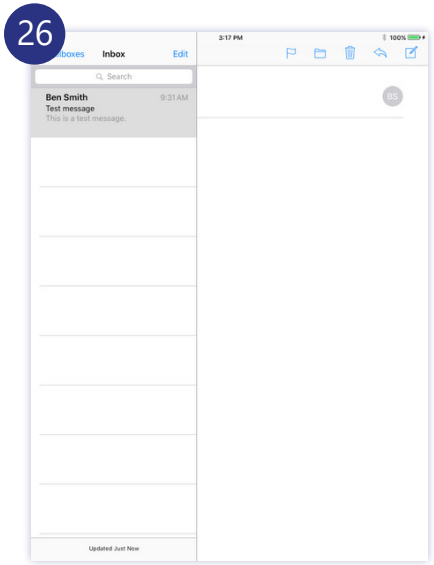












19. In the Passcode Requirement pop up, tap Continue.
20. Enter your current passcode, and then tap Continue.
21. Enter a new passcode, and then tap Continue.
22. Enter your new passcode a second time, and then tap Continue.
23. At the prompt to open the page in the Company Portal, tap Open.
24. In the Device Enrolled pop up, tap OK.
25. Press the home button, and then tap Mail.
26. In the Mail app, tap Inbox.

> If you refresh the mail, you should be able to see the test message you sent to this account at the beginning of the lab. Note that the message from the system informing you of the need to enroll the iOS device has disappeared from your inbox.

Verify Conditional Access on Android Device

In this exercise, you will configure a connection to an Exchange mailbox on an Android 4.0 + device. You will verify that, because your device is not enrolled and is out of compliance, you are not able to access your email. You will then step through the typical steps an end user would take to enroll the device and bring it into compliance. After enrolling the device and ensuring that it is in compliance, you will verify that you are now able to access the Exchange mailbox.

Please note that the Screenshots and instructions are specific to Android devices running Lollilop (Android version 5.0.2) on a Samsung Knox device. Because the device used for these instructions is using Knox, you may see some instructions that are specific to these kinds of devices only.

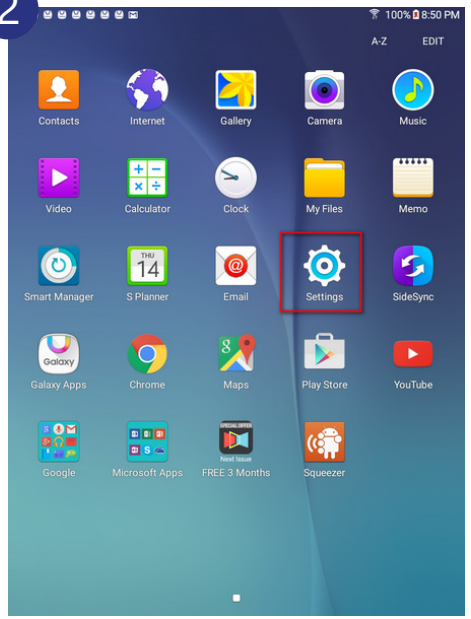
NOTE: To test the compliance rules on your Android device, you will need to have no password or a weak password configured on the device. Additionally, these steps assume you have not previously configured the built-in mail application on your Android device.

IMPORTANT: After verifying conditional access, you will need to remove the email account, remove the company portal app, and perform a selective wipe of the device to remove it from management. The selective wipe will not remove your personal data. However, please be sure you are willing to do these things before proceeding.

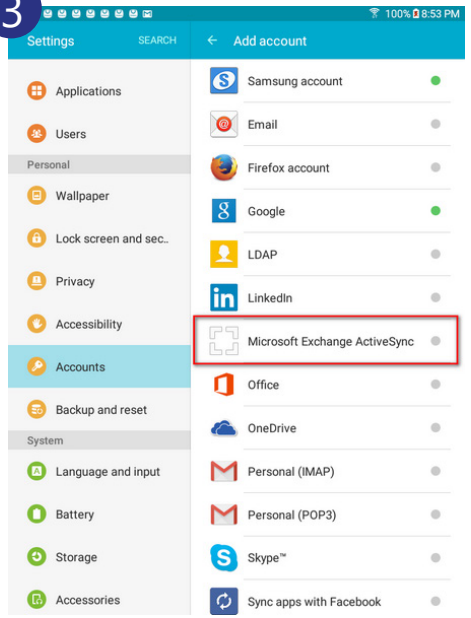
Perform these steps on your Android device

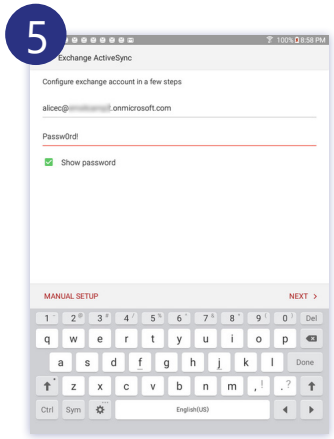
1. Sign in to your Android device.
2. Press the Home button, taps Apps, and then tap Settings.
3. In Settings, scroll down, tap Accounts, tap Add Account, and then tap Microsoft Exchange ActiveSync.
4. On the Exchange ActiveSync page, in user name, type alicec@[OrgName].onmicrosoft.com.

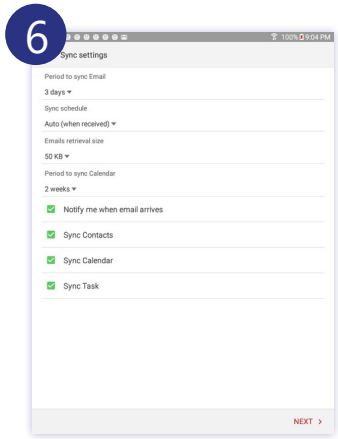
2

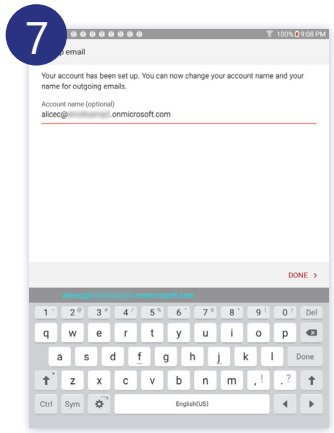


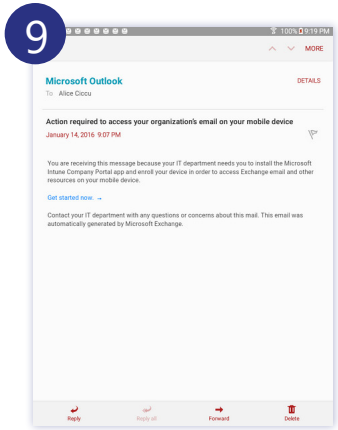
3

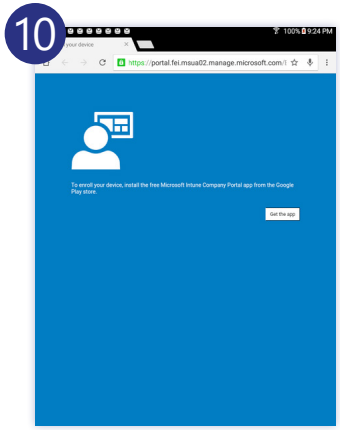


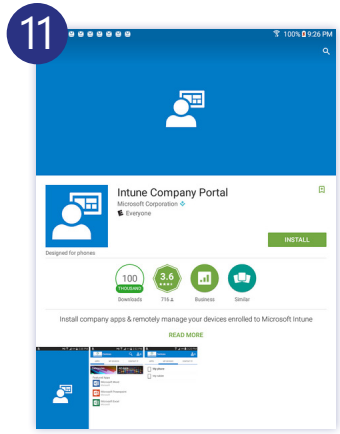












5. In Password, type Passw0rd!, and then tap Next. If prompted by an Activation message, tap OK.
6. On the Sync Settings page, accept the defaults, and then tap Next.
7. On the Set up email page, accept the default account name, and then tap Done.
8. Press the Home button, and then tap Mail.
9. In the inbox, tap the message from Microsoft Outlook, and then review the contents.

> Note that even though another message exists in your inbox, you can view only the message from the System. Once you follow the directions to enroll the device and bring it into compliance, you will gain full access to Exchange ActiveSync.

10. In the message, tap Get started now. The browser opens. On the Web page, tap Get the app.
11. On the Intune Company Portal page, tap Install.
12. When prompted, tap Accept.

> When the app finishes installing, you are presented with the option to open the app.

13. On the Intune Company Portal page, tap Open, and then tap Sign in.
14. On the Begin Company Access Setup page, tap Begin, and then on the Device Enrollment page, tap Enroll.
15. Review the activities that you will be allowing by activating administration, and then tap Activate.

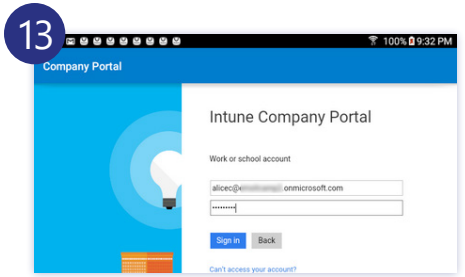
> If you have a Samsung Knox device, you will be presented with the ELM Agent privacy policy page. Check that you agree, and then tap Confirm.

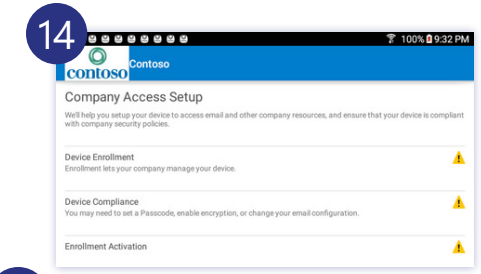
16. On the Screen unlock settings page, tap Password.

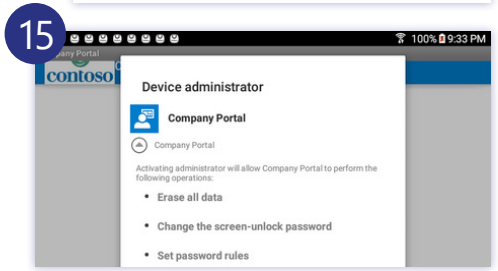
> Recall that you set the compliance rules for Android devices to require a password.

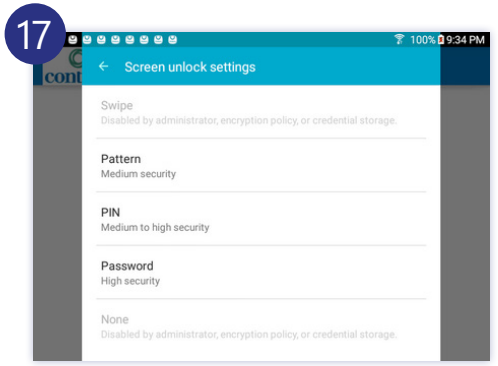
17. Follow the prompts to enter a password of your choice. If prompted to configure notifications on the lock screen, choose an option, and then tap Done.
18. On the Company Access page, tap Continue twice, and then tap Done.
19. Open the Mail app.

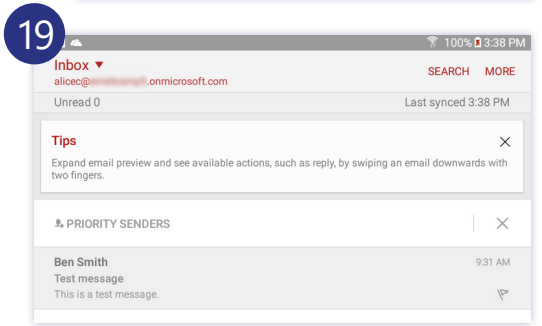
> Note that the original system message has disappeared and any other messages in your inbox will appear.











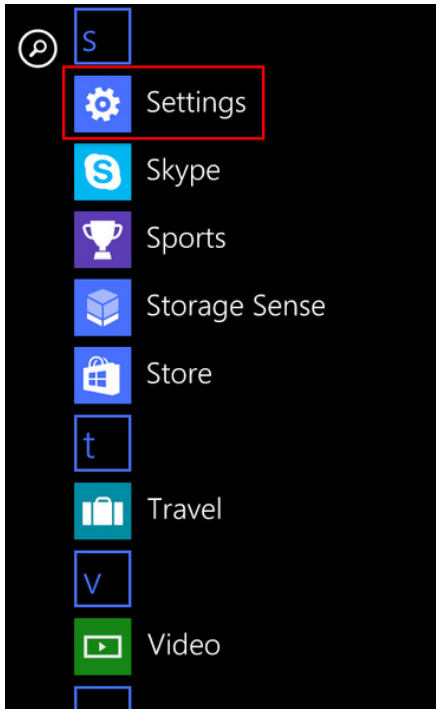
Verify Conditional Access on the Windows Phone Device

In this section, you will configure a connection to an Exchange mailbox on a Windows Phone 8.0+ device. You will verify that, because your device is not enrolled and is out of compliance, you are not able to access your email. You will then step through the typical steps an end user would take to enroll the device and bring it into compliance. After enrolling the device and ensuring it is in compliance, you will verify that you are now able to access the Exchange mailbox.

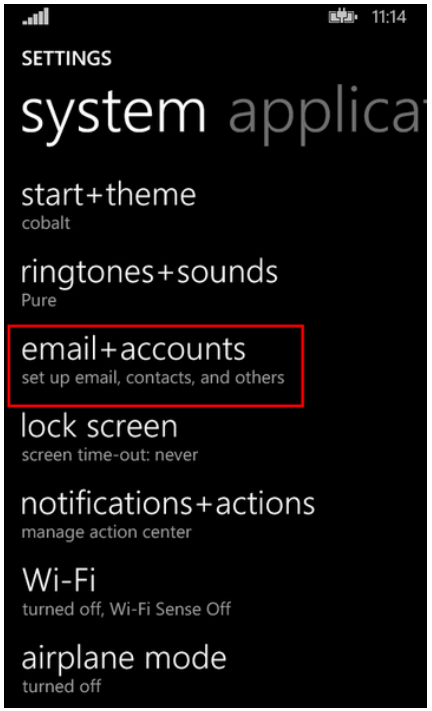
NOTE: To test the compliance rules on your Windows Phone device, you will need to have no PIN configured on the device. Additionally, these steps assume you have not previously configured the built-in mail application on your Android device.

IMPORTANT: After verifying conditional access, you will need to remove the email account, remove the company portal app, and perform a selective wipe of the device to remove it from management. The selective wipe will not remove your personal data. However, please be sure you are willing to do these things before proceeding.

Perform these steps on your Windows Phone 8.0 or higher device.



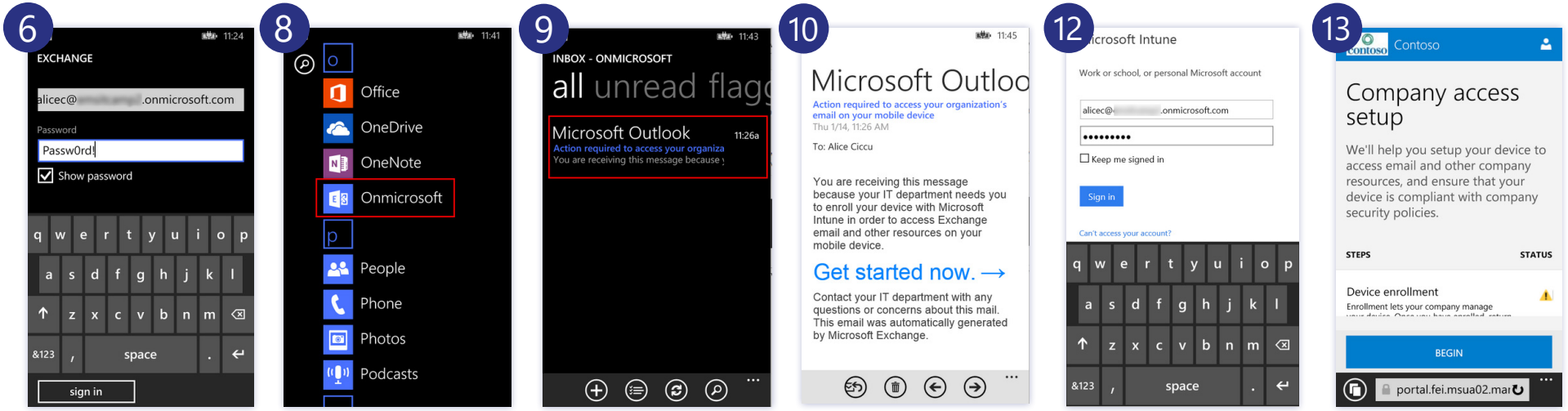
1. On the Windows Phone device, swipe left, and then tap Settings.



2. In SETTINGS, tap email+accounts.

3. Tap add an account.

4. In ADD AN ACCOUNT, tap Exchange.



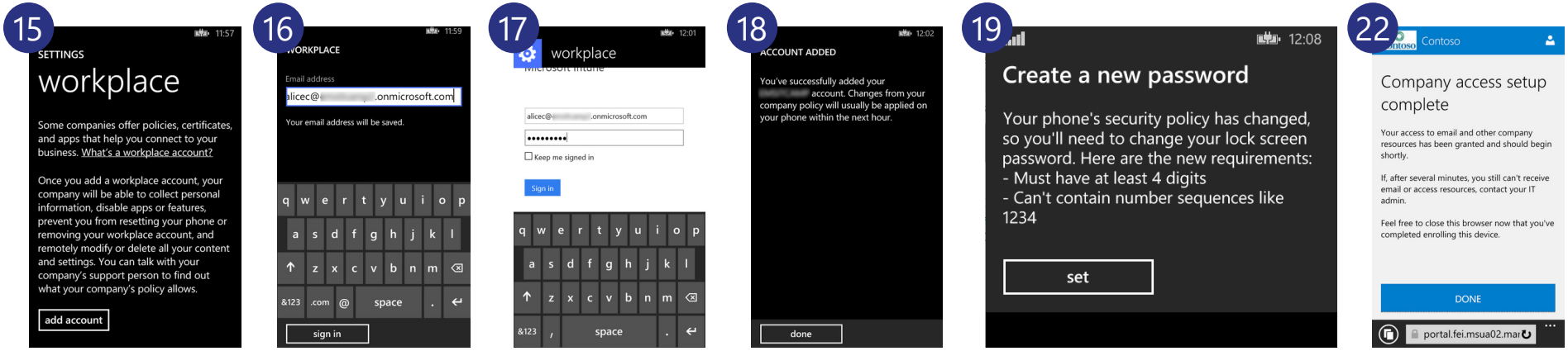
5. In EXCHANGE, in Email address, type alicec@[OrgName].onmicrosoft.com.
6. In password, type Passw0rd!, and then tap sign in.
7. After your settings have been found and the account added, click Done.
8. On your Windows Phone device, go to your apps list, and tap Onmicrosoft.
9. Tap the message from Microsoft Outlook.
10. Review the message, and then tap Get started now.

> If you are prompted to use recommended Internet Explorer settings, tap recommended.

11. On the Microsoft Intune page, in email, type alicec@[OrgName].onmicrosoft.com.
12. In password, type Passw0rd!, and then tap Sign in.

> If prompted to remember the password for the website, tap no.

13. On the Company access setup page, review the information, and then tap BEGIN.
14. On the Enroll your device page, tap enroll.



15. On the workplace page, tap add account.
16. On the Workplace page, type alicec@[OrgName].onmicrosoft.com, and then tap sign in.
17. On the Microsoft Intune page, in password, type Passw0rd!, and then tap Sign in.
18. On the account added page, tap Done.

> If your device is configured as per the lab recommendations, you will receive a notification to create or set a new password to bring the device into compliance with your policies.

19. On the Create a new password page, tap set.
20. Enter your new password, and then tap done.
21. On your phone, switch to the Internet Explorer app that was opened in a previous step.

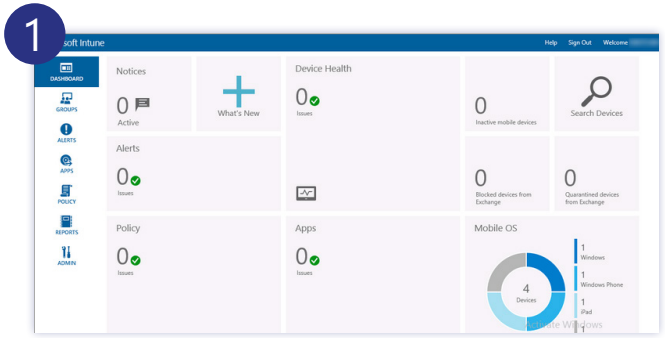
> After a few moments, you should see that your phone is in compliance.

22. On the Company access setup complete page, tap DONE.
23. When prompted to allow the window to close, tap yes.
24. Switch to Outlook, and then tap refresh.

> The original system message will disappear and any other messages in your inbox will appear.

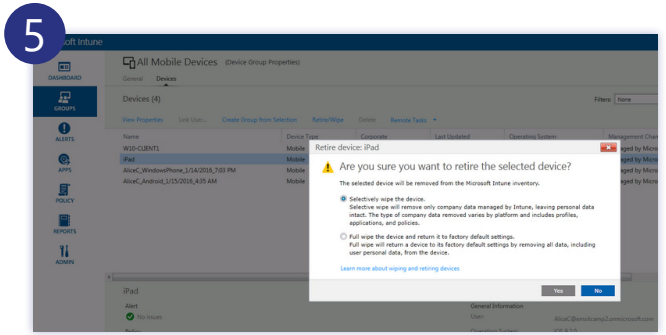
Reset Devices to Prepare for Subsequent Steps

Subsequent steps in this guide require that you use devices that are not currently enrolled in Intune. In this section, you will retire and selectively wipe any iOS, Android, or Windows Phone 8.0 + devices you used to test Exchange conditional access. Additionally, you will remove Exchange ActiveSync accounts and the company portal from any devices you configured in the previous steps.



- IMPORTANT: You must perform these steps for any devices you enrolled in the steps above. The next exercise in this guide assumes that you are using a device that has not been enrolled.
- Please ensure you are signed into the Microsoft Intune administrative console at https://manage.microsoft.com to perform these steps.

1. In the Intune admin portal, click DASHBOARD.
   - The dashboard provides a quick summary of important information, such as the number of devices not in compliance or blocked by conditional access rules.
2. Double-click the Mobile OS tile.
   - The Intune admin console opens the All Mobile Devices node.
3. On the All Mobile Devices page, select one of the devices you have enrolled.
4. On the menu, click Retire/Wipe.
5. In the Retire Device dialog box, ensure Selectively wipe the device is selected, and then click Yes.
   - Depending on the device, you may also have the option of performing a full wipe of the device and returning it to the default factory settings. There is no need for you to perform a full wipe of the device. Once the device has been unenrolled, access to corporate email will stop.
6. Repeat the steps to selectively wipe devices for all the devices you have enrolled.



Perform these next steps only if you enrolled an iOS device.

1. In the Microsoft Intune admin console, click GROUPS.
2. Under Groups \ All Mobile Devices, click All Exchange ActiveSync Managed Devices.
   - **If you enrolled an IOS device, it might revert to being managed as an Exchange ActiveSync device. Please ensure you retire the device.**
3. If an enrolled iOS device appears here, click Retire/Wipe.
4. In the Retire Device dialog box, ensure that Selectively wipe the device is selected, and then click Yes.

The next section of this guides assumes that you have not configured any corporate email settings on your device and that you have not enrolled the device. Follow the steps below to remove the ActiveSync email account and Company Portal from Android, iOS, and Windows phone devices.

Android Device

To remove the Exchange ActiveSync mail account from your Android device, follow these instructions:

1. Go to Settings.
2. Tap Accounts, tap Microsoft Exchange Active Sync, tap More, and then tap Remove account twice.

To remove the Company Portal from your Android device, follow these instructions:

3. Go to Settings. Tap Applications, tap Application Manager, tap Company Portal, and then tap Uninstall.

iOS Device

To remove the Exchange ActiveSync mail account from your iOS device, follow these instructions:

1. Go to Settings.
2. Tap Mail, Contacts, Calendars, tap Exchange, tap Delete Account, and then tap Delete.

To remove the Company Portal from the iOS device, follow these instructions:

3. Press the Home button. Tap and hold Comp Portal until it wiggles, click X, and then click Delete.

Windows Phone Device

To remove the Exchange ActiveSync mail account from your Windows Phone device, follow these instructions.

1. Wait a few minutes. A message will appear to inform you that your account has been deleted.
2. Tap Close.
3. Go to Settings.
4. Tap email+acccounts, tap and hold Onmicrosoft, and then tap delete.

The company portal is removed automatically. You do not need to manually remove it.

Part Five:
Configure and Deploy ActiveSync Email Profiles

Part Five:

Configure and Deploy ActiveSync Email Profiles

Configuring policies for devices that are enrolled in Intune helps to ensure that the devices are used in accordance with organizational requirements with minimal effort on the part of your users. Users simply have to install the company portal and follow any subsequent prompts to configure their devices to bring them into compliance. You can further assist your users in getting the most out of their enrolled devices by configuring pre-defined profiles that will automatically configure Wi-Fi, VPN, or email settings on their devices.

In this section, you will learn how to configure email profiles for Android (Knox), iOS, and Windows devices that will automatically configure Exchange email settings on enrolled devices. After configuring the email profiles, you will have an opportunity to verify the automated set up of the email settings on an iOS, Android, or Windows Phone device. You do not need to have any of these devices. The steps include screenshots that will give you a good idea of the user experience. However, to get the most of out of the exercise, having one or more of these devices is preferable.

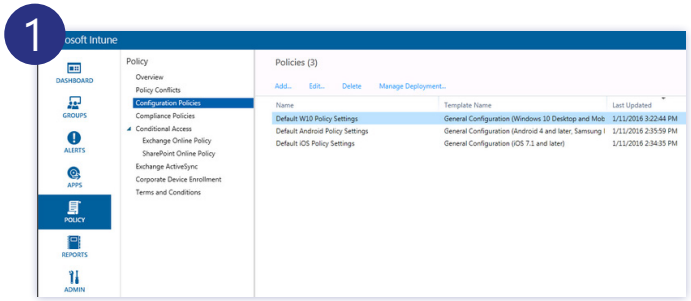
IMPORTANT: The steps in this section assume you have completed all the previous configuration steps in the Intune administrative console.

Configure an Android (Knox) Email Profile

In this task, you will configure an email profile that can be deployed to Android (Samsung KNOX Standard 4.0 and later) devices.

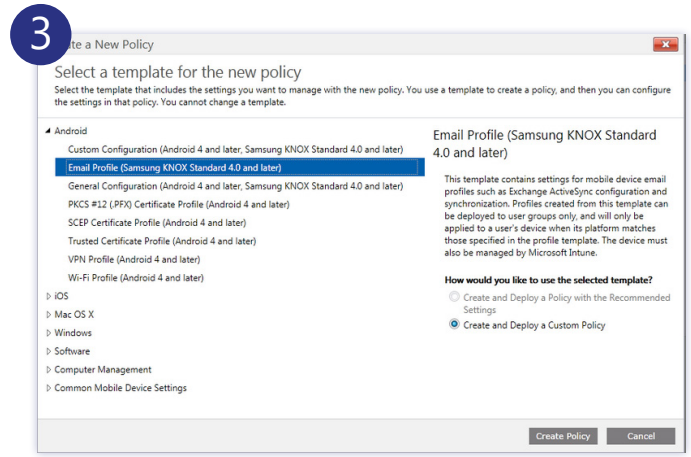
> Please ensure you are signed into the Microsoft Intune administrative console at https://manage.microsoft.com to perform these steps.

1. In the Intune admin portal, in the left navigation pane, click POLICY, and then under Policy, click Configuration Policies.



> You should see the three security policies that you created earlier.

2. Click Add.
3. In the Create a New Policy dialog box, expand Android, select Email Profile (KNOX Standard 4.0 and later), and then click Create Policy.

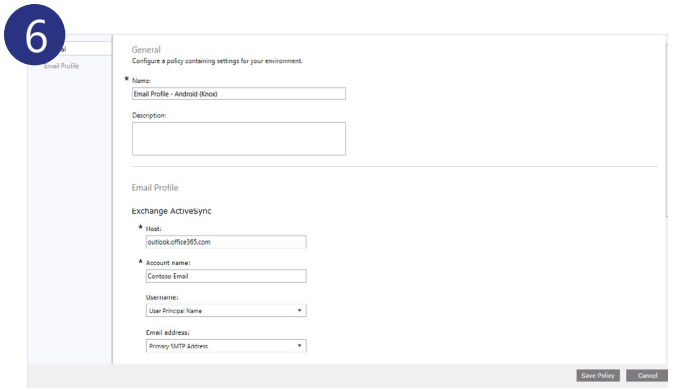


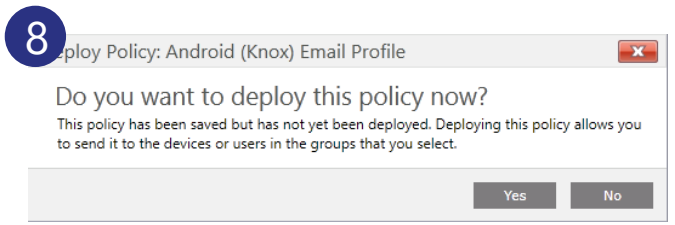
> NOTE: Among Android devices, only Samsung devices that are running Knox Standard 4.0 and later can have email profiles deployed to them.

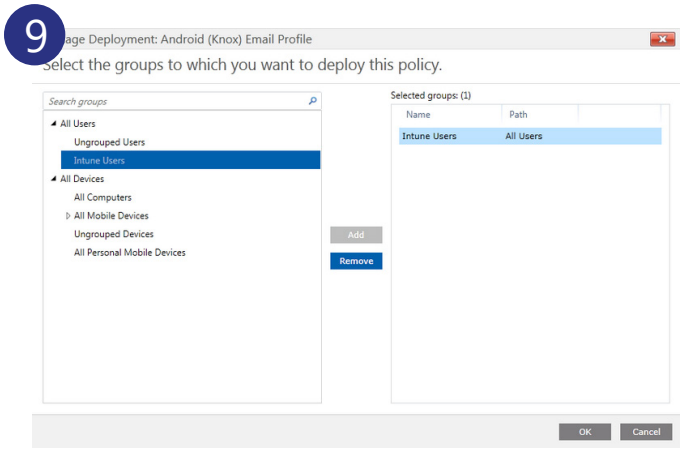
4. On the Create Policy page, in Name, type Email Profile - Android (Knox).
5. Configure the remaining properties as follows:

- Host: outlook.office365.com
- Account name: Contoso Email
- Username: User Principal Name
- Email address: Primary SMTP Address
- Authentication method: Username and Password
- Number of days of email to synchronize: Two weeks
- Sync schedule: Based on my usage
- Content type to synchronize: select all

6. Accept defaults for remaining properties
7. Click Save Policy.
8. When prompted to deploy the policy, click Yes.
9. In the Select the groups to which you want to deploy this policy dialog box, select Intune Users, click Add, and then click OK.







Configure an IOS Email Profile

In this task, you will configure an email profile that can be deployed to iOS devices.

Please ensure you are signed into the Microsoft Intune administrative console at https://manage.microsoft.com to perform these steps.

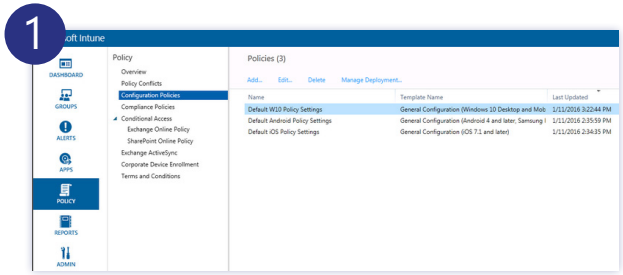
1. In the Intune admin portal, in the left navigation pane, click POLICY, and then under Policy, click Configuration Policies.

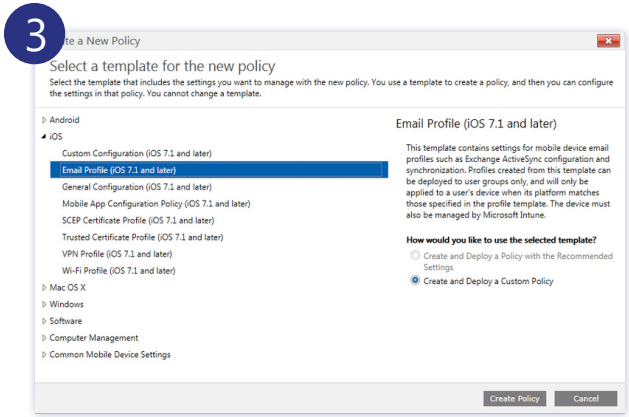
You should see the three security policies that you created earlier.

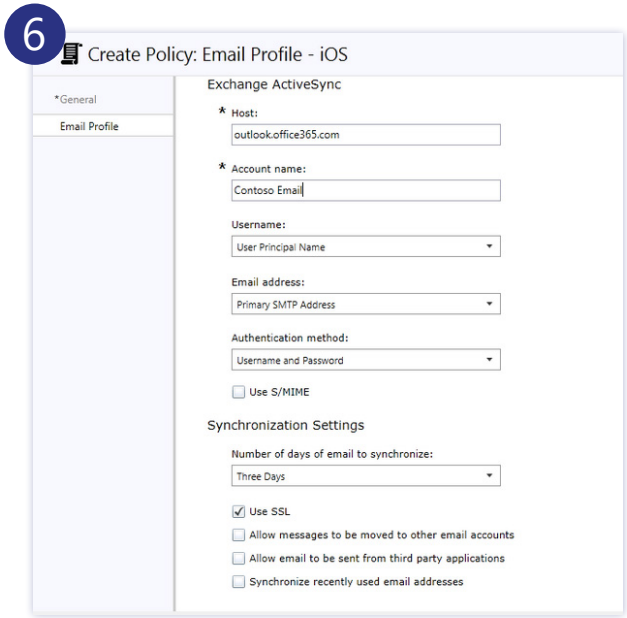
2. Click Add.
3. In the Create a New Policy dialog box, expand iOS, select Email Profile (iOS7.1 and later), and then click Create Policy.
4. On the Create Policy page, in Name, type Email Profile - iOS.
5. Configure the remaining properties as follows:

- Host: outlook.office365.com
- Account name: Contoso Email
- Username: User Principal Name
- Email address: Primary SMTP Address
- Authentication method: Username and Password
- Number of days of email to synchronize: 3 days

6. Accept remaining default values
7. Click Save Policy.
8. When prompted to deploy the policy, click Yes.
9. In the Select the groups to which you want to deploy this policy dialog box, select Intune Users, click Add, and then click OK.







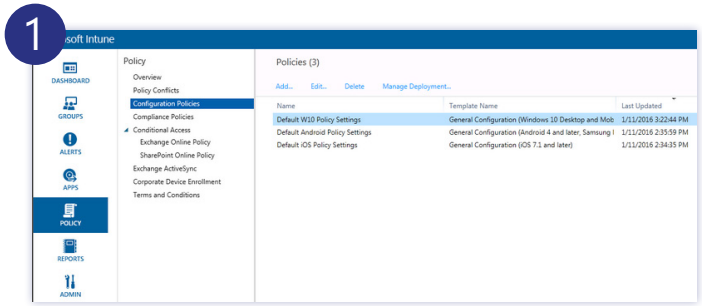
Configure a Windows Phone Email Profile

In this task, you will configure an email profile that can be deployed to Android (Samsung KNOX Standard 4.0 and later) devices.

> Please ensure you are signed into the Microsoft Intune administrative console at https://manage.microsoft.com to perform these steps.

1. In the Intune admin portal, in the left navigation pane, click POLICY, and then under Policy, click Configuration Policies.

> You should see the three security policies that you created earlier.



2. Click Add.
3. In the Create a New Policy dialog box, expand Windows, select Email Profile (Windows Phone 8 and later), and then click Create Policy.
4. On the Create Policy page, in Name, type Email Profile - Windows Phone.
5. Configure the remaining properties as follows:

- Host: outlook.office365.com
- Account name: Contoso Email
- Username: User Principal Name
- Email address: Primary SMTP Address
- Authentication method: Username and Password
- Number of days of email to synchronize: Two weeks
- Sync schedule: Based on my usage
- Content type to synchronize: select all

6. Accept defaults for remaining properties
7. Click Save Policy.
8. When prompted to deploy the policy, click Yes.
9. In the Select the groups to which you want to deploy this policy dialog box, select Intune Users, click Add, and then click OK.

Verify Deployment of Email Profile to IOS Device

In this exercise, you will install the Company Portal app from the Apple App Store on an iOS device, and then enroll the device. You will then confirm that the built-in email app is automatically configured with the email profile you configured earlier.

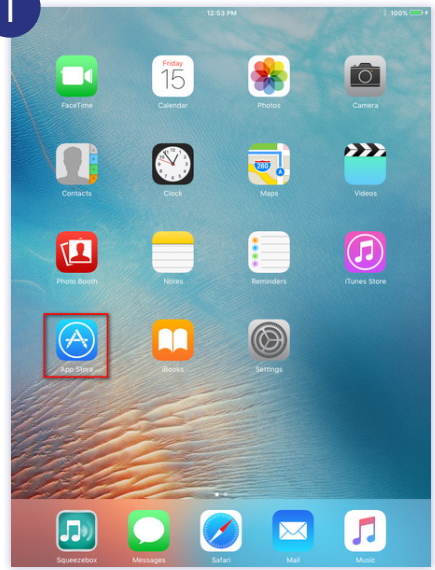
NOTE: If you do not have this kind of device, you can still review the steps in this section. They contain screenshots that will show you the process and the expected results and give you a good idea of the user experience.

IMPORTANT: The steps that follow assume that your iOS device conforms to the security and compliance policies you configured previously by using this guide. Furthermore, the steps assume that the company portal is not installed and that an Exchange email account is not configured on the device. Please note that if your iOS device does not have a password that contains both letters and numbers, you will be required to bring your device into compliance once you enroll the device.

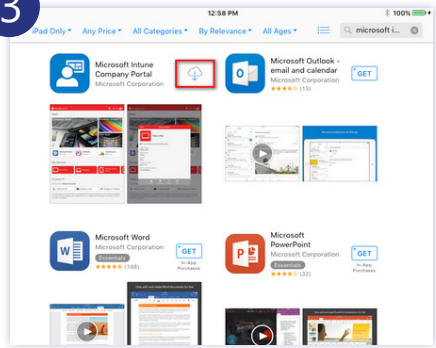
Perform these steps on your iOS device

1. On your iOS device, sign in (if necessary), press the Home button, and then tap App Store.
2. In the search box, type Microsoft Intune Company Portal.
3. In the results, beside Microsoft Intune Company Portal, tap download (cloud icon with down arrow).
4. Wait until the app finishes installing, and then, tap Open.

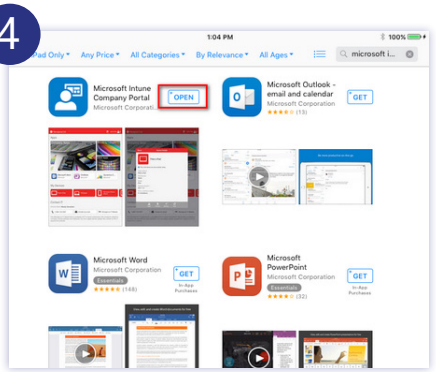
1

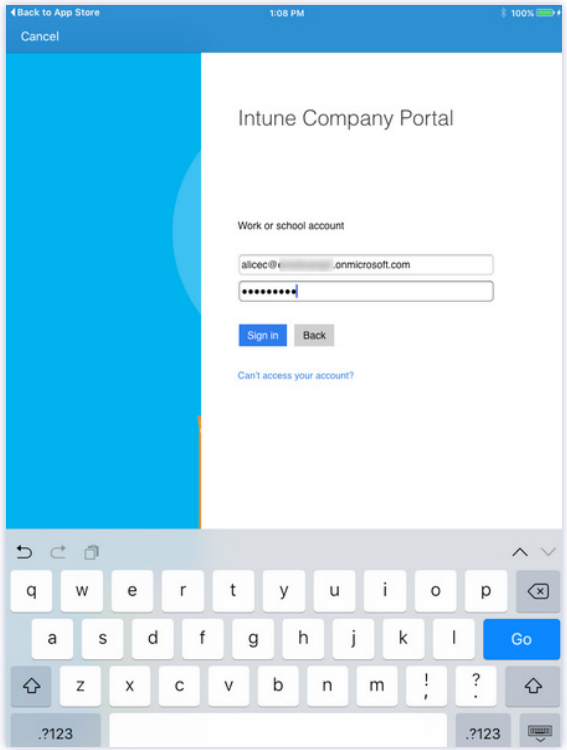


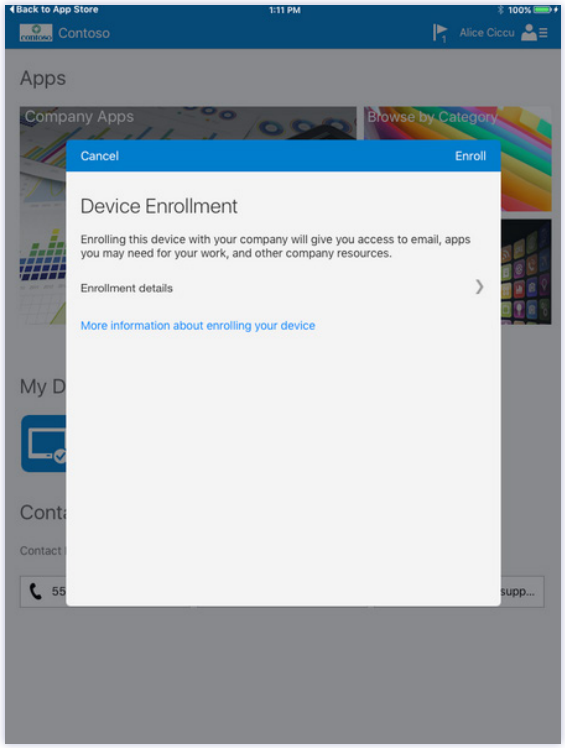
3

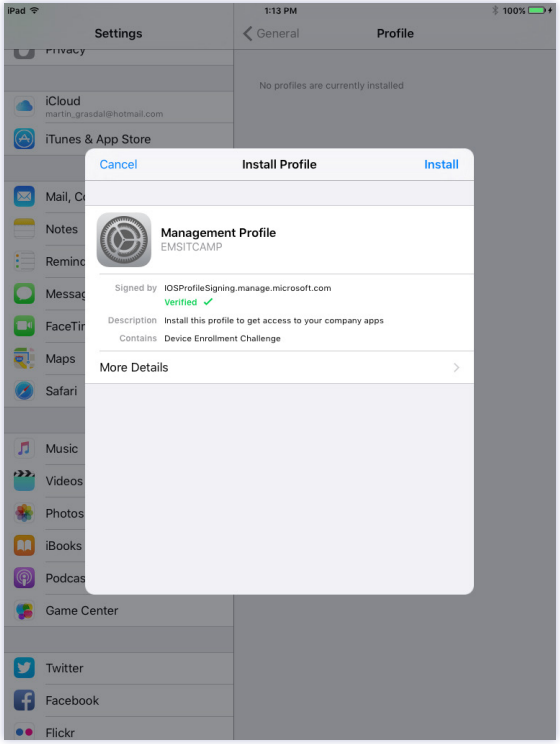


4









5. On the sign-in page, sign in as alicec@[OrgName].onmicrosoft.com using Passw0rd! as the password.

6. In the Device Enrollment notice, tap Enroll.

7. In the Install Profile notice, tap Install.

8. When prompted, enter your passcode, tap Done, and then tap Install.
9. In the warning notice, tap Install, and then tap Trust.

📌 Wait for the Password Required message to appear before moving to the next task.

10. In the Password Required box, type Passw0rd!, and then tap OK.

📌 You are prompted to enter the password as a consequence of the email profile you configured in the previous exercise.

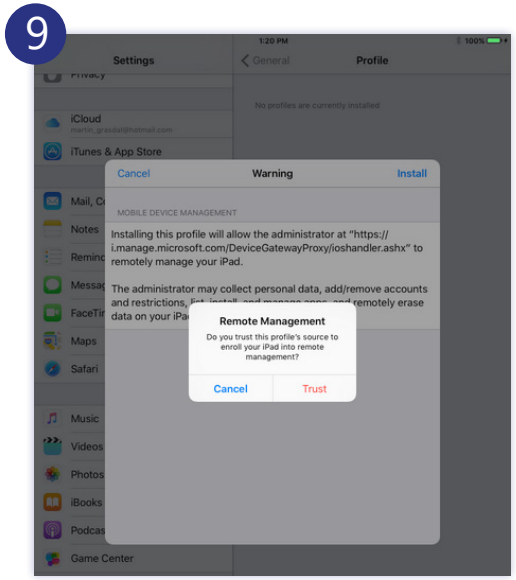
11. In the Profile Installed notice, tap Done.
12. When prompted to open page in the "Comp Portal," tap Open.
13. When notified that the device is enrolled, tap OK.
14. Press the Home button, and then tap Settings.
15. In Settings, tap Mail, Contacts, Calendars.

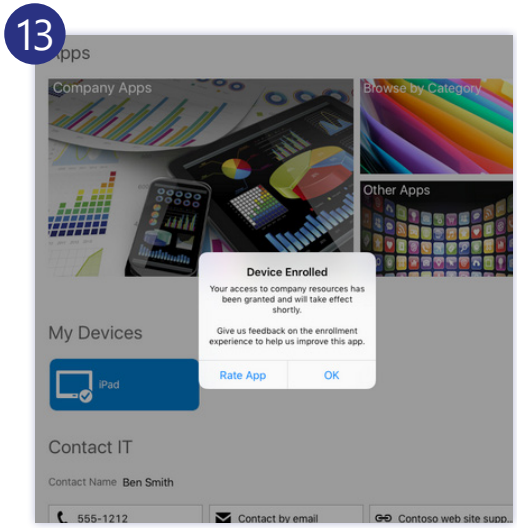
📌 The corporate Email account is displayed.

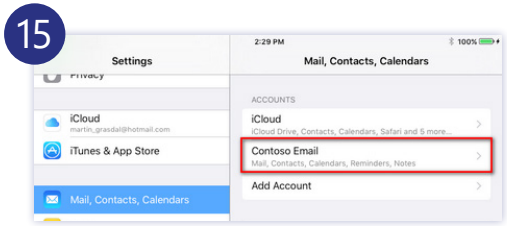
16. Press the Home button, and then tap Mail. In Mailboxes, tap Inbox.

📌 The test email message you sent to Alice Ciccu's Exchange mailbox earlier is displayed.

📌 Note that depending on how quickly you execute the lab steps, you may see the conditional access email notice you saw; however, because your device is enrolled and should be in compliance, this email will disappear and the emails in your inbox will appear shortly.







Verify Deployment of Email Profile to Android (Knox) Device

In this task, you will install the Company Portal app from the Google Play store on an Android device, and then enroll the device. You will then confirm that the built-in email app is automatically configured with the email profile you configured earlier.

NOTE: If you do not have this kind of device, you can still review the steps in this section. They contain screenshots that will show you the process and the expected results and give you a good idea of the user experience.

IMPORTANT: The steps that follow assume that your Android device conforms to the security and compliance policies you configured previously by using this guide. Furthermore, the steps assume that the company portal is not installed and that an Exchange email account is not configured on the device. Please note that if your iOS device does not have a password that contains both letters and numbers, you will be required to bring your device into compliance once you enroll the device.

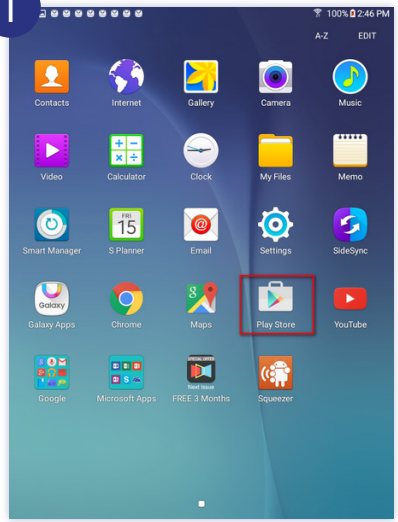
Perform these steps on your Android device

1. Sign in to your Android device. Press the Home button, tap Apps, and then tap Play Store.
2. In Google Play, in search, type Microsoft Intune Company Portal.

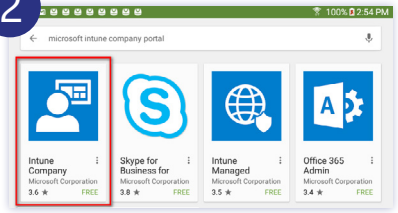
The Company Portal app is displayed.

3. In Google Play, tap Company Portal, and then tap Install.
4. When prompted, tap Accept.
5. When the Company Portal app finishes installing, tap Open.
6. On the Company Portal page, tap Sign in.
7. On the Sign in page, sign in as alicec@[OrgName].onmicrosoft.com using Passw0rd! as the password.

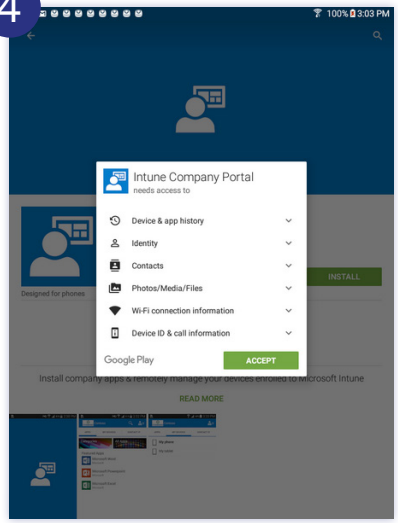
1



2



4



8. On the Device Enrollment page, tap Enroll.
9. In the Activate notification, tap Activate.
10. On the ELM Agent page, read the privacy policy, check I have read and agree to all the terms and conditions above, and then tap Confirm.

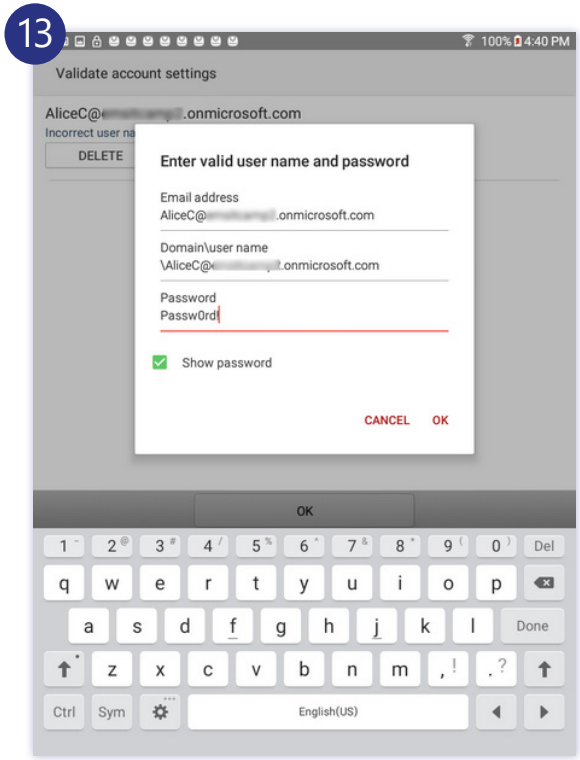
- During the enrollment process, you may hear a chime and see a notification that your email account has been received.

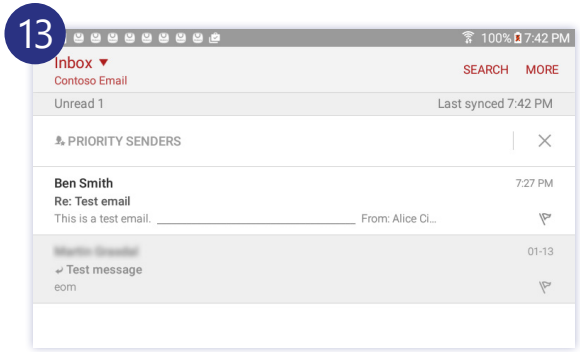
11. Press the Home button, tap Apps, and then tap Settings.
12. Tap Applications, and then tap Email.

- You are prompted to validate the email configuration.

13. On the Enter valid user name and password page, in Password, type Passw0rd!, and then tap OK.

- The email profile is deployed to your device. The configuration requires you to supply a password to authenticate to the Exchange Server.
- The test email message you sent to Alice Ciccu's Exchange mailbox earlier is displayed.
- Note that depending on how quickly you execute the lab steps, you may see the conditional access email notice you saw; however, because your device is enrolled and should be in compliance, this email will disappear and the emails in your inbox will appear shortly.





Verify Deployment of Email Profile to a Windows Phone Device

In this task, you will enroll your Windows Phone into Intune. You will then confirm that the built-in email app is automatically configured with the email profile settings you configured earlier.

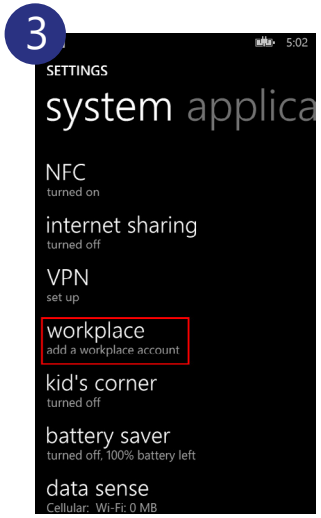
NOTE: If you do not have this kind of device, you can still review the steps in this section. They contain screenshots that will show you the process and the expected results and give you a good idea of the user experience.

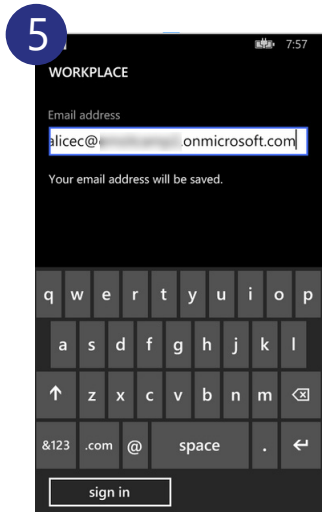
IMPORTANT: The steps that follow assume that your Windows Phone device conforms to the security and compliance policies you configured previously by using this guide. Furthermore, the steps assume that the company portal is not installed and that an Exchange email account is not configured on the device.

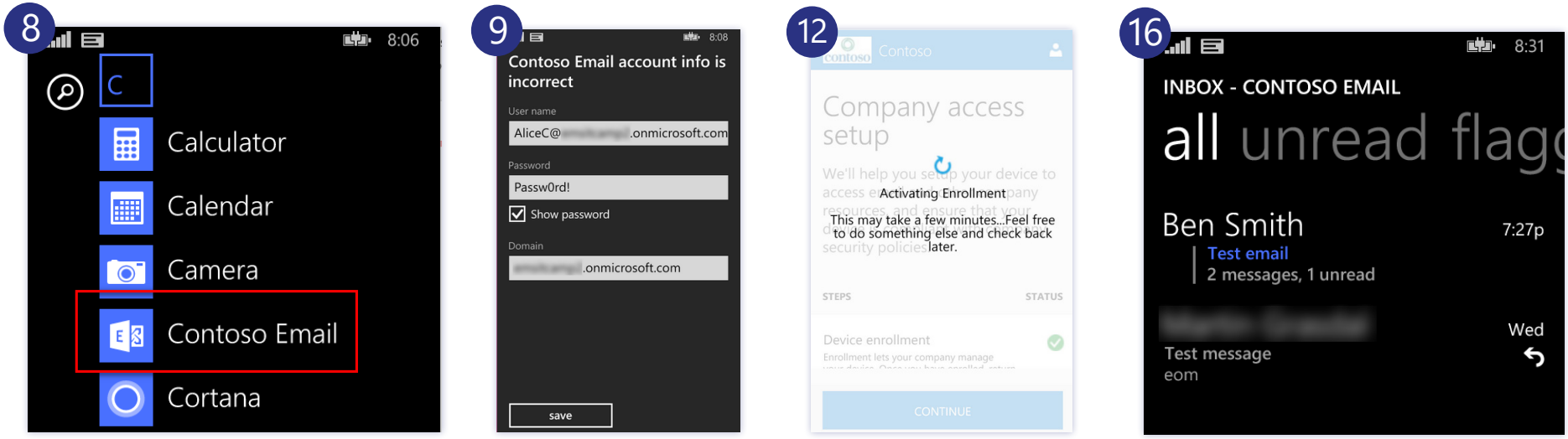
Perform these steps on your Windows Phone device

1. Sign in to your Windows Phone device.
2. From the home screen, swipe left to access the application list.
3. Tap Settings, and then tap workplace.
4. On the workplace page, tap add account.
5. When prompted for an email address, type alicec@[OrgName].onmicrosoft.com, and then tap sign in.
6. On the Microsoft Intune page, sign in as alicec@[OrgName].onmicrosoft.com using Passw0rd! as the password.
7. When you have authenticated, tap Done.

Very soon after your phone is enrolled, you will receive a notice that your Contoso email account needs attention.







8. On the Windows Phone, navigate to your apps list, and then tap Contoso Email.
9. When prompted to enter the correct settings for the Contoso email account, in Password, type Passw0rd! in domain, type [OrgName].onmicrosoft.com, and then tap save.

> You will receive the conditional access message, asking you to take action to enroll your phone and bring your device into compliance. You receive this message because your device has not completely synced with Intune. In the next steps, you will go through the enrollment process again to speed up the process of validating device compliance.

10. Open the email you received from Microsoft Outlook, and then tap Get started now.
11. On the Microsoft Intune page, tap Alicec@[OrgName].onmicrosoft.com.
12. When prompted, enter Passw0rd! as the password, and then tap Sign in.

> The Company Access Setup page appears showing that the enrollment is being activated.

13. Wait a few moments until the activation process completes, and then, on the Company access setup complete page, tap DONE.
14. Tap Yes to close the Web page.
15. On the Windows Phone, open Contoso Email.
16. In the mailbox, verify that you can see the test message(s) you sent earlier.

Remove Email Profile Targets

To avoid potential conflicts with a later lab, you will remove the target group configuration for the email profiles, which will effectively disable them.

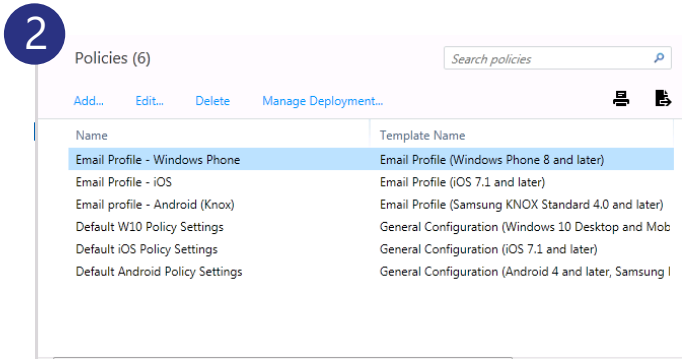
Please ensure you are signed into the Microsoft Intune administrative console at https://manage.microsoft.com to perform these steps.

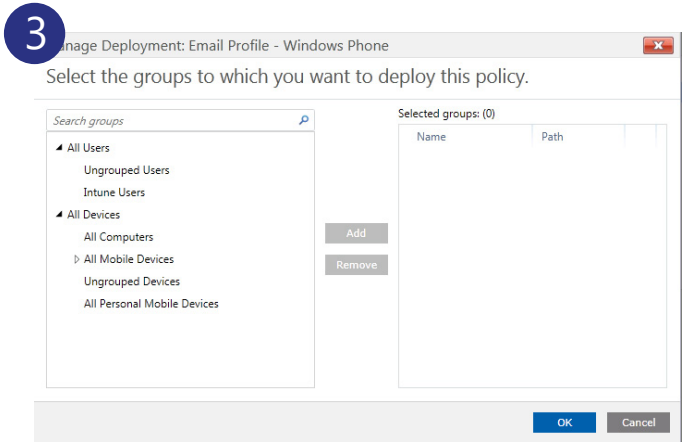
1. In the Intune admin console, click POLICY, and then click Configuration Policies.
2. On the Policies page, select Email Profile - Windows Phone, and then click Manage Deployment.
3. On the Select the groups to which you want to deploy this policy, select Intune Users, and then select Remove.

Rather than deleting the policy, you can remove its deployment.

4. Repeat these steps for each of the remaining email profiles.

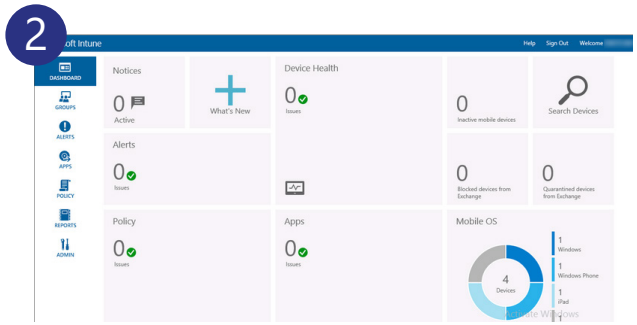
Please ensure you remove the deployments for all email profiles.





Remove Devices From Management and Uninstall Company Portal

In this task, you will unenroll any devices you have brought into management and selectively wipe data. By removing devices from management, you will learn what the end users' experience is like with regard to their email configuration. Furthermore, you will bring your devices to a state where they can be used for subsequent steps to configure mobile application management (MAM) without requiring device enrollment.



- NOTE: In the steps that follow, you will be performing a selective wipe of your device(s). You will not be resetting the device to the factory default settings.
- Please ensure you are signed into the Microsoft Intune administrative console at to perform these steps.

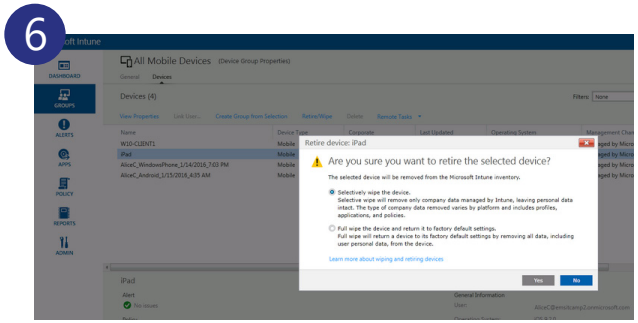
1. In the Intune admin portal, click DASHBOARD, and then double-click the Mobile OS tile. The Intune admin console opens the All Mobile Devices node.
2. In the Intune admin portal, click DASHBOARD.

- The dashboard provides a quick summary of important information, such as the number of devices not in compliance or blocked by conditional access rules.

3. Double-click the Mobile OS tile.

- The Intune admin console opens the All Mobile Devices node.

4. On the All Mobile Devices page, select one of the devices you have enrolled.
5. On the menu, click Retire/Wipe.
6. In the Retire Device dialog box, ensure Selectively wipe the device is selected, and then click Yes.



- Depending on the device, you may also have the option of performing a full wipe of the device and returning it to the default factory settings. There is no need for you to perform a full wipe of the device. Once the device has been unenrolled, access to corporate email will stop.

7. Repeat the steps to selectively wipe devices for all the devices you have enrolled.
8. After a few minutes, check the mail application on your device.

- You should see that the email profile you deployed in the previous steps has been removed.
- If the device still shows the email profile, wait a few moments and then try again.

Perform these next steps only if you enrolled an iOS device.

1. In the Microsoft Intune admin console, click GROUPS.
2. Under Groups \ All Mobile Devices, click All Exchange ActiveSync Managed Devices.

- If you enrolled an IOS device, it might revert to being managed as an Exchange ActiveSync device. Please ensure you retire the device.

3. If an enrolled iOS device appears here, click Retire/Wipe.
4. In the Retire Device dialog box, ensure that Selectively wipe the device is selected, and then click Yes.

The next section of this guide assumes that you have not configured any corporate email settings on your device and that you have not enrolled the device. Follow the steps below to remove the Company Portal from Android, iOS, and Windows phone devices.

📌 There is no need to remove the Exchange ActiveSync account. This is removed automatically when the device is unenrolled from Intune management.

Android Device

To remove the Company Portal from your Android device, follow these instructions:

- Go to Settings. Tap Applications, tap Application Manager, tap Company Portal, and then tap Uninstall.

iOS Device

To remove the Company Portal from the iOS device, follow these instructions:

- Press the Home button. Tap and hold Comp Portal until it wiggles, click X, and then click Delete.

Windows Phone Device

The company portal is removed automatically. You do not need to manually remove it.

Part Six:
Configure Mobile Application Management (MAM) Without Enrolling Devices

Part Six:

Configure Mobile Application Management (MAM) Without Enrolling Devices

Using the mobile application management policies in Microsoft Intune, IT administrators can manage applications and corporate data on users' devices without requiring those devices to enroll in mobile device management. With this model, users do not have to give up control over many aspects of their devices in order to gain access to corporate resources. Furthermore, this functionality can work in combination both with Intune and third-party mobile application management solutions.

In this section, you will use the new Azure portal to configure mobile application management policies for iOS and Android devices that are not enrolled in Intune. You will then install the managed app, OneDrive, on these devices and test some of their security features. For example, you will try to open some of the files using an unmanaged app and, on the Android device, attempt to take a screen capture of the files. You will also explore the multi-identity capabilities of the managed app that allows you to use both personal and corporate data in the same app, but keep these data separate from each other.

Configure Mobile Application Management (MAM)

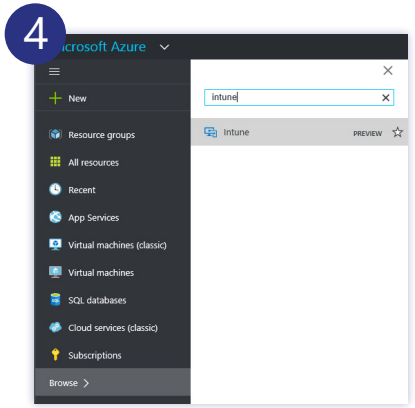
In this exercise, you will sign in to the Azure portal. From there, you will add and configure mobile application management policies for iOS and Android devices. You will examine the settings available with each policy and distinguish those policies that are unique to each device.

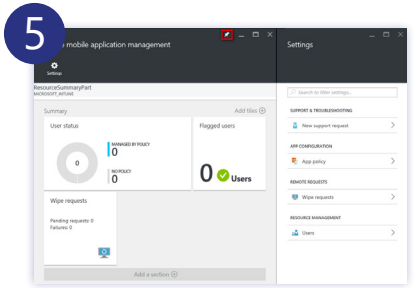
> Perform this task using Internet Explorer or other compatible browser.

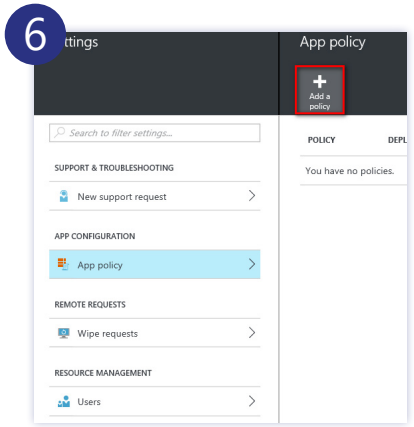
1. In an InPrivate or Incognito browser session, navigate to https://portal.azure.com.
2. On the sign in page, sign in as admin@[OrgName].onmicrosoft.com, the tenant administrator account you configured at the beginning of this guide.

> The new Azure portal will eventually become the home for a unified console to manage and monitor all cloud-related infrastructure, from virtual machines and Web applications to mobile device manager enrollment and Office 365 deployments. As an initial step in this direction, Intune's mobile application management features are managed through this portal.

3. In the left navigation pane of the Azure portal, click Browse.
4. In search, type Intune, and then in the results, click Intune.
5. In the Intune mobile application management blade, click Pin blade to dashboard (pin icon).
6. On the Settings blade, click App policy, and then in the App policy blade, click Add a policy.
7. On the Add a policy blade, in Name, type iOS secure apps policy. Make sure iOS is selected as the Platform.
8. On the Add a policy blade, click Apps.







9. On the Apps blade, accept the default OneDrive selection, and then click Select.

> As you will see in subsequent steps, iOS offers more apps for management than Android; however, in both cases, this list will grow in the future and include third-party apps. For more information on the future of supported mobile application management apps, please see http://blogs.technet.com/b/microsoftintune/archive/2015/11/17/enhancing-managed-mobile-productivity.aspx.

10. On the Add a policy blade, click Configure required settings.

11. On the Settings blade, review the settings, accept the default settings, and then click OK.

> As you will learn in subsequent steps, the settings for both Android and iOS devices are similar. The settings that are unique to iOS include Prevent iTunes and iCloud backups and Allow fingerprint instead of Pin. Note the setting to wipe data if the device is offline for a specified number of days. If this setting is 0, the feature is disabled. Also note the setting, Allow app to receive data from other apps. With this setting enabled, it will not be possible to view any documents in OneDrive unless other managed applications are available.

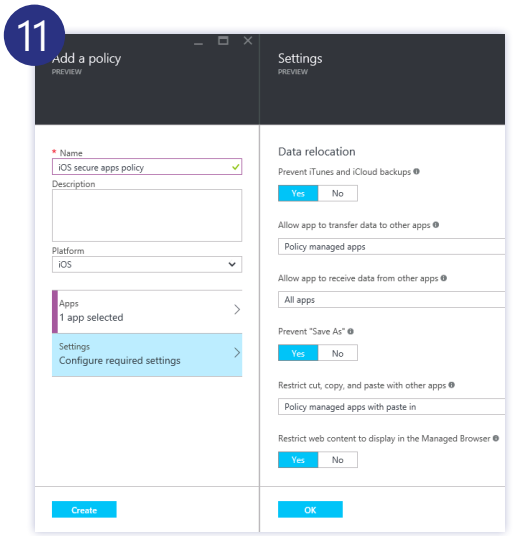
12. On the Add a policy blade, click Create.

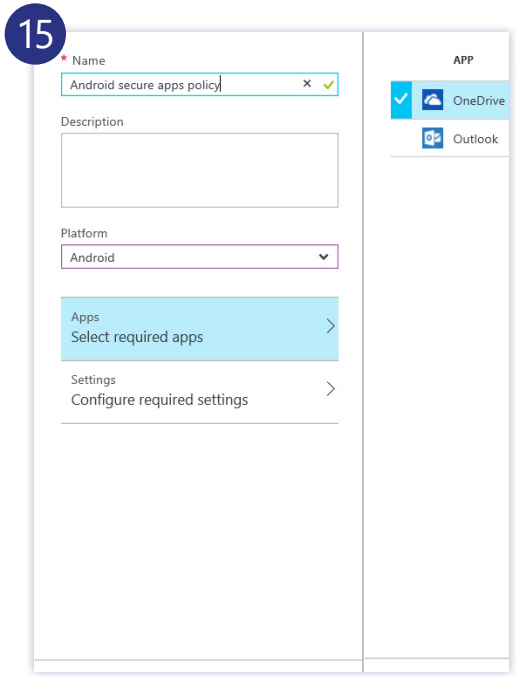
13. On the App policy blade, click Add a policy.

14. On the Add a policy blade, in Name, type Android secure apps policy, and then in platform, select Android.

15. Click Select required apps. In the Apps blade, select OneDrive, and then click Select.

16. On the add a policy blade, click Configure required settings.





17. On the Settings blade, review the settings, accept the default settings, and then click OK.

> The settings that are unique to Android include Prevent Android backups and Block screen capture and Android assistant. Please pay particular attention to the setting Allow app to receive data from other apps. With this setting enabled, it will not be possible to view any documents in OneDrive unless other managed applications are available.

18. On the App policy blade, click iOS secured app policy, and then on the iOS secured app policy blade, click User groups.

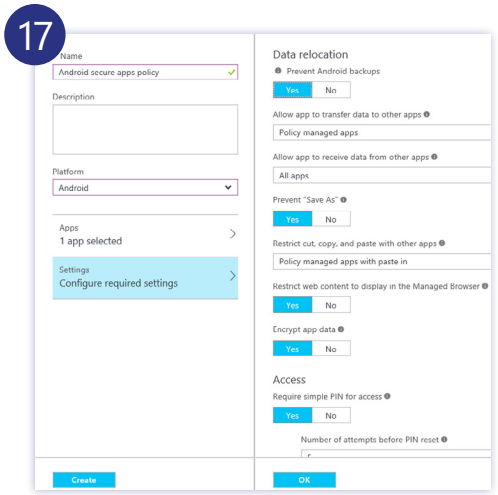
19. On the User group policy blade, click Add user group.

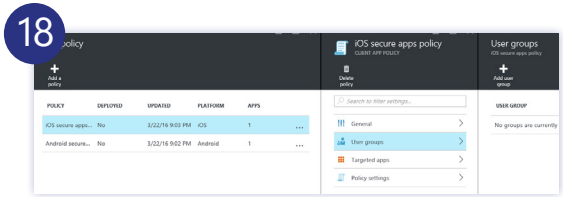
20. In the Add user group blade, search for and select Mobile Users, and then click Select.

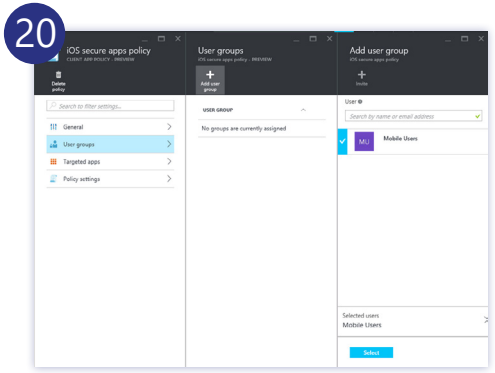
21. Repeat the steps 18–20 to target the Android secure apps policy to the Mobile Users group.

> Click the X in the upper-right corner of the blade to the far right to close it. Close all open blades. Note that the dashboard displays the Intune mobile application management tile that you pinned earlier.

22. Close the browser tab that is opened to the Azure portal.







Add Samples Files to OneDrive

In this task, you will sign on to OneDrive as Alice Ciccu, the test user you created earlier, and upload sample files to OneDrive. You are doing this to ensure that you have some data in OneDrive to verify the Mobile Application Management policy.

> TIP: Before proceeding with these steps, you may find it helpful to create a folder to hold your sample files. Then, copy some text, Word, and PDF files to the folder. Please make sure you include at least one text file, one Word document, and one PDF file.

> Perform this task using Internet Explorer or other compatible browser.

1. In an InPrivate or Incognito browser session, navigate to http://1drv.com.

> Use http, not https in the prefix.

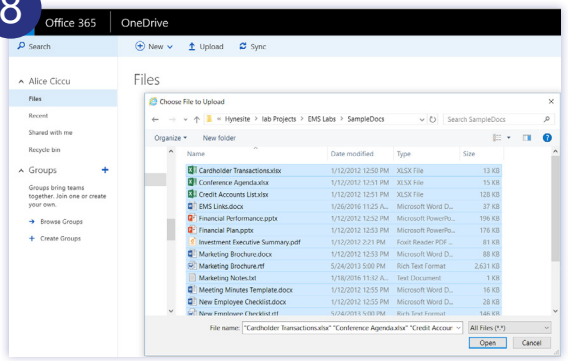
> You are redirected to the OneDrive sign in page.

2. On the OneDrive sign in page, click Sign in.
3. In Enter the email address of the account you want to sign in to, type alicec@[OrgName].onmicrosoft.com, and click Next.
4. On the Office 365 sign in page, in Password, type Passw0rd!, and click Sign in.
5. On the Welcome to OneDrive for Business page, click Next.
6. On the OneDrivePage, click Upload.
7. In the Choose File to Upload dialog box, navigate to a folder holding the sample files you wish to upload.
8. Select all the files you wish to upload, and then click Open.

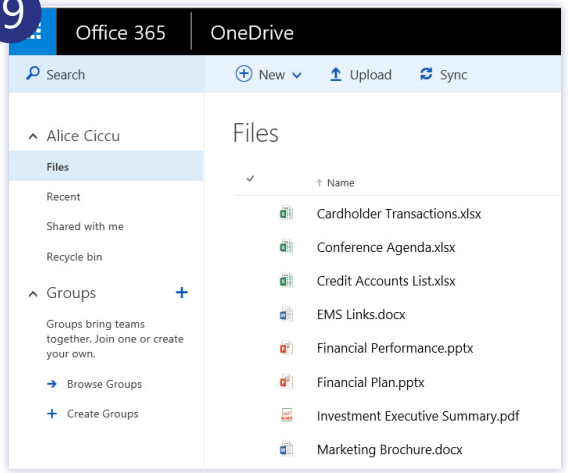
> The files displayed below are for example purposes only. Your files will differ.

9. The files appear in OneDrive.
10. Close the browser tab displaying the OneDrive files.

8



9



Verify iOS Secure App Policy

In this task, you will install the OneDrive app on your iOS device, and then sign in using your demonstration account (Alicec@[OrgName].onmicrosoft.com). You will then verify that you are unable to open documents in other programs. You will add a personal OneDrive and compare the differences between security settings.

> NOTE: To perform all the steps in this exercise, you must have a PDF reader installed on your iOS device, and you must also have access to a personal OneDrive account that has a PDF document available in it.

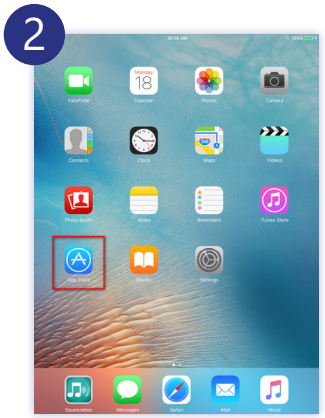
> Perform these steps on your iOS device.

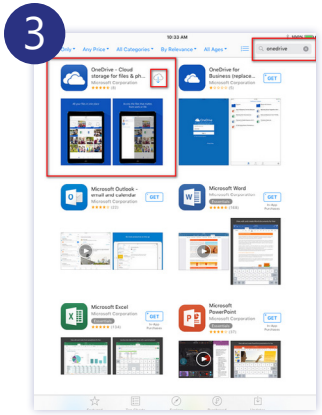
1. Sign in to your iOS device.
2. Press Home, and then tap App Store.
3. In the App Store, in Search, type OneDrive.
4. In the search results, to the right of OneDrive - Cloud storage for files & photos, tap download (cloud icon with down arrow).

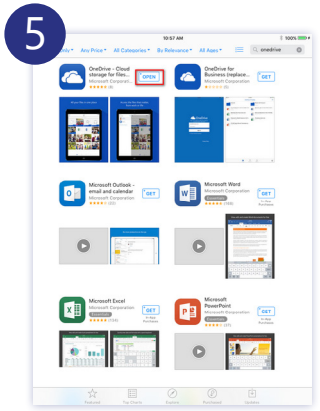
> Please do not install OneDrive for Business. The OneDrive app you are installing is more recent and belongs to a class of apps that support multi-identity, which enables the co-existence of policy-managed (Intune) and unmanaged (personal) files in a single app.

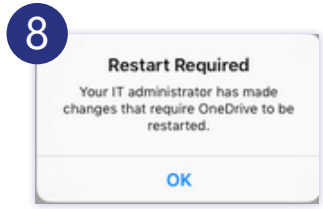
5. After OneDrive finishes installing, tap OPEN.
6. On the OneDrive page, enter alicec@[OrgName].onmicrosoft.com, and then tap Go.
7. On the Office 365 sign in page, sign in as alicec@[OrgName].onmicrosoft.com using Passw0rd! as the password.
8. When prompted, in the Restart Required notification, tap OK.

> This restart is currently required for apps that are managed by Intune. At some point in the future, this restart will not be required.









9. Tap the OneDrive app to open it again. When prompted, enter a 4-digit PIN.

- Because OneDrive is a managed application, you will be prompted for a PIN when you try to access corporate data.
- Please make a note of this PIN. You will be required to remember it in later steps.

a. With OneDrive open, identify a sample PDF file you uploaded earlier.
b. Press and hold the PDF file until it is selected.
c. On the bottom right, tap the ellipses (. . .), and then tap Open in Another App.

- You will receive a message stating that the file could not be opened.

10. Click OK to acknowledge the message.

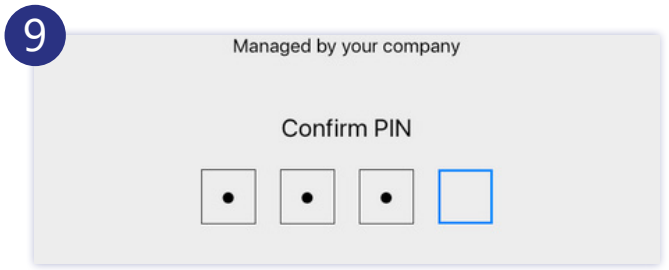
- The file is encrypted and will not open outside of OneDrive or other managed applications.

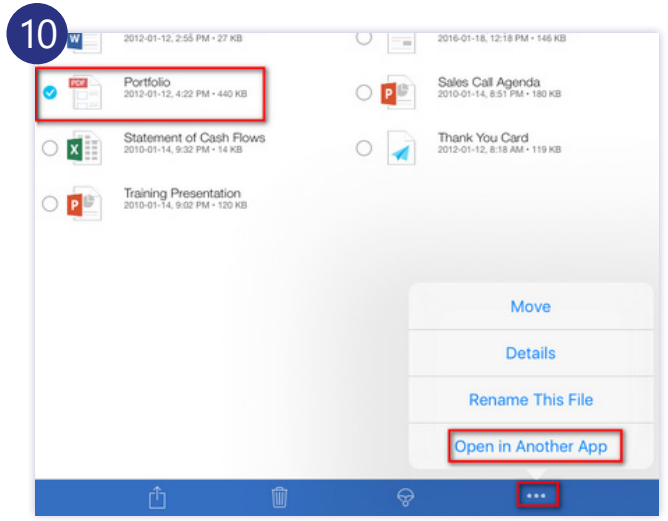
11. Deselect PDF file.
12. In the upper-left corner, tap the accounts icon (see the screenshot). Tap Add Account, and then follow the prompts to add a personal OneDrive account that you have access to.

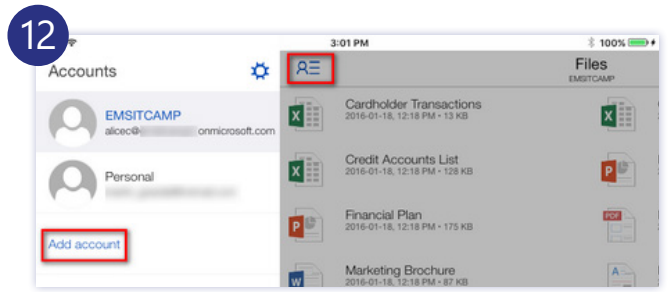
- The OneDrive app, along with a number of other apps, supports the multi-identity feature. Using this capability, you can keep corporate data and personal data separate in the same app. When you are no longer with the organization, access to corporate data can be removed without affecting your personal data. For more information on this feature, please see http://blogs.technet.com/b/microsoftintune/archive/2015/07/21/multi-identity-and-mobile-app-management-with-microsoft-intune.aspx.

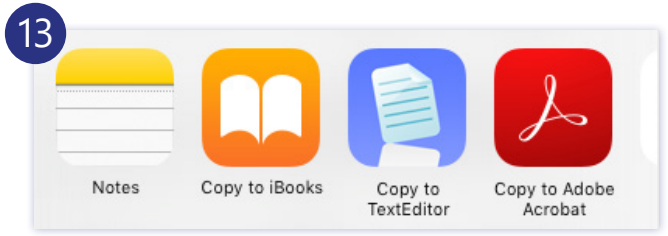
13. Select your personal OneDrive account, and then locate and select a PDF file in your OneDrive account. On the bottom right, tap the ellipses (. . .), and then tap Open in Another App.

- You should see a list of one or more PDF reader applications that can open the file.
- Because your personal files are not encrypted, any registered PDF reader should be able to open the PDF file from your personal OneDrive folder.



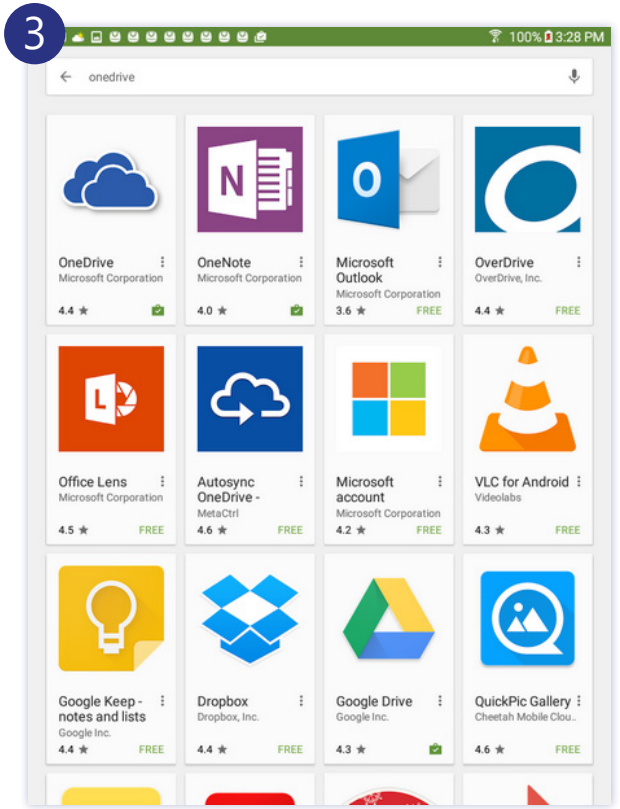






Verify an Android Secure App Policy

In this task, you will install the OneDrive app on your Android device, and then sign in using your demonstration account (Alicec@[OrgName].onmicrosoft.com). You will then verify that you are unable to open documents in other programs. You will add a personal OneDrive and compare the differences between security settings.



> NOTE: To perform all the steps in this exercise, you must have a PDF reader installed on your Android device, and you must also have access to a personal OneDrive account that has a PDF document available in it.

> Perform these steps on your Android device.

1. Sign in to your Android device.
2. Press Home, tap Apps, and then tap Play Store.
3. In the Play Store, in Search, type OneDrive.
4. In the search results, tap OneDrive, and then tap Install.

> IMPORTANT: If OneDrive is pre-installed on your device, please make sure you update the version. Or, if you have the option, uninstall the current version and install the newer one.

5. When OneDrive finishes installing, tap OneDrive and then sign in to OneDrive as alicec@[OrgName].onmicrosoft.com using Passw0rd! as the password.

> Upon sign in, you will be prompted to install the Intune Company Portal app. Please note that you are installing the Company Portal app to provide the desired management functionality for the OneDrive app. You are not required to enroll and bring the entire device under Intune management.

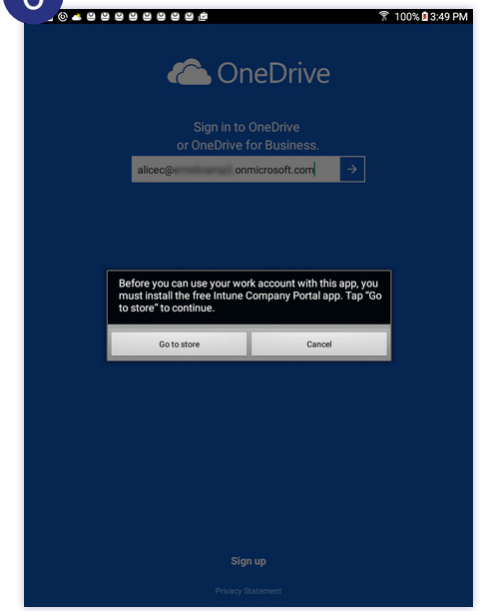
6. Tap Go to store to begin the installation of the app.
7. On the Intune Company Portal page, tap Install, and then tap Accept.

> You do not need to open the Company Portal app after you finish installing it.

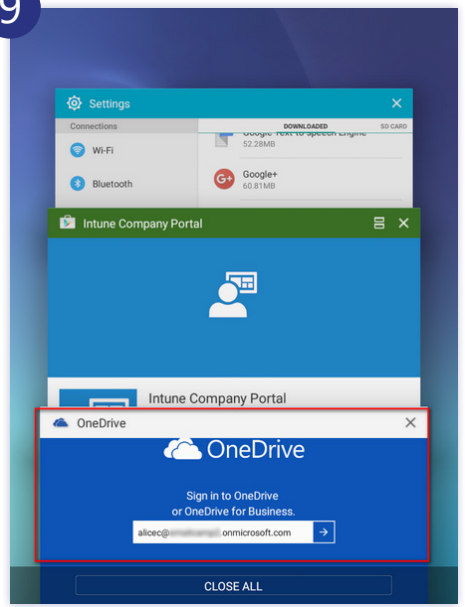
8. On your Android device, press Recent apps (button to the left of Home), and tap the OneDrive page.
9. Sign in to OneDrive as alicec@[OrgName].onmicrosoft.com using Passw0rd! as the password.
10. Upon sign in, you will be prompted to enter a PIN.

> If you are not prompted for a PIN, you may have an out-of-date version of the app. Please verify you have the most recent version. If you have the most recent version, remove the account (on your Android device, go to Settings > Accounts to do this), and then sign in again.

6



9



11. Choose a 4-digit PIN, and enter it. OneDrive opens.

- Please make a note of this PIN. You will be required to remember it in later steps.

12. With your OneDrive open, attempt to take a screen capture of the OneDrive files.

- On most Android devices, you take a screen capture by pressing the Sleep/Power and Home button simultaneously.
- You will see a message indicating that DRM is preventing you from taking a screen capture.

13. Locate a text file and try to open it.

- You uploaded a text file to the OneDrive account.
- Note that you have no authorized apps that can open this file.

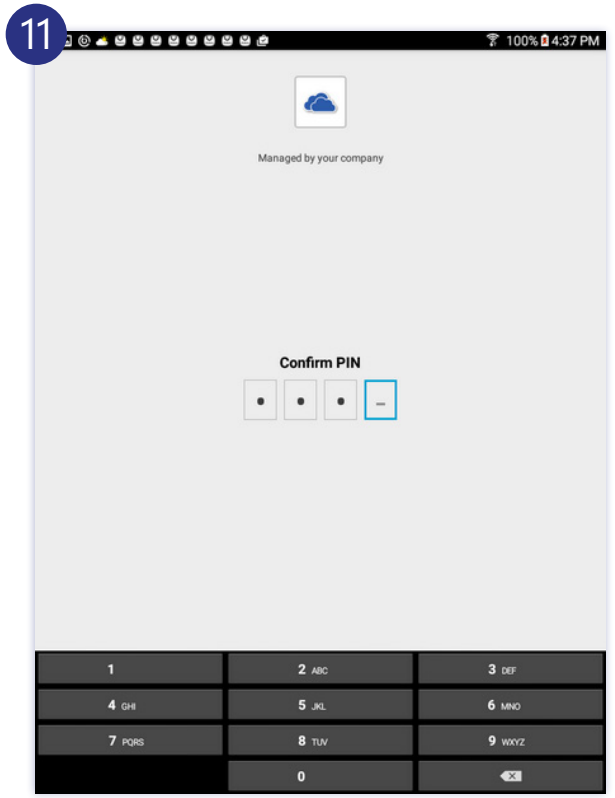
14. In the left side of the screen, tap Add another account.
15. Follow the prompts to add a personal OneDrive account that you have access to.

- The OneDrive app, along with a number of other apps, supports the multi-identity feature. Using this capability, you can keep corporate data and personal data separate in the same app. When you are no longer with the organization, access to corporate data can be removed without affecting your personal data. For more information on this feature, please see http://blogs.technet.com/b/microsoftintune/archive/2015/07/21/multi-identity-and-mobile-app-management-with-microsoft-intune.aspx.

16. On the Android device, press Home, tap Apps, and then tap Settings.

- In the next steps you will remove the company portal app. Having the company portal app installed before the beginning of the next section can cause problems with the enrollment process.
- IMPORTANT: Make sure you remove the company portal app before proceeding in this guide.

17. Tap Applications, tap Application Manager, and then tap Company Portal.
18. Tap Uninstall.



Part Seven: Configure Mobile Application Management

Part Seven:

Configure Mobile Application Management

In the previous section, you learned how to deploy managed applications to devices that were not enrolled into Intune Management.

To review, mobile application management policies in Microsoft Intune allow you to deploy managed apps that are in compliance with your organization's security and policy requirements. Some of the policies you can enforce with mobile application management are:

- Encrypt corporate data.
- Prevent Save as.
- Restrict cut, copy, and paste operations.
- Prevent Android, iTunes, or iCloud backups.
- Require a simple PIN or corporate credentials for app access.
- Open in-app website links in a managed browser application.

In this section, you will configure and deploy managed apps, including the managed browser, to iOS and Android devices.

Create and Send Test Email

In this task, you create and send a test email that you will use throughout this guide to verify your configuration on various devices.

> Please perform these steps using an InPrivate or Incognito browser session.

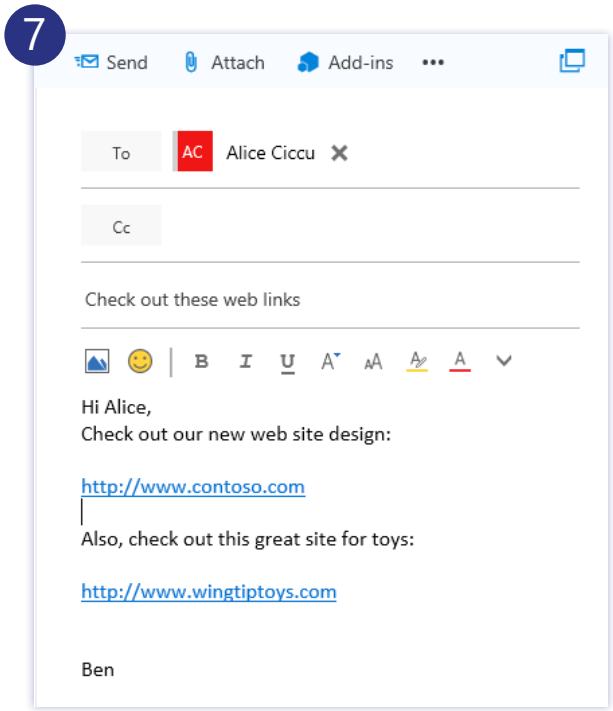
1. Open an InPrivate or Incognito browser session.

> You need to open an InPrivate browser session because you are going to be logging on to Office 365 Outlook Web access as one of the users you created earlier.

2. Browse to https://outlook.office365.com/owa.
3. When prompted, sign in as bens@[OrgName].onmicrosoft.com using Passw0rd! as the password.

> Ben Smith is a test user you created in an earlier step.

4. In the Outlook Web Access Inbox, click New.
5. In the To field, type Alice Ciccu.
6. In the Subject field, type Check out these Web links.
7. Type the message you find in the screenshot below.



> When you type in the Web addresses and press Enter at the end of the line, a website summary will appear (in this case, a summary of the Microsoft home page). Close the website summary.

8. When you have finished typing the message, click Send.

> You are going to use the links contained in this email to verify the functionality of the Managed Browser app.

9. Close the browser session.

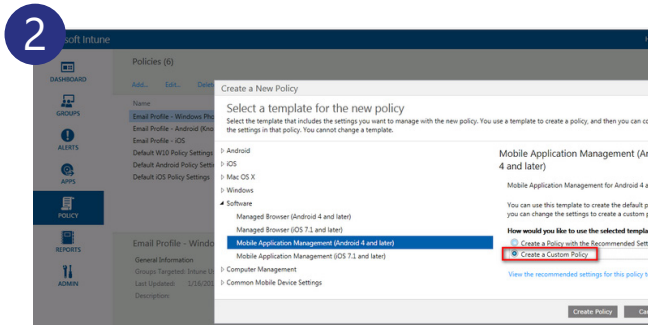
Create a Mobile Application Management (MAM) Policy

The mobile application management policy determines the restrictions that are placed on the managed apps you deploy to your Android or iOS devices. The policies are applied when the apps are initially deployed. They can also be applied after the apps have already been installed by the users. Some apps, such as Outlook for iOS and Android, support multiple identities: both a corporate account and a personal account can be used. In the case of multi-identity apps, corporate and personal data is kept separate. When the device is unenrolled or the app removed, the application's corporate data is removed, leaving the personal data behind and unaffected by the removal of corporate data.

In this task, you will configure mobile application management policies for Android and iOS devices.

- Please ensure you are signed into the Microsoft Intune administrative console at https://manage.microsoft.com to perform these steps.

1. In the Intune admin console, click POLICY, click Configuration Policies, and then click Add.
2. In the Create a New Policy dialog box, expand Software, select Mobile Application Management (Android 4 and later), select Create a Custom Policy, and then click Create Policy.

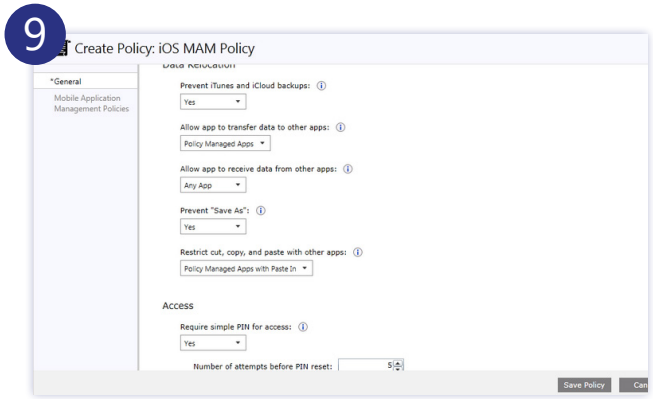


> You are selecting Create a Custom Policy so that you can view the default settings in the next task. Please note that this policy will not be deployed until it is associated with a published app.

3. On the General page, in Name, type Android MAM Policy.
4. Scroll down and review the default settings.

> At the bottom, note the setting to block screen captures when using the managed app. This setting is available for Android devices only; however, screen captures on iOS devices can be blocked using a device policy.

5. Click Save Policy.
6. On the Policies page, click Add.
7. In the Create a New Policy dialog box, expand Software, select Mobile Application Management (iOS 7.1 and later), select Create a Custom Policy, and then click Create Policy.
8. On the General page, in Name, type iOS MAM Policy.
9. Scroll down and review the default settings.
10. Click Save Policy.



Create a Managed Browser Application Policy

Using Intune mobile application policies, you can restrict managed apps from opening Web links in browsers other than the managed browser. If you put this restriction in place, then you must configure a managed browser application policy and deploy the managed browser app. In this task, you will create and configure managed browser policies for iOS and Android. In subsequent exercises, you will add the managed browser app to the software catalog, and then deploy it to your mobile devices.

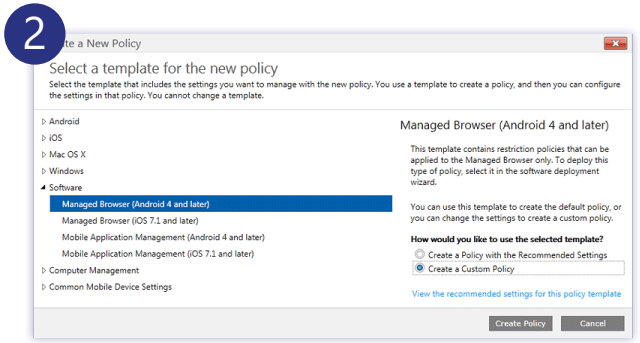
> Please ensure you are signed into the Microsoft Intune administrative console at https://manage.microsoft.com to perform these steps.

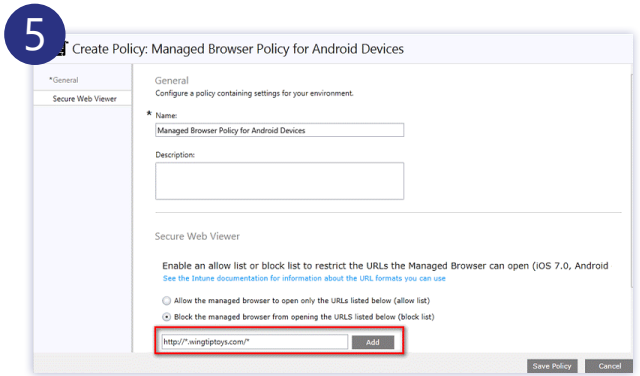
1. In the Intune admin console, click POLICY, click Configuration Policies, and then click Add.
2. In the Create a New Policy dialog box, expand Software, select Managed Browser (Android 4 and later), select Create a Custom Policy, and then click Create Policy.
3. On the Create Policy page, in Name, type Managed Browser Policy for Android Devices.
4. Ensure that Block the managed browser from opening the URLs listed below (block list) is selected.
5. In the URL field, type http://*.wingtiptoys.com/*, click Add, and then click Save Policy.

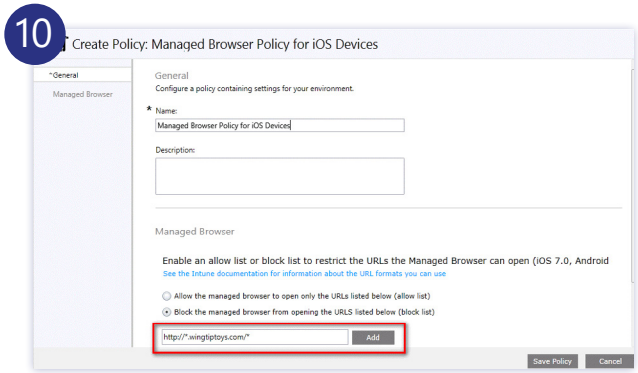
> Depending on your security model, you may wish to set an explicit allow list. This list would contain your intranet websites and other sites that you deemed trustworthy.

6. On the Polices page, click Add.
7. In the Create a New Policy dialog box, expand Software, select Managed Browser (iOS 7.1 and later), select Create a Custom Policy, and then click Create Policy.
8. On the Create Policy page, in Name, type Managed Browser Policy for iOS Devices.
9. Ensure that Block the managed browser from opening the URLs listed below (block list) is selected.
10. In the URL field, type http://*.wingtiptoys.com/*, click Add, and then click Save Policy.

> Please see https://technet.microsoft.com/en-ca/library/dn878029.aspx for more information on URL formats allowed by the managed browser policy.







Add Apps to the Intune Catalog

In this exercise, you will add a number of managed iOS and Android apps to the Intune app catalog. These apps are available in the Google Play Store and the iOS App Store. So, rather than adding the app itself to the catalog, you will add the links to the apps. Please note that not all apps can be used with mobile application management policies. For a current list of applications that can be used with mobile application management policies, please see https://technet.microsoft.com/library/dn708489.aspx.

> NOTE: If OneDrive is not installed on your target iOS or Android device, or if you did not perform these steps in Configure Mobile Application Management (MAM) without Enrolling Devices earlier in this guide, please upload OneDrive to the catalog along with the other applications you upload as part of this lab exercise. You can do this as a last step in the exercise.

> Please ensure you are signed into the Microsoft Intune administrative console at https://manage.microsoft.com to perform these steps.

1. In the Intune admin console, on the left navigation bar, click APPS.
2. Under Tasks, click Add Apps, and then in the Application Run - Security Warning dialog box, click Run.

> The Microsoft Intune Software Publisher application is installed on the local workstation.

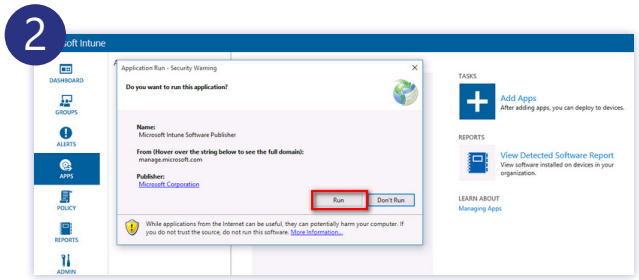
3. On the sign in page, sign in as admin@[OrgName].onmicrosoft.com.

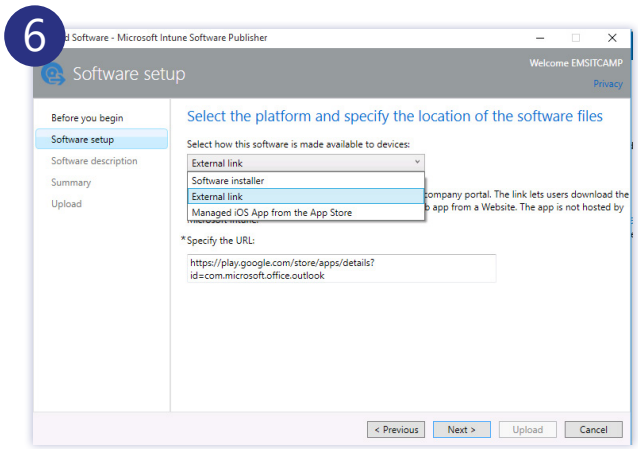
> The Before you begin page appears.

4. On the Before you begin page, click Next.
5. On the Select the platform and specify the location of the software files page, in the drop-down list, select External link.

> For Android apps, you select External link.

6. In Specify the URL, enter https://play.google.com/store/apps/details?id=com.microsoft.office.outlook, and then click Next.





7. On the Describe the software page, in Publisher, type Microsoft.
8. In Name, type Microsoft Outlook for Android.
9. In Description, type Microsoft Outlook for Android.
10. In Category, select Productivity, and then check Display this as a featured app, and highlight it in the company portal.
11. On the Describe the software page, click Next, review the summary information, and then click Upload.
12. When upload completes, click Close.
13. Under Apps, select Apps, and then on the Apps page, click Add App.
14. Using the URLs listed below, repeat steps 3–13 to add Microsoft Word and PowerPoint apps for Android devices from the Google Play store.

> Please note that if you did not do the previous lab, or if OneDrive is not installed on the iOS or Android device you will use for this lab, you should also upload the OneDrive app. You can find the link to the OneDrive app by searching the Google Play store.

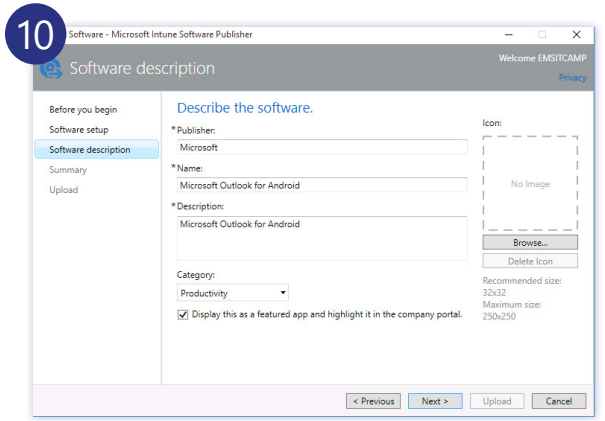
Microsoft Word:

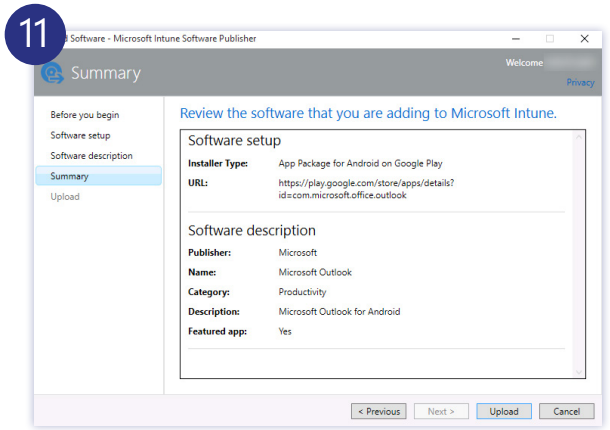
https://play.google.com/store/apps/details?id=com.microsoft.office.word

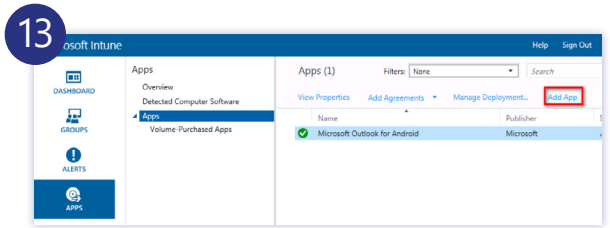
Microsoft PowerPoint:

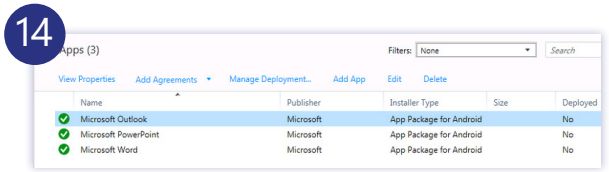
https://play.google.com/store/apps/details?id=com.microsoft.office.powerpoint

15. On the Apps page, click Add App.
16. On the Add Software - Sign in page, sign in as admin@[OrgName].onmicrosoft.com.
17. On the Before you begin page, click Next.
18. On the Select the platform and specify the location of the software files page, in the drop-down list, select Managed iOS App from the App Store.









19. In Specify the URL, enter https://itunes.apple.com/us/app/microsoft-outlook-email-calendar/id951937596?mt=8, and then click Next.

> Make sure you select Managed iOS App from the App Store.

20. In Publisher, type Microsoft.
21. In Name type Microsoft Outlook for iOS.
22. In Description, type Microsoft Outlook for iOS.
23. In Category, select Productivity.
24. Check Display this as a featured app, and highlight it in the company portal, and then click Next.
25. On the Specify the requirements that must be met on the target mobile devices before installation can start page, ensure that the Mobile device type is set to Any, and then click Next.
26. On the Summary page, click Upload, and then click Close.
27. Under Apps, select Apps. On the Apps page, click Add App.
28. Using the URLs listed below, repeat steps 15–26 to add Microsoft Word and PowerPoint apps for iOS devices from the Apple store.

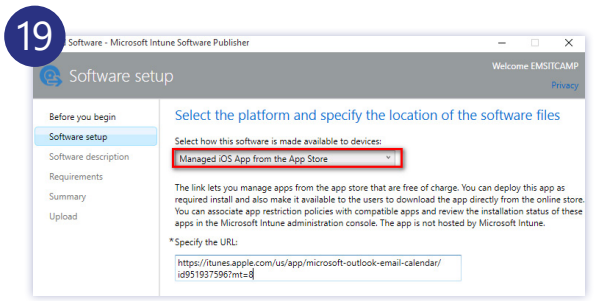
> Please note that if you did not do the previous lab, or if OneDrive is not installed on the iOS or Android device you will use for this lab, you should also upload the OneDrive app. You can find the link to the OneDrive app by searching the Apple store.

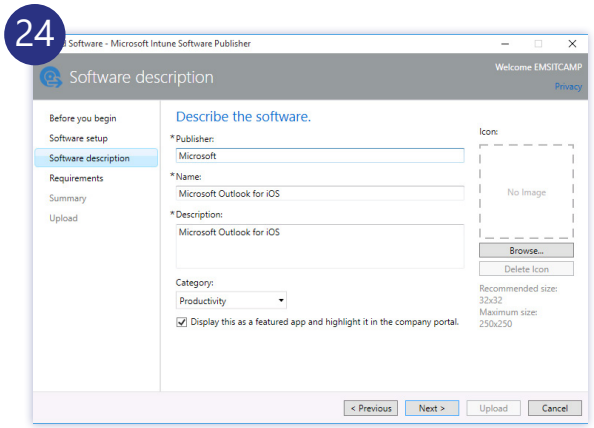
Microsoft Word:

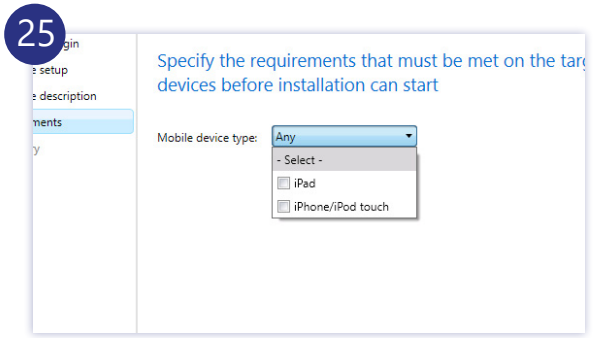
https://itunes.apple.com/us/app/microsoft-word/id586447913?mt=8

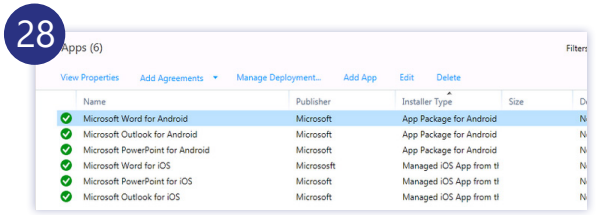
Microsoft PowerPoint:

https://itunes.apple.com/us/app/microsoft-powerpoint/id586449534?mt=8









Add Managed Browser App to Intune Catalog

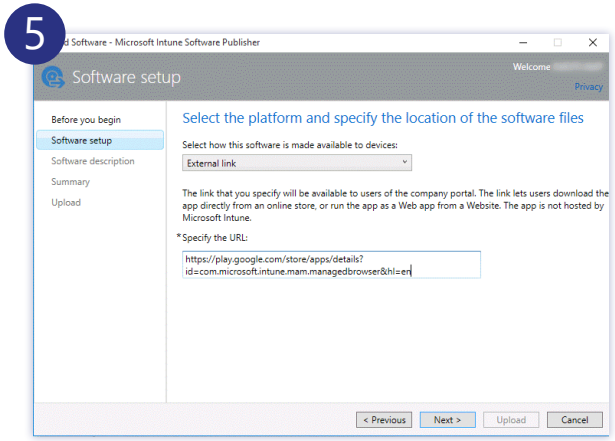
In this task, you will add a managed browser app for Android and iOS devices to the Intune app catalog. These apps are available in the Google Play Store and the iOS App Store. So, rather than adding the app itself to the catalog, you will add the links to the apps.

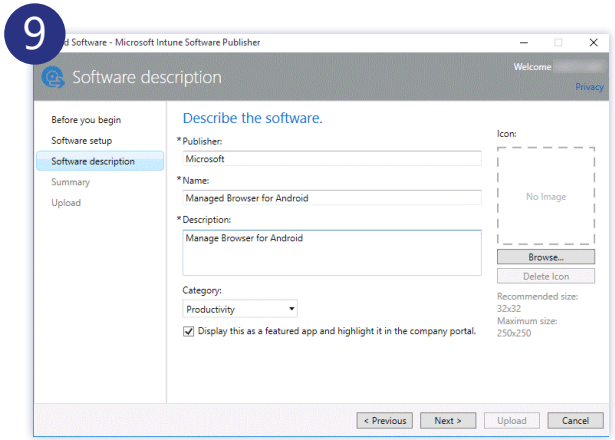
> Please ensure you are signed into the Microsoft Intune administrative console at https://manage.microsoft.com to perform these steps.

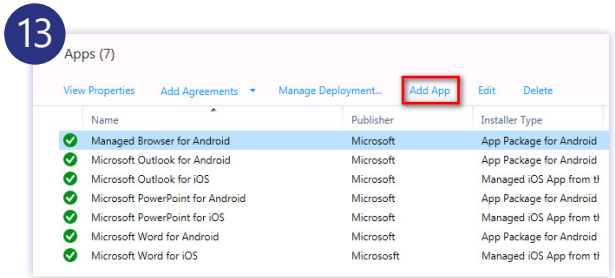
1. In the Intune admin console, on the left navigation bar, click APPS.
2. On the sign-in page, sign in as admin@[OrgName].onmicrosoft.com.

> When you have signed in, the Before you begin page appears.

3. On the Before you begin page, click Next.
4. On the Select the platform and specify the location of the software files page, in the drop-down list, select External link.
5. In Specify the URL, enter https://play.google.com/store/apps/details?id=com.microsoft.intune.mam.managedbrowser&hl=en, and then click Next.
6. On the Describe the software page, in Publisher, type Microsoft.
7. In Name, type Managed Browser for Android.
8. In Description, type Managed Browser for Android.
9. In Category, select Productivity, and then check Display this as a featured app, and highlight it in the company portal.
10. On the Describe the software page, click Next.
11. Review the summary information, and then click Upload.
12. When the upload completes, click Close
13. Under Apps, select Apps, and then on the Apps page, click Add App.

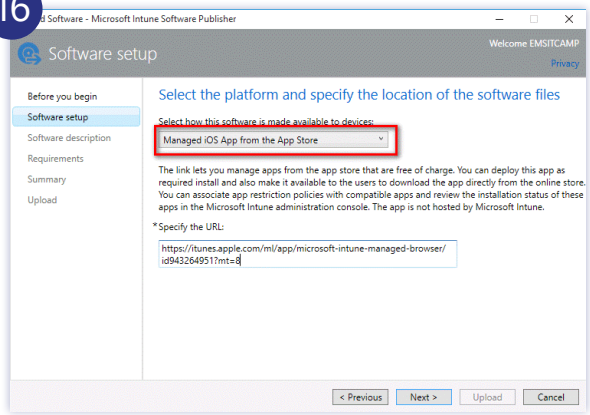




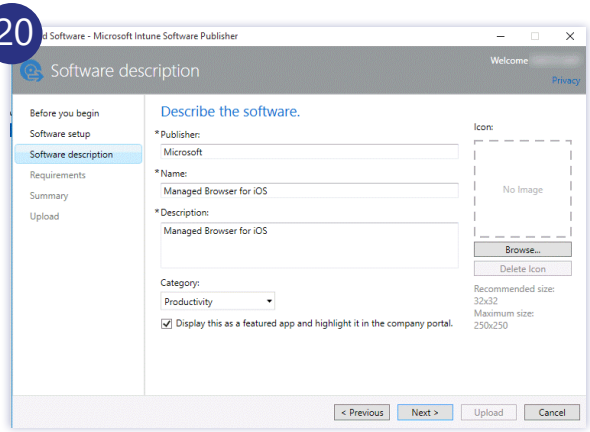


14. On the Add Software - Sign in page, sign in as admin@[OrgName].onmicrosoft.com, and then on the Before you begin page, click Next.
15. On the Select the platform and specify the location of the software files page, in the drop-down list, select Managed iOS App from the App Store.
16. In Specify the URL, enter https://itunes.apple.com/ml/app/microsoft-intune-managed-browser/id943264951?mt=8, and then click Next.
17. On the Describe the software page, in Publisher, type Microsoft.
18. In Name, type Managed Browser for iOS.
19. In Description, type Managed Browser for iOS.
20. In Category, select Productivity, and then check Display this as a featured app, and highlight it in the company portal.
21. On the Specify the requirements that must be met on the target mobile devices before installation can start page, ensure that the Mobile device type is set to Any, and then click Next.
22. On the Summary page, click Upload, and then click Close.

16



20



Deploy Apps With Mobile Application Policies

In this task, you will deploy Microsoft Outlook, Word, and PowerPoint, and then associate these applications with the mobile application management policies you created previously.

> Please ensure you are signed into the Microsoft Intune administrative console at https://manage.microsoft.com to perform these steps.

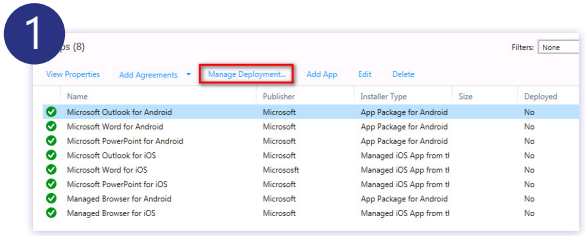
1. On the Apps page, select the instance of Microsoft Outlook for Android, and then select Manage Deployment.
2. In the Microsoft Outlook dialog box, on the Select Groups tab, select Intune Users, click Add, and then click Next.
3. On the Deployment Action tab, in Approval, select Available Install, and then click Next.

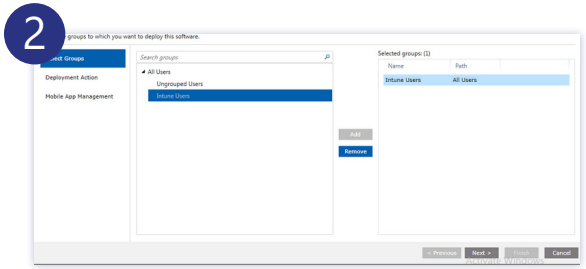
> The approval settings are:
>
> **Required:** mandatory install.
>
> **Available:** users can install from the company portal on demand.
>
> **Not applicable:** the app is not installed or shown in the company portal.
>
> **Uninstall:** the app will be uninstalled from targeted devices.

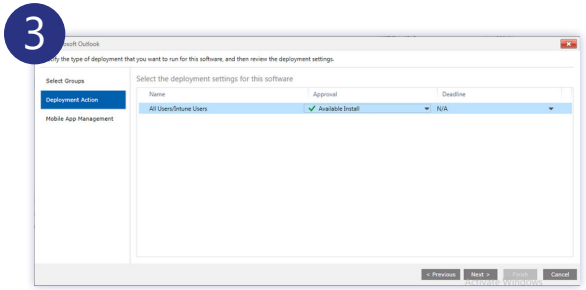
4. On the Mobile App Management tab, in the App Management Policy column, make sure Android MAM Policy is selected, and then click Finish.
5. Repeat steps 1–4 to deploy Microsoft Word and Microsoft PowerPoint for Android.

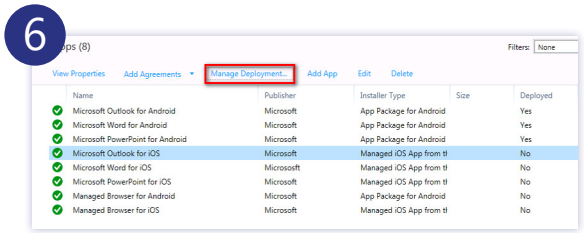
> Do NOT deploy the managed browser app. You will deploy the managed browser app in subsequent steps.

6. Select the Microsoft Outlook app for iOS, and then click Manage Deployment.









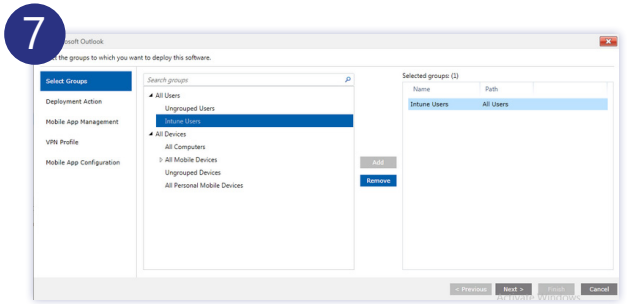
7. In the Microsoft Outlook dialog box, in the Select Groups tab, select Intune Users, click Add, and then click Next.

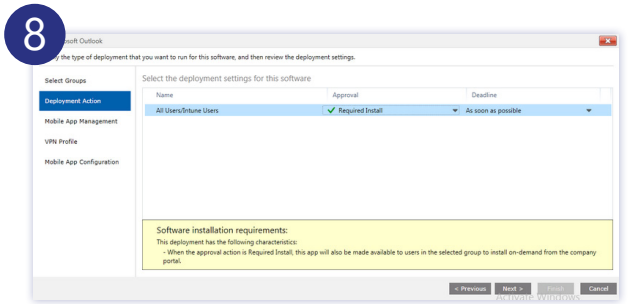
> Please note that with iOS devices, you also have the option of deploying apps to device groups.

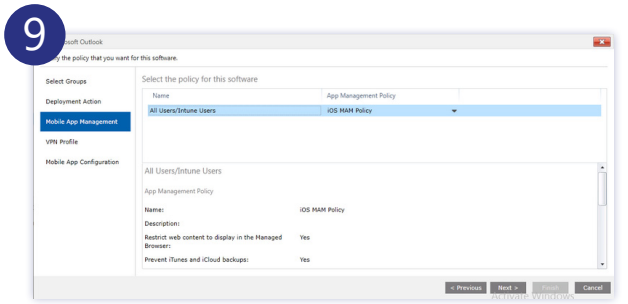
8. On the Deployment Action tab, in Approval, select Required Install, and then click Next.
9. On the Mobile App Management tab, in the App Management Policy column, make sure iOS MAM Policy is selected, and then click Next.
10. On the VPN Profile tab, click Next, and then on the Mobile App Configuration tab, click Finish.

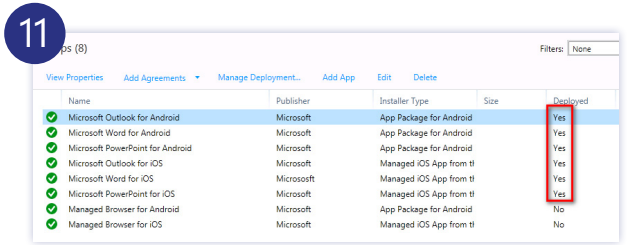
> VPN Profiles are used to deploy VPN settings to devices. For more information, please see https://technet.microsoft.com/en-ca/library/dn818905.aspx. Mobile configuration app policies are used to supply settings that may be required when the user runs an app, for example language and security settings. These settings can be deployed as well to reduce the risk of misconfiguration on the part of the user. For more information, please see https://technet.microsoft.com/en-us/library/mt481447.aspx.

11. Repeat steps 6–10 to deploy the remaining iOS apps.







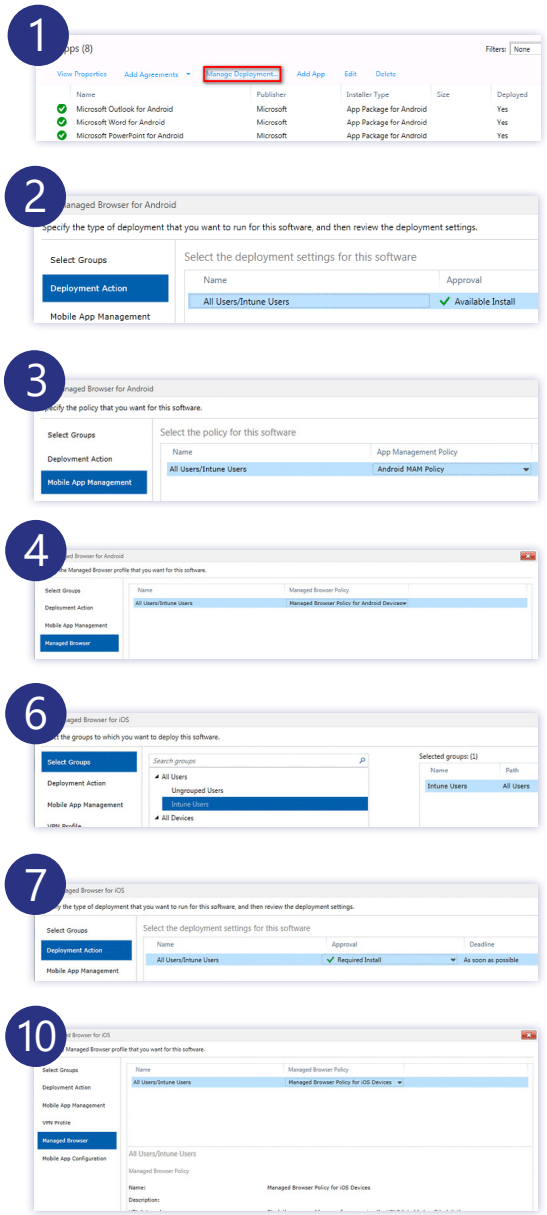


Deploy the Managed Browser App

In this exercise, you will deploy the managed browser, and then associate it with the policies you created earlier.

> Please ensure you are signed into the Microsoft Intune administrative console at https://manage.microsoft.com to perform these steps.

1. On the Apps page, select Managed Browser for Android, and then select Manage Deployment.
2. In the Managed Browser for Android dialog box, in the Select Groups tab, select Intune Users, click Add, and then click Next.
3. On the Mobile App Management tab, in the App Management Policy column, make sure Android MAM Policy is selected, and then click Next.
4. On the Managed Browser tab, in the Managed Browser Policy column, select Managed Browser Policy for Android Devices, and then click Finish.
5. On the Apps page, select Managed Browser for iOS, and then click Manage Deployment.
6. In the Managed Browser for iOS dialog box, in the Select Groups tab, select Intune Users, click Add, and then click Next.
7. On the Select the deployment settings for this software page, in the Approval column, select Required Install, and then click Next.
8. On the Select the policy for this software page, in the App Management Policy column, ensure that iOS MAM Policy is selected, and then click Next.
9. On the Specify the type of VPN that you want for this software, accept the default setting (None), and then click Next.
10. On the Specify the Managed Browser profile that you want for this software, in the Managed Browser Policy column, select Managed Browser Policy for iOS Devices, and then click Next.
11. On the Mobile App Configuration tab, click Finish.



Install Managed Apps on an Android Device

In this task, you will install Microsoft Outlook, Word, PowerPoint, and the Managed Browser on your Android device. You will then perform some simple tests to verify that the mobile application management policies you deployed with the application work as expected.

Perform these steps on your Android device.

1. Sign in to your Android device.
2. Press Home, tap Apps, and then tap Play Store.
3. In the Play Store search field, tap Intune Company Portal.

The Company Portal should not be installed on your Android device at this point.

4. On the Intune Company Portal page, tap Install, and then when the app finishes installing, tap Open.
5. Tap Sign in, and then when prompted for your sign-in email address, enter alicec@[OrgName].onmicrosoft.com.
6. When prompted for your password, enter Passw0rd!. When prompted, tap ENROLL, and then tap ACTIVATE.

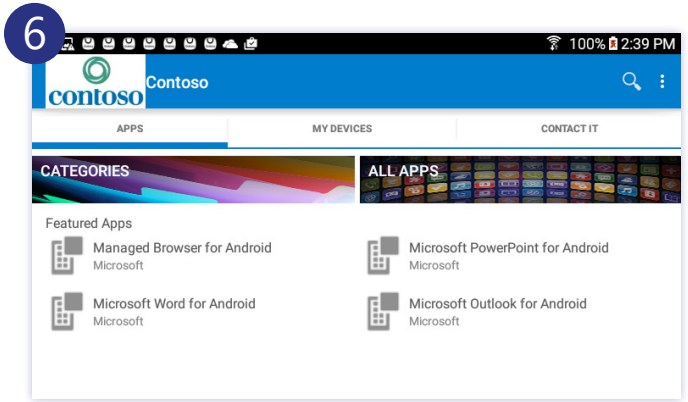
On devices running KNOX 4.0 or higher, you will see an ELM Agent page. Check I have read and agree to all the terms and conditions above, and then tap CONFIRM.

When you complete the enrollment of the Android device, you should see the 4 apps you deployed in the Company Portal.

7. In the Company Portal, tap Managed Browser for Android. Tap VIEW IN GOOGLE PLAY.

Recall that when you deployed the app, you deployed a link to the Google Play Store, not the actual app files themselves.

8. On the Microsoft Intune Managed Browser page, tap INSTALL, and then tap ACCEPT.
9. Return to the Company Portal app.



10. Tap Microsoft Outlook, and then tap VIEW IN GOOGLE PLAY.
11. On the Microsoft Outlook page, tap INSTALL, and then tap ACCEPT.
12. On the Microsoft Outlook page, tap OPEN, and then tap Get Started.
13. When presented with a tutorial on features in Outlook, tap SKIP (lower-left corner). On the Add Account page, tap Office 365.
14. When prompted, sign in to the company portal as Alicec@[OrgName].onmicrosoft.com, using Passw0rd! as the password.
15. When prompted, enter your PIN.

- You configured this PIN previously. If you did not do the previous lab, you will be prompted to create and confirm a PIN.
- Your Inbox opens, displaying the test messages you sent earlier.

16. In the inbox, open the test email message you sent at the beginning of this exercise that has the subject, "Check out these Web links."

- Because Outlook is a managed app, it is not possible to provide a screenshot of the open app on an Android device. This is the result of the default security settings for Android devices managed by Intune.

17. In the email, tap the link to http://www.contoso.com.

- The Managed Browser should open, showing the Microsoft.com home page.

18. Switch to the Outlook app.
19. In the email, tap the link to http://www.tailspintoys.com.

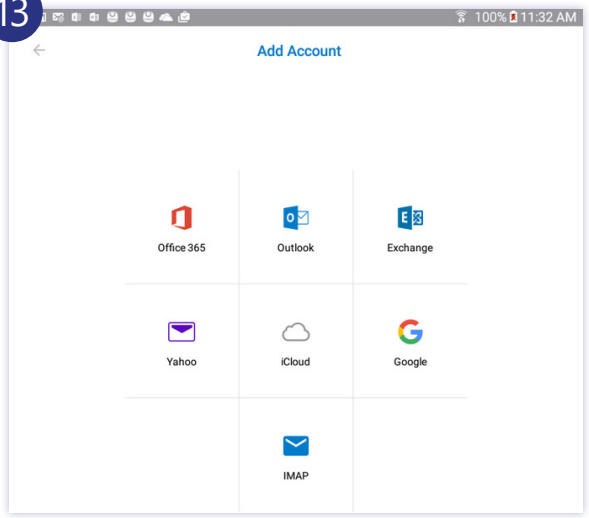
- The Managed Browser should open, denying you access to the website.

20. Tap Home, tap Apps, and then tap OneDrive.

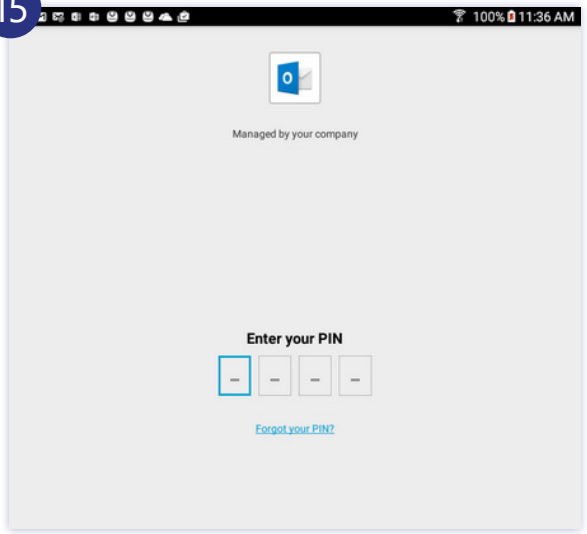
- If prompted, sign in, and then enter your PIN.
- If you did not do the previous lab, you have to deploy OneDrive as a managed app, and then install it on your Android device; however, please note that if you did configure OneDrive as a managed app without enrollment in the previous lab, it coexists and integrates with the managed apps you configured in this lab.

21. In OneDrive, select the sample PDF file you uploaded earlier.

13



15



22. In the upper-right corner, tap Share, and then tap Send files.
23. In Share, tap Outlook.

> Note that the only two applications you can share with are managed applications, Outlook, and OneDrive.

24. In the To field, enter Ben Smith, in Subject, type Portfolio, and then in the message body, type Here is the material you requested.
25. In the upper-right corner, tap Send.
26. Depending on your device, Word and PowerPoint may already be downloaded and installed by the manufacturer but not configured. If this is the case, open Word and PowerPoint, and then sign in as alicec@[OrgName].onmicrosoft.com using Passw0rd! as the password. Otherwise, install Word and PowerPoint using the Company Portal.

> When you open Word or PowerPoint for the first time, you may be prompted for your PIN. Likewise, if you have closed the applications for a certain amount of time, you may be prompted for your PIN again.

27. From the OneDrive, Word, or PowerPoint apps, open various documents to demonstrate that your managed applications are working as intended.

> If you intend to use your Android device for later steps in this guide to test multi-factor authentication, do NOT wipe or retire your device at this time. The steps related to the multi-factor authentication assume that you are using an enrolled device that has Outlook installed as a managed application.

Install Managed Apps on an iOS Device

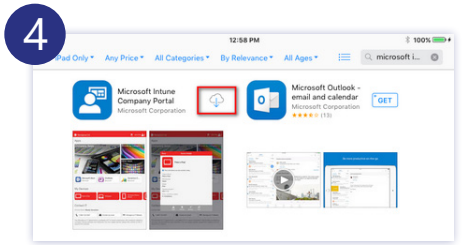
In this task, you will install the Company Portal on your iOS device and then enroll the device. You will then follow the on-screen instructions on your iOS device to install Microsoft Outlook, Word, PowerPoint, and the Managed Browser. You will then perform some simple tests to verify that the mobile application management policies you deployed with the application work as expected.

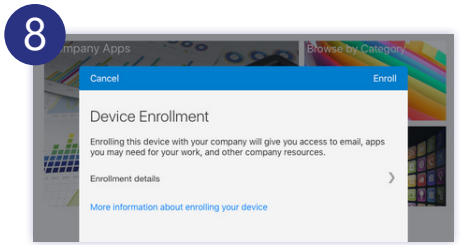
Perform these steps on your Android device.

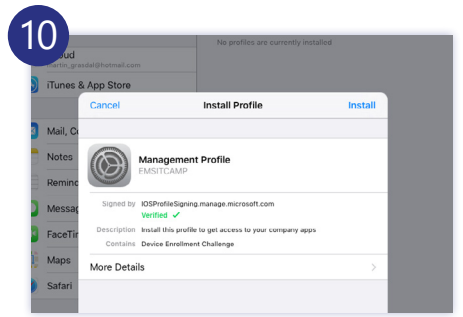
1. Sign in to your iOS device.
2. On the iOS device, tap App Store
3. In the search box, type Microsoft Intune Company Portal.
4. In the results, beside Microsoft Intune Company Portal, tap download (cloud icon with down arrow).
5. Wait for the app to finish installing.
6. In the App Store, beside Microsoft Intune Company Portal, tap Open.
7. On the sign-in page, sign in as alicec@[OrgName].onmicrosoft.com using Passw0rd! as the password.
8. In the Device Enrollment notice, tap Enroll.
9. In the Install Profile notice, tap Install.
10. When prompted, enter your passcode, tap Done, and then tap Install.
11. In the warning notice, tap Install, and then tap Trust.
12. In the Profile Installed page, tap Done.

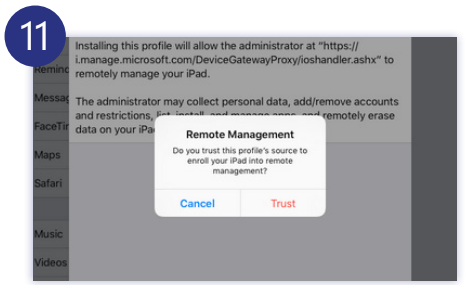
Pause on this screen and wait for notices to appear that indicate which software is about to be installed. In the Profile Installed notice, tap Done.

13. When prompted to open the page in the Comp Portal, tap Open.









14. When notified that the device is enrolled, tap OK.

- Depending on how quickly your device responds, you may be prompted to install the required apps before you complete this step.

15. When prompted by the notice to install the Managed Browser, tap Install.

- Recall that in a previous task, you configured the managed browser and other applications as required (mandatory) applications.
- If prompted, sign in to the iTunes store with your Apple ID.

16. You will receive notices that Outlook, Word, and PowerPoint need to be installed. Follow the prompts to install these apps.

- For Outlook and each subsequent application you are prompted to install, wait until the previous application is finished installing.

17. Press Home, and then wait until the Managed Browser, Outlook, Word, and PowerPoint finish installing.

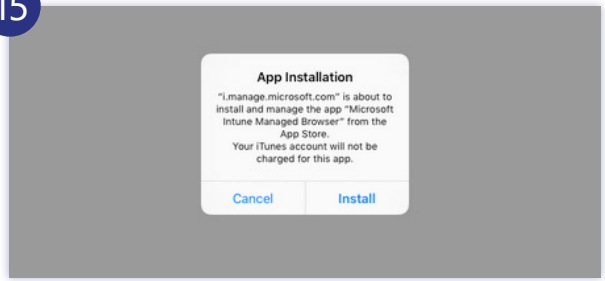
- None of the icons should be greyed out. Please see the screenshot below.
- Wait until you have installed all the apps before proceeding.

18. Tap Home, and then tap Outlook.
19. On the Outlook page, tap Get Started.
20. Scroll through the introductory tutorial, and then at the end of the tutorial, tap Add an Account.
21. On the Add an Account page, tap Office 365.

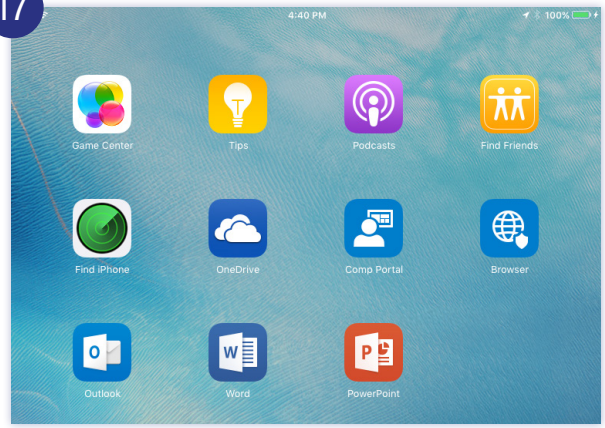
- The Office 365 sign-in page appears.

22. Sign in as alicec@[OrgName].onmicrosoft.com using Passw0rd! as the password.

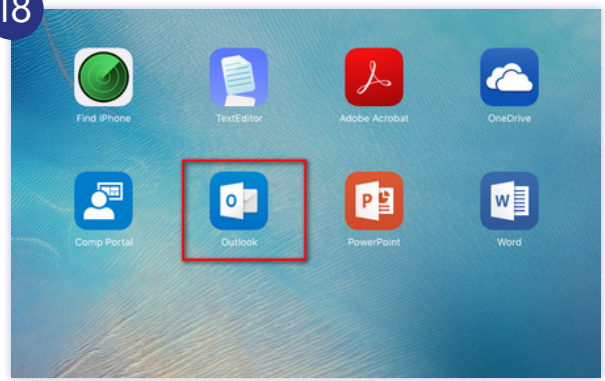
15



17



18



23. When prompted, enter and confirm a 4-digit PIN.

> 📌 You configured this PIN previously. If you did not do the previous lab, you will be prompted to create and confirm a PIN.

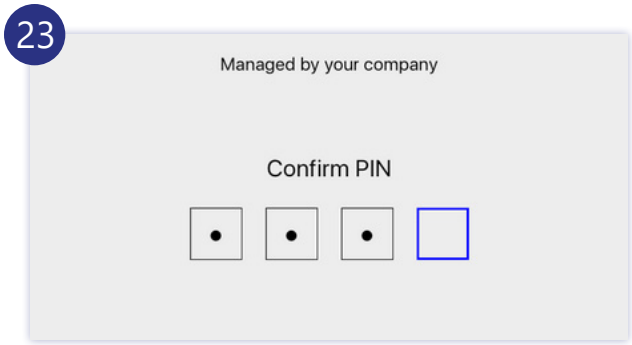
24. In the inbox, open the test email message you sent at the beginning of this exercise that has the subject, "Check out these Web links."
25. In the message, tap www.contoso.com, and then when prompted, tap Open.

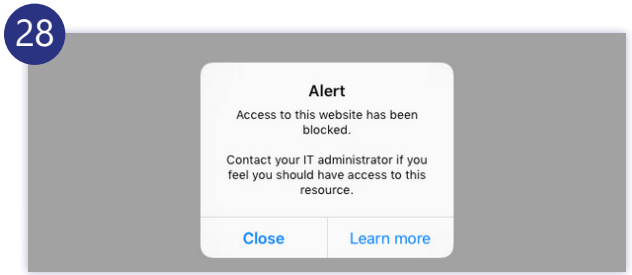
> 📌 The managed browser opens, and then the Web page for Contoso.com opens.

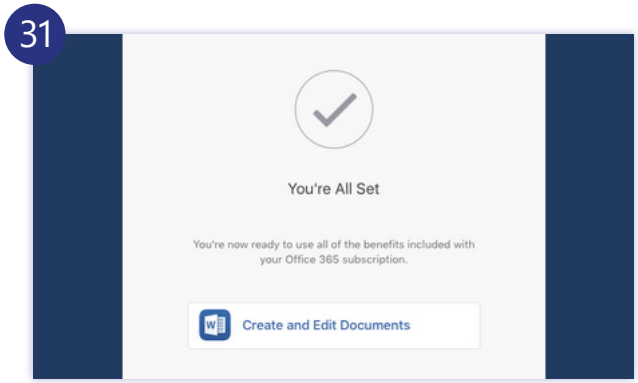
26. In the managed browser, tap Back to Outlook.
27. In the message, tap the link www.wingtiptoys.com.
28. When prompted by the alert, click Close.

> 📌 The managed browser opens. The Web page for wingtiptoys.com is blocked as per your policy configuration.

29. Press Home, and then tap Word. Word opens with an introductory tutorial screen.
30. Swipe to the end of the tutorial, and then sign in as Alicec@[OrgName].onmicrosoft.com using Passw0rd! as the password.
31. On the You're all Set page, tap Create and Edit Documents.
32. Configure PowerPoint, following similar steps to the ones you used to configure Word.







33. Open OneDrive, and then follow the prompts to reconfigure OneDrive or acknowledge that data in OneDrive is protected.
34. In OneDrive, tap one of the sample Word documents you uploaded previously, and then open it in Word.

📌 When the document opens in Word, you are informed that the document is protected.

35. Tap the Share icon in the upper-right corner, and then click Send Attachment.
36. In Send Attachment, tap Document, and then tap Send with Outlook.
37. In the message that is opened automatically, specify Ben Smith as the recipient, give the message a subject and message body, and then tap Send.

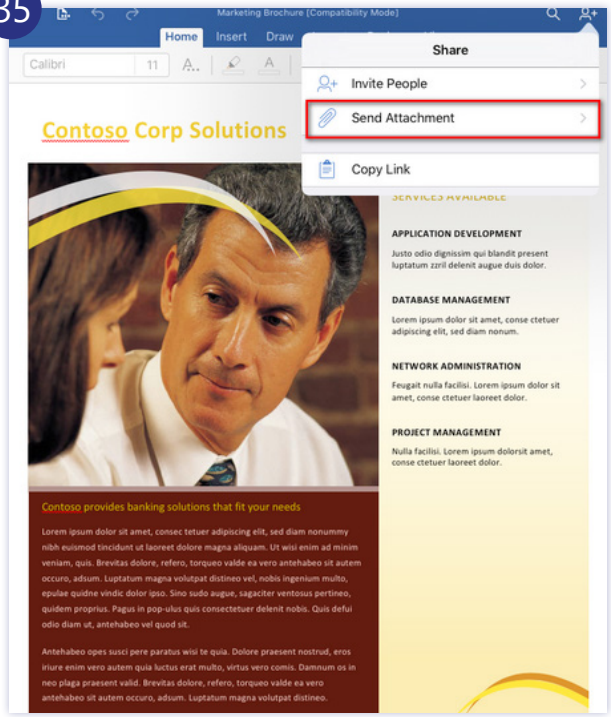
📌 Attaching the document demonstrates that both Word and Outlook are managed applications. If they were not managed applications, it would not be possible to send the document as an attachment.

38. Spend a few moments testing the security of managed apps. For example, try to open documents in other applications, and then try to copy and paste between different applications.

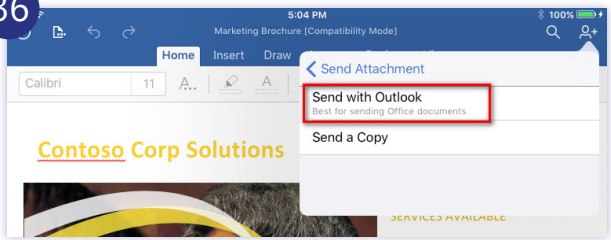
📌 TIP: You can open additional documents to your test user's OneDrive. To do so, open a Web browser using InPrivate or Incognito mode, navigate to http://1drv.com, and sign in as alicec@[OrgName].onmicrosoft.com. For example, you might want to create a Word document that contains links to http://www.contoso.com and http://www.wingtiptoys.com.

❗ If you intend to use your Android device for later steps in this guide to test multi-factor authentication, do NOT wipe or retire your device at this time. The steps related to the multi-factor authentication assume that you are using an enrolled device that has Outlook installed as a managed application.

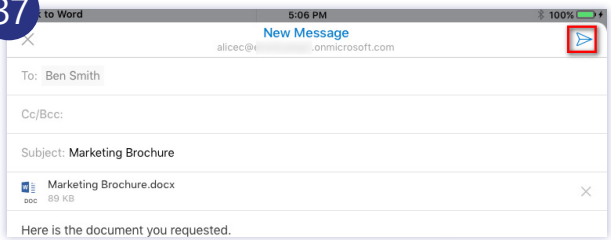
35



36



37



Part Eight:
Deploy MSI Applications to Windows 10 Devices Using Intune

Part Eight:

Deploy MSI Applications to Windows 10 Devices Using Intune

Among the benefits of using Microsoft Intune is the ability to deploy applications to managed devices, such as PCs, phones, and tablets. Until recently, it was possible to deploy only .xap., .appx, and .appxbundle file types to managed mobile devices, including Windows 10 devices that were enrolled in mobile device management. It is now possible to deploy Windows Installer (*.msi) file types to Windows 10 devices that are enrolled in and managed by Intune.

In this lab, you will learn how to upload an .msi file to the Intune catalog and deploy it to a targeted Intune group. You will enroll a Windows 10 device and verify that the .msi file is installed on the managed Windows 10 device.

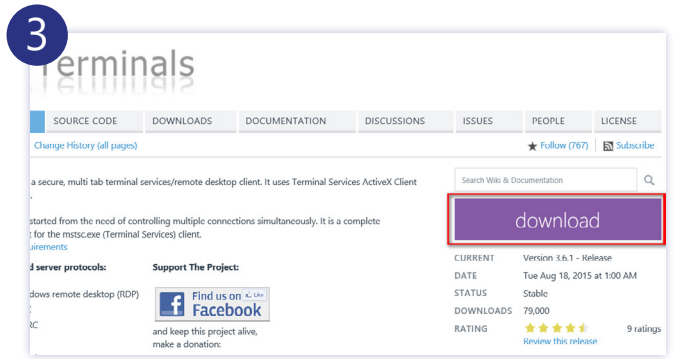
NOTE: In order to perform all the steps in this section, you must have access to a Windows 10 computer, either physical or virtual. The computer should not be joined to a domain.

Download Sample MSI Application

In this task, you will download a small, sample MSI application that you will use to demonstrate the deployment of MSI applications.

Please perform these steps using a browser.

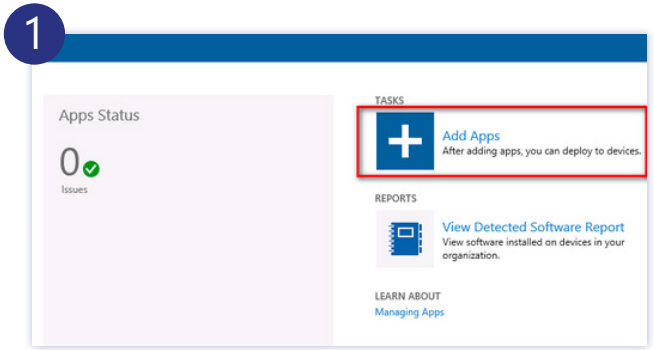
1. Open an InPrivate or Incognito browser session.
2. Navigate to https://terminals.codeplex.com/.
3. Click download.
4. When prompted to run or save TerminalsSetup_3.6.1.msi, save the file in a convenient location.



Publish and Deploy Sample MSI Application

Until recently, you were able to deploy only .appx, .xap, and .appxbundle file types to mobile devices using Microsoft Intune. It is now possible to publish and deploy MSI (Windows Installer) applications to mobile devices, such as Windows 8.1 and Windows 10 devices that are enrolled and managed as mobile devices.

In this section, you will publish a simple MSI application in the Intune catalog. Although the lab uses a single, small application as a demonstration, the same capabilities of Intune can be used to publish larger and more complex applications, such as Office Pro Plus.



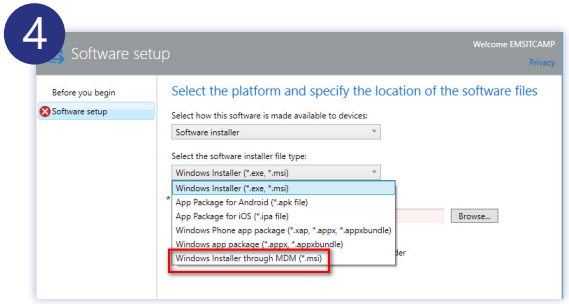
> Please ensure you are signed into the Microsoft Intune administrative console at https://manage.microsoft.com to perform these steps.

1. In the left navigation bar, click APPS, and then under Tasks, click Add Apps.
2. In the Application Run - Security Warning dialog box, click Run.

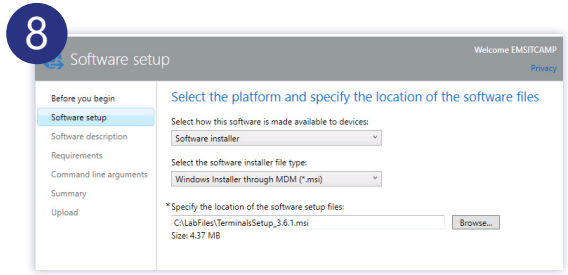
> If you have installed the Microsoft Intune Software Publisher in an earlier step, you will not have to perform this step.

3. On the Add Software page, sign in to Intune as admin@[OrgName].onmicrosoft.com.

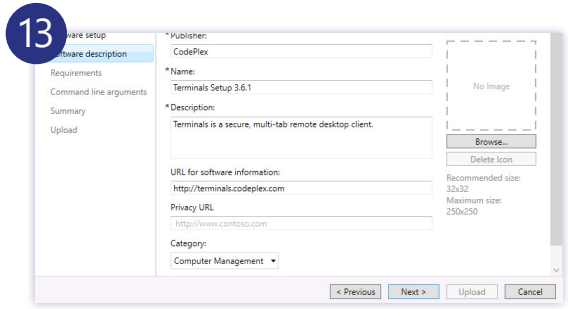
4. On the Select the platform and specify the location of the software files page, in the select the software installer file type drop-down list, select Windows Installer through MDM (*.msi).



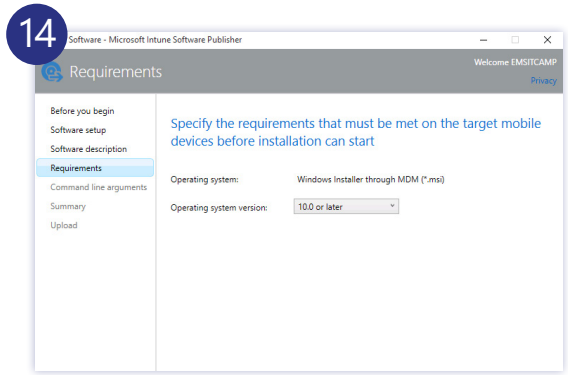
> Windows Installer through MDM (*.msi) is the latest addition to this list. There are some rules and limitations you should consider when using Windows Installer through MDM:
>
> - You can only upload a single file with the extension .msi.
> - The file's product code and product version are used for app detection.
> - The default restart behavior of the app will be used. Intune does not control this.
> - Per-user MSI packages will be installed for a single user.
> - Per-machine MSI packages will be installed for all users on the device.
> - Dual-mode MSI packages currently only install for all users on the device.
> - App updates are supported when the MSI product code of each version is the same.



5. In the Specify the location of the software setup files, click Browse.
6. In the Open dialog box, navigate to the folder where you saved the TerminalsSetup_3.6.1.msi file.
7. Select TerminalsSetup_3.6.1.msi, and then click Open.
8. Check Display this as a featured app and highlight it in the company portal, and then click Next.



9. On the Software description page, in Publisher, type CodePlex.
10. In Name, type Terminals Setup 3.6.1.
11. In Description, type Terminals is a secure, multi-tab remote desktop client.
12. In URL for software information, type http://terminals.codeplex.com.
13. In Category, select Computer Management, and then click Next.

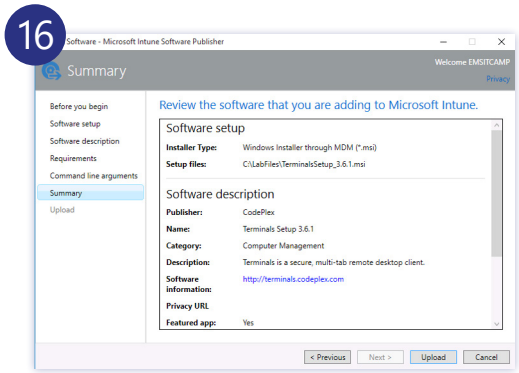


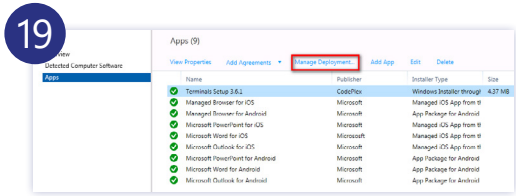
14. On the Specify the requirement that must be met page, accept the default setting, and then click Next.

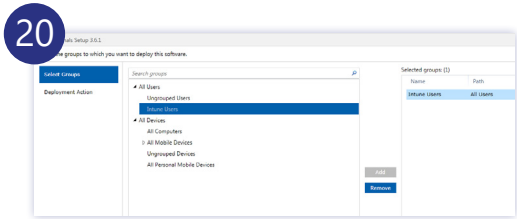
15. On the Command line arguments page, click Next.
16. On the Summary page, review the settings, and then click Upload.
17. When the upload is complete, click Close.
18. Select Apps.
19. On the Apps page, select Terminals Setup 3.6.1, and then click Manage Deployment.

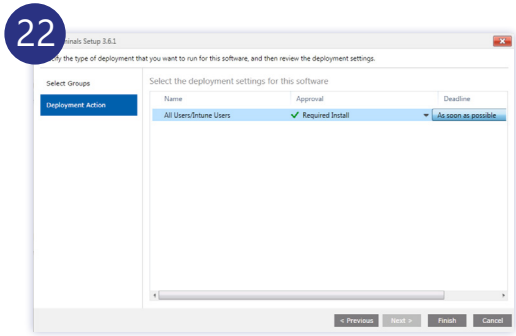
> Note that for this application, you are not required to have a mobile application management (MAM) policy.

20. On the Select Groups tab, click Intune Users, click Add, and then click Next.
21. On the Deployment Action tab, under Approval, select Require Install.
22. Under Deadline, select As soon as possible, and then click Finish.





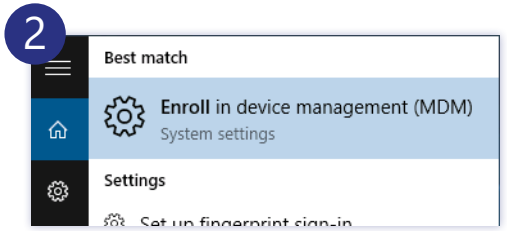




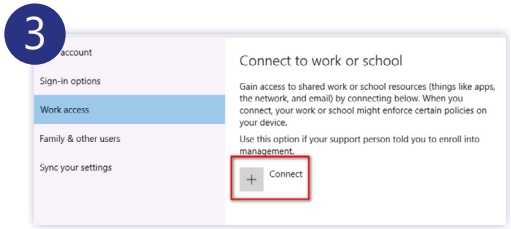
Enroll a Windows 10 Device and Install Software

In this exercise, you will enroll (workplace join) a Windows 10 device so that it can be managed by Windows Intune. You will then verify that the MSI software deployment installs on the device.

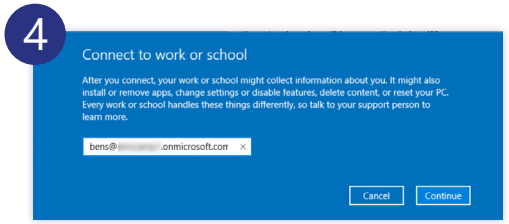
Perform this task on a Windows 10 device that is not domain or workplace-joined.



1. On the Windows 10 computer, in Search, type enroll.
2. In the search results, click Enroll in device management (MDM).

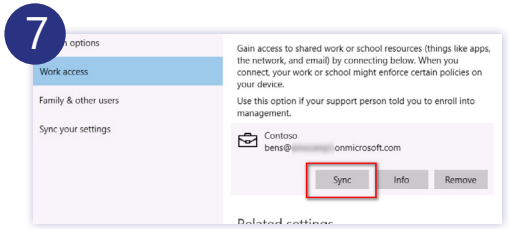


3. On the Connect to work or school page, click Connect.

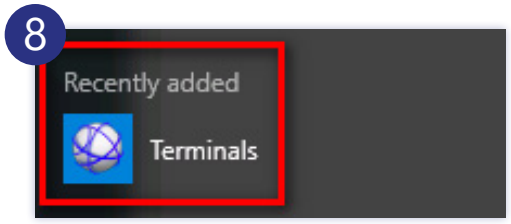


4. When prompted for an email address, type bens@[OrgName].onmicrosoft.com, and then click Continue.

5. On the sign-in page, type Passw0rd! for the password, and then click Sign In.
6. When the sign-in process completes, click Done.



7. On the Connect to work or school account page, click the account used for the workplace join, and then click Sync.



8. After a minute or two, click Start.
9. Open the Terminals application to verify that it has been installed correctly.

Unenroll a Windows 10 Device

In this exercise, you will unenroll the Windows 10 device to prepare it for later steps.

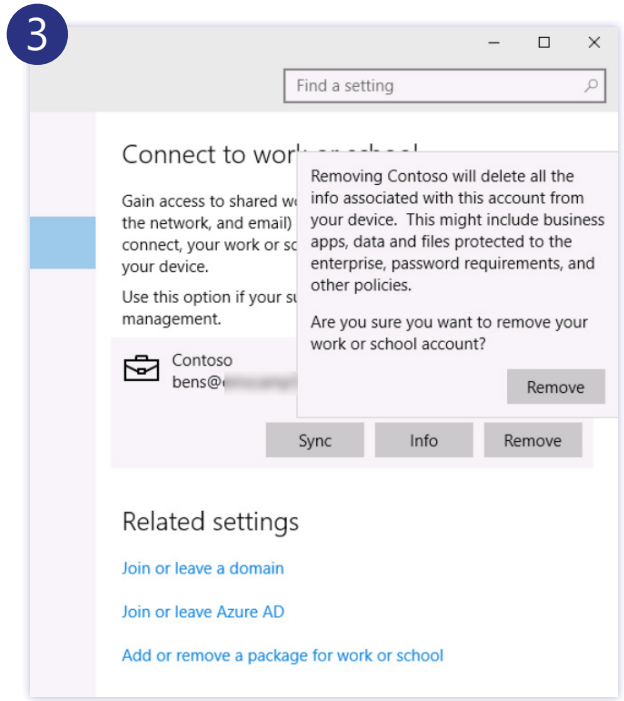
> Perform this task on a Windows 10 device that is not domain or workplace joined.

1. On the Windows 10 computer, in Search, type enroll.
2. In the search results, click Enroll in device management (MDM).
3. Click the account used for the workplace join, click Remove, and then click Remove again.

> Previously, you used the Intune admin console to retire devices. Here, you remove the device from mobile device management as the user.

4. In Search, type terminals.

> Note that the terminals application is no longer present on the system. The application was uninstalled when the computer was removed from management.



Part Nine:
Configure Multi-Factor Authentication for Mobile Device Management

Part Nine:

Configure Multi-Factor Authentication for Mobile Device Management

Azure Multi-Factor Authentication provides additional security for access to corporate resources by requiring a second factor of authentication in addition to a username and password combination. Multi-Factor Authentication requires two or more of the following authentication methods:

- Something you know (password)
- Something you possess and that is associated with you (phone or other trusted device)
- Something you are (biometrics)

By implementing two or more authentication factors, you can provide greater assurance of the identity of the person who is attempting to get authorization to access corporate resources.

In this section, you will learn how to configure Multi-Factor Authentication using text message and mobile app verification to provide the second level of authentication. You will learn how to enable Intune Multi-Factor Authentication for Windows device enrollment. You will learn how to enable Azure Multi-Factor Authentication for users. You will also learn what the user experience is like after users have been enabled for Multi-Factor Authentication and have registered for Multi-Factor Authentication. Finally, you will see how managed applications can coexist with Multi-Factor Authentication and how to bypass Multi-Factor Authentication when devices are on trusted networks.

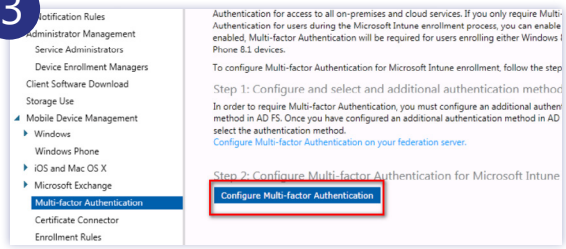
Configure Multi-Factor Authentication for Windows Phone and Device Enrollment

Microsoft Intune provides a limited version of Multi-Factor Authentication for Windows Phone 8.1 (and higher) and Windows 8.1 (and higher) device enrollment. When this version of Multi-Factor Authentication is enabled, it is used only for device enrollment. After the device is enrolled, no additional authentication methods are used when the user requires access to corporate resources. In this lab exercise, you will enable Microsoft Intune Multi-Factor Authentication. You will then enroll a Windows 10 device to observe the end-user process.

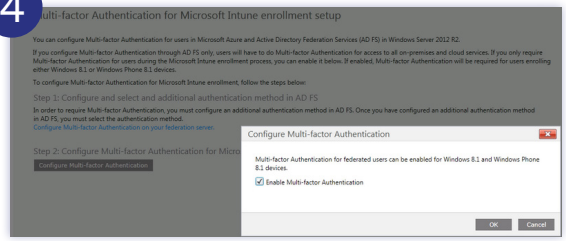
> Please ensure you are signed into the Microsoft Intune administrative console at https://manage.microsoft.com to perform these steps.

1. In the Intune admin console, in the left navigation bar, click ADMIN.
2. Under Administration, click Multi-Factor Authentication.
3. On the Multi-Factor Authentication for Microsoft Intune enrollment setup page, click Configure Multi-Factor Authentication.
4. In the Configure Multi-Factor Authentication dialog box, check Enable Multi-Factor Authentication, and then click OK.
5. If necessary, switch to the Windows 10 device that you will use to test enrollment in Intune.
6. In the Windows 10 device, in Search, type enroll, and then click Enroll in device management (MDM).
7. On the Connect to work or school page, click Connect.
8. When prompted for an email address, type bens@[OrgName].onmicrosoft.com, and then click Continue.

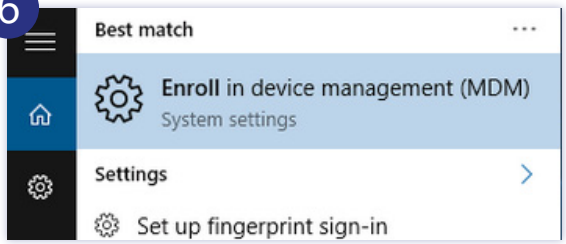
3



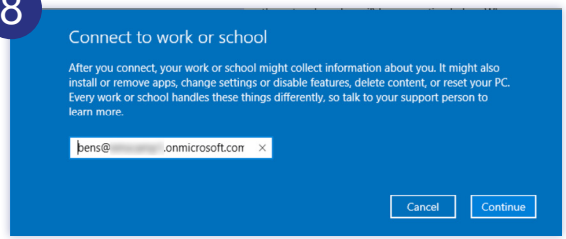
4



6



8



9. On the sign-in page, type Passw0rd! for the password, and then click Sign In.
10. When the sign-in process completes, click Done.

📌 Upon signing in, you will be prompted to set up additional security verification. You are prompted for additional security verification because of the change you made in an earlier step to require Multi-Factor Authentication for enrollment of Windows 8.1 (and higher) phones and devices.

11. On the Microsoft Intune page, click Set it up now.
12. On the Additional security verification page, select Authentication phone.

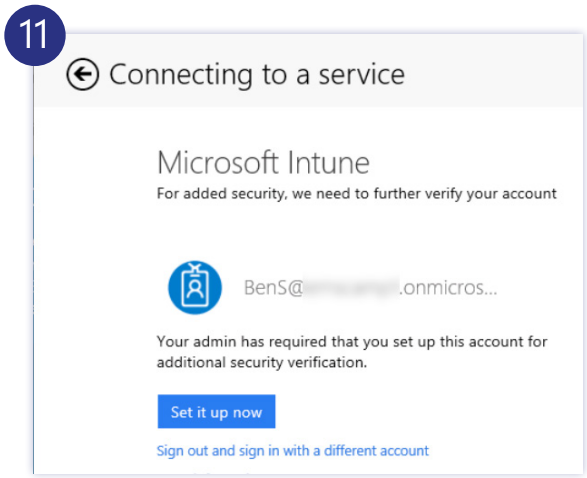
📌 Note that you can also select Office phone and Mobile as choices for the second factor of authentication. In later steps, you will install and configure a mobile app as the second factor of authentication.

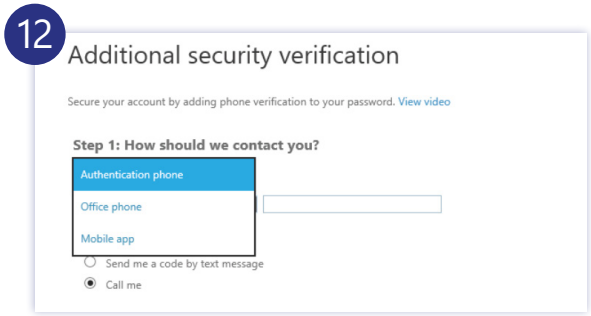
13. Select your country, enter your cell phone number, select Send me a code by text message, and then click Contact me.

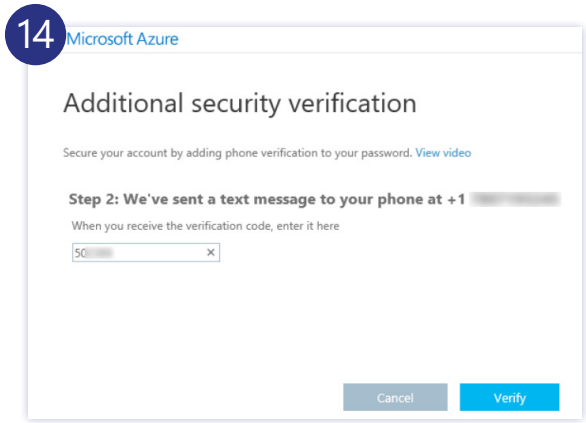
📌 Wait to receive the text message containing the verification code before proceeding.

14. On the Additional security verification page, enter the code, click Verify, and then click Done.

📌 Once you enter the verification code, the enrollment process can complete.

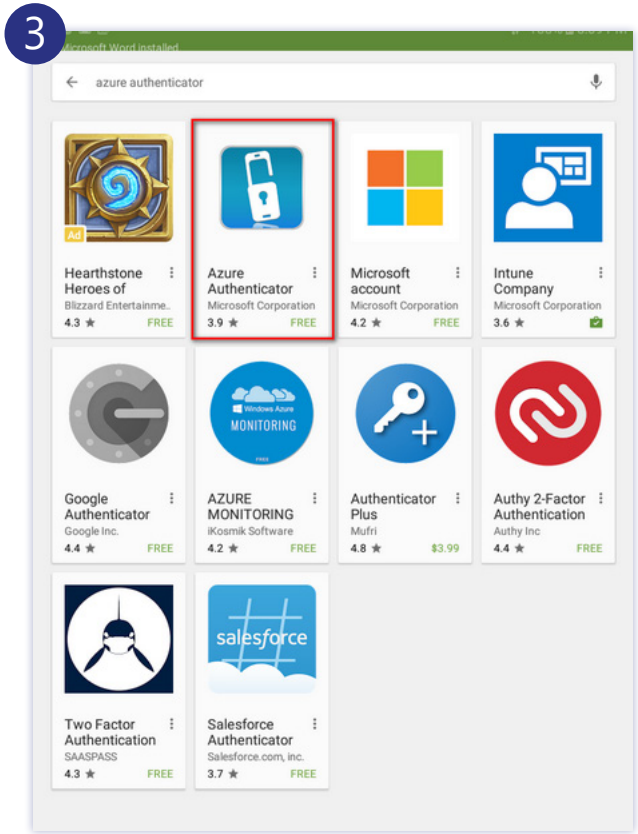






Install the Azure Authenticator App on an Android Device

For Multi-Factor Authentication, you will use a device to provide the second factor of authentication. This device, as you learned in the previous exercise, could be a smartphone that can receive text and voice messages. Alternatively, and to provide greater convenience, you can use an Azure Authenticator app that you install on your Windows, Android, or iOS device. In this exercise, you will install the Azure Authenticator app on your Android device.



Perform these steps on your Android device.

1. Sign in to your Android device.
2. Press Home, tap Apps, and then tap Play Store.
3. In the search field, enter Azure Authenticator.
4. In the Play Store, tap Azure Authenticator, tap Install, and then tap Accept.

Please note that this app requires that you have a QR scanner app installed. If you do not have a QR Scanner app installed, you will be prompted to install one when you try to scan a QR code.

5. When the Azure Authenticator finishes installing, tap OPEN.

Leave the app open for subsequent steps.

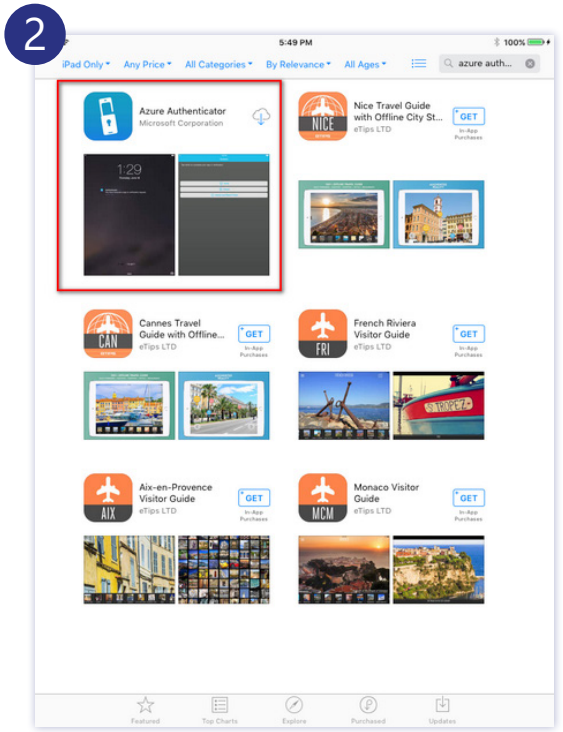
Install the Azure Authenticator App on an iOS Device

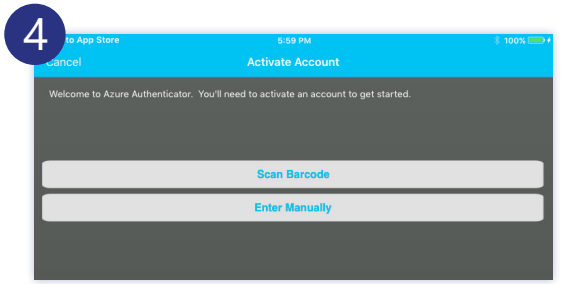
For Multi-Factor Authentication, you will use a device to provide the second factor of authentication. This device, as you learned in the previous exercise, could be a smartphone that can receive text and voice messages. Alternatively, and to provide greater convenience, you can use an Azure Authenticator app that you install on your Windows, Android, or iOS device. In this exercise, you will install the Azure Authenticator app on your iOS device.

Perform these steps on your iOS device.

1. Sign in to your iOS device.
2. Tap App Store, and then in Search, enter Azure Authenticator.
3. In the Azure Authenticator tile, tap download.
4. When the app finishes downloading and installing, tap Open, and then click OK to permit the app to send you notifications.

Leave the app open for subsequent steps.





Enable Users for Multi-Factor Authentication

Azure Multi-Factor Authentication is included in an Azure Active Directory Premium subscription. As a result, it is also included with the Enterprise Mobility Suite (EMS). Consequently, if you have an Enterprise Mobility Suite or Azure Active Directory Premium subscription, you can enable a greater level of security through Multi-Factor Authentication than is available with Intune alone. For example, when Multi-Factor Authentication is enabled through Office 365 or Azure Active Directory, Multi-Factor Authentication is supported for authentication to the company portal, on a per-user or batch basis, and on Windows, iOS, and Android devices.

In this task, you will enable Multi-Factor Authentication for a user. You will then sign in as the Multi-Factor Authentication-enabled user and go through the registration process.

> Perform this task in an InPrivate or Incognito Web browser session

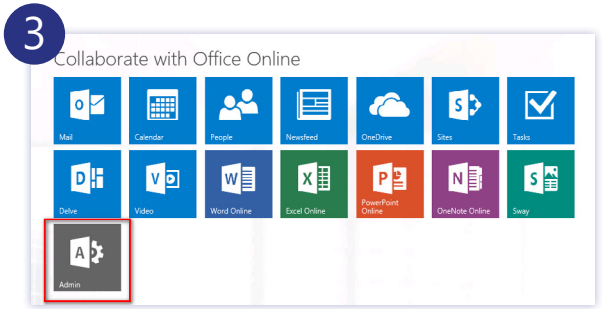
1. In your Web browser, navigate to https://portal.office.com.
2. When prompted, sign in as admin@[OrgName].onmicrosoft.com.
3. On the home page, click Admin.
4. In the Office 365 admin center, expand USERS, and then click Active Users.
5. On the Active Users page, to the right of Set Multi-Factor authentication requirements, click Set up.
6. On the Multi-Factor Authentication page, check Alice Ciccu.

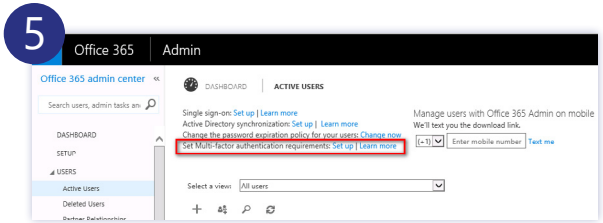
> Note the URL for the MFA page: https://account.activedirectory.windowsazure.com. This page is the same as the one that is accessible through the Azure classic portal.

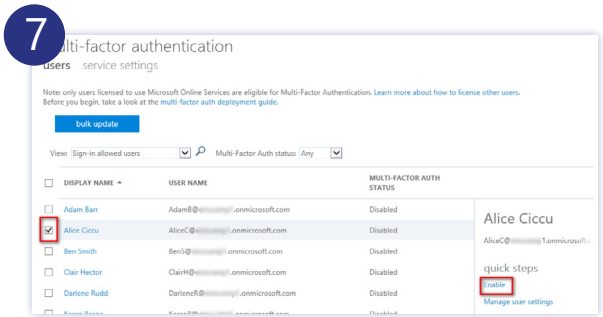
7. Under quick links, click Enable.

> A pop-up window appears to inform you about enabling Multi-Factor Authentication.

8. Read the messages, click enable multi-factor auth, and then click close.
9. Optionally, enable other users.







10. Stay signed in to Office 365 for subsequent tasks.
11. Open another InPrivate or Incognito browser session.

📌 In the next step you are going to sign in as Alice Ciccu. You need to open a separate browser session to avoid being automatically logged in as your tenant admin account.

❗ Leave the current Web browser session open for subsequent steps.

12. In the new Web browser session, navigate to https://aka.ms/mfasetup.
13. When prompted, sign in as alicec@[OrgName].onmicrosoft.com using Passw0rd! as the password.

📌 When you sign in, the Multi-Factor Authentication setup page appears.

14. Click Set it up now.
15. On the additional security verification page, select Mobile app, select Receive notifications for verification, and click Set up.

❗ Perform the next steps on either an iOS or Android device, but not both. You can set up only one device for the second factor of authentication.

16. If you have an Android device, follow these steps:
a. In the Azure Authenticator app you left open in a previous exercise, tap SCAN QR CODE.

📌 If you are prompted to install a QR code-reading app, install it, and then try again.

b. Point your camera at the code on the screen, and then tap the screen when the code is aligned with the on-screen markers.

📌 If successful, you are notified that the account was successfully added.

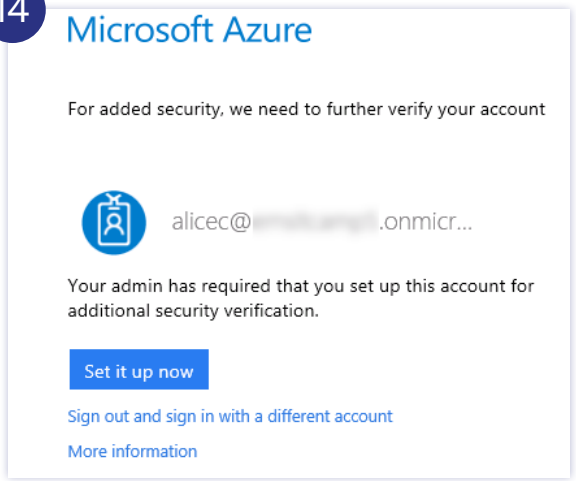
17. If you have an iOS device, follow these steps:
a. In the Azure Authenticator app you left open in a previous exercise, tap Scan Barcode.
b. Hold the camera in front of the code and align it with the on-screen markers.

📌 If successful, the account will be added.

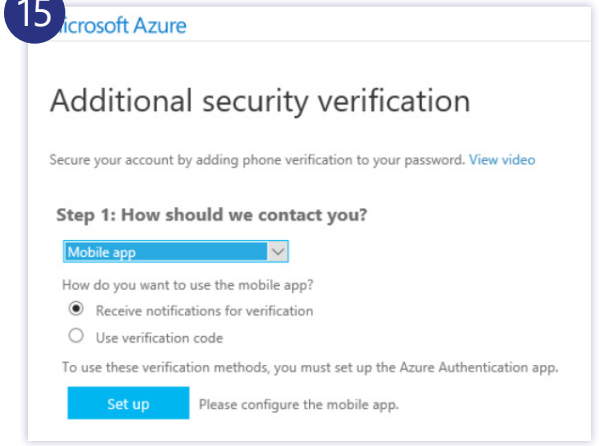
18. Click contact me.
19. On either your Android or your iOS device, in the Azure Authenticator app, tap Verify.

📌 The screenshot below shows the app on an iOS device.

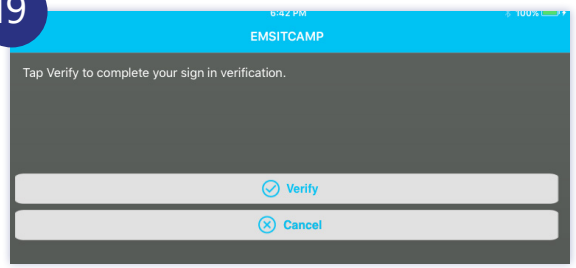
14



15



19



20. In the Web browser, on the Additional security verification page, enter your cell phone number, and then click Next.

21. On the Additional security verification page, record the app password that appears, and then click Done.

> The app password provides an additional level of security and is used for older nonbrowser apps. Newer apps support Multi-Factor Authentication and do not need the app password.

22. When prompted, sign in as alicec@[OrgName].onmicrosoft.com using Passw0rd! as the password.

23. Wait to receive the notification on your Android or iOS device, and then tap Verify.

> When you sign in, you will see the access panel for the user, as shown below.

24. Click Additional security verification.

> On this page, you can change and configure security verification methods. This same page is also accessible through the user account settings on the Office 365 site.

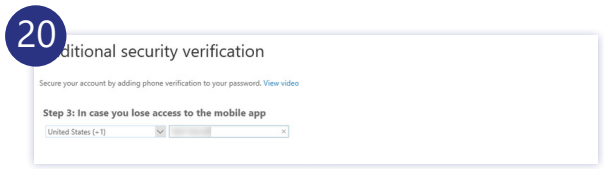
25. On the additional security verification page, click app passwords.

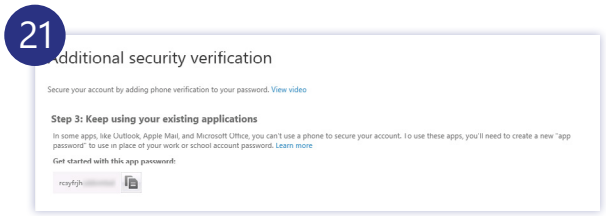
26. On the app passwords page, click create.

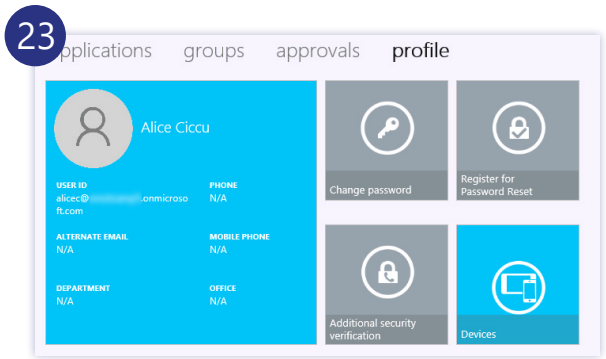
> As noted earlier, only older apps will need to use app passwords. You will not need to use app passwords in the currently configured environment and are performing these next few steps as a demonstration only.

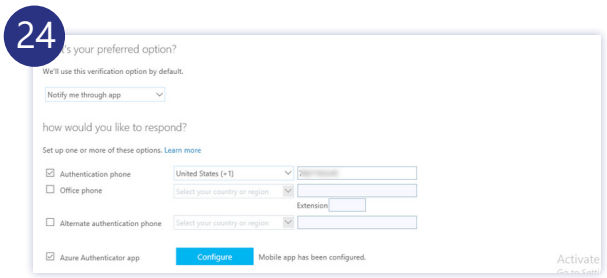
27. In the Create app password dialog box, in name, type iPad, and then click Next.

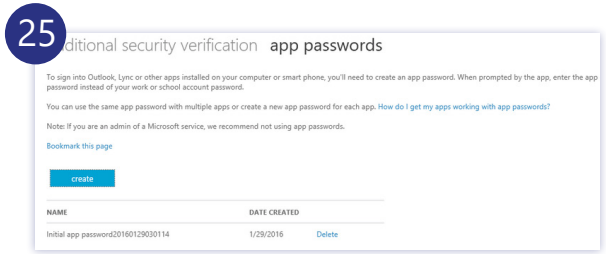
> If you use multiple devices, you need to create an app password for each device. Even though you can use a different app password for each Office application, the recommendation is to use app passwords on a per-device rather than a per-application basis.









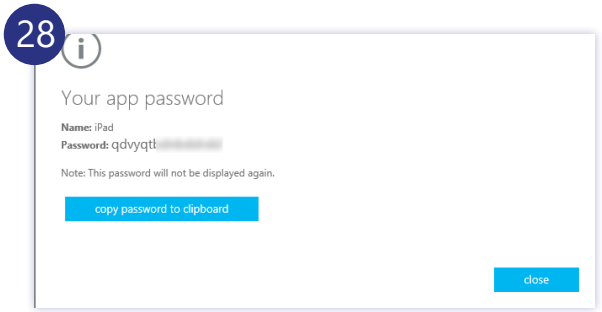


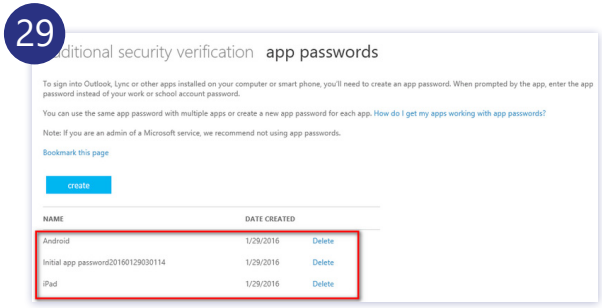
28. In the Your app password dialog box, record the displayed password, and then click close.

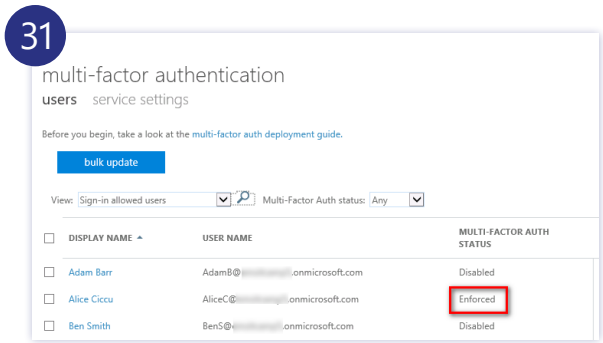
29. Repeat steps 26–28 to create an app password named Android.

30. Switch to the browser session that shows the Azure Multi-Factor Authentication page you used to enable MFA for Alice Ciccu.

31. On the Multi-Factor Authentication page, note that the MULTI-FACTOR AUTH STATUS has changed from Enabled to Enforced.







32. Leave this page open for subsequent tasks.

Do NOT close this page.

Verify Multi-Factor Authentication on Your Device

In this exercise, you will verify that Multi-Factor Authentication is working as expected.

- Perform this task on either your Android or your iOS device.

1. On your Android or iOS device, tap Company Portal.

- NOTE: If you have not enrolled the device, and the Company Portal is not installed, you can install it now. During the enrollment process, you will be prompted to provide additional security verification.

2. On the sign-in page, sign in as alicec@[OrgName].onmicrosoft.com, using Passw0rd! as the password.

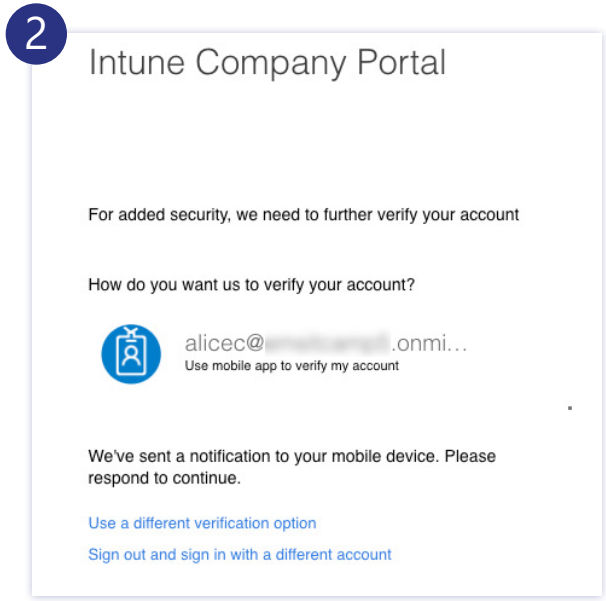
- You are prompted to perform additional verification using the mobile app.
- If you are signed in with cached credentials and do not see a sign-in screen, close the app or restart your device.

3. On your iOS or Android device, open the Azure Authenticator app, check for the notification, and then tap Verify.
4. On your Android or iOS device, tap Outlook.
5. If prompted, enter the 4-digit PIN you configured for managed applications in a previous lab.
6. On the sign-in page, sign in as alicec@[OrgName].onmicrosoft.com, using Passw0rd! as the password.

- You are prompted to provide verification through the mobile app.

7. Open Azure Authenticator, check for notifications, and then tap Verify.
8. To prepare for the next exercise, restart your iOS or Android device.

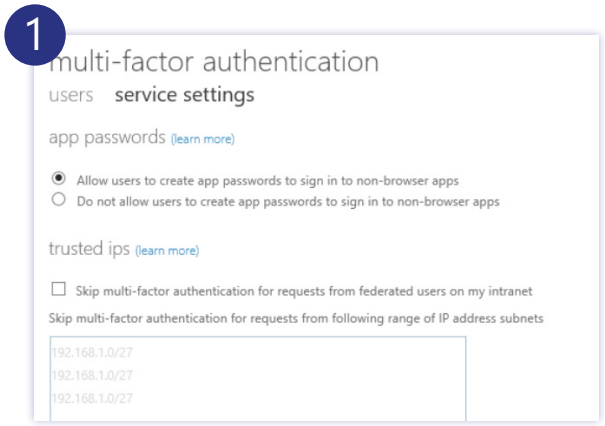
- You are taking this action because you want to ensure that cached credentials will not affect the results in the next exercise.



Configure Trusted IP Addresses

Azure Multi-Factor Authentication allows you to configure a range of trusted IP addresses. When devices have IP addresses that belong to the defined range of trusted IP addresses, Multi-Factor Authentication is skipped when MFA-enabled users access corporate resources and services from their mobile devices.

In this task, you will determine the public IP address used by your Android or iOS device. You use this IP address to simulate a trusted IP address (it may actually be a trusted IP address if it represents your home or work public IP address). Finally, you will verify that Multi-Factor Authentication is skipped when you access corporate services from a trusted IP address.



> Perform this task using the Web browser session that displays the Multi-Factor Authentication configuration page you left open in a previous task.

1. On the Multi-Factor Authentication page, click service settings.

> If you accidentally closed this page, open an InPrivate or Incognito browser session, and navigate to https://account.activedirectory.windowsazure.com/UserManagement/MfaSettings.aspx. When prompted log in as your tenant admin.

2. Switch to your Android or iOS device.
3. On the Android or iOS device, open a Web browser and navigate to http://www.whatismyip.com.

4. Record the IP address that is displayed on the page.

   📌 You need to determine the public IP address of your iOS or Android device. If you are behind a NAT device, your device knows nothing about the public IP address that is used for its communications on the Internet.

5. Switch to the browser displaying the MFA service settings page.
6. Under trusted IPs, check Skip multi-factor authentication for requests from federated users on my intranet.
7. Enter the IP address you determined in the previous step, and then give it a subnet range of /28, as shown in the Screenshot below.

   📌 By using a 28-bit subnet mask, you are specifying a narrow range of IP addresses (16 addresses).

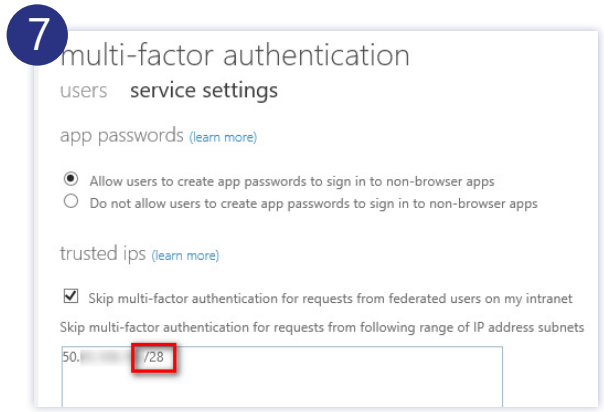
8. Scroll down, click save, and then click close.
9. On your iOS or Android device, tap Company Portal.

   📌 You are required to sign in again.

10. Sign in as alicec@[OrgName].onmicrosoft.com, using Passw0rd! as the password.

    📌 Depending on the device, you may be prompted to sign in again with a username and password as some reconfiguration occurs on the device. Note that you are not required to provide a second authentication factor.

11. On the service settings tab, clear the Skip multi-factor authentication check box, and then click save.



Part Ten:
Retire Devices Used in Walkthroughs

Part Ten:

Retire Devices Used in Walkthroughs

The previous walkthrough represents the end of the practical walkthroughs in this guide. If you have used any devices for these walkthroughs, you should return the device to its initial state at the beginning of this lab series. This means retiring or wiping the device and removing any applications or data that the device acquired over the course of these labs.

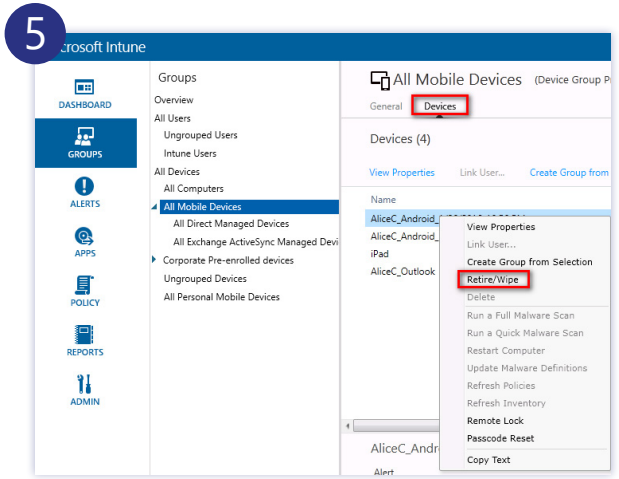
In this exercise, you will retire the iOS and Android devices you used in this lab series, and then return them to their initial state.

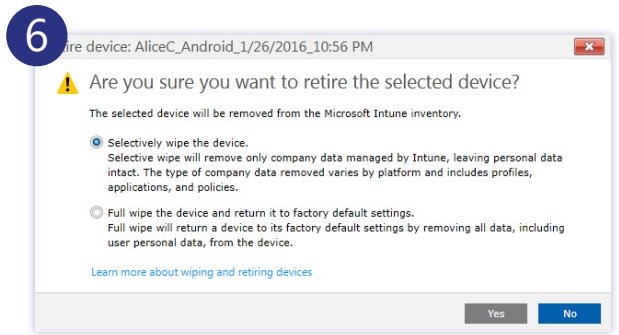
> Please ensure you are signed into the Microsoft Intune administrative console at https://manage.microsoft.com to perform these steps.

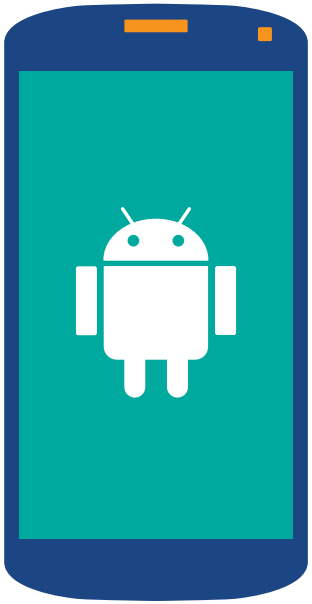
1. In the Intune console, in the left navigation bar, click GROUPS.
2. Under Groups, select All Mobile Devices.
3. On the All Mobile Devices page, click Devices.
4. Select and then right-click the top device that is listed.
5. Click Retire/Wipe.
6. When prompted to retire the selected device, choose either to selectively wipe the device or perform a full wipe of the device.

> WARNING: Performing a full wipe will return the device to its factory state. Only perform a full wipe if you are not concerned about losing data or apps on the device.

7. Select the next device in the list, and then repeat the above steps to retire or wipe the device.
8. Repeat until you have retired or wiped all the mobile devices.
9. If you did a selective wipe, you should remove the Company Portal and other applications that were installed as part of this lab.







Android Device

To remove applications, using the Company Portal as an example, from your Android device follow these instructions:

1. Go to Settings.
2. Tap Applications, tap Application Manager, tap Company Portal, and then tap Uninstall.

iOS Device

To remove applications, using the Company Portal as an example, from your iOS device follow these instructions:

1. Press the Home button.
2. Tap and hold Comp Portal until it wiggles, click X, and then click Delete.